

Modicon

MCSESM, MCSESM-E, MCSESP Managed Switch GUI Reference Manual

The information provided in this documentation contains general descriptions and/or technical characteristics of the performance of the products contained herein. This documentation is not intended as a substitute for and is not to be used for determining suitability or reliability of these products for specific user applications. It is the duty of any such user or integrator to perform the appropriate and complete risk analysis, evaluation and testing of the products with respect to the relevant specific application or use thereof. Neither Schneider Electric nor any of its affiliates or subsidiaries shall be responsible or liable for misuse of the information contained herein. If you have any suggestions for improvements or amendments or have found errors in this publication, please notify us.

You agree not to reproduce, other than for your own personal, noncommercial use, all or part of this document on any medium whatsoever without permission of Schneider Electric, given in writing. You also agree not to establish any hypertext links to this document or its content. Schneider Electric does not grant any right or license for the personal and noncommercial use of the document or its content, except for a non-exclusive license to consult it on an "as is" basis, at your own risk. All other rights are reserved.

All pertinent state, regional, and local safety regulations must be observed when installing and using this product. For reasons of safety and to help ensure compliance with documented system data, only the manufacturer must perform repairs to components.

When devices are used for applications with technical safety requirements, the relevant instructions must be followed.

Failure to use Schneider Electric software or approved software with our hardware products may result in injury, harm, or improper operating results.

Failure to observe this information can result in injury or equipment damage.

As part of a group of responsible, inclusive companies, we are updating our communications that contain non-inclusive terminology. Until we complete this process, however, our content may still contain standardized industry terms that may be deemed inappropriate by our customers.

© 2022 Schneider Electric. All Rights Reserved.

Contents

	Safety information	9
	About this Manual	11
	Key	12
	Notes on the Graphical User Interface	13
1	Basic Settings	19
1.1	System	19
1.2	Network	23
1.2.1	Global	24
1.2.2	IPv4	26
1.2.3	IPv6	29
1.3	Out of Band over USB	32
1.4	Software	35
1.5	Load/Save	38
1.6	External Memory	49
1.7	Port	52
1.8	Power over Ethernet (MCSESP)	59
1.8.1	PoE Global	60
1.8.2	PoE Port	63
1.9	Restart	66
2	Time	69
2.1	Basic Settings	69
2.2	SNTP	73
2.2.1	SNTP Client	74
2.2.2	SNTP Server	78
2.3	PTP	80
2.3.1	PTP Global	81
2.3.2	PTP Boundary Clock	83
2.3.2.1	PTP Boundary Clock Global	84
2.3.2.2	PTP Boundary Clock Port	89
2.3.3	PTP Transparent Clock	93
2.3.3.1	PTP Transparent Clock Global	94
2.3.3.2	PTP Transparent Clock Port	98
2.4	802.1AS	99
2.4.1	802.1AS Global	100
2.4.2	802.1AS Port	104
2.4.3	802.1AS Statistics	109
3	Device Security	111
3.1	User Management	111
3.2	Authentication List	117
3.3	LDAP	119
3.3.1	LDAP Configuration	120

3.3.2	LDAP Role Mapping	126
3.4	Management Access	128
3.4.1	Server	129
3.4.2	IP Access Restriction	143
3.4.3	Web	147
3.4.4	Command Line Interface	148
3.4.5	SNMPv1/v2 Community	151
3.5	Pre-login Banner	152
4	Network Security	155
4.1	Network Security Overview	155
4.2	Port Security	157
4.3	802.1X Port Authentication	164
4.3.1	802.1X Global	165
4.3.2	802.1X Port Configuration	168
4.3.3	802.1X Port Clients	174
4.3.4	802.1X EAPOL Port Statistics	176
4.3.5	802.1X Port Authentication History	178
4.3.6	802.1X Integrated Authentication Server	180
4.4	RADIUS	181
4.4.1	RADIUS Global	182
4.4.2	RADIUS Authentication Server	184
4.4.3	RADIUS Accounting Server	186
4.4.4	RADIUS Authentication Statistics	188
4.4.5	RADIUS Accounting Statistics	190
4.5	DoS	191
4.5.1	DoS Global	192
4.6	DHCP Snooping	195
4.6.1	DHCP Snooping Global	197
4.6.2	DHCP Snooping Configuration	199
4.6.3	DHCP Snooping Statistics	202
4.6.4	DHCP Snooping Bindings	203
4.7	IP Source Guard	204
4.7.1	IP Source Guard Port	206
4.7.2	IP Source Guard Bindings	207
4.8	Dynamic ARP Inspection	208
4.8.1	Dynamic ARP Inspection Global	210
4.8.2	Dynamic ARP Inspection Configuration	212
4.8.3	Dynamic ARP Inspection ARP Rules	215
4.8.4	Dynamic ARP Inspection Statistics	216
4.9	ACL	217
4.9.1	ACL IPv4 Rule	218
4.9.2	ACL MAC Rule	221
4.9.3	ACL Assignment	224
5	Switching	227
5.1	Switching Global	227
5.2	Rate Limiter	229

5.3	Filter for MAC Addresses	232
5.4	IGMP Snooping	234
5.4.1	IGMP Snooping Global	235
5.4.2	IGMP Snooping Configuration	237
5.4.3	IGMP Snooping Enhancements	241
5.4.4	IGMP Snooping Querier	244
5.4.5	IGMP Snooping Multicasts	247
5.5	Time-Sensitive Networking	248
5.5.1	TSN Configuration	249
5.5.2	TSN Gate Control List	251
5.5.2.1	TSN Configured Gate Control List	252
5.5.2.2	TSN Current Gate Control List	255
5.6	MRP-IEEE	256
5.6.1	MRP-IEEE Configuration	257
5.6.2	MRP-IEEE Multiple MAC Registration Protocol	258
5.6.3	MRP-IEEE Multiple VLAN Registration Protocol	263
5.7	GARP	266
5.7.1	GMRP	267
5.7.2	GVRP	269
5.8	QoS/Priority	270
5.8.1	QoS/Priority Global	271
5.8.2	QoS/Priority Port Configuration	272
5.8.3	802.1D/p Mapping	274
5.8.4	IP DSCP Mapping	276
5.8.5	Queue Management	278
5.9	VLAN	279
5.9.1	VLAN Global	281
5.9.2	VLAN Configuration	282
5.9.3	VLAN Port	284
5.9.4	VLAN Voice	286
5.10	L2-Redundancy	288
5.10.1	MRP	289
5.10.2	HIPER Ring	293
5.10.3	Spanning Tree	295
5.10.3.1	Spanning Tree Global	296
5.10.3.2	Spanning Tree Dual RSTP (MCSESM-E)	302
5.10.3.3	Spanning Tree Port	308
5.10.4	Link Aggregation	315
5.10.5	Link Backup	322
5.10.6	FuseNet	325
5.10.6.1	Sub Ring	327
5.10.6.2	Ring/Network Coupling	332
5.10.6.3	Redundant Coupling Protocol (MCSESM-E)	338
6	Diagnostics	343
6.1	Status Configuration	343
6.1.1	Device Status	344

6.1.2	Security Status	348
6.1.3	Signal Contact	355
6.1.3.1	Signal Contact 1 / Signal Contact 2	356
6.1.4	MAC Notification	360
6.1.5	Alarms (Traps)	363
6.2	System	365
6.2.1	System Information	366
6.2.2	Hardware State	367
6.2.3	IP Address Conflict Detection	368
6.2.4	ARP	372
6.2.5	Selftest	374
6.3	Email Notification	376
6.3.1	Email Notification Global	377
6.3.2	Email Notification Recipients	381
6.3.3	Email Notification Mail Server	382
6.4	Syslog	384
6.5	Ports	387
6.5.1	SFP	388
6.5.2	TP cable diagnosis	390
6.5.3	Port Monitor	392
6.5.4	Auto-Disable	404
6.5.5	Port Mirroring	408
6.6	LLDP	410
6.6.1	LLDP Configuration	411
6.6.2	LLDP Topology Discovery	415
6.7	Loop Protection	418
6.8	Report	424
6.8.1	Report Global	425
6.8.2	Persistent Logging	430
6.8.3	System Log	433
6.8.4	Audit Trail	434
7	Advanced	437
7.1	DHCP L2 Relay	437
7.1.1	DHCP L2 Relay Configuration	439
7.1.2	DHCP L2 Relay Statistics	442
7.2	DHCP Server	443
7.2.1	DHCP Server Global	444
7.2.2	DHCP Server Pool	446
7.2.3	DHCP Server Lease Table	451
7.3	DNS	452
7.3.1	DNS Client	452
7.3.1.1	DNS Client Global	453
7.3.1.2	DNS Client Current	454
7.3.1.3	DNS Client Static	455
7.3.1.4	DNS Client Static Hosts	457
7.4	Industrial Protocols	458

7.4.1	IEC61850-MMS	459
7.4.2	Modbus TCP	462
7.4.3	EtherNet/IP	464
7.5	Digital IO Module	466
7.6	Command Line Interface	469
A	Index	471

Safety information

Note: Read these instructions carefully, and look at the equipment to become familiar with the device before trying to install, operate, or maintain it. The following special messages may appear throughout this documentation or on the equipment to warn of potential hazards or to call attention to information that clarifies or simplifies a procedure.



The addition of this symbol to a "Danger" or "Warning" safety label indicates that an electrical hazard exists, which will result in personal injury if the instructions are not followed.



This is the safety alert symbol. It is used to alert you to potential personal injury hazards. Obey all safety messages that follow this symbol to avoid possible injury or death.

DANGER

DANGER indicates an imminently hazardous situation which, if not avoided, **will result in** death or serious injury.

WARNING

WARNING indicates a potentially hazardous situation which, if not avoided, **can result in** death or serious injury.

CAUTION

CAUTION indicates a potentially hazardous situation which, if not avoided, **can result in** minor or moderate injury.

NOTICE

NOTICE is used to address practices not related to physical injury.

Note: Electrical equipment should be installed, operated, serviced, and maintained only by qualified personnel. No responsibility is assumed by Schneider Electric for any consequences arising out of the use of this material.

A qualified person is one who has skills and knowledge related to the construction and operation of electrical equipment and its installation, and has received safety training to recognize and avoid the hazards involved.

© 2022 Schneider Electric. All Rights Reserved.

About this Manual

Validity Note

The data and illustrations found in this book are not binding. We reserve the right to modify our products in line with our policy of continuous product development. The information in this document is subject to change without notice and should not be construed as a commitment by Schneider Electric.

User Comments

We welcome your comments about this document. You can reach us by e-mail at techpub@schneider-electric.com

Related Documents

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 ConneXium Network Manager 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 device supports the following operating systems:

- ▶ Windows 10
- ▶ Linux

The Graphical User Interface of the device is divided as follows:

- ▶ Navigation area
- ▶ Dialog area
- ▶ Buttons

Navigation area

The Navigation area is located on the left side of the Graphical User Interface.

The Navigation area contains the following elements:

- ▶ Toolbar
- ▶ Filter
- ▶ Menu

You have the option of collapsing the entire Navigation area, for example when displaying the Graphical User Interface on small screens. To collapse or expand, you click the small arrow at the top of the navigation area.

Toolbar

The toolbar at the top of the navigation area contains several buttons.

- When you position the mouse pointer over a button, a tooltip displays further information.
- If the connection to the device is lost, then the toolbar is grayed out.



The device automatically refreshes the toolbar information every 5 seconds.

Clicking the button refreshes the toolbar manually.



When you position the mouse pointer over the button, a tooltip displays the following information:

- ▶ *User:*
Name of the logged in user
- ▶ *Device name:*
Name of the device

Clicking the button opens the *Device Security > User Management* dialog.



When you position the mouse pointer over the button, a tooltip displays the summary of the *Diagnostics > System > Configuration Check* dialog.

Clicking the button opens the *Diagnostics > System > Configuration Check* dialog.



Clicking the button logs out the current user and displays the login dialog.

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* dialog.

- To permanently save the changes, click the *Yes* button in the *Warning* dialog.
- To discard the changes, click the *No* button in the *Warning* dialog.



Displays the remaining time in seconds until the device automatically logs out an inactive user.

Clicking the button opens the *Device Security > Management Access > Web* dialog. There you can specify the timeout.



When the configuration profile in the volatile memory (*RAM*) differs from the "Selected" configuration profile in the non-volatile memory (*NVM*), this button is visible. Otherwise, the button is hidden.

Clicking the button opens the *Basic Settings > Load/Save* dialog.

By right-clicking the button you can save the current settings in the non-volatile memory (*NVM*).



When you position the mouse pointer over the button, a tooltip displays the following information:

- ▶ *Device Status*: This section displays a compressed view of the *Device status* frame in the *Basic Settings > System* dialog. The section displays the alarm that is currently active and whose occurrence was recorded first.
- ▶ *Security Status*: This section displays a compressed view of the *Security status* frame in the *Basic Settings > System* dialog. The section displays the alarm that is currently active and whose occurrence was recorded first.
- ▶ *Boot Parameter*: If you permanently save changes to the settings and at least one boot parameter differs from the configuration profile used during the last restart, then this section displays a note.

The following settings cause the boot parameters to change:

- *Basic Settings > External Memory* dialog, *Software auto update* parameter
- *Basic Settings > External Memory* dialog, *Config priority* parameter
- *Device Security > Management Access > Server* dialog, *SNMP* tab, *UDP port* parameter
- *Diagnostics > System > Selftest* dialog, *RAM test* parameter
- *Diagnostics > System > Selftest* dialog, *SysMon1 is available* parameter
- *Diagnostics > System > Selftest* dialog, *Load default config on error* parameter

Clicking the button opens the *Diagnostics > Status Configuration > Device Status* dialog.

Filter

The filter enables you to reduce the number of menu items in the menu. When filtering, the menu displays only menu items matching the search string entered in the filter field.

Menu

The menu displays the menu items.

You have the option of filtering the menu items. See section “Filter”.

To display the corresponding dialog in the dialog area, you click the desired menu item. If the selected menu item is a node containing sub-items, then the node expands or collapses while clicking. The dialog area keeps the previously displayed dialog.

You have the option of expanding or collapsing every node in the menu at the same time. When you right-click anywhere in the menu, a context menu displays the following entries:

- ▶ *Expand*
Expands every node in the menu at the same time. The menu displays the menu items for every level.
- ▶ *Collapse*
Collapses every node in the menu at the same time. The menu displays the top level menu items.

Dialog area

The Dialog area is located on the right side of the Graphical User Interface. When you click a menu item in the Navigation area, the Dialog area displays the corresponding dialog.

Updating the display

If a dialog remains opened 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.

Saving the settings

Saving, transfers the changed settings to the volatile memory (*RAM*) of the device. Perform the following step:

- Click the  button.

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

- Open the *Basic Settings > Load/Save* dialog.
- In the table highlight the desired configuration profile.
- When in the *Selected* column the checkbox is *unmarked*, click the  button and then the *Select* item.
- Click the  button and then the *Save* item.

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.

Working with tables

The dialogs display numerous settings in table form.

When you modify a table cell, the table cell displays a red mark in its top-left corner. The red mark indicates that your modifications are not yet transferred to the volatile memory (*RAM*) of the device.

You have the option of customizing the look of the tables to fit your needs. When you position the mouse pointer over a column header, the column header displays a drop-down list button. When you click this button, the drop-down list displays the following entries:

- ▶ Sort ascending
Sorts the table entries in ascending order based on the entries of the selected column.
You recognize sorted table entries by an arrow in the column header.
- ▶ Sort descending
Sorts the table entries in descending order based on the entries of the selected column.
You recognize sorted table entries by an arrow in the column header.
- ▶ Columns
Displays or hides columns.
You recognize hidden columns by an unmarked checkbox in the drop-down list.
- ▶ Filters
The table only displays the entries whose content matches the specified filter criteria of the selected column.
You recognize filtered table entries by an emphasized column header.

You have the option of selecting multiple table entries simultaneously and subsequently applying an action to them. This is useful when you are going to remove multiple table entries at the same time.



- ▶ Select several consecutive table entries:
 - Click the first desired table entry to highlight it.
 - Press and hold the <SHIFT> key.
 - Click the last desired table entry to highlight every desired table entry.
- ▶ Select multiple individual table entries:
 - Click the first desired table entry to highlight it.
 - Press and hold the <CTRL> key.
 - Click the next desired table entry to highlight it.
Repeat until every desired table entry is highlighted.

Buttons

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



Transfers the changes to the volatile memory (*RAM*) of the device and applies them to the device. To save the changes in the non-volatile memory, proceed as follows:

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



Updates the fields with the values that are saved in the volatile memory (*RAM*) of the device.



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

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



Displays a submenu with menu items corresponding to the respective dialog.



Opens the *Wizard* dialog.



Adds a new table entry.



Removes the highlighted table entry.



Opens the online help.

1 Basic Settings

The menu contains the following dialogs:

- ▶ System
- ▶ Network
- ▶ Out of Band over USB
- ▶ Software
- ▶ Load/Save
- ▶ External Memory
- ▶ Port
- ▶ Power over Ethernet (MCSESP)
- ▶ Restart

1.1 System

[Basic Settings > System]

In this dialog you monitor individual operating statuses.

Device status

The fields in this frame display the device status and inform you about alarms that have occurred. When an alarm currently exists, the frame is highlighted.

You specify the parameters that the device monitors in the [Diagnostics > Status Configuration > Device Status](#) dialog.

Note: If you connect only one power supply unit for the supply voltage to a device with a redundant power supply unit, then the device reports an alarm. To help avoid this alarm, you deactivate the monitoring of the missing power supply units in the [Diagnostics > Status Configuration > Device Status](#) dialog.

Alarm counter

Displays the number of currently existing alarms.



When there is at least one currently existing alarm, the icon is visible.

When you position the mouse pointer over the icon, a tooltip displays the cause of the currently existing alarms and the time at which the device triggered the alarm.

If a monitored parameter differs from the desired status, then the device triggers an alarm. The [Diagnostics > Status Configuration > Device Status](#) dialog, *Status* tab displays an overview of the alarms.

Security status

The fields in this frame display the security status and inform you about alarms that have occurred. When an alarm currently exists, the frame is highlighted.

You specify the parameters that the device monitors in the [Diagnostics > Status Configuration > Security Status](#) dialog.

Alarm counter

Displays the number of currently existing alarms.



When there is at least one currently existing alarm, the icon is visible.

When you position the mouse pointer over the icon, a tooltip displays the cause of the currently existing alarms and the time at which the device triggered the alarm.

If a monitored parameter differs from the desired status, then the device triggers an alarm. The [Diagnostics > Status Configuration > Security Status](#) dialog, [Status](#) tab displays an overview of the alarms.

Signal contact status

The fields in this frame display the signal contact status and inform you about alarms that have occurred. When an alarm currently exists, the frame is highlighted.

You specify the parameters that the device monitors in the [Diagnostics > Status Configuration > Signal Contact > Signal Contact 1/Signal Contact 2](#) dialog.

Alarm counter

Displays the number of currently existing alarms.



When there is at least one currently existing alarm, the icon is visible.

When you position the mouse pointer over the icon, a tooltip displays the cause of the currently existing alarms and the time at which the device triggered the alarm.

If a monitored parameter differs from the desired status, then the device triggers an alarm. The [Diagnostics > Status Configuration > Signal Contact > Signal Contact 1/Signal Contact 2](#) dialog, [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 for which the device is known in the network.

Possible values:

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

When creating HTTPS X.509 certificates, the application generating the certificate uses the specified value as the domain name and common name.

The following functions use the specified value as a host name or FQDN (Fully Qualified Domain Name). For compatibility, it is recommended to use only small letters, since not every system compares the case in the FQDN. Verify that this name is unique in the whole network.

- ▶ DHCP client
- ▶ *Syslog*
- ▶ *IEC61850-MMS*

Location

Specifies the location of the device.

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 device.

Power supply 1 Power supply 2

Displays the status of the power supply unit on the relevant voltage supply connection.

Possible values:

- ▶ *present*
- ▶ *defective*
- ▶ *not installed*
- ▶ *unknown*

Uptime

Displays the time that has elapsed since this 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 thresholds in the [Diagnostics > Status Configuration > Device Status](#) dialog.

Upper temp. limit [°C]

Specifies the upper temperature threshold in °C.

Possible values:

- ▶ `-99..99` (integer)
If the temperature in the device exceeds this value, then the device generates an alarm.

Lower temp. limit [°C]









Specifies the lower temperature threshold in °C.

Possible values:

- ▶ `-99..99` (integer)
If the temperature in the device falls below this value, then the device generates an alarm.

LED status








This frame displays the states of the device status LEDs at the time of the last update. The “Installation” user manual contains detailed information about the device status LEDs.

Parameters	Color	Meaning
<i>Status</i>		There is currently no device status alarm. The device status is OK.
		There is currently at least one device status alarm. Therefore, see the Device status frame above.
<i>Power</i>		Device variant with 2 power supply units: Only one supply voltage is active.
		Device variant with 1 power supply unit: The supply voltage is active.
		Device variant with 2 power supply units: Both supply voltages are active.
<i>EAM</i>		No external memory connected.
		The external memory is connected, but not ready for operation.
		The external memory is connected and ready for operation.

Port status

This frame displays a simplified view of the ports of the device at the time of the last update.

The icons represent the status of the individual ports. In some situations, the following icons interfere with one another. When you position the mouse pointer over the appropriate port icon, a tooltip displays a detailed information about the port state.

Parameters	Status	Meaning
<Port number>		The port is inactive. The port does not send or receive any data.
		The port is inactive. The cable is connected. Active link.
		The port is active. No cable connected or no active link.
		The port is active. The cable is connected. Connection okay. Active link. Full-duplex mode
		The half-duplex mode is enabled. Verify the settings in the Basic Settings > Ports dialog, Configuration tab.
		The port is in a blocking state due to a redundancy function.
		The port operates as a router interface.

Buttons

You find the description of the standard buttons in section “Buttons” on page 17.

1.2 Network

[Basic Settings > Network]

The menu contains the following dialogs:

- ▶ Global
- ▶ IPv4
- ▶ IPv6

1.2.1 Global

[Basic Settings > Network > Global]

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

Management interface

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

VLAN ID

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

Possible values:

▶ 1..4042 (default setting: 1)

The prerequisite is that the VLAN is already configured. See the [Switching > VLAN > Configuration](#) dialog.

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

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

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

MAC address

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

Ethernet Switch Configurator protocol v1/v2

This frame lets you specify settings for the access to the device using the Ethernet Switch Configurator protocol.

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

Note: With the Ethernet Switch Configurator 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 Ethernet Switch Configurator function in the device.

Possible values:

- ▶ *On* (default setting)
Ethernet Switch Configurator is enabled.
You can use the Ethernet Switch Configurator software to access the device from your PC.
- ▶ *Off*
Ethernet Switch Configurator is disabled.

Access

Enables/disables the write access to the device using Ethernet Switch Configurator.

Possible values:

- ▶ *readWrite* (default setting)
The Ethernet Switch Configurator software is given write access to the device.
With this setting you can change the IP parameters in the device.
- ▶ *readOnly*
The Ethernet Switch Configurator software is given read-only access to the device.
With this setting you can view the IP parameters in the device.

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 Ethernet Switch Configurator 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.

Buttons

You find the description of the standard buttons in section [“Buttons” on page 17](#).

1.2.2 IPv4

[Basic Settings > Network > IPv4]

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

Management interface

IP address assignment

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

Possible values:

- ▶ *Local*
The device uses the IP parameters from the internal memory. You specify the settings for this in the *IP parameter* frame.
- ▶ *BOOTP*
The device receives its IP parameters from a BOOTP or DHCP server.
The server evaluates the MAC address of the device, then assigns the IP parameters.
- ▶ *DHCP* (default setting)
The device receives its IP parameters from a DHCP server.
The server evaluates the MAC address, the DHCP name, or other parameters of the device, then assigns the IP parameters.
When the server also provides the addresses of DNS servers, the device displays these addresses in the *Advanced > DNS > Cache > 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.

BOOTP/DHCP

Client ID

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

The DHCP client ID that the device sends is the device name specified in the *System name* field in the *Basic Settings > System* dialog.

DHCP option 66/67/4/42

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

Possible values:

▶ *On* (default setting)

The *DHCP option 66/67/4/42* function is enabled.

The device loads the configuration profile and receives the time server information using the following DHCP options:

– Option 66: TFTP server name

Option 67: Boot file name

The device automatically loads the configuration profile from the DHCP server into the volatile memory (*RAM*) using the TFTP protocol. The device uses the settings of the imported configuration profile in the *running-config*.

– Option 4: Time Server

Option 42: Network Time Protocol Servers

The device receives the time server information from the DHCP server.

▶ *Off*

The *DHCP option 66/67/4/42* function is disabled.

– The device does not load a configuration profile using DHCP Options 66/67.

– The device does not receive time server information using DHCP Options 4/42.

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

Remaining lease time

Lease time [s]

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

To update the display, click the  button.

Buttons

You find the description of the standard buttons in section [“Buttons” on page 17](#).

1.2.3 IPv6

[Basic Settings > Network > IPv6]

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

Operation

Operation

Enables/disables the IPv6 protocol in the device.

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

Possible values:

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

Configuration

Dynamic IP address assignment

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

Possible values:

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

DHCP

Client ID

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

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

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

IP parameter

Gateway address

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

Possible values:

- ▶ Valid IPv6 address (except loopback and *Multicast* addresses)

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

Duplicate Address Detection

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

Number of neighbor solicitants

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

Possible values:

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

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

Table

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

Prefix

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

PrefixLength

Displays the prefix length of the IPv6 address.

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

Possible values:

- ▶ 0..128

IP address

Displays the full IPv6 address in a compressed format.

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

Possible values:

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

For more information on IPv6 compression rules and address types, refer to the “Configuration” manual.

EUI option

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

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

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

Possible values:

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

Origin

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

Possible values:

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

- ▶ *Manual*
The device received the IPv6 address manually.
- ▶ *DHCP*
The device received the IPv6 address from a DHCPv6 server.
- ▶ *Linklayer*
The device automatically configures a link-local type IPv6 address. The link-local address cannot be changed.

Status

Displays the current status of the IPv6 address.

Possible values:

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

Note: When the IPv6 address is manually specified, you can manually change between *active* and *notInService* states. To do this change, in the *Status* column, select the necessary state in the drop-down list related to your entry.

Buttons

You find a description of the standard buttons in section “Buttons” on page 17.

1.3 Out of Band over USB

[Basic Settings > Out of Band over USB]

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

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

- ▶ HTTP
- ▶ HTTPS
- ▶ SSH
- ▶ Telnet
- ▶ SNMP
- ▶ FTP
- ▶ TFTP
- ▶ SFTP
- ▶ SCP

When accessing the device management there are the following limitations:

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

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

Operation

Operation

Enables/disables the USB network interface.

Possible values:

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

Management interface

Device MAC address

Displays the MAC address of the USB network interface.

Host MAC address

Displays the MAC address of the connected management station.

IP parameter

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

- management interface

IP address

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

Possible values:

- ▶ Valid IPv4 address

(default setting: 91.0.0.100)

The device assigns this IP address, increased by 1, to the management station which is connected to the device.

Example: 91.0.0.100 for the USB network interface, 91.0.0.101 for the management station.

Netmask

Specifies the netmask.

Possible values:

- ▶ Valid IPv4 netmask

(default setting: 255.255.255.0)

Buttons

You find the description of the standard buttons in section [“Buttons” on page 17](#).

1.4 Software

[Basic Settings > Software]

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

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

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

Version

Stored version

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

Running version

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

Backup version

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

Restore

Restores the device software saved as a backup. In the process, the device changes the [Stored version](#) and the [Backup version](#) of the device software.

Upon restart, the device loads the [Stored version](#).

Bootcode

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

Software update


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

URL

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

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

► Software update from the PC

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

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

Start

Updates the device software.

The device installs the selected file in the flash memory, replacing the previously saved device software. Upon restart, the device loads the installed device software.

The device copies the existing software into the backup memory.

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

Table

File location

Displays the storage location of the device software.

Possible values:

- ▶ *ram*
Volatile memory of the device
- ▶ *flash*
Non-volatile memory (NVM) of the device
- ▶ *usb*
External USB memory (EAM)

Index

Displays the index of the device software.

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

- ▶ 1
Upon restart, 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.

Buttons

You find the description of the standard buttons in section [“Buttons” on page 17](#).

1.5 Load/Save

[Basic Settings > Load/Save]

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

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

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

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

External memory

Selected external memory

Displays the type of the external memory.

Possible values:

- ▶ *usb*
External USB memory (EAM)

Status

Displays the operating state of the external memory.

Possible values:

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

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

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

- 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 inoperative device.
- Install the external memory from the inoperative device in the new device.
- Restart the new device.

When you restart the device, the device loads the configuration profile with the settings of the inoperative device from the external memory. The device copies the settings into the volatile memory (*RAM*) and into the non-volatile memory (*NVM*).

Delete

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

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

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

Information

NVM in sync with running config

Displays if the configuration profile in the volatile memory (*RAM*) and the "Selected" configuration profile in the non-volatile memory (*NVM*) are the same.

Possible values:

- ▶ *marked*
The configuration profiles are the same.
- ▶ *unmarked*
The configuration profiles differ.

External memory in sync with NVM

Displays if the "Selected" configuration profile in the external memory and the "Selected" configuration profile in the non-volatile memory (*NVM*) are the same.

Possible values:

- ▶ *marked*
The configuration profiles are the same.
- ▶ *unmarked*
The configuration profiles differ.

Possible causes:

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

Backup config on a remote server when saving

Operation

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

Possible values:

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

URL

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

Possible values:

- ▶ Alphanumeric ASCII character string with 0..128 characters
Example: `tftp://192.9.200.1/cfg/config.xml`
The device supports the following wildcards:
 - `%d`
System date in the format `YYYY-mm-dd`
 - `%t`
System time in the format `HH_MM_SS`
 - `%i`
IP address of the device
 - `%m`
MAC address of the device in the format `AA-BB-CC-DD-EE-FF`
 - `%p`
Product name of the device

Set credentials

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

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

Possible values:

- Alphanumeric ASCII character string with 1..32 characters

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

Possible values:

- ▶ Alphanumeric ASCII character string with 6..64 characters

The following characters are allowed:

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

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. Current changes, that are saved temporarily, are therefore maintained in the device.

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)


Table

Storage type

Displays the storage location of the configuration profile.

Possible values:


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

- ▶ *NVM* (non-volatile memory of the device)
 When applying the *Undo configuration modifications* function or during a restart, 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:
 - In the table highlight the configuration profile.
 - Click the  button and then the *Activate* item.
- ▶ *ENVM* (external memory)
 In the external memory, the device saves a backup copy of the “Selected” configuration profile. The prerequisite is that in the *Basic Settings > External Memory* dialog you mark the *Backup config when saving* checkbox.


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 by highlighting an existing configuration profile in the table, clicking the  button and then the *Save as..* item.

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


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

Modification date (UTC)


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

Selected

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

To designate another configuration profile as “Selected”, you highlight 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 a restart, the device loads the configuration profile into the volatile memory (*RAM*).
 - When you click the  button, the device saves the temporarily saved settings in this configuration profile.
- ▶ *unmarked*
 Another configuration profile is designated as “Selected”.

Encrypted

Displays if the configuration profile is encrypted.

Possible values:

- ▶ `marked`
The configuration profile is encrypted.
- ▶ `unmarked`
The configuration profile is unencrypted.

You activate/deactivate the encryption of the configuration profile in the [Configuration encryption](#) frame.

Encryption verified

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

Possible values:

- ▶ `marked`
The passwords match. The device is able to unencrypt the configuration profile.
- ▶ `unmarked`
The passwords are different. The device is unable to unencrypt the configuration profile.

Software version

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

Fingerprint

Displays the checksum saved in the configuration profile.

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

Fingerprint verified

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

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

Possible values:

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

The device verifies the checksum correctly only if the configuration profile has been saved before as follows:

- on an identical device
- with the same software version, which the device is running

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.

Buttons

You find the description of the standard buttons in section “Buttons” on page 17.



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

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

Save as..

Copies the configuration profile highlighted in the table and saves it with a user-specified name in the non-volatile memory (*NVM*). The device designates the new configuration profile as “Selected”.

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

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”.

Activate

Loads the settings of the configuration profile highlighted 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 highlighted in the table as “Selected”. In the *Selected* column, the checkbox is then *marked*.

When applying the *Undo configuration modifications* function or during a restart, 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.

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

- When *External memory* is selected above, in the *Import profile from external memory* frame you specify the configuration profile file to be imported.
In the *Profile name* drop-down list, select the name of the configuration profile to be imported.
- In the *Destination* frame you specify where the device saves the imported configuration profile.
In the *Profile name* field you specify the name under which the device saves the configuration profile.
In the *Storage type* field you specify the storage location for the configuration profile. The prerequisite is that in the *Select source* drop-down list you select the *PC/URL* item.
 - ▶ *RAM*
The device saves the configuration profile in the volatile memory (*RAM*) of the device. This replaces the *running-config*, the device uses the settings of the imported configuration profile immediately. The device terminates the connection to the Graphical User Interface. Reload the Graphical User Interface. Log in again.
 - ▶ *NVM*
The device saves the configuration profile in the non-volatile memory (*NVM*) of the device.

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

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

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

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

Export...

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

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

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


- ▶ Export to an FTP server
To save the file on an FTP server, specify the URL for the file in the following form:
`ftp://<user>:<password>@<IP address>:<port>/<file name>`
- ▶ Export to a TFTP server
To save the file on a TFTP server, specify the URL for the file in the following form:
`tftp://<IP address>/<path>/<file name>`
- ▶ Export to an SCP or SFTP server
To save the file on an SCP or SFTP server, specify the URL for the file in one of the following forms:
 - `scp://` or `sftp://<IP address>/<path>/<file name>`
When you click the *Ok* button, the device displays the *Credentials* window. There you enter *User name* and *Password*, to log in to the server.
 - `scp://` or `sftp://<user>:<password>@<IP address>/<path>/<file name>`

Load running-config as script

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

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

▶ Import from the PC

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

▶ Import from an FTP server

When the file is located on an FTP server, specify the URL for the file in the following form:

```
ftp://<user>:<password>@<IP address>:<port>/<file name>
```

▶ Import from a TFTP server

When the file is located on a TFTP server, specify the URL for the file in the following form:

```
tftp://<IP address>/<path>/<file name>
```

▶ Import from an SCP or SFTP server

When the file is located on an SCP or SFTP server, specify the URL for the file in one of the following forms:

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

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.

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.

Back to factory...

Resets the settings in the device to the default values.

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

Back to default

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

1.6 External Memory

[Basic Settings > External Memory]

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

Table

Type

Displays the type of the external memory.

Possible values:

- ▶ `usb`
External USB memory (EAM)

Status

Displays the operating state of the external memory.

Possible values:

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

Writable

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

Possible values:

- ▶ `marked`
The device has write access to the external memory.
- ▶ `unmarked`
The device has read-only access to the external memory. Possibly the write protection is activated in the external memory.

Software auto update

Activates/deactivates the automatic device software update during the restart.

Possible values:

▶ **marked** (default setting)

The automatic device software update during the restart is activated. The device updates the device software when the following files are located in the external memory:

- the image file of the device software
- a text file `startup.txt` with the content `autoUpdate=<image_file_name>.bin`

▶ **unmarked**

The automatic device software update during the restart is deactivated.

SSH key auto upload

Activates/deactivates the loading of the RSA key from an external memory upon restart.

Possible values:

▶ **marked** (default setting)

The loading of the RSA key is activated.

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

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

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

▶ **unmarked**

The loading of the RSA key is deactivated.

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

Config priority

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

Possible values:

▶ **disable**

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

▶ **first**

The device loads the configuration profile from the external memory.

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

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

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

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

Backup config when saving

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

Possible values:

▶ **marked** (default setting)

Creating a copy is activated. When you click in the *Basic Settings > Load/Save* dialog the *Save* button, the device generates a copy of the configuration profile on the active external memory.

▶ **unmarked**

Creating a copy is deactivated. The device does not generate a copy of the configuration profile.

Manufacturer ID

Displays the name of the memory manufacturer.

Revision

Displays the revision number specified by the memory manufacturer.

Version

Displays the version number specified by the memory manufacturer.

Name

Displays the product name specified by the memory manufacturer.

Serial number

Displays the serial number specified by the memory manufacturer.

Buttons

You find the description of the standard buttons in section [“Buttons” on page 17](#).

1.7 Port

[Basic Settings > Port]

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

The dialog contains the following tabs:

- ▶ [Configuration]
- ▶ [Statistics]
- ▶ [Utilization]

[Configuration]

Table

Port

Displays the port number.

Name

Name of the port.

Possible values:

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

Port on

Activates/deactivates the port.

Possible values:

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

State

Displays if the port is currently physically enabled or disabled.

Possible values:

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

Power state (port off)

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

Possible values:

- ▶ `marked`
The port remains physically enabled. A connected device receives an active link.
- ▶ `unmarked` (default setting)
The port is physically disabled.

Auto power down

Specifies how the port behaves when no cable is connected.

Possible values:

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

Automatic configuration

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

Possible values:

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

Manual configuration

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

Possible values:

- ▶ 10 Mbit/s HDX
Half duplex connection
- ▶ 10 Mbit/s FDX
Full duplex connection
- ▶ 100 Mbit/s HDX
Half duplex connection
- ▶ 100 Mbit/s FDX
Full duplex connection
- ▶ 1000 Mbit/s FDX
Full duplex connection
- ▶ 2500 Mbit/s FDX
Full duplex connection

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

Link/Current settings

Displays the operating mode which the port currently uses.

Possible values:

- ▶ -
No cable connected, no link.
- ▶ 10 Mbit/s HDX
Half duplex connection
- ▶ 10 Mbit/s FDX
Full duplex connection
- ▶ 100 Mbit/s HDX
Half duplex connection
- ▶ 100 Mbit/s FDX
Full duplex connection
- ▶ 1000 Mbit/s FDX
Full duplex connection
- ▶ 2500 Mbit/s FDX
Full duplex connection

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

Manual cable crossing (Auto. conf. off)

Specifies the devices connected to a TP port.

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

Possible values:

- ▶ *mdi*
The device interchanges the send- and receive-line pairs on the port.
- ▶ *mdix* (default setting on TP ports)
The device helps prevent the interchange of the send- and receive-line pairs on the port.

- ▶ *auto-mdix*
The device detects the send and receive line pairs of the connected device and automatically adapts to them.
Example: When you connect an end device with a crossed cable, the device automatically resets the port from *mdix* to *mdi*.
- ▶ *unsupported* (default setting on optical ports or TP-SFP ports)
The port does not support this function.

Flow control

Activates/deactivates the flow control on the port.

Possible values:

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

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

Send trap (Link up/down)

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

Possible values:

- ▶ *marked* (default setting)
The sending of SNMP traps is active.
When the device detects a link up/down status change, the device sends an SNMP trap.
- ▶ *unmarked*
The sending of SNMP traps is inactive.

The prerequisite for sending SNMP traps is that you enable the function in the *Diagnostics > Status Configuration > Alarms (Traps)* dialog and specify at least one trap destination.

MTU

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

Possible values:

- ▶ *1518..9720* (default setting: *1518*)
With the setting *1518*, the port transmits the Ethernet packets up to the following size:
 - 1518 bytes without VLAN tag
(1514 bytes + 4 bytes CRC)
 - 1522 bytes with VLAN tag
(1518 bytes + 4 bytes CRC)

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

The following list contains possible applications:

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

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

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

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.

Buttons

You find the description of the standard buttons in section “Buttons” on page 17.

Clear port statistics

Resets the counter for the port statistics to 0.

[Statistics]

This tab displays the following overview per port:


- ▶ Number of data packets/bytes received in the device
 - *Received packets*
 - *Received octets*
 - *Received unicast packets*
 - *Received multicast packets*
 - *Received broadcast packets*
- ▶ Number of data packets/bytes sent from the device
 - *Transmitted packets*
 - *Transmitted octets*
 - *Transmitted unicast packets*
 - *Transmitted multicast packets*
 - *Transmitted broadcast packets*
- ▶ Number of errors detected by the device
 - *Received fragments*
 - *Detected CRC errors*
 - *Detected collisions*

- ▶ Number of data packets per size category received in 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 row.

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 and then the *Clear port statistics* item.
- or
- In the *Basic Settings > Restart* dialog, click the *Clear port statistics* button.

Buttons

You find the description of the standard buttons in section “Buttons” on page 17.

Clear port statistics

Resets the counter for the port statistics to 0.

[Utilization]

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

Table

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 of the received data quantity to the maximum possible data quantity at the currently configured data rate.

Lower threshold [%]

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

Possible values:

▶ 0.00..100.00 (default setting: 0.00)

The value 0 deactivates the lower threshold.

Upper threshold [%]

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

Possible values:

▶ 0.00..100.00 (default setting: 0.00)

The value 0 deactivates the upper threshold.

Control interval [s]

Specifies the interval in seconds.

Possible values:

▶ 1..3600 (default setting: 30)

Alarm

Displays the utilization alarm status.

Possible values:

▶ *marked*

The utilization of the port is below the value specified in the *Lower threshold [%]* column or above the value specified in the *Upper threshold [%]* column. The device sends an SNMP trap.

▶ *unmarked*

The utilization of the port is above the value specified in the *Lower threshold [%]* column and below the value specified in the *Upper threshold [%]* column.

The prerequisite for sending SNMP traps is that you enable the function in the *Diagnostics > Status Configuration > Alarms (Traps)* dialog and specify at least one trap destination.

Buttons

You find the description of the standard buttons in section “Buttons” on page 17.

Clear port statistics

Resets the counter for the port statistics to 0.

1.8 Power over Ethernet (MCSESP)

[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 power supplied to the ports according to configured priority. The device turns off power supplied to the ports starting with ports configured as a low priority first. When several ports have a low priority, the device turns off power starting with the higher numbered ports.

The menu contains the following dialogs:

- ▶ *PoE Global*
- ▶ *PoE Port*

1.8.1 PoE Global

[Basic Settings > Power over Ethernet > Global]

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

Operation

Operation

Enables/disables the *Power over Ethernet* function.

Possible values:

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

Configuration

Send trap

Activates/deactivates the sending of SNMP traps.

If the power consumption exceeds the user-specified threshold, then the device sends an SNMP trap.

Possible values:

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

The prerequisite for sending SNMP traps is that you enable the function in the *Diagnostics > Status Configuration > Alarms (Traps)* dialog and specify at least one trap destination.

Threshold [%]

Specifies the threshold value for the power consumption in percent.

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

Possible values:

▶ 0..99 (default setting: 90)

System power

Budget [W]

Displays the sum of the power available for the global budget.

Reserved [W]

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

Delivered [W]

Displays the actual power delivered to the modules in watts.

Delivered [mA]

Displays the actual current delivered to the modules in milliamperes.

Table

Module

Device module to which the table entries relate.

Configured power budget [W]

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

Possible values:

▶ 0..n (default setting: n)

Here, n corresponds to the value in the *Max. power budget [W]* column.

Max. power budget [W]

Displays the maximum power available for this module.

Reserved power [W]

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

Delivered power [W]

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

Delivered current [mA]

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

Power source

Displays the power sourcing equipment for the device.

Possible values:

- ▶ `internal`
Internal power source
- ▶ `external`
External power source

Threshold [%]

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

Possible values:

- ▶ `0..99` (default setting: 90)

Send trap

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

Possible values:

- ▶ `marked`
The sending of SNMP traps is active.
If the power consumption of the module exceeds the user-defined threshold, then the device sends an SNMP trap.
- ▶ `unmarked` (default setting)
The sending of SNMP traps is inactive.

The prerequisite for sending SNMP traps is that you enable the function in the [Diagnostics > Status Configuration > Alarms \(Traps\)](#) dialog and specify at least one trap destination.

Buttons

You find the description of the standard buttons in section [“Buttons” on page 17](#).

1.8.2 PoE Port

[Basic Settings > Power over Ethernet > Port]

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

Table

Port

Displays the port number.

PoE enable

Activates/deactivates the PoE power provided to the port.

When the function is activated or deactivated, the device logs an event in the log file (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)

Buttons

You find the description of the standard buttons in section “Buttons” on page 17.

1.9 Restart

[Basic Settings > Restart]

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

Restart

Restart in

Displays the remaining time until the device restarts.

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

Cancel

Aborts a delayed restart.

Cold start...

Opens the *Restart* dialog 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* dialog.

- To permanently save the changes, click the *Yes* button in the *Warning* dialog.
- To discard the changes, click the *No* button in the *Warning* dialog.
- In the *Restart in* field you specify the delay time for the delayed restart.

Possible values:

- 00:00:00..596:31:23 (default setting: 00:00:00)

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

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

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

Buttons

You find the description of the standard buttons in section "Buttons" on page 17.

Reset MAC address table

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

Reset ARP table

Removes the dynamically set up addresses from the ARP table.

See the *Diagnostics > System > ARP* dialog.

Clear port statistics

Resets the counter for the port statistics to 0.

See the *Basic Settings > Port* dialog, *Statistics* tab.

Clear management access statistics

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

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

Reset IGMP snooping data

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

See the *Switching > IGMP Snooping > Global* dialog.

Delete log file

Removes the logged events from the log file.

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

Delete persistent log file

Removes the log files from the external memory.

See the *Diagnostics > Report > Persistent Logging* dialog.

Clear email notification statistics

Resets the counters in the *Information* frame to 0.

See the *Diagnostics > Email Notification > Global* dialog.

2 Time

The menu contains the following dialogs:

- ▶ Basic Settings
- ▶ SNTP
- ▶ PTP
- ▶ 802.1AS

2.1 Basic Settings

[Time > Basic Settings]

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

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

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

The dialog contains the following tabs:

- ▶ [Global]
- ▶ [Daylight saving time]

[Global]

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

Configuration

System time (UTC)

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

Set time from PC

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

System time

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

Time source

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

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

Possible values:

- ▶ *local*
System clock of the device.
- ▶ *sntp*
The *SNTP* client is activated and the device is synchronized by an *SNTP* server.
- ▶ *ptp*
PTP is activated and the clock of the device is synchronized with a *PTP* master clock.

Local offset [min]

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

Possible values:

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

Buttons

You find the description of the standard buttons in section “Buttons” on page 17.

[Daylight saving time]

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

Operation

Daylight saving time

Enables/disables the *Daylight saving time* mode.

Possible values:

- ▶ *On*
The *Daylight saving time* mode is enabled.
The device automatically changes between summertime and wintertime.
- ▶ *OFF* (default setting)
The *Daylight saving time* mode is disabled.

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

Profile...

Displays the *Profile...* dialog. There you select a pre-defined profile for the beginning and the end of summertime. This profile overwrites the settings in the *Summertime begin* and *Summertime end* frames.

Summertime begin

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

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

Week

Specifies the week in the current month.

Possible values:

- ▶ *none* (default setting)
- ▶ *first*
- ▶ *second*
- ▶ *third*
- ▶ *fourth*
- ▶ *last*

Day

Specifies the day of the week.

Possible values:

- ▶ *none* (default setting)
- ▶ *Sunday*
- ▶ *Monday*
- ▶ *Tuesday*
- ▶ *Wednesday*
- ▶ *Thursday*
- ▶ *Friday*
- ▶ *Saturday*

Month

Specifies the month.

Possible values:

- ▶ *none* (default setting)
- ▶ *January*
- ▶ *February*
- ▶ *March*
- ▶ *April*
- ▶ *May*
- ▶ *June*

- ▶ *July*
- ▶ *August*
- ▶ *September*
- ▶ *October*
- ▶ *November*
- ▶ *December*

System time

Specifies the time.

Possible values:

- ▶ *<HH:MM>* (default setting: *00:00*)

Summertime end

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

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

Week

Specifies the week in the current month.

Possible values:

- ▶ *none* (default setting)
- ▶ *first*
- ▶ *second*
- ▶ *third*
- ▶ *fourth*
- ▶ *last*

Day

Specifies the day of the week.

Possible values:

- ▶ *none* (default setting)
- ▶ *Sunday*
- ▶ *Monday*
- ▶ *Tuesday*
- ▶ *Wednesday*
- ▶ *Thursday*
- ▶ *Friday*
- ▶ *Saturday*

Month

Specifies the month.

Possible values:

- ▶ *none* (default setting)
- ▶ *January*
- ▶ *February*
- ▶ *March*
- ▶ *April*
- ▶ *May*
- ▶ *June*
- ▶ *July*
- ▶ *August*
- ▶ *September*
- ▶ *October*
- ▶ *November*
- ▶ *December*

System time

Specifies the time.

Possible values:

- ▶ *<HH:MM>* (default setting: *00:00*)

Buttons

You find the description of the standard buttons in section “Buttons” on page 17.

2.2 SNTP

[Time > SNTP]

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

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

The menu contains the following dialogs:

- ▶ *SNTP Client*
- ▶ *SNTP Server*

2.2.1 SNTP Client

[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 the time information from both *SNTP* servers and *NTP* servers and synchronizes the local clock with the time of the time server.

Operation

Operation

Enables/disables the *SNTP Client* function of the device.

Possible values:

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

Configuration

Mode

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

Possible values:

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

Request interval [s]

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

Possible values:

- ▶ *5..3600* (default setting: 30)

Broadcast rcv timeout [s]

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

Possible values:

- ▶ *128..2048* (default setting: 320)

Disable client after successful sync

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

Possible values:

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

State

State

Displays the status of the *SNTP* client.

Possible values:

- ▶ *disabled*
The *SNTP* client is disabled.
- ▶ *notSynchronized*
The *SNTP* client is not synchronized with any *SNTP* or *NTP* server.
- ▶ *synchronizedToRemoteServer*
The *SNTP* client is synchronized with an *SNTP* or *NTP* server.

Table

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

Index

Displays the index number to which the table entry relates.

Possible values:

- ▶ 1..4

The device automatically assigns this number.

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

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

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

Name

Specifies the name of the *SNTP* server.

Possible values:

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

Address

Specifies the IP address of the *SNTP* server.

Possible values:

- ▶ Valid IPv4 address (default setting: 0.0.0.0)
- ▶ Valid IPv6 address
- ▶ Hostname

Destination UDP port

Specifies the UDP Port on which the *SNTP* server expects the time information.

Possible values:

- ▶ 1..65535 (default setting: 123)
Exception: Port 2222 is reserved for internal functions.

Status

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

Possible values:

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

- ▶ *badDateEncoded*
The time information received contains protocol errors - synchronization was unsuccessful.
- ▶ *other*
 - The value `0.0.0.0` is entered for the IP address of the *SNTP* server - synchronization was unsuccessful.
 - or
 - The *SNTP* client is using a different *SNTP* server.
- ▶ *requestTimedOut*
The device has not received a reply from the *SNTP* server - synchronization was unsuccessful.
- ▶ *serverKissOfDeath*
The *SNTP* server is overloaded. The device is requested to synchronize itself with another *SNTP* server. When no other *SNTP* server is available, the device checks at intervals longer than the setting in the *Request interval [s]* field, if the server is still overloaded.
- ▶ *serverUnsynchronized*
The *SNTP* server is not synchronized with either a local or an external reference time source - synchronization was unsuccessful.
- ▶ *versionNotSupported*
The *SNTP* versions on the client and the server are incompatible with each other - synchronization was unsuccessful.

Active

Activates/deactivates the connection to the *SNTP* server.

Possible values:

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

Buttons

You find the description of the standard buttons in section “Buttons” on page 17.

2.2.2 SNTP Server

[Time > SNTP > Server]

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

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

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

Operation

Operation

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

Possible values:

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

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

Configuration

UDP port

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

Possible values:

- ▶ *1..65535* (default setting: *123*)
Exception: Port *2222* is reserved for internal functions.

Broadcast admin mode

Activates/deactivates the Broadcast mode.

- ▶ *marked*
The *SNTP* server replies to requests from *SNTP* clients in Unicast mode and also sends *SNTP* packets in Broadcast mode as Broadcasts or Multicasts.
- ▶ *unmarked* (default setting)
The *SNTP* server replies to requests from *SNTP* clients in the Unicast mode.

Broadcast destination address

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

Possible values:

- ▶ Valid IPv4 address (default setting: 0.0.0.0)

Broadcast and Multicast addresses are permitted.

Broadcast UDP port

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

Possible values:

- ▶ 1..65535 (default setting: 123)
Exception: Port 2222 is reserved for internal functions.

Broadcast VLAN ID

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

Possible values:

- ▶ 0
The *SNTP* server sends the *SNTP* packets in the same VLAN in which the access to the device management is possible. See the *Basic Settings > Network* dialog.
- ▶ 1..4042 (default setting: 1)

Broadcast send interval [s]

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

Possible values:

- ▶ 64..1024 (default setting: 128)

Disable server at local time source

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

Possible values:

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

State

State

Displays the state of the *SNTP* server.

Possible values:

- ▶ *disabled*
The *SNTP* server is disabled.
- ▶ *notSynchronized*
The *SNTP* server is not synchronized with either a local or an external reference time source.
- ▶ *syncToLocal*
The *SNTP* server is synchronized with the hardware clock of the device.
- ▶ *syncToRefclock*
The *SNTP* server is synchronized with an external reference time source, for example PTP.
- ▶ *syncToRemoteServer*
The *SNTP* server is synchronized with an *SNTP* server that is higher than the device in a cascade.

Buttons

You find the description of the standard buttons in section “Buttons” on page 17.

2.3 PTP

[Time > PTP]

The menu contains the following dialogs:

- ▶ PTP Global
- ▶ PTP Boundary Clock
- ▶ PTP Transparent Clock

2.3.1 PTP Global

[Time > PTP > Global]

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

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

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

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

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

The protocol differentiates between the following clocks:

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

Operation IEEE1588/PTP

Operation IEEE1588/PTP

Enables/disables the *PTP* function.

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

Possible values:

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

Configuration IEEE1588/PTP

PTP mode

Specifies the PTP version and mode of the local clock.

Possible values:

- ▶ `v2-transparent-clock` (default setting)
- ▶ `v2-boundary-clock`

Sync lower bound [ns]

Specifies the lower threshold value in nanoseconds for the path difference between the local clock and the reference time source (*Grandmaster*). If the path difference falls below this value once, then the local clock is classed as synchronized.

Possible values:

- ▶ `0..999999999` (default setting: 30)

Sync upper bound [ns]

Specifies the upper threshold value in nanoseconds for the path difference between the local clock and the reference time source (*Grandmaster*). If the path difference exceeds this value once, then the local clock is classed as unsynchronized.

Possible values:

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

PTP management

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

Possible values:

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

Status

Is synchronized

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

If the path difference between the local clock and the reference time source (*Grandmaster*) falls below the synchronization lower threshold one time, then the local clock is synchronized. This status is kept until the path difference exceeds the synchronization upper threshold one time.

You specify the synchronization thresholds in the [Configuration IEEE1588/PTP](#) frame.

Max. offset absolute [ns]

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

PTP time

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

Buttons

You find the description of the standard buttons in section “Buttons” on page 17.

2.3.2 PTP Boundary Clock

[Time > PTP > Boundary Clock]

With this menu you can configure the Boundary Clock mode for the local clock.

The menu contains the following dialogs:

- ▶ PTP Boundary Clock Global
- ▶ PTP Boundary Clock Port

2.3.2.1 PTP Boundary Clock Global

[Time > PTP > Boundary Clock > Global]

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

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

Operation IEEE1588/PTPv2 BC

Priority 1

Specifies *priority 1* for the device.

Possible values:

▶ 0..255 (default setting: 128)

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

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

Priority 2

Specifies *priority 2* for the device.

Possible values:

▶ 0..255 (default setting: 128)

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

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

Domain number

Assigns the device to a *PTP* domain.

Possible values:

▶ 0..255 (default setting: 0)

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

Status IEEE1588/PTPv2 BC

Two step

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

Steps removed

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

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

Offset to master [ns]

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

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

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

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

Delay to master [ns]

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

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

The prerequisite is that the delay mechanism value of the slave ports is specified as *e2e*.

Grandmaster

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

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

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

Priority 1

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

Time

[Time > PTP > Boundary Clock > Global]

Clock class

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

Clock accuracy

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

Clock variance

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

Priority 2

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

Local time properties

Time source

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

Possible values:

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

UTC offset [s]

Specifies the difference between the *PTP* time scale and the UTC.

See the *PTP timescale* checkbox.

Possible values:

- ▶ *-32768..32767*

Note: The default setting is the value valid on the creation date of the device software. You can find further information in the "Bulletin C" of the Earth Rotation and Reference Systems Service (IERS): <http://www.iers.org/iers/EN/Publications/Bulletins/bulletins.html>

UTC offset valid

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

Possible values:

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

Time traceable

Displays if the device gets the time from a primary UTC reference, for example from an NTP server.

Possible values:

- ▶ `marked`
- ▶ `unmarked`

Frequency traceable

Displays if the device gets the frequency from a primary UTC reference, for example from an NTP server.

Possible values:

- ▶ `marked`
- ▶ `unmarked`

PTP timescale

Displays if the device uses the PTP time scale.

Possible values:

- ▶ `marked`
- ▶ `unmarked`

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

In contrast to UTC, TAI does not use leap seconds.

As of July 1, 2020, the TAI time is 37 s ahead of the UTC time.

Identities

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

The identification numbers (UUID) are made up as follows:

- ▶ The device identification number consists of the MAC address of the device, with the values `ff` and `fe` added between byte 3 and byte 4.
- ▶ The port UUID consists of the device identification number followed by a 16-bit port ID.

Clock identity

Displays the device's own identification number (UUID).

Time

[Time > PTP > Boundary Clock > Global]

Parent port identity

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

Grandmaster identity

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

Buttons

You find the description of the standard buttons in section [“Buttons” on page 17](#).

2.3.2.2 PTP Boundary Clock Port

[Time > PTP > Boundary Clock > Port]

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

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

Table

Port

Displays the port number.

PTP enable

Activates/deactivates *PTP* synchronization message transmission on the port.

Possible values:

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

PTP status

Displays the current status of the port.

Possible values:

- ▶ `initializing`
Initialization phase
- ▶ `faulty`
Faulty mode: error in the *PTP* protocol.
- ▶ `disabled`
PTP is disabled on the port.
- ▶ `listening`
Device port is waiting for *PTP* synchronization messages.
- ▶ `pre-master`
PTP pre-master mode
- ▶ `master`
PTP master mode
- ▶ `passive`
PTP passive mode
- ▶ `uncalibrated`
PTP uncalibrated mode
- ▶ `slave`
PTP slave mode

Sync interval

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

Possible values:

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

Delay mechanism

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

Possible values:

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

P2P delay

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

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

P2P delay interval [s]

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

The prerequisite is that you have specified the value *p2p* on this port and on the port of the remote device.

Possible values:

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

Network protocol

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

Possible values:

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

Announce interval [s]

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

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

Possible values:

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

Announce timeout

Specifies the number of announce intervals.

Example:

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

Possible values:

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

E2E delay interval [s]

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

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

V1 hardware compatibility

Specifies if the port adjusts the length of the *PTP* synchronization messages when you have set in the *Network protocol* column the value *udpIpv4*.

It is possible that other devices in the network expect the *PTP* synchronization messages to be the same length as PTPv1 messages.

Possible values:

- ▶ *auto* (default setting)
The device automatically detects if other devices in the network expect the *PTP* synchronization messages to be the same length as PTPv1 messages. If this is the case, then the device extends the length of the *PTP* synchronization messages before transmitting them.

Time

[Time > PTP > Boundary Clock > Port]

- ▶ *on*
The device extends the length of the *PTP* synchronization messages before transmitting them.
- ▶ *off*
The device transmits *PTP* synchronization messages without changing the length.

Asymmetry

Corrects the measured delay value corrupted by asymmetrical transmission paths.

Possible values:

- ▶ *-2000000000..2000000000* (default setting: 0)

The value represents the delay symmetry in nanoseconds.

A measured delay value of y ns corresponds to an asymmetry of $y \times 2$ ns.

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

VLAN

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

Possible values:

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

Verify that the port is a member of the VLAN.

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

VLAN priority

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

Possible values:

- ▶ *0..7* (default setting: 6)

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

Buttons

You find the description of the standard buttons in section [“Buttons” on page 17](#).

2.3.3 PTP Transparent Clock

[Time > PTP > Transparent Clock]

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

The menu contains the following dialogs:

- ▶ PTP Transparent Clock Global
- ▶ PTP Transparent Clock Port

2.3.3.1 PTP Transparent Clock Global

[Time > PTP > Transparent Clock > Global]

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

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

Operation IEEE1588/PTPv2 TC

Delay mechanism

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

Possible values:

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

Primary domain

Assigns the device to a *PTP* domain.

Possible values:

- ▶ *0..255* (default setting: 0)

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

Network protocol

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

Possible values:

- ▶ *ieee8023* (default setting)
- ▶ *udpIpv4*

Multi domain mode

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

Possible values:

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

VLAN ID

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

Possible values:

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

VLAN priority

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

Possible values:

- ▶ *0..7* (default setting: 6)

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

Local synchronization

Syntonize

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

Possible values:

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

Synchronize local clock

Activates/deactivates the synchronization of the local system time.

Possible values:

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

Current master

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

If the value contains only zeros, this is because:

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

Offset to master [ns]

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

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

Delay to master [ns]

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

Prerequisite:

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

Status IEEE1588/PTPv2 TC

Clock identity

Displays the device's own identification number (UUID).

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

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

Buttons

You find the description of the standard buttons in section [“Buttons” on page 17](#).

2.3.3.2 PTP Transparent Clock Port

[Time > PTP > Transparent Clock > Port]

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

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

Table

Port

Displays the port number.

PTP enable

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

Possible values:

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

P2P delay interval [s]

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

The prerequisite is that you specify the value *p2p* on this port and on the port of the remote terminal. See the *Delay mechanism* option list in the *Time > PTP > Transparent Clock > Global* dialog.

Possible values:

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

P2P delay

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

The prerequisite is that you select in the *Delay mechanism* option list the *p2p* radio button. See the *Delay mechanism* field in the *Time > PTP > Transparent Clock > Global* dialog.

Asymmetry

Corrects the measured delay value corrupted by asymmetrical transmission paths.

Possible values:

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

The value represents the delay symmetry in nanoseconds.

A measured delay value of y ns corresponds to an asymmetry of $y \times 2$ ns.

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

Buttons

You find the description of the standard buttons in section “Buttons” on page 17.

2.4 802.1AS

[Time > 802.1AS]

The *802.1AS* protocol is a procedure described in the IEEE 802.1AS-2011 standard that defines how to synchronize time accurately between devices in the network. When you use the *802.1AS* protocol over the Ethernet, you can think of the protocol as a profile of the IEEE 1588-2008 standard.

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

The *802.1AS* protocol has the following specifications:

- ▶ In the device, either the *802.1AS* function or the *PTP* function can be enabled.
- ▶ If the *SNTP* function and the *802.1AS* function are enabled in the device at the same time, then the *802.1AS* function has priority.
- ▶ The *802.1AS* function supports only one domain.

The menu contains the following dialogs:

- ▶ 802.1AS Global
- ▶ 802.1AS Port
- ▶ 802.1AS Statistics

2.4.1 802.1AS Global

[Time > 802.1AS > Global]

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

Operation

Operation

Enables/disables the **802.1AS** function.

Possible values:

- ▶ **On**
The **802.1AS** function is enabled.
The device synchronizes its clock using the **802.1AS** protocol.
Consider to activate the **802.1AS** protocol on the individual ports.
- ▶ **OFF** (default setting)
The **802.1AS** function is disabled.

Configuration

Priority 1

Specifies *priority 1* for the device.

Possible values:

- ▶ **0..255** (default setting: 246)

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

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

If you specify the value 255, then the device is not designated as the reference time source (*Grandmaster*). See the *Grandmaster* frame.

Priority 2

Specifies *priority 2* for the device.

Possible values:

- ▶ **0..255** (default setting: 248)

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

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

Sync lower bound [ns]

Specifies the lower threshold value in nanoseconds for the measured time difference between the local clock and the reference time source (*Grandmaster*). If the measured time difference falls below this value once, then the local clock is classed as synchronized.

Possible values:

▶ 0..999999999 (default setting: 30)

Sync upper bound [ns]

Specifies the upper threshold value in nanoseconds for the measured time difference between the local clock and the reference time source (*Grandmaster*). If the measured time difference exceeds this value once, then the local clock is classed as unsynchronized.

Possible values:

▶ 31..1000000000 (default setting: 5000)

UTC offset [s]

Displays the difference between the *802.1AS* time scale and the UTC.

UTC offset valid

Displays if the value displayed in the *UTC offset [s]* field is correct.

Possible values:

▶ marked

▶ unmarked

Status

Offset to master [ns]

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

Max. offset absolute [ns]

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

Is synchronized

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

If the measured time difference between the local clock and the reference time source (*Grandmaster*) falls below the synchronization lower threshold, then the local clock is synchronized. This status is kept until the measured time difference exceeds the synchronization upper threshold.

You specify the synchronization thresholds in the *Configuration* frame.

Steps removed

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

For a *802.1AS* slave, the value *1* means that the clock is connected with the reference time source (*Grandmaster*) directly through *1* communication path.

Clock identity

Displays the clock identification number of the device.

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

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

Grandmaster

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

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

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

Priority 1

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

Clock class

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

Clock accuracy

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

Clock variance

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

Priority 2

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

Clock identity

Displays the identification number of the reference time source (*Grandmaster*) device. The device displays the identification number as byte sequences in hexadecimal notation.

Parent

Clock identity

Displays the port identification number of the directly superior master device. The device displays the identification number as byte sequences in hexadecimal notation.

Port

Displays the port number of the directly superior master device.

Cumulative rate ratio [ppm]

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

Buttons

You find the description of the standard buttons in section [“Buttons” on page 17](#).

2.4.2 802.1AS Port

[Time > 802.1AS > Port]

In this dialog you specify the *802.1AS* settings on each individual port.

Table

Port

Displays the port number.

Active

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

Possible values:

- ▶ *marked* (default setting)
The protocol is active on the port.
On the port, the device synchronizes its clock using the *802.1AS* protocol.
- ▶ *unmarked*
The protocol is inactive on the port.

Role

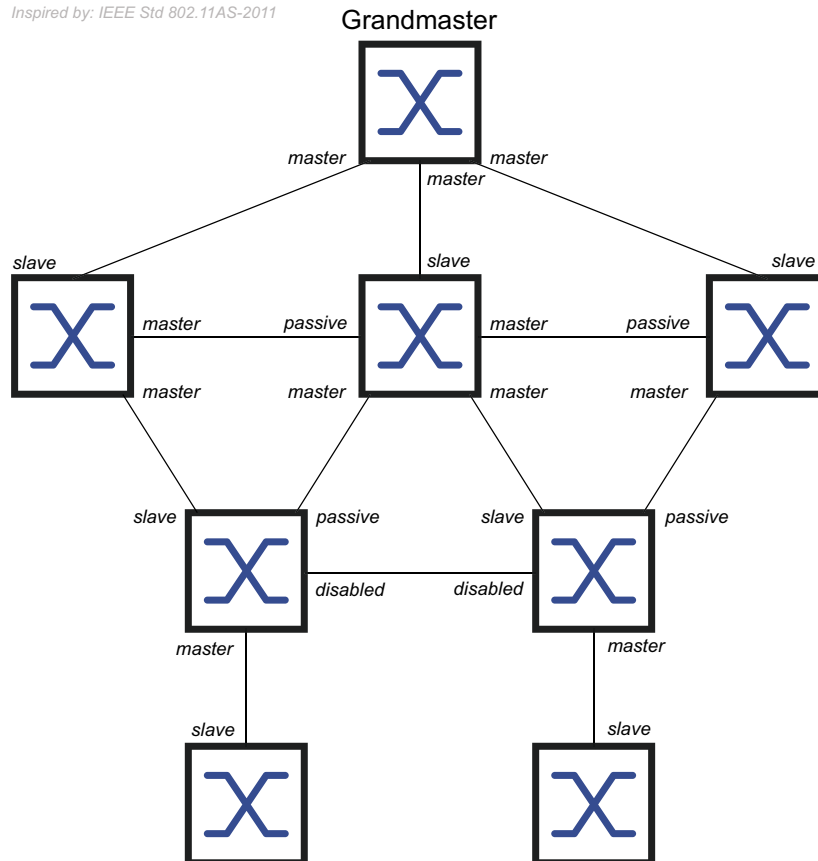
Displays the current role of the port, considering the *802.1AS* protocol.

Possible values:

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

- ▶ *passive*
The port operates in the *Passive Port* role.
- ▶ *slave*
The port operates in the *Slave Port* role.

Inspired by: IEEE Std 802.11AS-2011



AS capable

Displays if the *802.1AS* protocol is active on the port.

Possible values:

- ▶ *marked*
The *802.1AS* protocol is active on the port. The prerequisites are:
 - The port measures a *Peer delay*, the checkbox in the *Measuring delay* column is marked.
 - The value in the *Peer delay [ns]* column is lower than the value in the *Peer delay threshold [ns]* column.
- ▶ *unmarked*
The *802.1AS* protocol is inactive on the port.

Announce interval [s]

Specifies the interval in seconds at which the port (in the *Master Port* role) transmits *Announce* messages for *802.1AS* topology discovery.

Possible values:

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

Announce timeout

Specifies the number of *Announce interval [s]* at which the port (in the *Slave Port* role) waits for *Announce* messages.

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

Example: In the default setting (*Announce interval [s]* = 1, *Announce timeout* = 3), the timeout is $3 \times 1 \text{ s} = 3 \text{ s}$.

Possible values:

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

Sync interval [s]

Specifies the interval in seconds at which the port (in the *Master Port* role) transmits *Sync* messages for time synchronization.

Possible values:

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

Sync timeout

Specifies the number of *Sync interval [s]* at which the port (in the *Slave Port* role) waits for *Sync* messages.

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

Example: In the default setting (*Sync interval [s]* = 0.125, *Sync timeout* = 3), the timeout is $3 \times 0.125 \text{ s} = 0.375 \text{ s}$.

Possible values:

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

Peer delay interval [s]

Specifies the interval in seconds at which the port (in the *Master Port*, *Passive Port* or *Slave Port* role) transmits a *Peer delay request* message to measure the *Peer delay*.

Possible values:

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

The port does not transmit *Peer delay request* messages.

Peer delay timeout

Specifies the number of *Peer delay interval [s]* at which the port (in the *Master Port*, *Passive Port* or *Slave Port* role) waits for *Delay response* messages.

When the number of intervals elapses without receiving an *Delay response* message, the device assigns the *Disabled Port* role to the port. The port is no longer *802.1AS*-capable.

Possible values:

- ▶ 2..10 (default setting: 3)

Peer delay threshold [ns]

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

Possible values:

- ▶ 0..1000000000 (default setting: 10000)

Measuring delay

Displays if the port measures a *Peer delay*.

Possible values:

- ▶ *marked*
The port measures a *Peer delay*. You find the measured value in the *Peer delay [ns]* column.
- ▶ *unmarked*
The port does not measure a *Peer delay*.

Peer delay [ns]

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

Neighbor rate ratio [ppm]

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

Buttons

You find the description of the standard buttons in section [“Buttons” on page 17](#).

2.4.3 802.1AS Statistics

[Time > 802.1AS > Statistics]

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

Table

Port

Displays the port number.

Received messages

Displays the counters for messages received on the ports:

Sync messages

Displays the number of *Sync* messages.

Sync follow-up messages

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

Delay request messages

Displays the number of *Peer delay request* messages.

Delay response messages

Displays the number of *Peer delay response* messages.

Delay response follow-up messages

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

Announce messages

Displays the number of *Announce* messages.

Discarded messages

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

Sync timeout

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

Announce timeout

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

Delay timeout

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

Transmitted messages

Displays the counters for messages transmitted on the ports:

Sync messages

Displays the number of *Sync* messages.

Sync follow-up messages

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

Delay request messages

Displays the number of *Peer delay request* messages.

Delay response messages

Displays the number of *Peer delay response* messages.

Delay response follow-up messages

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

Announce messages

Displays the number of *Announce* messages.

Buttons

You find the description of the standard buttons in section “Buttons” on page 17.

3 Device Security

The menu contains the following dialogs:

- ▶ [User Management](#)
- ▶ [Authentication List](#)
- ▶ [LDAP](#)
- ▶ [Management Access](#)
- ▶ [Pre-login Banner](#)

3.1 User Management

[Device Security > User Management]

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

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

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

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

Configuration

This frame lets you specify settings for the login.

Login attempts

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

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

Possible values:

- ▶ [0..5](#) (default setting: 0)

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

The device lets only users with the [administrator](#) authorization remove the lock.

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

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)

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)

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 you mark the checkbox in the *Policy check* column.

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.

User name

Displays the name of the user account.

To create a new 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 with this user name.

▶ *unmarked* (default setting)

The user account is inactive. The device rejects the login of a user with this user name.

When one user account exists with the *administrator* access role, 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 in. To change the password, click the relevant field.

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

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

Possible values:

- ▶ Alphanumeric ASCII character string with 6..64 characters
The following characters are allowed:

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

Possible values:

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

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

User locked

Unlocks the user account.

Possible values:

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

Policy check

Activates/deactivates the password check.

Possible values:

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

SNMP auth type

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

Possible values:

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

SNMP auth password

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

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

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

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

Possible values:

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

SNMP encryption type

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

Possible values:

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

SNMP encryption password

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

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

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

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

Possible values:

- ▶ Alphanumeric ASCII character string with 6..64 characters

The following characters are allowed:

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

Buttons

You find the description of the standard buttons in section “Buttons” on page 17.



Opens the *Create* window to add a new entry to the table.

- ▶ In the *User name* field, you specify the name of the user account.

Possible values:

- Alphanumeric ASCII character string with 1..32 characters

3.2 Authentication List

[Device Security > Authentication List]

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

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

- ▶ User management of the device
- ▶ LDAP
- ▶ RADIUS

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

- ▶ RADIUS
- ▶ IAS (Integrated Authentication Server)

In the default setting the following authentication lists are available:


- ▶ `defaultDot1x8021AuthList`
- ▶ `defaultLoginAuthList`
- ▶ `defaultV24AuthList`

Table

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.

Name

Displays the name of the list.

To create a new list, click the  button.

Possible values:

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

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 authentication depending on which policy you try first. The following list contains authentication scenarios:
 - If the first policy in the authentication list is *local* and the device accepts the login credentials of the user, then it logs the user in without attempting the other policies.
 - If the first policy in the authentication list is *local* and the device denies the login credentials of the user, then it attempts to log the user in using the other policies in the order specified.
 - If the first policy in the authentication list is *radius* or *ldap* and the device rejects a login, then the login is immediately rejected without attempting to log in the user using another policy.
If there is no response from the RADIUS or LDAP server, then the device attempts to authenticate the user with the next policy.
 - If the first policy in the authentication list is *reject*, then the device 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 via 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 Port Authentication > Integrated Authentication Server](#) dialog.
You can only assign this value to the authentication list `defaultDot1x8021AuthList`.
- ▶ *ldap*
The device authenticates the users with authentication data and access role saved in a central location. You specify the Active Directory server that the device uses in the [Network 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 and then the [Allocate applications](#) item. The device lets you assign each application to exactly one list.

Active

Activates/deactivates the list.

Possible values:

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

Buttons

You find the description of the standard buttons in section “Buttons” on page 17.

Allocate applications

Opens the *Allocate applications* window.

- ▶ The left field displays the applications that can be allocated to the highlighted list.
- ▶ The right field displays the applications that are allocated to the highlighted list.
- ▶ Buttons:
 - Moves every entry to the right field.
 - Moves the highlighted entries from the left field to the right field.
 - Moves the highlighted entries from the right field to the left field.
 - Moves every entry to the left field.

Note: When you move the entry *WebInterface* to the left field, the connection to the device is lost, after you click the *Ok* button.

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 LDAP protocol. The authentication server decides if the login data is valid and transfers the user’s authorizations to the device.

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

The menu contains the following dialogs:

- ▶ LDAP Configuration
- ▶ LDAP Role Mapping

3.3.1 LDAP Configuration

[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 rows *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 role *administrator*. This provides you access to the device as administrator after logging in through LDAP.

Possible values:

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

Configuration

Client cache timeout [min]

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

Possible values:

- ▶ *1..1440* (default setting: 10)

Bind user

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

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

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

Possible values:

- ▶ Alphanumeric ASCII character string with 0..64 characters

Bind user password

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

Possible values:

- ▶ Alphanumeric ASCII character string with 0..64 characters

Base DN

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

Possible values:

- ▶ Alphanumeric ASCII character string with 0..255 characters

User name attribute

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

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

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

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

Possible values:

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

Default domain

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

Possible values:

- ▶ Alphanumeric ASCII character string with 0..64 characters

CA certificate

URL


Specifies the path and file name of the certificate.

The device accepts certificates with the following properties:

- X.509 format
- .PEM file name extension
- Base64-coded, enclosed by
-----BEGIN CERTIFICATE-----
and
-----END CERTIFICATE-----

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

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

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

Start

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

Table

Index

Displays the index number to which the table entry relates.

Description

Specifies the description.

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

Possible values:

- ▶ Alphanumeric ASCII character string with 0..255 characters

Address

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

Possible values:

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

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

Destination TCP port

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

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

Possible values:

- ▶ 0..65535 (default setting: 389)
Exception: Port 2222 is reserved for internal functions.

Frequently used TCP-Ports:

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

Connection security

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

Possible values:

- ▶ *none*
No encryption.
The device establishes an LDAP connection to the server and transmits the communication including the passwords in clear text.
- ▶ *ssl*
Encryption with SSL.
The device establishes a TLS connection to the server and tunnels the LDAP communication over it.
- ▶ *startTLS* (default setting)
Encryption with startTLS extension.
The device establishes an LDAP connection to the server and encrypts the communication.

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

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

Server status

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

Possible values:

- ▶ *ok*
The server is reachable.
If in the *Connection security* row a value other than *none* is specified, then the device has verified the certificate of the server.
- ▶ *unreachable*
Server is unreachable.
- ▶ *other*
The device has not established a connection to the server yet.

Active

Activates/deactivates the use of the server.

Possible values:

- ▶ *marked*
The device uses the server.
- ▶ *unmarked* (default setting)
The device does not use the server.

Buttons

You find the description of the standard buttons in section [“Buttons” on page 17](#).

Flush cache

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

3.3.2 LDAP Role Mapping

[Device Security > LDAP > Role Mapping]

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

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

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

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

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

On this basis, the device checks any mapping.

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

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

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

Configuration

Matching policy

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

Possible values:

- ▶ *highest* (default setting)
The device applies the role with more extensive authorizations.
- ▶ *first*
The device applies the rule which has the lower value in the *Index* column to the user.

Table

Index

Displays the index number to which the table entry relates.

Role

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

Possible values:

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

Type

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

Possible values:

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

Parameter

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

Possible values:

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

Active

Activates/deactivates the role mapping.

Possible values:

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

Buttons

You find the description of the standard buttons in section “Buttons” on page 17.



Opens the *Create* window to add a new entry to the table.

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

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

SNMPv1

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

Possible values:

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

SNMPv2

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

Possible values:

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

SNMPv3

Displays if the server service is active or inactive, which authorizes access to the device using SNMP version 3. See the [SNMP](#) tab.

Possible values:

- ▶ [marked](#)
Server service is active.
- ▶ [unmarked](#)
Server service is inactive.

Telnet server

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

Possible values:

- ▶ [marked](#)
Server service is active.
- ▶ [unmarked](#)
Server service is inactive.

SSH server

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

Possible values:

- ▶ [marked](#)
Server service is active.
- ▶ [unmarked](#)
Server service is inactive.

HTTP server

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

Possible values:

- ▶ [marked](#)
Server service is active.
- ▶ [unmarked](#)
Server service is inactive.

HTTPS server

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

Possible values:

- ▶ [marked](#)
Server service is active.
- ▶ [unmarked](#)
Server service is inactive.

Buttons

You find the description of the standard buttons in section “Buttons” on page 17.

[SNMP]

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

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

Configuration

SNMPv1

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

Possible values:

- ▶ `marked` (default setting)
Access is activated.
- ▶ `unmarked`
Access is deactivated.

You specify the community names in the [Device Security > Management Access > SNMPv1/v2 Community](#) dialog.

SNMPv2

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

Possible values:

- ▶ `marked` (default setting)
Access is activated.
- ▶ `unmarked`
Access is deactivated.

You specify the community names in the [Device Security > Management Access > SNMPv1/v2 Community](#) dialog.

SNMPv3

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

Possible values:

- ▶ `marked` (default setting)
Access is activated.
- ▶ `unmarked`
Access is deactivated.

Network management systems like ConneXium Network Manager use this protocol to communicate with the device.



UDP port

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

Possible values:

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

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

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

Buttons

You find the description of the standard buttons in section [“Buttons” on page 17](#).

[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:

- ▶ The Telnet server is enabled.
The access to the device management is possible through the Command Line Interface using an unencrypted Telnet connection.
- ▶ 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 (default setting: 23)
Exception: Port 2222 is reserved for internal functions.

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

Connections

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

Connections (max.)

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

Possible values:

- ▶ 1..5 (default setting: 5)

Session timeout [min]

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

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

Possible values:

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

Buttons

You find the description of the standard buttons in section [“Buttons” on page 17](#).

[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 via a reliable channel, they have the option to compare both fingerprints. If the character sequences match, then the client is connected to the correct server.

The device lets you create the private and public keys (host keys) required for RSA directly in the device. Otherwise you have the option to copy your own keys to the device in PEM format.

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

Operation

SSH server

Enables/disables the SSH server.

Possible values:

- ▶ *On* (default setting)
The SSH server is enabled.
The access to the device management is possible through the Command Line Interface using an encrypted SSH connection.
You can start the server only if there is an RSA signature in the device.
- ▶ *Off*
The SSH server is disabled.
When you disable the SSH server, the existing connections remain established. However, the device helps prevent new connections from being set up.

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

Configuration

TCP port

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

Possible values:

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

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

Sessions

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

Sessions (max.)

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

Possible values:

- ▶ 1..5 (default setting: 5)

Session timeout [min]

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

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

Possible values:

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

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*
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.

Signature

RSA present

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

Possible values:

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

Create

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

Length of the key created:

- ▶ 2048 bit (RSA)

To get the SSH server to use the generated host key, re-enable the SSH server.

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

Delete

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

Oper status

Displays if the device currently generates a host key.

It is possible that another user triggered this action.

Possible values:

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

Key import

URL


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

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

- 2048 bit (RSA)

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

▶ Import from the PC

When the host key is located on your PC or on a network drive, drag and drop the file that contains the key in the  area. Alternatively click in the area to select the file.

▶ Import from an FTP server

When the key is on an FTP server, specify the URL for the file in the following form:
ftp://<user>:<password>@<IP address>:<port>/<file name>

▶ Import from a TFTP server

When the key is on a TFTP server, specify the URL for the file in the following form:
tftp://<IP address>/<path>/<file name>

▶ Import from an SCP or SFTP server

When the key is on an SCP or SFTP server, specify the URL for the file in the following form:

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

When you click the *Start* button, the device displays the *Credentials* window. There you enter *User name* and *Password*, to log in to the server.

- scp://<user>:<password>@<IP address>/<path>/<file name>

Start

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

Buttons


You find the description of the standard buttons in section “Buttons” on page 17.

[HTTP]

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

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

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

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

Operation

HTTP server

Enables/disables the *HTTP* protocol for the web server.

Possible values:

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

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

Configuration

TCP port

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

Possible values:

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

Buttons

You find the description of the standard buttons in section “Buttons” on page 17.

[HTTPS]

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

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

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

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

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

Operation

HTTPS server

Enables/disables the *HTTPS* protocol for the web server.

Possible values:

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

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

Configuration

TCP port

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

Possible values:

- ▶ *1..65535* (default setting: *443*)
Exception: Port *2222* is reserved for internal functions.

Fingerprint

The fingerprint is an easily verified hexadecimal number sequence that uniquely identifies the digital certificate of the HTTPS server.

After importing a new digital certificate, the device displays the current fingerprint until you restart the server.

Fingerprint type

Specifies which fingerprint the *Fingerprint* field displays.

Possible values:

- ▶ *sha1*
The *Fingerprint* field displays the SHA1 fingerprint of the certificate.
- ▶ *sha256*
The *Fingerprint* field displays the SHA256 fingerprint of the certificate.

Fingerprint

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

Note: If the device uses a certificate that is not signed by a certification authority, then the web browser displays a message while loading the Graphical User Interface. To continue, add an exception rule for the certificate in the web browser.

Present

Displays if the digital certificate is present in the device.

Possible values:

- ▶ *marked*
The certificate is present.
- ▶ *unmarked*
The certificate has been removed.

Create

Generates a digital certificate in the device.

Until restarting the web server uses the previous certificate.

To get the web server to use the newly generated certificate, restart the web server. Restarting the web server is possible only through the Command Line Interface.

Alternatively, you have the option of copying your own certificate to the device. See the *Certificate import* frame.

Delete

Deletes the digital certificate.

Until restarting the web server uses the previous certificate.

Oper status

Displays if the device currently generates or deletes a digital certificate.

It is possible that another user has triggered the action.

Possible values:

- ▶ *none*
The device does currently not generate or delete a certificate.
- ▶ *delete*
The device currently deletes a certificate.
- ▶ *generate*
The device currently generates a certificate.

Certificate import

URL


Specifies the path and file name of the certificate.

The device accepts certificates with the following properties:

- X.509 format
- .PEM file name extension
- Base64-coded, enclosed by


```
-----BEGIN PRIVATE KEY-----
and
-----END PRIVATE KEY-----
as well as
-----BEGIN CERTIFICATE-----
and
-----END CERTIFICATE-----
```
- RSA key with 2048 bit length

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

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

Start

Copies the certificate specified in the [URL](#) field to the device.

Buttons

You find the description of the standard buttons in section [“Buttons” on page 17](#).

3.4.2 IP Access Restriction

[Device Security > Management Access > IP Access Restriction]

This dialog enables you to restrict the access to the device management to specific IP address ranges and selected IP-based applications.

- ▶ If the function is disabled, then the access to the device management is possible from any IP address and using every application.
- ▶ If the function is enabled, then the access is restricted. You have access to the device management only under the following conditions:
 - At least one table entry is activated.
 - and
 - You are accessing the device with a permitted application from a permitted IP address range.

Operation

Note: Before you enable the function, verify that at least one active entry in the table lets you access. Otherwise, if you change the settings, then the connection to the device terminates. The access to the device management is possible only using the Command Line Interface through the serial interface.

Operation

Enables/disables the *IP Access Restriction* function.

Possible values:

- ▶ *On*
The *IP Access Restriction* function is enabled.
The access to the device management is restricted.
- ▶ *OFF* (default setting)
The *IP Access Restriction* function is disabled.

Table

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

Index

Displays the index number to which the table entry relates.

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

Possible values:

- ▶ 1..16

Address

Specifies the IP address of the network from which you allow the access to the device management. You specify the network range in the *Netmask* column.

Possible values:

- ▶ Valid IPv4 address (default setting: 0.0.0.0)

Netmask

Specifies the range of the network specified in the *Address* column.

Possible values:

- ▶ Valid netmask (default setting: 0.0.0.0)

HTTP

Activates/deactivates the HTTP access.

Possible values:

- ▶ *marked* (default setting)
Access is activated for the adjacent IP address range.
- ▶ *unmarked*
Access is deactivated.

HTTPS

Activates/deactivates the HTTPS access.

Possible values:

- ▶ *marked* (default setting)
Access is activated for the adjacent IP address range.
- ▶ *unmarked*
Access is deactivated.

SNMP

Activates/deactivates the SNMP access.

Possible values:

- ▶ *marked* (default setting)
Access is activated for the adjacent IP address range.
- ▶ *unmarked*
Access is deactivated.

Telnet

Activates/deactivates the Telnet access.

Possible values:

- ▶ `marked` (default setting)
Access is activated for the adjacent IP address range.
- ▶ `unmarked`
Access is deactivated.

SSH

Activates/deactivates the SSH access.

Possible values:

- ▶ `marked` (default setting)
Access is activated for the adjacent IP address range.
- ▶ `unmarked`
Access is deactivated.

IEC61850-MMS

Activates/deactivates the access to the MMS server.

Possible values:

- ▶ `marked` (default setting)
Access is activated for the adjacent IP address range.
- ▶ `unmarked`
Access is deactivated.

Modbus TCP

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

Possible values:

- ▶ `marked` (default setting)
Access is activated for the adjacent IP address range.
- ▶ `unmarked`
Access is deactivated.

EtherNet/IP

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

Possible values:

- ▶ `marked` (default setting)
Access is activated for the adjacent IP address range.
- ▶ `unmarked`
Access is deactivated.

Active

Activates/deactivates the table entry.

Possible values:

- ▶ `marked` (default setting)
Table entry is activated. The device restricts the access to the device management to the adjacent IP address range and the selected IP-based applications.
- ▶ `unmarked`
Table entry is deactivated.

Buttons

You find the description of the standard buttons in section [“Buttons” on page 17](#).

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 in.

Possible values:

▶ 0..160 (default setting: 5)

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

Buttons

You find the description of the standard buttons in section [“Buttons” on page 17](#).

3.4.4 Command Line Interface

[Device Security > Management Access > CLI]

In this dialog you specify settings for the Command Line Interface. You find detailed information about the Command Line Interface in 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: (MCSESM-E)

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

Serial interface timeout [min]

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

Possible values:

- ▶ 0..160 (default setting: 5)
- The value 0 deactivates the function, and the user remains logged in when inactive.

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

For the *Telnet* server and the *SSH* server, you specify the timeout in the *Device Security > Management Access > Server* dialog.

Buttons

You find the description of the standard buttons in section “Buttons” on page 17.

[Login banner]

In this tab you replace the start screen of the Command Line Interface with your own text.

In the default setting, the start screen displays information about the device, such as the software version and the device settings. With the function in this tab, you deactivate this information and replace it with an individually specified text.

To display your own text in the Command Line Interface and in the Graphical User Interface before the login, you use the *Device Security > Pre-login Banner* dialog.

Operation

Operation

Enables/disables the *Login banner* function.

Possible values:

- ▶ *On*
The *Login banner* function is enabled.
The device displays the text information specified in the *Banner text* field to the users that log in with the Command Line Interface.
- ▶ *Off* (default setting)
The *Login banner* function is disabled.
The start screen displays information about the device. The text information in the *Banner text* field is kept.

Banner text

Banner text

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

Possible values:

- ▶ Alphanumeric ASCII character string with 0..1024 characters (0x20..0x7E) including space characters
- ▶ <Tab>
- ▶ <Line break>

Remaining characters

Displays how many characters are still remaining in the *Banner text* field for the text information.

Possible values:

▶ 1024..0

Buttons

You find the description of the standard buttons in section “Buttons” on page 17.

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.

Applications send requests via SNMPv1/v2 with a community name in the SNMP data packet header. Depending on the community name, the application gets read authorization or read and write authorization for the device.

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

Table

Community

Displays the authorization for SNMPv1/v2 applications to the device:

- ▶ [Write](#)
For requests with the community name entered, the application receives read and write authorization for the device.
- ▶ [Read](#)
For requests with the community name entered, the application receives read authorization for the device.

Name

Specifies the community name for the adjacent authorization.

Possible values:

- ▶ Alphanumeric ASCII character string with 0..32 characters
 - [admin](#) (default setting for read and write authorizations)
 - [user](#) (default setting for read authorization)

Buttons

You find the description of the standard buttons in section [“Buttons” on page 17](#).

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 in.

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

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

Operation

Operation

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

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

Possible values:

- ▶ [On](#)
The [Pre-login Banner](#) function is enabled.
The device displays the text specified in the [Banner text](#) field in the login dialog.
- ▶ [OFF](#) (default setting)
The [Pre-login Banner](#) function is disabled.
The device does not display a text in the login dialog. When you enter a text in the [Banner text](#) field, this text is saved in the device.

Banner text

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>](#)

Remaining characters

Displays how many characters are still remaining in the *Banner text* field.

Possible values:

▶ 512..0

Buttons

You find the description of the standard buttons in section “Buttons” on page 17.

4 Network Security

The menu contains the following dialogs:

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

4.1 Network Security Overview

[Network Security > Overview]

This dialog displays the network security rules used in the device.

Parameter

Port/VLAN

Specifies if the device displays VLAN- and/or port-based rules.

Possible values:

- ▶ *All* (default setting)
The device displays the VLAN- and port-based rules specified by you.
- ▶ *Port: <Port Number>*
The device displays port-based rules for a specific port. This selection is available, when you specified one or more rules for this port.
- ▶ *VLAN: <VLAN ID>*
The device displays VLAN-based rules for a specific VLAN. This selection is available, when you specified one or more rules for this VLAN.

ACL

Displays the *ACL* rules in the overview.

You edit *ACL* rules in the *Network Security > ACL* dialog.

All

Marks the adjacent checkboxes. The device displays the related rules in the overview.

None

Unmarks the adjacent checkboxes. The device does not display any rules in the overview.

Buttons

You find the description of the standard buttons in section [“Buttons” on page 17](#).

4.2 Port Security

[Network Security > Port Security]


The device lets you transmit only data packets from desired senders on one port. When this function is enabled, the device checks the VLAN ID and MAC address or the VLAN ID and IP address of the sender before it transmits a data packet. The device discards data packets from other senders and logs this event.

The device also offers the function to check the IP address of the sender before it transmits a data packet.

Note: If in the *Mode* frame the *IP* radio button is selected, the *Port Security* function indirectly operates on Layer 2. When you set up an allowed IP address, the device retrieves the MAC address currently associated with the IP address. The device uses an ARP request and internally saves the associated MAC address. The prerequisite for specifying an allowed IP address is that the connected device is reachable and responds to ARP requests.

If a connected device sends data packets with an allowed IP address, but with a MAC address other than the associated MAC address, then the device discards the related data packets. If you replace the connected device and use the same IP address as before, then respecify the IP address as allowed. After this step, the device uses the new associated MAC address.

If the *Auto-Disable* function is activated, the device disables the port. This restriction makes MAC Spoofing attacks more difficult. The *Auto-Disable* function enables the relevant port again automatically when the parameters are no longer being exceeded.

In this dialog a *Wizard* window helps you to connect the ports with one or more desired sources. In the device, these addresses are known as *Static entries (x/y)*. To view the specified static addresses, highlight the relevant port and click the  button.

To simplify the setup process, the device lets you record the desired senders automatically. The device “learns” the senders 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 and transmits only the data packets of the senders already recorded. 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 1st data packet from unknown senders. Using this 1st data packet, the device checks if the upper limit has been reached. The device records the sender until the upper limit is reached. Afterwards, the device transmits data packets that it receives on the relevant port from this sender.

Operation

Operation

Enables/disables the *Port Security* function.

Possible values:

- ▶ *On*
The *Port Security* function is enabled.
The device checks the VLAN ID and the source MAC address before it transmits a data packet. The device transmits a received data packet only if the VLAN ID and the source MAC address of the data packet are allowed on the relevant port. For this setting to take effect, you also activate the checking of the source address on the relevant ports.
- ▶ *OFF* (default setting)
The *Port Security* function is disabled.
The device transmits every received data packet without checking the source address.

Note: If in the *Mode* frame the *MAC* radio button is selected, the device checks the source MAC address against the allowed source MAC addresses. If the *IP* radio button is selected, the device checks the source MAC address against the MAC addresses associated with the allowed source IP addresses.

Configuration

Auto-disable

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

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.
- ▶ *unmarked* (default setting)
The *Auto-Disable* function for *Port Security* is inactive.

Mode

Mode

Specifies if the *Port Security* function uses either the allowed MAC addresses or the allowed IP addresses to check a received packet.

Possible values:

- ▶ *MAC* (default setting)
The *Port Security* function uses the allowed source MAC addresses.
The device checks the VLAN ID and the source MAC address against the allowed source MAC addresses before it transmits a data packet.
- ▶ *IP*
The *Port Security* function uses the allowed source IP addresses.
The device checks the VLAN ID and the source MAC address against the MAC addresses associated with the allowed source IP addresses before it transmits a data packet

Table

Port

Displays the port number.

Active

Activates/deactivates the checking of the source address on the port.

Possible values:

- ▶ *marked*
The device checks every data packet received on the port and transmits it only if the source address of the data packet is allowed. Also enable the *Port Security* function in the *Operation* frame.
- ▶ *unmarked* (default setting)
The device transmits every data packet received on the port without checking the source address.

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

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

Auto-disable

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

Possible values:

- ▶ *marked* (default setting)
The *Auto-Disable* function is active on the port.
The prerequisite is that you mark the checkbox *Auto-disable* in the *Configuration* frame.
 - If the port registers source MAC addresses that are not allowed or more source MAC addresses than specified in the *Dynamic limit* column, then the device disables the port. The “Link status” LED for the port flashes 3× per period.
 - The *Diagnostics > Ports > Auto-Disable* dialog displays which ports are currently disabled due to the parameters being exceeded.
 - The *Auto-Disable* function reactivates the port automatically. For this you go to the *Diagnostics > Ports > Auto-Disable* dialog and specify a waiting period for the relevant port in the *Reset timer [s]* column.
- ▶ *unmarked*
The *Auto-Disable* function on the port is inactive.

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.
If the device discards data packets from a sender that is not allowed on the port, then the device sends an SNMP trap.
- ▶ *unmarked* (default setting)
The sending of SNMP traps is inactive.

The prerequisite for sending SNMP traps is that you enable the function in the *Diagnostics > Status Configuration > Alarms (Traps)* dialog and specify at least one trap destination.

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 sources (*Dynamic entries*). When the upper limit is reached, the device stops “learning” on this port.

Adjust the value to the number of expected sources.

If the port registers more senders than specified here, then the port disables the *Auto-Disable* function. 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
Deactivates the automatic registering of sources on this port.
- ▶ 1..600 (default setting: 600)

Static limit

Specifies the upper limit for the number of sources connected to the port (*Static entries (x/y)*). The *Wizard* window, *MAC addresses* dialog, helps you to connect the port with one or more desired sources.

Possible values:

- ▶ 0..64 (default setting: 64)

The value 0 helps prevent you from connecting a source with the port.

Dynamic entries

Displays the number of senders that the device has automatically determined.

See the *Wizard* window, *MAC addresses* dialog, *Dynamic entries* field.

If you select the *IP* value in the *Mode* frame, then the *Dynamic entries* column displays the value 0.

Static MAC entries

Displays the number of senders that are linked with the port.

See the *Wizard* window, *MAC addresses* dialog, *Static entries (x/y)* field.

Static IP entries

Displays the number of IP addresses allowed on the port.

See the *Wizard* window, *IP addresses* dialog, *Static entries (x/y)* field.

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.

Buttons

You find the description of the standard buttons in section “Buttons” on page 17.

[Port security (Wizard)]

The *Wizard* window helps you to connect the ports with one or more desired sources. After you specify the settings, click the *Finish* button.

Note: The device saves the sources connected with the port until you deactivate the checking of the source on the relevant port or in the *Operation* frame.

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

[Port security (Wizard) – Select port]

Port

Specifies the port that you assign to the sender in the next step.

[Port security (Wizard) – MAC addresses]

VLAN ID

Specifies the VLAN ID of the desired source.

Possible values:

▶ 1..4042

To transfer the VLAN ID and the MAC address to the *Static entries (x/y)* field, click the *Add* button.

MAC address

Specifies the MAC address of the desired source.

Possible values:

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

To transfer the VLAN ID and the MAC address to the *Static entries (x/y)* field, click the *Add* button.

Add

Transfers the values specified in the *VLAN ID* and *MAC address* fields to the *Static entries (x/y)* field.

Static entries (x/y)

Displays the VLAN ID and MAC address of desired senders connected to the port.

The device uses this field to display the number of senders connected to the port and the upper limit. You specify the upper limit for the number of entries in the table, *Static limit* field.

Note: You cannot assign a MAC address that you assign to this port to any other port.

Remove

Removes the entries highlighted in the *Static entries (x/y)* field.



Moves the entries highlighted in the *Dynamic entries* field to the *Static entries (x/y)* field.



Moves every entry from the *Dynamic entries* field to the *Static entries (x/y)* field.

When the *Dynamic entries* field contains more entries than are allowed in the *Static entries (x/y)* field, the device moves the foremost entries until the upper limit is reached.



Dynamic entries

Displays in ascending order the VLAN ID and MAC address of the senders automatically recorded on this port. The device transmits data packets from these senders when receiving the data packets on this port.

The prerequisites for the device to display MAC addresses are:

- The *Port Security* function is enabled. See the *Operation* frame.
- The device checks every data packet received on the port. The checkbox in the *Active* column is marked.

You specify the upper limit for the number of entries in the table, *Dynamic limit* field.

The  and  buttons allow you to transfer entries from this field into the *Static entries (x/y)* field. In this way, you connect the relevant senders with the port.

[Port security (Wizard) – IP addresses]

VLAN ID

Specifies the VLAN ID of the desired source.

Possible values:

▶ 1..4042

Note: Assign the VLAN ID of the management VLAN.

To transfer the *VLAN ID* and the *IP address* to the *Static entries (x/y)* field, click the *Add* button.

IP address

Specifies the IP address of the desired source.

Possible values:

▶ Valid IPv4 address

To transfer the *VLAN ID* and the *IP address* to the *Static entries (x/y)* field, click the *Add* button.

Add

Transfers the values specified in the *VLAN ID* and *IP address* fields to the *Static entries (x/y)* field.

Static entries (x/y)

Displays the VLAN ID and IP address of desired senders connected to the port.

The device uses this field to display the number of senders connected to the port and the upper limit. You can specify a maximum number of 10 IP addresses.

Remove

Removes the entries highlighted in the *Static entries (x/y)* field.

4.3 802.1X Port Authentication

[Network Security > 802.1X Port Authentication]

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 via the EAPoL (Extensible Authentication Protocol over LANs) authentication protocol.

The device supports the following methods to authenticate end devices:

- ▶ *radius*
A RADIUS server in the network authenticates the end devices.
- ▶ *ias*
The Integrated Authentication Server (IAS) implemented in the device authenticates the end devices. Compared to RADIUS, the IAS provides only basic functions.

The menu contains the following dialogs:

- ▶ *802.1X Global*
- ▶ *802.1X Port Configuration*
- ▶ *802.1X Port Clients*
- ▶ *802.1X EAPoL Port Statistics*
- ▶ *802.1X Port Authentication History*
- ▶ *802.1X Integrated Authentication Server*

4.3.1 802.1X Global

[Network Security > 802.1X Port Authentication > Global]

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

Operation

Operation

Enables/disables the *802.1X Port Authentication* function.

Possible values:

- ▶ *On*
The *802.1X Port Authentication* 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 Port Authentication* 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 Authentication > Port Configuration* dialog, *Assigned VLAN ID* row.

Dynamic VLAN creation

Activates/deactivates the automatic creation of the VLAN assigned by the RADIUS authentication server if the VLAN does not exist.

Possible values:

- ▶ *marked*
The automatic VLAN creation is active.
The device creates the VLAN if it does not exist.
- ▶ *unmarked* (default setting)
The automatic VLAN creation is inactive.
If the assigned VLAN does not exist, then the port remains assigned to the original VLAN.

Monitor mode

Activates/deactivates the monitor mode.

Possible values:

- ▶ `marked`
The monitor mode is active.
The device monitors the authentication and helps with diagnosing detected errors. If an end device has not logged in successfully, then the device gives the end device access to the network.
- ▶ `unmarked` (default setting)
The monitor mode is inactive.

MAC authentication bypass format options

Group size

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

Possible values:

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

Group separator

Specifies the character which separates the groups.

Possible values:

- ▶ `-`
dash
- ▶ `:`
colon
- ▶ `.`
dot

Upper or lower case

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

Possible values:

- ▶ `lower-case`
- ▶ `upper-case`

Password

Specifies the optional password for the clients which use the authentication bypass.

Possible values:

- ▶ Alphanumeric ASCII character string with 0..64 characters
After entering the field displays ***** (asterisk) instead of the password.
- ▶ `<empty>`
The device uses the user name of the client also as the password.

Information

Monitor mode clients

Displays to how many end devices the device gave network access even though they did not log in successfully.

The prerequisite is that you activate the *Monitor mode* function. See the *Configuration* frame.

Non monitor mode clients

Displays the number of end devices to which the device gave network access after successful login.

Policy 1

Displays the method that the device currently uses to authenticate the end devices using IEEE 802.1X.

You specify the method used in the *Device Security > Authentication List* dialog.

- To authenticate the end devices through a RADIUS server, you assign the `radius` policy to the `8021x` list.
- To authenticate the end devices through the Integrated Authentication Server (IAS) you assign the `ias` policy to the `8021x` list.

Buttons

You find the description of the standard buttons in section “Buttons” on page 17.

4.3.2 802.1X Port Configuration

[Network Security > 802.1X Port Authentication > Port Configuration]

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

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

Table

Port

Displays the port number.

Port initialization

Activates/deactivates the port initialization in order to activate the access control on the port or reset it to its initial state. Use this function only on ports in which the *Port control* column contains the value *auto* or *multiClient*.

Possible values:

- ▶ *marked*
The port initialization is active.
When the initialization is complete, the device changes the value to *unmarked* again.
- ▶ *unmarked* (default setting)
The port initialization is inactive.
The device keeps the current port status.

Port reauthentication

Activates/deactivates the one-time reauthentication request.

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

The device also lets you periodically request the end device to log in again. See the *Periodic reauthentication* column.

Possible values:

- ▶ *marked*
The one-time reauthentication request is active.
The device requests the end device to log in again. Afterwards, the device changes the value to *unmarked* again.
- ▶ *unmarked* (default setting)
The one-time reauthentication request is inactive.
The device keeps the end device logged in.

Authentication activity

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*

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.

Users (max.)

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

Possible values:

- ▶ *1..16* (default setting: 16)

Port control

Specifies how the device grants access to the network (*Port control mode*).

Possible values:

- ▶ *forceUnauthorized*
The device blocks the access to the network. You use this setting if an end device is connected to the port that does not receive access to the network.
- ▶ *auto*
The device grants access to the network if the end device logged in successfully. You use this setting if an end device is connected to the port that logs in at the authenticator.

Note: If other end devices are connected through the same port, then they get access to the network without additional authentication.

- ▶ *forceAuthorized* (default setting)
When end devices do not support IEEE 802.1X, the device grants access to the network. You use this setting if an end device is connected to the port that receives access to the network without logging in.
- ▶ *multiClient*
The device grants access to the network if the end device logs in successfully.
If the end device does not send any EAPOL data packets, then the device grants or denies access to the network individually depending on the MAC address of the end device. See the *MAC authorized bypass* column.
You use this setting if multiple end devices are connected to the port or if the *MAC authorized bypass* function is required.

Quiet period [s]

Specifies the time period in seconds in which the authenticator does not accept any more logins from the end device after an unsuccessful login attempt (*Quiet period [s]*).

Possible values:

▶ 0..65535 (default setting: 60)

Transmit period [s]

Specifies the period in seconds after which the authenticator requests the end device to log in again. After this waiting period, the device sends an EAP request/identity data packet to the end device.

Possible values:

▶ 1..65535 (default setting: 30)

Supplicant timeout period [s]

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

Possible values:

▶ 1..65535 (default setting: 30)

Server timeout [s]

Specifies the period in seconds for which the authenticator waits for the response from the authentication server (RADIUS or IAS).

Possible values:

▶ 1..65535 (default setting: 30)

Requests (max.)

Specifies how many times the authenticator requests the end device to log in until the time specified in the *Supplicant timeout period [s]* column has elapsed. The device sends an EAP request/identity data packet to the end device as often as specified here.

Possible values:

▶ 0..10 (default setting: 2)

Assigned VLAN ID

Displays the ID of the VLAN that the authenticator assigned to the port. This value applies only on ports in which the *Port control* column contains the value *auto*.

Possible values:

▶ 0..4042 (default setting: 0)

You find the VLAN ID that the authenticator assigned to the ports in the *Network Security > 802.1X Port Authentication > Port Clients* dialog.

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

Assignment reason

Displays the cause for the assignment of the VLAN ID. This value applies only on ports in which the *Port control* column contains the value *auto*.

Possible values:

- ▶ *notAssigned* (default setting)
- ▶ *radius*
- ▶ *guestVlan*
- ▶ *unauthenticatedVlan*

You find the VLAN ID that the authenticator assigned to the ports for a supplicant in the *Network Security > 802.1X Port Authentication > Port Clients* dialog.

Reauthentication period [s]

Specifies the period in seconds after which the authenticator periodically requests the end device to log in again.

Possible values:

- ▶ *1..65535* (default setting: *3600*)

Periodic reauthentication

Activates/deactivates periodic reauthentication requests.

Possible values:

- ▶ *marked*
The periodic reauthentication requests are active.
The device periodically requests the end device to log in again. You specify this time period in the *Reauthentication period [s]* column.
If the authenticator assigned the ID of a Voice VLAN, Unauthenticated VLAN or Guest VLAN to the end device, then this setting becomes ineffective.
- ▶ *unmarked* (default setting)
The periodic reauthentication requests are inactive.
The device keeps the end device logged in.

Guest VLAN ID

Specifies the ID of the VLAN that the authenticator assigns to the port if the end device does not log in during the time period specified in the *Guest VLAN period* column. This value applies only on ports in which the *Port control* column contains the value *auto* or *multiClient*.

This function lets you grant end devices, without IEEE 802.1X support, access to selected services in the network.

Possible values:

- ▶ *0* (default setting)
The authenticator does not assign a Guest VLAN to the port.
When you enable the MAC-based authentication in the *MAC authorized bypass* column, the device automatically sets the value to *0*.
- ▶ *1..4042*

Note: The *MAC authorized bypass* function and the *Guest VLAN ID* function cannot be in use simultaneously.

Guest VLAN period

Specifies 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.

Possible values:

- ▶ 1..300 (default setting: 90)

Unauthenticated VLAN ID

Specifies the ID of the VLAN that the authenticator assigns to the port if the end device does not log in successfully. This value applies only on ports in which the *Port control* column contains the value *auto*.

This function lets you grant end devices without valid login data access to selected services in the network.

Possible values:

- ▶ 0..4042 (default setting: 0)

The effect of the value 0 is that the authenticator does not assign a Unauthenticated VLAN to the port.

Note: Assign to the port a VLAN set up statically in the device.

MAC authorized bypass

Activates/deactivates the MAC-based authentication.

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

Possible values:

- ▶ *marked*
The MAC-based authentication is active.
The device sends the MAC address of the end device to the RADIUS authentication server. The device assigns the supplicant by its MAC address to the corresponding VLAN as if the authentication was performed through IEEE 802.1X directly.
- ▶ *unmarked* (default setting)
The MAC-based authentication is inactive.

Buttons

You find the description of the standard buttons in section [“Buttons” on page 17](#).

4.3.3 802.1X Port Clients

[Network Security > 802.1X Port Authentication > Port Clients]

This dialog displays information on the connected end devices.

Table

Port

Displays the port number.

User name

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

MAC address

Displays the MAC address of the end device.

Assigned VLAN ID

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

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

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 Authentication > Port Configuration* dialog, *Port control* column the value *auto* or *multiClient* is specified.

The authentication server assigns the timeout period to the device through RADIUS. The value 0 means that the authentication server has not assigned a timeout.

Termination action

Displays the action performed by the device when the login has elapsed.

Possible values:

- ▶ *default*
- ▶ *reauthenticate*

Buttons

You find the description of the standard buttons in section [“Buttons” on page 17](#).

4.3.4 802.1X EAPOL Port Statistics

[Network Security > 802.1X Port Authentication > Statistics]

This dialog displays which EAPOL data packets the end device has sent and received for the authentication of the end devices.

Table

Port

Displays the port number.

Received packets

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

Transmitted packets

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

Start packets

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

Logoff packets

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

Response/ID packets

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

Response packets

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

Request/ID packets

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

Request packets

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

Invalid packets

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

Received error packets

Displays the number of EAPOL data packets with an invalid packet body length field that the device received on the port.

Packet version

Displays the protocol version number of the EAPOL data packet that the device last received on the port.

Source of last received packet

Displays the sender MAC address of the EAPOL data packet that the device last received on the port.

The value `00:00:00:00:00:00` means that the port has not received any EAPOL data packets yet.

Buttons

You find the description of the standard buttons in section [“Buttons” on page 17](#).

4.3.5 802.1X Port Authentication History

[Network Security > 802.1X Port Authentication > 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

Port

Displays the port number.

Authentication time stamp

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

Result age

Displays since when this entry has been entered in the table.

MAC address

Displays the MAC address of the end device.

VLAN ID

Displays the ID of the VLAN that was assigned to the end device before the login.

Authentication status

Displays the status of the authentication on the port.

Possible values:

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

Access status

Displays if the device grants the end device access to the network.

Possible values:

- ▶ *granted*
The device grants the end device access to the network.
- ▶ *denied*
The device denies the end device access to the network.

Assigned VLAN ID

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

Assignment type

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

Possible values:

- ▶ `default`
- ▶ `radius`
- ▶ `unauthenticatedVlan`
- ▶ `guestVlan`
- ▶ `monitorVlan`
- ▶ `notAssigned`

Assignment reason

Displays the reason for the assignment of the VLAN ID and the VLAN type.

802.1X Port Authentication History

Port

Simplifies the table and displays only the entries relating to the port selected here. This makes it easier for you to record the table and sort it as you desire.

Possible values:

- ▶ `all`
The table displays the entries for every port.
- ▶ `<Port number>`
The table displays the entries that apply to the port selected here.

Buttons

You find the description of the standard buttons in section [“Buttons” on page 17](#).

4.3.6 802.1X Integrated Authentication Server

[Network Security > 802.1X Port Authentication > Integrated Authentication Server]

The Integrated Authentication Server (IAS) lets you authenticate end devices using IEEE 802.1X. Compared to RADIUS, the IAS has a very limited range of functions. The authentication is based only on the user name and the password.


In this dialog you manage the login data of the end devices. The device lets you set up to 100 sets of login data.

To authenticate the end devices through the Integrated Authentication Server you assign in the [Device Security > Authentication List](#) dialog the `ias` policy to the 8021x list.

Table

User name

Displays the user name of the end device.

To create a new user, 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 through IEEE 802.1X using this login data.
- ▶ `unmarked` (default setting)
The login data is inactive.

Buttons

You find the description of the standard buttons in section [“Buttons” on page 17](#).

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 enables you to 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 users' login data to the primary authentication server. The authentication server decides if the login data is valid and transfers the user's authorizations to the device.

The device assigns the Service Type transferred in the response of a RADIUS server as follows to a user 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

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).

Buttons

You find the description of the standard buttons in section “Buttons” on page 17.

Reset

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

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

Index

Displays the index number to which the table entry relates.

Name

Displays the name of the server.

To change the value, click the relevant field.

Possible values:

- ▶ Alphanumeric ASCII character string with 1..32 characters (default setting: `Default-RADIUS-Server`)

Address

Specifies the IP address of the server.

Possible values:

- ▶ Valid IPv4 address

Destination UDP port

Specifies the number of the UDP port on which the server receives requests.

Possible values:

- ▶ `0..65535` (default setting: `1812`)
Exception: Port `2222` is reserved for internal functions.

Secret

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

Possible values:

- ▶ Alphanumeric ASCII character string with 1..64 characters

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

Primary server

Specifies the authentication server as primary or secondary.

Possible values:

- ▶ **marked**
The server is specified as the primary authentication server. The device sends the login data for authenticating the users to this authentication server.
When you activate multiple servers, the device specifies the last server activated as the primary authentication server.
- ▶ **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 rows *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.

Buttons

You find the description of the standard buttons in section “Buttons” on page 17.



Opens the **Create** window to add a new entry to the table.

- ▶ In the **Index** field, you specify the index number.
- ▶ In the **Address** field, you specify the IP address of the 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 you activate in the *Network Security > RADIUS > Global* menu the *Accounting* function.

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

Index

Displays the index number to which the table entry relates.

Possible values:

▶ 1..8

Name

Displays the name of the server.

To change the value, click the relevant field.

Possible values:

▶ Alphanumeric ASCII character string with 1..32 characters
(default setting: *Default-RADIUS-Server*)

Address

Specifies the IP address of the server.

Possible values:

▶ Valid IPv4 address

Destination UDP port

Specifies the number of the UDP port on which the server receives requests.

Possible values:

▶ 0..65535 (default setting: 1813)
Exception: Port 2222 is reserved for internal functions.

Secret

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

Possible values:

▶ Alphanumeric ASCII character string with 1..16 characters

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

Active

Activates/deactivates the connection to the server.

Possible values:

- ▶ **marked** (default setting)
The connection is active. The device sends traffic data to this server if the preconditions named above are fulfilled.
- ▶ **unmarked**
The connection is inactive. The device does not send any traffic data to this server.

Buttons

You find the description of the standard buttons in section [“Buttons” on page 17](#).



Opens the **Create** window to add a new entry to the table.

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

To delete the statistic, click in the *Network Security > RADIUS > Global* dialog the  button and then the *Reset* item.

Table

Name

Displays the name of the server.

Address

Displays the IP address of the server.

Round trip time

Displays the time interval in hundredths of a second between the last response received from the server (Access Reply/Access Challenge) and the corresponding data packet sent (Access Request).

Access requests

Displays the number of access data packets that the device sent to the server. This value does not take repetitions into account.

Retransmitted access-request packets

Displays the number of access data packets that the device retransmitted to the server.

Access accepts

Displays the number of access accept data packets that the device received from the server.

Access rejects

Displays the number of access reject data packets that the device received from the server.

Access challenges

Displays the number of access challenge data packets that the device received from the server.

Malformed access responses

Displays the number of malformed access response data packets that the device received from the server (including data packets with an invalid length).

Bad authenticators

Displays the number of access response data packets with an invalid authenticator that the device received from the server.

Pending requests

Displays the number of access request data packets that the device sent to the server to which it has not yet received a response from the server.

Timeouts

Displays how many times no response to the server was received before the specified waiting time elapsed.

Unknown types

Displays the number data packets with an unknown data type that the device received from the server on the authentication port.

Packets dropped

Displays the number of data packets that the device received from the server on the authentication port and then discarded them.

Buttons

You find the description of the standard buttons in section [“Buttons” on page 17](#).

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 row.

To delete the statistic, click in the *Network Security > RADIUS > Global* dialog the  button and then the *Reset* item.

Table

Name

Displays the name of the server.

Address

Displays the IP address of the server.

Round trip time

Displays the time interval in hundredths of a second between the last response received from the server (Accounting Response) and the corresponding data packet sent (Accounting Request).

Accounting-request packets

Displays the number of accounting request data packets that the device sent to the server. This value does not take repetitions into account.

Retransmitted accounting-request packets

Displays the number of accounting request data packets that the device retransmitted to the server.

Received packets

Displays the number of accounting response data packets that the device received from the server.

Malformed packets

Displays the number of malformed accounting response data packets that the device received from the server (including data packets with an invalid length).

Bad authenticators

Displays the number of accounting response data packets with an invalid authenticator that the device received from the server.

Pending requests

Displays the number of accounting request data packets that the device sent to the server to which it has not yet received a response from the server.

Timeouts

Displays how many times no response to the server was received before the specified waiting time elapsed.

Unknown types

Displays the number 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.

Buttons

You find the description of the standard buttons in section [“Buttons” on page 17](#).

4.5 DoS

[Network Security > DoS]

Denial of Service (DoS) is a cyber-attack that aims to bring down specific services or devices. In this dialog you can set up several filters to help protect the device itself and other devices in the network from DoS attacks.

The menu contains the following dialogs:

▶ [DoS Global](#)

4.5.1 DoS Global

[Network Security > DoS > Global]

In this dialog you specify the DoS settings for the TCP/UDP, IP and ICMP protocols.

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.

IP

This frame lets you activate or deactivate the Land Attack filter. With the land attack method, the attacking station sends data packets whose source and destination addresses are identical to those of the recipient. When you activate this filter, the device detects data packets with identical source and destination addresses and discards these data packets.

Land Attack filter

Activates/deactivates the Land Attack filter.

The Land Attack filter detects incoming IP data packets whose source and destination IP address are identical and discards them.

Possible values:

- ▶ `marked`
The filter is active.
- ▶ `unmarked` (default setting)
The filter is inactive.

ICMP

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

- ▶ Fragmented data packets
- ▶ ICMP packets from a specific size upwards
- ▶ Broadcast pings

Filter fragmented packets

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.

Filter by packet size

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 *Filter by packet size* checkbox if you want the device to discard incoming data packets whose payload size exceeds the maximum allowed size for ICMP packets.

Possible values:

- ▶ 0..1472 (default setting: 512)

Drop broadcast ping

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

Possible values:

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

Information

Packets dropped

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

Buttons

You find the description of the standard buttons in section [“Buttons” on page 17](#).

4.6 DHCP Snooping

[Network Security > DHCP Snooping]

DHCP Snooping is a function that supports the network security. DHCP Snooping monitors DHCP packets between the DHCP client and the DHCP server and acts like a firewall between the unsecured hosts and the secured DHCP servers.

In this dialog you configure and monitor the following device properties:

- ▶ Validate DHCP packets from untrusted sources and filter out invalid packets.
- ▶ Limit DHCP data traffic from trusted and untrusted sources.
- ▶ Set up and update the DHCP Snooping binding database. This database contains the MAC address, IP address, VLAN and port of DHCP clients at untrusted ports.
- ▶ Validate follow-up requests from untrusted hosts on the basis of the DHCP Snooping binding database.

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

The menu contains the following dialogs:

- ▶ DHCP Snooping Global
- ▶ DHCP Snooping Configuration
- ▶ DHCP Snooping Statistics
- ▶ DHCP Snooping Bindings

4.6.1 DHCP Snooping Global

[Network Security > DHCP Snooping > Global]

This dialog lets you configure the global DHCP Snooping parameters for your device:

- ▶ Activate/deactivate *DHCP Snooping* globally.
- ▶ Activate/deactivate *Auto-Disable* globally.
- ▶ Enable/disable the checking of the source MAC address.
- ▶ Configure the name, storage location and storing interval for the binding database.

Operation

Operation

Enables/disables the DHCP Snooping function globally.

Possible values:

- ▶ *On*
- ▶ *Off* (default setting)

Configuration

Verify MAC

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

Possible values:

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

Auto-disable

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

Possible values:

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

Binding database

Remote file name

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

Note:

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

Remote IP address

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

Possible values:

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

Store interval [s]

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

Possible values:

- ▶ `15..86400` (default setting: 300)

Buttons

You find the description of the standard buttons in section [“Buttons” on page 17](#).

4.6.2 DHCP Snooping Configuration

[Network Security > DHCP Snooping > Configuration]

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

The dialog contains the following tabs:

- ▶ [Port]
- ▶ [VLAN ID]

[Port]

In this tab you configure the *DHCP Snooping* function for individual ports.

- ▶ Configure a port as trusted/untrusted.
- ▶ Activate/deactivate the logging of invalid packets for individual ports.
- ▶ Limit the number of DHCP packets.
- ▶ Deactivate a port automatically if the DHCP data traffic exceeds the specified limit.

Table

Port

Displays the port number.

Trust

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

When this function is active, the port is configured as trusted. Typically, you have connected the trusted port to a DHCP server.

When this function is inactive, the port is configured as untrusted.

Possible values:

- ▶ *marked*
The port is specified as trusted. DHCP Snooping forwards permissible client packets through trusted ports.
- ▶ *unmarked* (default setting)
The port is configured as untrusted. On untrusted ports, the device compares the receiver port with the client port in the binding database.

Log

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

Possible values:

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

Rate limit

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

Possible values:

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

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

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

Burst interval

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

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

Possible values:

- ▶ `1..15` (default setting: 1)

Auto-disable

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

Possible values:

- ▶ `marked` (default setting)
The *Auto-Disable* function is active on the port.
The prerequisite is that in the *Network Security > DHCP Snooping > Global* dialog the *Auto-disable* checkbox in the *Configuration* frame is marked.
 - If the port receives more DHCP packets than specified in the *Rate limit* field in the time specified in the *Burst interval* column, then the device disables the port. The “Link status” LED for the port flashes 3× per period.
 - The *Diagnostics > Ports > Auto-Disable* dialog displays which ports are currently disabled due to the parameters being exceeded.
 - The *Auto-Disable* function reactivates the port automatically. For this you go to the *Diagnostics > Ports > Auto-Disable* dialog and specify a waiting period for the relevant port in the *Reset timer [s]* column.
- ▶ `unmarked`
The *Auto-Disable* function on the port is inactive.

Buttons

You find the description of the standard buttons in section “Buttons” on page 17.

[VLAN ID]

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

Table

VLAN ID

Displays the VLAN ID to which the table entry relates.

Active

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

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

Possible values:

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

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

Buttons

You find the description of the standard buttons in section “Buttons” on page 17.

4.6.3 DHCP Snooping Statistics

[Network Security > DHCP Snooping > Statistics]

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

The device logs the following:

- ▶ Errors detected when validating the MAC address of the DHCP client
- ▶ DHCP client messages with a detected incorrect port
- ▶ DHCP server messages to untrusted ports

Table

Port

Displays the port number.

MAC verify failures

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

Invalid client messages

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

Invalid server messages

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

Buttons

You find the description of the standard buttons in section [“Buttons” on page 17](#).

Reset

Resets the entire table.

4.6.4 DHCP Snooping Bindings

[Network Security > DHCP Snooping > Bindings]

DHCP Snooping uses DHCP messages to set up and update the binding database.

- ▶ Static bindings
The device lets you enter up to 256 static DHCP Snooping bindings in the database.
- ▶ Dynamic bindings
The dynamic binding database contains data for clients only on untrusted ports.

This menu lets you specify the settings for static and dynamic bindings.

- ▶ Set up new static bindings and set them to active/inactive.
- ▶ Display, activate/deactivate or delete static bindings that have been set up.

Table

MAC address

Specifies the MAC address in the table entry that you bind to a *IP address* and *VLAN ID*.

Possible values:

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

IP address

Specifies the IP address for the static DHCP Snooping binding.

Possible values:

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

VLAN ID

Specifies the ID of the VLAN to which the table entry applies.

Possible values:

- ▶ `<ID of the VLANs that are set up>`

Port

Specifies the port for the static DHCP Snooping binding.

Possible values:

- ▶ Available ports

Remaining binding time

Displays the remaining time for the dynamic DHCP Snooping binding.

Active

Activates/deactivates the specified static DHCP Snooping binding.

Possible values:

- ▶ `marked`
The static DHCP Snooping binding is active.
- ▶ `unmarked` (default setting)
The static DHCP Snooping binding is inactive.

Buttons

You find the description of the standard buttons in section “Buttons” on page 17.



Opens the *Create* window to add a new entry to the table.

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



Removes the highlighted table entry.

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

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

4.7 IP Source Guard

[Network Security > IP Source Guard]

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

IPSG and DHCP Snooping

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

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

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

IPSG and port security

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

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

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

Note: In order for the device to check the IP address and the MAC address of the data packets received on the port, enable the *Verify MAC* function.

In order for the device to check the VLAN ID and the MAC address of the source before forwarding the data packet, additionally enable the *Port Security* function. See the *Network Security > Port Security* dialog.

The menu contains the following dialogs:

- ▶ *IP Source Guard Port*
- ▶ *IP Source Guard Bindings*

4.7.1 IP Source Guard Port

[Network Security > IP Source Guard > Port]

This dialog lets you display and configure the following device properties for each port:

- ▶ Include/exclude source MAC addresses for the filtering.
- ▶ Activate/deactivate the *IP Source Guard* function.

Table

Port

Displays the port number.

Verify MAC

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

Possible values:

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

Active

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

Possible values:

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

Buttons

You find the description of the standard buttons in section “Buttons” on page 17.

4.7.2 IP Source Guard Bindings

[Network Security > IP Source Guard > Bindings]

This dialog displays static and dynamic IP Source Guard bindings.

- ▶ The device learns dynamic bindings through DHCP Snooping. See the [Network Security > DHCP Snooping > Configuration](#) dialog.
- ▶ Static bindings are IP Source Guard bindings manually set up by the user. The dialog lets you edit static bindings.

Table

MAC address

Displays the MAC address of the binding.

IP address

Displays the IP address of the binding.

VLAN ID

Displays the VLAN ID of the binding.

Port

Displays the number of the port of the binding.

Hardware status

Displays the hardware status of the binding.

The device applies the binding to the hardware only if the settings are correct. Before the device applies the static IPSG binding to the hardware, it checks the following prerequisites:

- The *Active* checkbox is marked.
- The *IP Source Guard* function on the port is active, in the [Network Security > IP Source Guard > Port](#) dialog the *Active* checkbox is marked.

Possible values:

- ▶ *marked*
The binding is active, the device applies the binding to the hardware.
- ▶ *unmarked*
The binding is inactive.

Active

Activates/deactivates the specified static IPSPG binding between the specified MAC address and the specified IP address, for the specified VLAN on the specified port.

Possible values:

- ▶ `marked`
The static IPSPG binding is active.
- ▶ `unmarked` (default setting)
The static IPSPG binding is inactive.

Note: To make the static binding effective, activate the *IP Source Guard* function on the corresponding port. In the *Network Security > IP Source Guard > Port* dialog, mark the *Active* checkbox.

Buttons

You find the description of the standard buttons in section “Buttons” on page 17.



Opens the *Create* window to add a new entry to the table.

- ▶ In the *MAC address* field, you specify the MAC address for the static binding.
- ▶ In the *IP address* field, you specify the IP address for the static binding.
- ▶ In the *VLAN ID* field, you specify the VLAN ID.
- ▶ In the *Port* field, you specify the ID of the VLAN.



Removes the highlighted table entry.

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

4.8 Dynamic ARP Inspection

[Network Security > Dynamic ARP Inspection]

Dynamic ARP Inspection is a function that supports the network security. This function analyzes ARP packets, logs them, and discards invalid and hostile ARP packets.

The *Dynamic ARP Inspection* function helps prevent a range of man-in-the-middle attacks. With this kind of attack, a hostile station listens in on the data traffic from other subscribers by encroaching on the ARP cache of its unsuspecting neighbors. The hostile station sends ARP requests and ARP responses and enters the IP address of another subscriber for its own MAC address in the IP-to-MAC address relationship (binding).

Using the following measures, the *Dynamic ARP Inspection* function helps ensure that the device only forwards valid ARP requests and ARP responses.

- ▶ Listening in on ARP requests and ARP responses on untrusted ports.
- ▶ Verifying that the determined packets have a valid IP to MAC address relationship (binding) before the device updates the local ARP cache and before the device forwards the packets to the related destination address.
- ▶ Discarding invalid ARP packets.

The device lets you specify up to 100 active ARP ACLs (access lists). You can activate up to 20 rules for each ARP ACL.

The menu contains the following dialogs:

- ▶ *Dynamic ARP Inspection Global*
- ▶ *Dynamic ARP Inspection Configuration*
- ▶ *Dynamic ARP Inspection ARP Rules*
- ▶ *Dynamic ARP Inspection Statistics*

4.8.1 Dynamic ARP Inspection Global

[Network Security > Dynamic ARP Inspection > Global]

Configuration

Verify source MAC

Activates/deactivates the source MAC address verification. The device executes the check in both ARP requests and ARP responses.

Possible values:

- ▶ `marked`
The source MAC address verification is active.
The device checks the source MAC address of the received ARP packets.
 - The device transmits ARP packets with a valid source MAC address to the related destination address and updates the local ARP cache.
 - The device discards ARP packets with an invalid source MAC address.
- ▶ `unmarked` (default setting)
The source MAC address verification is inactive.

Verify destination MAC

Activates/deactivates the destination MAC address verification. The device executes the check in ARP responses.

Possible values:

- ▶ `marked`
The destination MAC address verification is active.
The device checks the destination MAC address of the incoming ARP packets.
 - The device transmits ARP packets with a valid destination MAC address to the related destination address and updates the local ARP cache.
 - The device discards ARP packets with an invalid destination MAC address.
- ▶ `unmarked` (default setting)
The checking of the destination MAC address of the incoming ARP packets is inactive.

Verify IP address

Activates/deactivates the IP address verification.

In ARP requests, the device checks the source IP address. In ARP responses, the device checks the destination and source IP address.

The device designates the following IP addresses as invalid:

- `0.0.0.0`
- Broadcast addresses `255.255.255.255`
- Multicast addresses `224.0.0.0/4` (Class D)
- Class E addresses `240.0.0.0/4` (reserved for subsequent purposes)
- Loopback addresses in the range `127.0.0.0/8`.

Possible values:

- ▶ **marked**
The IP address verification is active.
The device checks the IP address of the incoming ARP packets. The device transmits ARP packets with a valid IP address to the related destination address and updates the local ARP cache. The device discards ARP packets with an invalid IP address.
- ▶ **unmarked** (default setting)
The IP address verification is inactive.

Auto-disable

Activates/deactivates the *Auto-Disable* function for *Dynamic ARP Inspection*.

Possible values:

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

Buttons

You find the description of the standard buttons in section “Buttons” on page 17.

4.8.2 Dynamic ARP Inspection Configuration

[Network Security > Dynamic ARP Inspection > Configuration]

The dialog contains the following tabs:

- ▶ [Port]
- ▶ [VLAN ID]

[Port]

Table

Port

Displays the port number.

Trust

Activates/deactivates the monitoring of ARP packets on untrusted ports.

Possible values:

- ▶ `marked`
Monitoring is active.
The device monitors ARP packets on untrusted ports.
The device immediately forwards ARP packets on trusted ports.
- ▶ `unmarked` (default setting)
Monitoring is inactive.

Rate limit

Specifies the maximum number of ARP packets per interval on this port. If the rate of incoming ARP packets is currently exceeding the specified limit in a burst interval, then the device discards the additional incoming ARP packets. You specify the burst interval in the *Burst interval* column.

Optionally, the device also deactivates the port if you activate the auto-disable function. You enable/disable the *Auto-Disable* function in the *Auto-disable* column.

Possible values:

- ▶ `-1` (default setting)
Deactivates the limitation of the number of ARP packets per burst interval on this port.
- ▶ `0..300` packets per interval
Limits the maximum number of ARP packets per burst interval on this port.

Burst interval

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

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

Possible values:

- ▶ 1..15 (default setting: 1)

Auto-disable

Activates/deactivates the *Auto-Disable* function for the parameters that the *Dynamic ARP Inspection* function is monitoring on the port.

Possible values:

- ▶ *marked* (default setting)
The *Auto-Disable* function is active on the port.
The prerequisite is that in the *Network Security > Dynamic ARP Inspection > Global* dialog the *Auto-disable* checkbox in the *Configuration* frame is marked.
 - If the port receives more ARP packets than specified in the *Rate limit* field in the time specified in the *Burst interval* column, then the device disables the port. The “Link status” LED for the port flashes 3× per period.
 - The *Diagnostics > Ports > Auto-Disable* dialog displays which ports are currently disabled due to the parameters being exceeded.
 - The *Auto-Disable* function reactivates the port automatically. For this you go to the *Diagnostics > Ports > Auto-Disable* dialog and specify a waiting period for the relevant port in the *Reset timer [s]* column.
- ▶ *unmarked*
The *Auto-Disable* function on the port is inactive.

Buttons

You find the description of the standard buttons in section “Buttons” on page 17.

[VLAN ID]

Table

VLAN ID

Displays the VLAN ID to which the table entry relates.

Log

Activates/deactivates the logging of invalid ARP packets that the device determines in this VLAN. If the device detects an error when checking the IP, source MAC or destination MAC address, or when checking the IP-to-MAC address relationship (binding), then the device identifies an ARP packet as invalid.

Possible values:

- ▶ *marked*
The logging of invalid packets is active.
The device registers invalid ARP packets.
- ▶ *unmarked* (default setting)
The logging of invalid packets is inactive.

Binding check

Activates/deactivates the checking of incoming ARP packets that the device receives on untrusted ports and on VLANs for which the *Dynamic ARP Inspection* function is active. For these ARP packets the device checks the ARP ACL and the DHCP Snooping relationship (bindings).

Possible values:

- ▶ *marked* (default setting)
The binding check of ARP packets is active.
- ▶ *unmarked*
The binding check of ARP packets is inactive.

ACL strict

Activates/deactivates the strict checking of incoming ARP packets based on the ARP ACL rules specified.

Possible values:

- ▶ *marked*
The strict checking is active.
The device checks the incoming ARP packets based on the ARP ACL rule specified in the *ARP ACL* column.
- ▶ *unmarked* (default setting)
The strict checking is inactive.
The device checks the incoming ARP packets based on the ARP ACL rule specified in the *ARP ACL* column and subsequently on the entries in the DHCP Snooping database.

ARP ACL

Specifies the ARP ACL that the device uses.

Possible values:

- ▶ *<rule name>*
You create and edit the rules in the *Network Security > Dynamic ARP Inspection > ARP Rules* dialog.

Active

Activates/deactivates the *Dynamic ARP Inspection* function in this VLAN.

Possible values:

- ▶ *marked*
The *Dynamic ARP Inspection* function is active in this VLAN.
- ▶ *unmarked* (default setting)
The *Dynamic ARP Inspection* function is inactive in this VLAN.

Buttons

You find the description of the standard buttons in section “Buttons” on page 17.

4.8.3 Dynamic ARP Inspection ARP Rules

[Network Security > Dynamic ARP Inspection > ARP Rules]

This dialog lets you specify rules for checking and filtering ARP packets.

Table

Name

Displays the name of the ARP rule.

Source IP address

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

Possible values:

- ▶ Valid IPv4 address
The device applies the rule to IP data packets with the specified source address.

Source MAC address

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

Possible values:

- ▶ Valid MAC address
The device applies the rule to MAC data packets with the specified source address.

Active

Activates/deactivates the *ARP* rule.

Possible values:

- ▶ *marked* (default setting)
The rule is active.
- ▶ *unmarked*
The rule is inactive.

Buttons

You find the description of the standard buttons in section “Buttons” on page 17.



Opens the *Create* window to add a new entry to the table.

- ▶ In the *Name* field, you specify the name of the ARP rule.
- ▶ In the *Source IP address* field, you specify the source IP address of the ARP rule.
- ▶ In the *Source MAC address* field, you specify the source MAC address of the ARP rule.

4.8.4 Dynamic ARP Inspection Statistics

[Network Security > Dynamic ARP Inspection > Statistics]

This window displays the number of discarded and forwarded ARP packets in an overview.

Table

VLAN ID

Displays the VLAN ID to which the table entry relates.

Packets forwarded

Displays the number of ARP packets that the device forwards after checking them using the *Dynamic ARP Inspection* function.

Packets dropped

Displays the number of ARP packets that the device discards after checking them using the *Dynamic ARP Inspection* function.

DHCP drops

Displays the number of ARP packets that the device discards after checking the DHCP Snooping relationship (binding).

DHCP permits

Displays the number of ARP packets that the device forwards after checking the DHCP Snooping relationship (binding).

ACL drops

Displays the number of ARP packets that the device discards after checking them using the ARP ACL rules.

ACL permits

Displays the number of ARP packets that the device forwards after checking them using the ARP ACL rules.

Bad source MAC

Displays the number of ARP packets that the device discards after the *Dynamic ARP Inspection* function detected an error in the source MAC address.

Bad destination MAC

Displays the number of ARP packets that the device discards after the *Dynamic ARP Inspection* function detected an error in the destination MAC address.

Invalid IP address

Displays the number of ARP packets that the device discards after the *Dynamic ARP Inspection* function detected an error in the IP address.

Buttons

You find the description of the standard buttons in section “Buttons” on page 17.

Reset

Resets the entire table.

4.9 ACL

[Network Security > ACL]

In this menu, you specify the settings for the Access Control Lists (ACL). Access Control Lists contain rules which the device applies successively to the data stream on its ports or VLANs.

If a data packet complies with the criteria of one or more rules, then the device applies the action specified in the first rule that applies to the data stream. The device ignores the rules following.

Possible actions include:

- ▶ *permit*: The device transmits the data packet to a port or to a VLAN.
- ▶ *deny*: The device drops the data packet.

In the default setting, the device forwards every data packet. Once you assign an Access Control List to an interface or VLAN, there is changing this behavior. 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 meet any of the rules. If you want a different behavior, then add a "permit" 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*

4.9.1 ACL IPv4 Rule

[Network Security > ACL > IPv4 Rule]

In this dialog you specify the rules that the device applies to the IP data packets.

An Access Control List (group) contains one or more rules. The device applies the rules of an Access Control List successively, beginning with the rule with the 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

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.

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

Match every packet

Specifies to which IP data packets the device applies the rule.

Possible values:

- ▶ *marked* (default setting)
The device applies the rule to every IP data packet.
- ▶ *unmarked*
The device applies the rule to IP data packets depending on the value in the *Source IP address*, *Destination IP address*, and *Protocol* fields.

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 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 protocol type of the IP data packets to which the device applies the rule.

Possible values:

- ▶ `any` (default setting)
The device applies the rule to every IP data packet without considering the protocol type.
- ▶ `icmp`
- ▶ `igmp`
- ▶ `ip-in-ip`
- ▶ `tcp`
- ▶ `udp`
- ▶ `ip`

Source TCP/UDP port

Specifies the source port of the IP data packets to which the device applies the rule. The prerequisite is that you specify in the *Protocol* column the value `TCP` or `UDP`.

Possible values:

- ▶ `any` (default setting)
The device applies the rule to every IP data packet without considering the source port.
- ▶ `1..65535`
The device applies the rule only to IP data packets containing the specified source port.

Destination TCP/UDP port

Specifies the destination port of the IP data packets to which the device applies the rule. The prerequisite is that you specify in the *Protocol* column the value `TCP` or `UDP`.

Possible values:

- ▶ `any` (default setting)
The device applies the rule to every IP data packet without considering the destination port.
- ▶ `1..65535`
The device applies the rule only to IP data packets containing the specified destination port.

Action

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

Possible values:

- ▶ `permit` (default setting)
The device transmits 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 activated.
The prerequisite is that you assign the Access Control List in the *Network Security > ACL > Assignment* dialog 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 deactivated.

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

Buttons

You find the description of the standard buttons in section “Buttons” on page 17.



Opens the *Create* window to add a new entry to the table.

- ▶ In the *Group name* field, you specify the name of the Access Control List to which the rule belongs.
- ▶ 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 value first.

4.9.2 ACL MAC Rule

[Network Security > ACL > MAC Rule]

In this dialog you specify the rules that the device applies to the MAC data packets.

An Access Control List (group) contains one or more rules. The device applies the rules of an Access Control List successively, beginning with the rule with the lowest value in the *Index* column.

The device lets you filter for the source or destination MAC address of a data packet.

Table

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.

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

Match every packet

Specifies to which MAC data packets the device applies the rule.

Possible values:

- ▶ *marked* (default setting)
The device applies the rule to every MAC data packet.
- ▶ *unmarked*
The device applies the rule to MAC data packets depending on the value in the *Source MAC address* and *Destination MAC address* fields.

Source MAC address

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

Possible values:

- ▶ *?:?:?:?:?:?:?:?* (default setting)
The device applies the rule to MAC data packets with any source address.
- ▶ Valid MAC address
The device applies the rule to MAC data packets with the specified source address. You use the *?* character as a wild card.
Example *00:11:?:?:?:?:?:?*: The device applies the rule to MAC data packets whose source address begins with *00:11*.
- ▶ Valid MAC address/bit mask
The device applies the rule to MAC data packets with the specified source address. The bit mask lets you specify the address range with bit-level accuracy.
Example *00:11:22:33:44:54/FF:FF:FF:FF:FF:FC*: The device applies the rule to MAC data packets with a source address in the range from *00:11:22:33:44:54* to *...:57*.

Destination MAC address

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

Possible values:

- ▶ `?:?:?:?:?:?:?:?` (default setting)
The device applies the rule to MAC data packets with any destination address.
- ▶ Valid MAC address
The device applies the rule to MAC data packets with the specified destination address. You use the `?` character as a wild card.
Example `00:11:?:?:?:?:?:?:?`: The device applies the rule to MAC data packets whose destination address begins with `00:11`.
- ▶ Valid MAC address/bit mask
The device applies the rule to MAC data packets with the specified source address. The bit mask lets you specify the address range with bit-level accuracy.
Example `00:11:22:33:44:54/FF:FF:FF:FF:FF:FC`: The device applies the rule to MAC data packets with a destination address in the range from `00:11:22:33:44:54` to `...:57`.

Action

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

Possible values:

- ▶ `permit` (default setting)
The device transmits the MAC data packets.
- ▶ `deny`
The device discards the MAC data packets.

Log

Activates/deactivates the logging in the log file. See the [Diagnostics > Report > System Log](#) dialog.

Possible values:

- ▶ `marked`
Logging is activated.
The prerequisite is that you assign the Access Control List in the [Network Security > ACL > Assignment](#) dialog to a VLAN or port.
The device registers in the log file, in an interval of 30 s, how many times it applied the deny rule to MAC data packets.
- ▶ `unmarked` (default setting)
Logging is deactivated.

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

Buttons

You find the description of the standard buttons in section [“Buttons” on page 17](#).



Opens the *Create* window to add a new entry to the table.

- ▶ In the *Group name* field, you specify the name of the Access Control List to which the rule belongs.
- ▶ 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 value first.

4.9.3 ACL Assignment

[Network Security > ACL > Assignment]

This dialog lets you assign one or more Access Control Lists to the ports and VLANs of the device. By assigning a priority you specify the processing sequence, provided you assign one or more Access Control Lists to a port or VLAN.

The device applies rules successively, namely in the sequence specified by the rule index. You specify the priority of a group in the *Priority* column. The lower the number, the higher the priority. In this process, the device applies the rules with a high priority before the rules with a low priority.

The assignment of Access Control Lists to ports and VLANs results in the following different types of ACL:

- ▶ 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 entry 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

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.

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.

Possible values:

- ▶ 1..4294967295

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.

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.

Buttons

You find the description of the standard buttons in section “Buttons” on page 17.



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

- ▶ In the *Port/VLAN* field, you specify the port or the VLAN ID.
- ▶ In the *Priority* field, you specify the source MAC address of the ARP rule.
- ▶ In the *Direction* field, you specify the data packets to which the device applies the rule.
- ▶ In the *Group name* field, you specify which rule the device assigns to the port or VLAN.

5 Switching

The menu contains the following dialogs:

- ▶ Switching Global
- ▶ Rate Limiter
- ▶ Filter for MAC Addresses
- ▶ IGMP Snooping
- ▶ Time-Sensitive Networking
- ▶ MRP-IEEE
- ▶ GARP
- ▶ QoS/Priority
- ▶ VLAN
- ▶ L2-Redundancy

5.1 Switching Global

[Switching > Global]

This dialog lets you specify the following settings:

- ▶ Change the Aging time of the address table
- ▶ Enable the flow control in the device

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

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

- ▶ In full-duplex mode, the device sends a pause data packet.
- ▶ In half-duplex mode, the device simulates a collision.

Then the connected devices do not send any more data packets for as long as the signaling takes. On uplink ports, this can possibly cause undesired sending breaks in the higher-level network segment (“wandering backpressure”).

Configuration

MAC address

Displays the MAC address of the device.

Aging time [s]

Specifies the aging time in seconds.

Possible values:

- ▶ 10..500000 (default setting: 30)

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

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

Flow control

Activates/deactivates the flow control in the device.

Possible values:

- ▶ `marked`
The flow control is active in the device.
Additionally activate the flow control on the required ports. See the [Basic Settings > Port](#) dialog, [Configuration](#) tab, checkbox in the [Flow control](#) column.
- ▶ `unmarked` (default setting)
The flow control is inactive in the device.

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

Buttons

You find the description of the standard buttons in section [“Buttons” on page 17](#).

5.2 Rate Limiter

[Switching > Rate Limiter]

The device lets you limit the traffic on the ports in order to help provide stable operation even with a large traffic volume. If the traffic on a port exceeds the traffic value entered, then the device discards the excess traffic 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 traffic the port receives. If the traffic on this port exceeds the threshold value, then the device discards the excess traffic on this port.

Table

Port

Displays the port number.

Threshold unit

Specifies the unit for the threshold value:

Possible values:

- ▶ *percent* (default setting)
Specifies the threshold value as a percentage of the data rate of the port.
- ▶ *pps*
Specifies the threshold value in data packets per second.

Broadcast mode

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

Possible values:

- ▶ *marked*
- ▶ *unmarked* (default setting)

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

Broadcast threshold

Specifies the threshold value for received broadcasts on this port.

Possible values:

▶ `0..14880000` (default setting: 0)

The value 0 deactivates the rate limiter function on this port.

- If you select the value *percent* in the *Threshold unit* column, then enter a percentage value from 1 to 100.
- If you select the value *pps* in the *Threshold unit* column, then enter an absolute value for the data rate.

Known multicast mode

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

Possible values:

▶ `marked`

▶ `unmarked` (default setting)

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

Known multicast threshold

Specifies the threshold value for received multicasts on this port.

Possible values:

▶ `0..14880000` (default setting: 0)

The value 0 deactivates the rate limiter function on this port.

- If you select the value *percent* in the *Threshold unit* column, then enter a percentage value from 0 to 100.
- If you select the value *pps* in the *Threshold unit* column, then enter an absolute value for the data rate.

Unknown frame mode

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

Possible values:

▶ `marked`

▶ `unmarked` (default setting)

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

Unknown frame threshold

Specifies the threshold value for received unicasts with an unknown destination address on this port.

Possible values:

▶ 0..14880000 (default setting: 0)

The value 0 deactivates the rate limiter function on this port.

- If you select the value *percent* in the *Threshold unit*, then enter a percentage value from 0 to 100.
- If you select the value *pps* in the *Threshold unit* column, then enter an absolute value for the data rate.

Buttons

You find the description of the standard buttons in section “Buttons” on page 17.

[Egress]

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

Table

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.

Buttons

You find the description of the standard buttons in section “Buttons” on page 17.

5.3 Filter for MAC Addresses

[Switching > Filter for MAC Addresses]

This dialog lets you display and edit address filters for the address table. Address filters specify the way the data packets are forwarded in the device based on the destination MAC address.

Each row in the table represents one filter. The device automatically sets up the filters. The device lets you set up additional filters manually.

The device transmits the data packets as follows:

- ▶ When the table contains an entry for the destination address of a data packet, the device transmits the data packet from the receiving port to the port specified in the table entry.
- ▶ When there is no table entry for the destination address, the device transmits the data packet from the receiving port to every other port.

Table

To delete the learned MAC addresses from the address table, click in the [Basic Settings > Restart](#) dialog the [Reset MAC address table](#) button.

Address

Displays the destination MAC address to which the table entry applies.

VLAN ID

Displays the ID of the VLAN to which the table entry applies.

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

Status

Displays how the device has set up the address filter.

Possible values:

- ▶ *learned*
Address filter set up automatically by the device based on received data packets.
- ▶ *permanent*
Address filter set up manually. The address filter stays set up permanently.
- ▶ *IGMP*
Address filter automatically set up by IGMP Snooping.
- ▶ *mgmt*
MAC address of the device. The address filter is protected against changes.
- ▶ *MRP-MMRP*
Multicast address filter automatically set up by MMRP.
- ▶ *GMRP*
Multicast address filter automatically set up by GMRP.

<Port number>

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

Possible values:

- ▶ `-`
The port does not transmit any data packets to the destination address.
- ▶ `learned`
The port transmits data packets to the destination address. The device created the filter automatically based on received data packets.
- ▶ `IGMP learned`
The port transmits data packets to the destination address. The device created the filter automatically based on IGMP.
- ▶ `unicast static`
The port transmits data packets to the destination address. A user created the filter.
- ▶ `multicast static`
The port transmits data packets to the destination address. A user created the filter.

Buttons

You find the description of the standard buttons in section [“Buttons” on page 17](#).



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

- ▶ In the [Address](#) field, you specify the destination MAC address.
- ▶ In the [VLAN ID](#) field, you specify the ID of the VLAN.
- ▶ In the [Port](#) field, you specify the port.
 - Select one port if the destination MAC address is a unicast address.
 - Select one or more ports if the destination MAC address is a multicast address.
 - Select no port to create a discard filter. The device discards data packets with the destination MAC address specified in the table entry.

Reset MAC address table

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

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 transmits the Multicast data packets to every port.
- ▶ With the activated IGMP Snooping function, the device transmits the Multicast data packets only on ports to which Multicast receivers are connected. This reduces the network load. The device evaluates the IGMP data packets transmitted on Layer 3 and uses the information on Layer 2.

Activate the IGMP Snooping function not until the following conditions are fulfilled:

- ▶ There is a Multicast router in the network that creates IGMP queries (periodic queries).
- ▶ The devices participating in IGMP Snooping forward the IGMP queries.

The device links the IGMP reports with the entries in its address table. When a multicast receiver joins a multicast group, the device creates a table entry for this port in the [Switching > Filter for MAC Addresses](#) dialog. When the multicast receiver leaves the multicast group, the device removes the table entry.

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* protocol in the device and also configure it 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

Multicast control packets processed

Displays the number of Multicast control data packets processed.

This statistic encompasses the following packet types:

- IGMP Reports
- IGMP Queries version V1
- IGMP Queries version V2
- IGMP Queries version V3
- IGMP Queries with an incorrect version
- PIM or DVMRP packets

The device uses the Multicast control data packets to create the address table for transmitting the Multicast data packets.

Possible values:

- ▶ $0..2^{31}-1$

You use the *Reset IGMP snooping data* button in the *Basic Settings > Restart* dialog or the command `clear igmp-snooping` using the Command Line Interface to reset the IGMP Snooping entries, including the counter for the processed multicast control data packets.

Buttons

You find the description of the standard buttons in section “Buttons” on page 17.

Reset IGMP snooping counters

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

5.4.2 IGMP Snooping Configuration

[Switching > IGMP Snooping > Configuration]

This dialog lets you enable the *IGMP Snooping* function in the device and also configure it for each port and each VLAN.

The dialog contains the following tabs:

- ▶ [VLAN ID]
- ▶ [Port]

[VLAN ID]

In this tab you configure the *IGMP Snooping* function for every VLAN.

Table

VLAN ID

Displays the ID of the VLAN to which the table entry applies.

Active

Activates/deactivates the *IGMP Snooping* function for this VLAN.

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

Possible values:

- ▶ *marked*
IGMP Snooping is activated for this VLAN. The VLAN has joined the Multicast data stream.
- ▶ *unmarked* (default setting)
IGMP Snooping is deactivated for this VLAN. The VLAN has left the Multicast data stream.

Group membership interval

Specifies the time in seconds for which a VLAN from a dynamic Multicast group remains entered in the address table when the device does not receive any more report data packets from the VLAN.

Specify a value larger than the value in the *Max. response time* column.

Possible values:

- ▶ *2..3600* (default setting: *260*)

Max. response time

Specifies the time in seconds in which the members of a Multicast group respond to a query data packet. For their response, the members specify a random time within the response time. You thus help prevent the multicast group members from responding to the query at the same time.

Specify a value smaller than the value in the *Group membership interval* column.

Possible values:

- ▶ 1..25 (default setting: 10)

Fast leave admin mode

Activates/deactivates the Fast Leave function for this VLAN.

Possible values:

- ▶ *marked*
When the Fast Leave function is active and the device receives an IGMP Leave message from a multicast group, the device immediately removes the entry from its address table.
- ▶ *unmarked* (default setting)
When the Fast Leave function is inactive, the device first sends MAC-based queries to the members of the multicast group and removes an entry when a VLAN does not send any more report messages.

MRP expiration time

Multicast Router Present Expiration Time. Specifies the time in seconds for which the device waits for a query on this port that belongs to a VLAN. When the port does not receive a query data packet, the device removes the port from the list of ports with connected multicast routers.

You have the option of configuring this parameter only if the port belongs to an existing VLAN.

Possible values:

- ▶ 0
unlimited timeout - no expiration time
- ▶ 1..3600 (default setting: 260)

Buttons

You find the description of the standard buttons in section [“Buttons” on page 17](#).

[Port]

In this tab you configure the *IGMP Snooping* function for every port.

Table

Port

Displays the port number.

Active

Activates/deactivates the *IGMP Snooping* function for this port.

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

Possible values:

- ▶ `marked`
IGMP Snooping is active on this port. The device includes the port in the multicast data stream.
- ▶ `unmarked` (default setting)
IGMP Snooping is inactive on this port. The port left the multicast data stream.

Group membership interval

Specifies the time in seconds for which a port, from a dynamic multicast group, remains entered in the address table when the device does not receive any more report data packets from the port.

Possible values:

- ▶ `2..3600` (default setting: `260`)

Specify the value larger than the value in the *Max. response time* column.

Max. response time

Specifies the time in seconds in which the members of a Multicast group respond to a query data packet. For their response, the members specify a random time within the response time. You thus help prevent the multicast group members from responding to the query at the same time.

Possible values:

- ▶ `1..25` (default setting: `10`)

Specify a value lower than the value in the *Group membership interval* column.

MRP expiration time

Specifies the Multicast Router Present Expiration Time. The MRP expiration time is the time in seconds for which the device waits for a query packet on this port. When the port does not receive a query data packet, the device removes the port from the list of ports with connected multicast routers.

Possible values:

- ▶ `0`
unlimited timeout - no expiration time
- ▶ `1..3600` (default setting: `260`)

Fast leave admin mode

Activates/deactivates the Fast Leave function for this port.

Possible values:

- ▶ `marked`
When the Fast Leave function is active and the device receives an IGMP Leave message from a multicast group, the device immediately removes the entry from its address table.
- ▶ `unmarked` (default setting)
When the Fast Leave function is inactive, the device first sends MAC-based queries to the members of the multicast group and removes an entry when a port does not send any more report messages.

Static query port

Activates/deactivates the *Static query port* mode.

Possible values:

▶ *marked*

The *Static query port* mode is active.

The port is a static query port in the VLANs that are set up.

If you use the *Redundant Coupling Protocol* function and the device operates as slave, then do not activate the *Static query port* mode for the ports on the secondary ring/network.

▶ *unmarked* (default setting)

The *Static query port* mode is inactive.

The port is not a static query port. The device transmits IGMP report messages to the port only if it receives IGMP queries.

VLAN IDs

Displays the ID of the VLANs to which the table entry applies.

Buttons

You find the description of the standard buttons in section “Buttons” on page 17.

5.4.3 IGMP Snooping Enhancements

[Switching > IGMP Snooping > Snooping Enhancements]

This dialog lets you select a port for a VLAN ID and to configure the port.

Table

VLAN ID

Displays the ID of the VLAN to which the table entry applies.

<Port number>

Displays for every VLAN set up in the device if the relevant port is a query port. Additionally, the field displays if the device transmits every Multicast stream in the VLAN to this port.

Possible values:

- ▶ -
The port is not a query port in this VLAN.
- ▶ 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 configured query port.
- ▶ A= Automatic
The device detected the port as a query port. The prerequisite is that you configure 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 configured query ports.
To assign this value, perform the following steps:
 - Open the *Wizard* window.
 - In the *Configuration* dialog, 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 Schneider Electric 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.
 - In the *Configuration* dialog, mark the *Learn by LLDP* checkbox.
- ▶ F= Forward All (manual setting)
A user specified the port so that the device transmits every received Multicast stream in the VLAN to this port. Use this setting for diagnostics purposes, for example.
To assign this value, perform the following steps:
 - Open the *Wizard* window.
 - In the *Configuration* dialog, 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.

- ▶ *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.

Buttons

You find the description of the standard buttons in section “Buttons” on page 17.




Opens the *Wizard* window that helps you to select and configure the ports.

[Selection VLAN/Port (Wizard)]

In the *Selection VLAN/Port* dialog you assign a VLAN ID to port.

In the *Configuration* dialog you specify the settings for the port.

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

[Selection VLAN/Port (Wizard) – Selection VLAN/Port]

VLAN ID

Select the ID of the VLAN.

Possible values:

▶ 1..4042

Port

Select the port.

Possible values:

▶ <Port number>

[Selection VLAN/Port (Wizard) – Configuration]

VLAN ID

Displays the ID of the selected VLAN.

Port

Displays the number of the selected port.

Static

Specifies the port as a static query port in the VLANs that are set up. The device transmits IGMP report messages to the ports at which it receives IGMP queries. This lets you also transmit IGMP report messages to other selected ports (enable) or connected Schneider Electric devices (*Automatic*).

Learn by LLDP

Specifies the port as *Learn by LLDP*. Lets the device detect directly connected Schneider Electric devices using LLDP and learn the related ports as a query port.

Forward all

Specifies the port as *Forward all*. With the *Forward all* setting, the device transmits at this port every data packet with a Multicast address in the destination address field.

5.4.4 IGMP Snooping Querier

[Switching > IGMP Snooping > Querier]

The device lets you send a Multicast stream only to those ports to which a Multicast receiver is connected.

To determine which ports Multicast receivers are connected to, the device sends query data packets to the ports at a definable interval. When a Multicast receiver is connected, it joins the Multicast stream by responding to the device with a report data packet.

This dialog lets you configure the Snooping Querier settings globally and for the VLANs that are set up.

Operation

Operation

Enables/disables the IGMP Querier function globally in the device.

Possible values:

- ▶ *On*
- ▶ *OFF* (default setting)

Configuration

In this frame you specify the IGMP Snooping Querier settings for the general query data packets.

Protocol version

Specifies the IGMP version of the general query data packets.

Possible values:

- ▶ *1*
IGMP v1
- ▶ *2* (default setting)
IGMP v2
- ▶ *3*
IGMP v3

Query interval [s]

Specifies the time in seconds after which the device generates general query data packets itself when it has received query data packets from the Multicast router.

Possible values:

- ▶ 1..1800 (default setting: 60)

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 VLANs that are set up.

VLAN ID

Displays the ID of the VLAN to which the table entry applies.

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.

Address

Specifies the IP address that the device adds as the source address in generated general query data packets. You use the address of the multicast router.

Possible values:

- ▶ Valid IPv4 address (default setting: 0.0.0.0)

Protocol version

Displays the IGMP protocol version of the general query data packets.

Possible values:

- ▶ 1
IGMP v1
- ▶ 2
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.

Buttons

You find the description of the standard buttons in section [“Buttons” on page 17.](#)

5.4.5 IGMP Snooping Multicasts

[Switching > IGMP Snooping > Multicasts]

The device lets you specify how it transmits data packets with unknown Multicast addresses: Either the device discards these data packets, floods them to every port, or transmits them only to the ports that previously received query packets.

The device also lets you transmit the data packets with known Multicast addresses to the query ports.

Configuration

Unknown multicasts

Specifies how the device transmits the data packets with unknown Multicast addresses.

Possible values:

- ▶ *discard*
The device discards data packets with an unknown MAC/IP Multicast address.
- ▶ *flood* (default setting)
The device forwards data packets with an unknown MAC/IP Multicast address to every port.

Table

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

VLAN ID

Displays the ID of the VLAN to which the table entry applies.

Known multicasts

Specifies how the device transmits the data packets with known Multicast addresses.

Possible values:

- ▶ *send to query and registered ports*
The device forwards data packets with an unknown 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 an unknown MAC/IP Multicast address to registered ports.

Buttons

You find the description of the standard buttons in section [“Buttons” on page 17](#).

5.5 Time-Sensitive Networking

[Switching > TSN]

The menu contains the following dialogs:

- ▶ TSN Configuration
- ▶ TSN Gate Control List

5.5.1 TSN Configuration

[Switching > TSN > Configuration]

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

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

The feature helps to avoid latency and congestion loss for reserved data streams. The precise synchronization of cycles and gate states using IEEE1588 (PTP) makes congestion-free, low-latency communication possible. The prerequisite is that every device in the network supports IEEE 802.1 Qbv.

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

Operation

Operation

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

Possible values:

▶ *On*

The *TSN* function is globally enabled.

The device processes link local frames on the TSN-capable ports with the priority of traffic class 6. As a result, the link local frames compete with other data packets with the same or higher priority when forwarding. This affects the following frame types:

- RSTP
- LLDP
- IEEE 802.1AS
- PTP Peer Delay

▶ *Off* (default setting)

The *TSN* function is globally disabled.

As long as the *TSN* function is active on a port, the port uses the opened gates 0, 1, 2, 3, 4, 5, 6, 7. This setting is preset by the manufacturer.

Base time

Date
Time
[ns]

Specifies the time at which the cycle starts related to the UTC time.

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

Possible values:

- ▶ `MM/DD/YY`
Month/Day/Year
(depending on the language preferences of your web browser)
- ▶ `hh:mm:ss`
Hour:Minute:Second
- ▶ `0..999999999`
Specifies the offset of nanoseconds.

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

Configuration

Cycle time [ns]

Specifies the duration of a cycle in nanoseconds.

Possible values:

- ▶ `50000..10000000` (default setting: `1000000`)
50 μ s .. 10 ms

Table

Port

Displays the port number.

Active

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

Possible values:

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

Port state

Displays the status of the cycle on the port.

Possible values:

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

Time of last activation

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

This value relates to the PTP time.

Buttons

You find the description of the standard buttons in section “Buttons” on page 17.

5.5.2 TSN Gate Control List

[Switching > TSN > Gate Control List]

The menu contains the following dialogs:

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

5.5.2.1 TSN Configured Gate Control List

[Switching > TSN > Gate Control List > Configured]

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

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

The dialog contains the following tabs:

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

[<Port number>]

Configuration

Status

Displays the template assigned to the Gate Control List.

Possible values:

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

Template

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

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

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

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

Delete

Removes the template assigned to the Gate Control List. After that no more entries are assigned to the Gate Control List.

Table

Index

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

Gate states

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

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

Possible values:

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

Interval [ns]

Specifies the duration of the time slot in nanoseconds.

Possible values:

- ▶ 1000..10000000

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

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

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

Buttons

You find the description of the standard buttons in section [“Buttons”](#) on page 17.

5.5.2.2 TSN Current Gate Control List

[Switching > TSN > Gate Control List > Current]

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

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

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

The dialog contains the following tabs:

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

[<Port number>]

Table

Index

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

Gate states

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

Interval [ns]

Displays the duration of the time slot in nanoseconds.

Buttons

You find the description of the standard buttons in section “Buttons” on page 17.

5.6 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 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 traffic transversing a LAN. Defining resource requirements regulates the level of traffic, allowing the devices to determine the required resources and provides for dynamic maintenance of the allocated resources.

The menu contains the following dialogs:

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

5.6.1 MRP-IEEE Configuration

[Switching > MRP-IEEE > Configuration]

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

When you reconfigure the timers, maintain the following relationships:

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

Table

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)

Buttons

You find the description of the standard buttons in section [“Buttons” on page 17](#).

5.6.2 MRP-IEEE Multiple MAC Registration Protocol

[Switching > MRP-IEEE > MMRP]

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

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

The dialog contains the following tabs:

- ▶ [Configuration]
- ▶ [Service requirement]
- ▶ [Statistics]

[Configuration]

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

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

Operation

Operation

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

Possible values:

- ▶ *On*
The device is a normal participant in MMRP message exchanges.
- ▶ *Off* (default setting)
The device ignores MMRP messages.

Configuration

Periodic state machine

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

Possible values:

- ▶ *On*
With MMRP *Operation* enabled globally, the device transmits MMRP messages in one-second intervals, on MMRP participating ports.
- ▶ *Off* (default setting)
Disables the periodic state machine in the device.

Table

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.

Buttons

You find the description of the standard buttons in section [“Buttons” on page 17](#).

[Service requirement]

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

A port is setup only as *ForwardAll* or *Forbidden*.

Table

VLAN ID

Displays the ID of the VLAN.

<Port number>

Specifies the service requirement handling for the port.

Possible values:

- ▶ *FA*
Specifies the *ForwardAll* traffic setting on the port. The device forwards traffic destined to MMRP registered multicast MAC addresses on the VLAN. The device forwards traffic to ports which MMRP has dynamically setup or ports which the administrator has statically setup as *ForwardAll* ports.
- ▶ *F*
Specifies the *Forbidden* traffic setting on the port. The device blocks dynamic MMRP *ForwardAll* service requirements. With *ForwardAll* requests blocked on this port in this VLAN, the device blocks traffic 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.

Buttons

You find the description of the standard buttons in section [“Buttons” on page 17](#).

[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 traffic statistics for each port.

Information

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

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 last MAC address from which the port received MMRPPDUs.

Buttons

You find the description of the standard buttons in section [“Buttons”](#) on page 17.

Reset

Resets the port statistics counters and the values in the [Last received MAC address](#) column.

5.6.3 MRP-IEEE Multiple VLAN Registration Protocol

[Switching > MRP-IEEE > MVRP]

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

The dialog contains the following tabs:

- ▶ [Configuration]
- ▶ [Statistics]

[Configuration]

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

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

Operation

Operation

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

Possible values:

- ▶ *On*
Normal Participant. The Applicant state machine participates in MMRP message exchanges.
- ▶ *OFF* (default setting)
Non-Participant. The Applicant state machine ignores MMRP messages.

Configuration

Periodic state machine

Enables/disables the periodic state machine in the device.

Possible values:

- ▶ *On*
The periodic state machine is enabled.
With MVRP *Operation* enabled globally, the device transmits MVRP periodic events in 1 second intervals, on MVRP participating ports.
- ▶ *Off* (default setting)
The periodic state machine is disabled.
Disables the periodic state machine in the device.

Table

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 create a dynamic VLAN for this entry.
- ▶ *unmarked* (default setting)
Disables the *Restricted VLAN registration* function on this port.

Buttons

You find the description of the standard buttons in section [“Buttons” on page 17](#).

[Statistics]

Devices on a LAN exchange Multiple VLAN Registration Protocol Data Units (MVRPDU) to maintain statuses of VLANs on active ports. This tab lets you monitor the MVRP traffic.

Information

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

Port

Displays the port number.

Transmitted MVRP PDU

Displays the number of MVRPDUs transmitted on the port.

Received MVRP PDU

Displays the number of MVRPDUs received on the port.

Received bad header PDU

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

Received bad format PDU

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

Transmission failed

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

Registrations failed

Displays the number of unsuccessful registration attempts on the port.

Last received MAC address

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

Buttons

You find the description of the standard buttons in section “Buttons” on page 17.

Reset

Resets the port statistics counters and the values in the *Last received MAC address* column.

5.7 GARP

[Switching > GARP]

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

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

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

The menu contains the following dialogs:

- ▶ *GMRP*
- ▶ *GVRP*

5.7.1 GMRP

[Switching > GARP > GMRP]

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

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

Operation

Operation

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

Possible values:

- ▶ *On*
GMRP is enabled.
- ▶ *Off* (default setting)
The device ignores GMRP messages.

Multicasts

Unknown multicasts

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

Possible values:

- ▶ *discard*
The device discards unknown multicast data.
- ▶ *flood* (default setting)
The device forwards unknown multicast data to every port.

Table

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.

Buttons

You find the description of the standard buttons in section [“Buttons” on page 17](#).

5.7.2 GVRP

[Switching > GARP > GVRP]

The GARP VLAN Registration Protocol (GVRP) or Generic VLAN Registration Protocol is a protocol that facilitates control of Virtual Local Area Networks (VLANs) within a larger network. GVRP is a Layer 2 network protocol, used to automatically configure devices in a VLAN network.

GVRP is a GARP application that provides IEEE 802.1Q-compliant VLAN pruning, and creating dynamic VLAN on 802.1Q trunk ports. With GVRP, the device exchanges VLAN configuration information with other GVRP devices. Thus, the device reduces the unnecessary broadcast and unknown unicast traffic. Exchanging VLAN configuration information also lets you dynamically create and manage VLANs connected through the 802.1Q trunk ports.

Operation

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

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.

Buttons

You find the description of the standard buttons in section “Buttons” on page 17.

5.8 QoS/Priority

[Switching > QoS/Priority]

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

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

The device provides the following setting options:

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

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

The menu contains the following dialogs:

- ▶ QoS/Priority Global
- ▶ QoS/Priority Port Configuration
- ▶ 802.1D/p Mapping
- ▶ IP DSCP Mapping
- ▶ Queue Management

5.8.1 QoS/Priority Global

[Switching > QoS/Priority > Global]

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

Configuration

VLAN priority for management packets

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

Possible values:

▶ 0..7 (default setting: 0)

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

IP DSCP value for management packets

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

Possible values:

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

Some values in the list also have a DSCP keyword, for example 0 (be/cs0), 10 (af11) and 46 (ef). These values are compatible with the IP precedence model.

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

Queues per port

Displays the number of priority queues per port.

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

Buttons

You find the description of the standard buttons in section “Buttons” on page 17.

5.8.2 QoS/Priority Port Configuration

[Switching > QoS/Priority > Port Configuration]

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

Table

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 transmits the data packet depending on the value specified in the *Trust mode* column.

Possible values:

- ▶ 0..7 (default setting: 0)

Trust mode

Specifies how the device handles a received data packet if the data packet contains QoS/priority information.

Possible values:

- ▶ *untrusted*
The device transmits the data packet according to the priority specified in the *Port priority* column. The device ignores the priority information contained in the data packet.
In the *Switching > QoS/Priority > 802.1D/p Mapping* dialog, you assign a traffic class to every VLAN priority.
- ▶ *trustDot1p* (default setting)
The device transmits the data packet according to the priority information in the VLAN tag.
In the *Switching > QoS/Priority > 802.1D/p Mapping* dialog, you assign a traffic class to every VLAN priority.
- ▶ *trustIpDscp*
 - If the data packet is an IP packet, then:
The device transmits the data packet according to the IP DSCP value contained in the data packet.
In the *Switching > QoS/Priority > IP DSCP Mapping* dialog you assign a traffic class to every IP DSCP value.
 - If the data packet is not an IP packet, then:
The device transmits the data packet according to the priority specified in the *Port priority* column.
In the *Switching > QoS/Priority > 802.1D/p Mapping* dialog, you assign a traffic class to every VLAN priority.

Untrusted traffic class

Displays the traffic class assigned to the VLAN priority information specified in the *Port priority* column. In the *Switching > QoS/Priority > 802.1D/p Mapping* dialog, you assign a traffic class to every VLAN priority.

Possible values:

▶ 0..7

Buttons

You find the description of the standard buttons in section “Buttons” on page 17.

5.8.3 802.1D/p Mapping

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

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

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

Table

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.

Buttons

You find the description of the standard buttons in section [“Buttons” on page 17](#).

Default assignment of the VLAN priority to traffic classes

VLAN Priority	Traffic class	Content description according to IEEE 802.1D
0	2	Best Effort Normal data without prioritizing
1	0	Background Non-time-sensitive data and background services
2	1	Standard Normal data
3	3	Excellent Effort Crucial data
4	4	Controlled Load Time-sensitive data with a high priority

VLAN Priority	Traffic class	Content description according to IEEE 802.1D
5	5	Video Video transmission with delays and jitter < 100 ms
6	6	Voice Voice transmission with delays and jitter < 10 ms
7	7	Network Control Data for network management and redundancy mechanisms

5.8.4 IP DSCP Mapping

[Switching > QoS/Priority > IP DSCP Mapping]

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

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

Table

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.

Buttons

You find the description of the standard buttons in section [“Buttons” on page 17](#).

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

DSCP Value	DSCP Name	Traffic class
40	CS5	5
41,42,43,44,45,47		5
46	EF	5
48	CS6	6
49-55		6
56	CS7	7
57-63		7

5.8.5 Queue Management

[Switching > QoS/Priority > Queue Management]

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

You also have the option of assigning a minimum bandwidths to every traffic classes which the device uses to process the priority queues with "Weighted Fair Queuing"

Table

Traffic class

Displays the traffic class.

Strict priority

Activates/deactivates the processing of the port priority queue with *Strict priority* for this traffic class.

Possible values:

▶ *marked* (default setting)

The processing of the port priority queue with *Strict priority* is active.

- The port forwards only data packets that are in the priority queue with the highest priority. When this priority queue is empty, the port forwards data packets that are in the priority queue with the next lower priority.
- The port forwards data packets with a lower traffic class after the priority queues with a higher priority are empty. In unfavorable situations, the port does not send these data packets.
- When you select this setting for a traffic class, the device also enables the function for traffic classes with a higher priority.
- Use this setting for applications such as VoIP or video that require the least possible delay.

▶ *unmarked*

The processing of the port priority queue with *Strict priority* is inactive. The device uses "Weighted Fair Queuing"/"Weighted Round Robin" (WRR) to process the port priority queue.

- The device assigns a minimum bandwidth to each traffic class.
- Even under a high network load the port transmits data packets with a low traffic class.
- When you select this setting for a traffic class, the device also disables the function for traffic classes with a lower priority.

Min. bandwidth [%]

Specifies the minimum bandwidth for this traffic class when the device is processing the priority queues of the ports with "Weighted Fair Queuing".

Possible values:

▶ *0..100* (default setting: 0 = the device does not reserve any bandwidth for this traffic class)

The value specified in percent refers to the available bandwidth on the port. When you disable the *Strict priority* function for every traffic class, the maximum bandwidth is available on the port for the "Weighted Fair Queuing".

The maximum total of the assigned bandwidths is 100 %.

Max. bandwidth [%]

Specifies the shaping rate at which a Traffic Class transmits packets (Queue Shaping).

Possible values:

- ▶ 0 (default setting)
The device does not reserve any bandwidth for this traffic class.
- ▶ 1..100
The device reserves the specified bandwidth for this traffic class. The specified value in percent refers to the maximum available bandwidth on this port.

For example, using queue shaping lets you limit the rate of a strict-high priority queue. Limiting a strict-high priority queue lets the device also process low-priority queues. To use queue shaping, you set the maximum bandwidth for a particular queue.

Buttons

You find the description of the standard buttons in section [“Buttons” on page 17](#).

5.9 VLAN

[Switching > VLAN]

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

- ▶ High flexibility
 - With VLAN you distribute the data traffic 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 traffic among individual logical networks makes unwanted accessing more difficult and strengthens the system against attacks such as MAC Flooding or MAC Spoofing.

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

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

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

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

- ▶ Voice VLAN
- ▶ Port-based VLAN

The menu contains the following dialogs:

- ▶ VLAN Global
- ▶ VLAN Configuration
- ▶ VLAN Port
- ▶ VLAN Voice

5.9.1 VLAN Global

[Switching > VLAN > Global]

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

Configuration

Max. VLAN ID

Highest ID assignable to a VLAN.

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

VLANs (max.)

Displays the maximum number of VLANs possible.

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

VLANs

Number of VLANs currently configured in the device.

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

The VLAN ID 1 is constantly present in the device.

Buttons

You find the description of the standard buttons in section [“Buttons” on page 17](#).

Clear...

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

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

5.9.2 VLAN Configuration

[Switching > VLAN > Configuration]

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

You distinguish between the following VLANs:

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

For the following functions the device creates dynamic VLANs:

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

Table

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 Port Authentication* function. See the *Network Security > 802.1X Port Authentication* 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 changes in the non-volatile memory, then the VLANs with this setting remain set up after a restart.
- ▶ *dynamicMvrp*
VLAN set up using the *MVRP* function. See the *Switching > MRP-IEEE > MVRP* dialog.
VLANs with this setting are write-protected. The device removes a VLAN from the table as soon as the last port leaves the VLAN.

Creation time

Displays the time of VLAN creation.

The field displays the time stamp for the operating time (system uptime).

Name

Specifies the name of the VLAN.

Possible values:

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

<Port number>

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

Possible values:

- ▶ - (default setting)
The port is not a member of the VLAN and does not transmit data packets of the VLAN.
- ▶ T = Tagged
The port is a member of the VLAN and transmits the data packets with a VLAN tag. You use this setting for uplink ports, for example.
- ▶ T = Tagged Learned
The port is a member of the VLAN and transmits the data packets with a VLAN tag. The device created the entry automatically based on the *GVRP* or *MVRP* function.
- ▶ F = Forbidden
The port is not a member of the VLAN and does not transmit data packets of this VLAN. Additionally, the device helps prevent the port from becoming a VLAN member through the *MVRP* function.
- ▶ 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.
- ▶ U = Untagged Learned
The port is a member of the VLAN and transmits the data packets without a VLAN tag. The device created the entry automatically based on the *GVRP* or *MVRP* function.

Note: Verify that the port on which the network management station is connected is a member of the VLAN in which the device transmits the management data. In the default setting, the device transmits the management data on VLAN 1. Otherwise, the connection to the device terminates when you transfer the changes to the device. The access to the device management is possible only using the Command Line Interface through the serial interface.

Buttons

You find the description of the standard buttons in section [“Buttons” on page 17](#).



Opens the *Create* window to add a new entry to the table.

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

5.9.3 VLAN Port

[Switching > VLAN > Port]

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

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

Additionally, you also specify for each port how the device transmits data packets and one of the following situations occurs:

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

Table

Port

Displays the port number.

Port-VLAN ID

Specifies the ID of the VLAN which the device assigns to data packets without a VLAN tag.

Prerequisites:

- In the *Acceptable packet types* column, you specify the value *admitAll*.

Possible values:

- ▶ ID of a VLAN you set up (default setting: 1)

If you use the *MRP* function and you did not assign a VLAN to the ring ports, then you specify the value 1 here for the ring ports. Otherwise, the device assigns the value to the ring ports automatically.

Acceptable packet types

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

Possible values:

- ▶ *admitAll* (default setting)
The port accepts data packets both with and without a VLAN tag.
- ▶ *admitOnlyVlanTagged*
The port accepts only data packets tagged with a VLAN ID ≥ 1 .

Ingress filtering

Activates/deactivates the ingress filtering.

Possible values:

- ▶ `marked`
The ingress filtering is active.
The device compares the VLAN ID in the data packet with the VLANs of which the device is a member. See the [Switching > VLAN > Configuration](#) dialog. If the VLAN ID in the data packet matches one of these VLANs, then the port transmits the data packet. Otherwise, the device discards the data packet.
- ▶ `unmarked` (default setting)
The ingress filtering is inactive.
The device transmits received data packets without comparing the VLAN ID. Thus the port also transmits data packets with a VLAN ID of which the port is not a member.

Buttons

You find the description of the standard buttons in section [“Buttons” on page 17](#).

5.9.4 VLAN Voice

[Switching > VLAN > Voice]

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

The device detects VoIP phones using the Link Layer Discovery Protocol - Media Endpoint Discovery (LLDP-MED). The device then adds the appropriate port to the member set of the configured Voice VLAN. The member set is either tagged or untagged. Tagging depends on the Voice VLAN interface mode (VLAN ID, Dot1p, None, Untagged).

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

Operation

Operation

Enables/disables the *VLAN Voice* function of the device globally.

Possible values:

- ▶ *On*
- ▶ *Off* (default setting)

Table

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 *VLAN Voice* function for this table entry.
- ▶ *none*
Lets the IP telephone use its own configuration for sending untagged voice traffic.
- ▶ *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 traffic on the particular port.

The device uses this mode for data traffic on the voice VLAN, when it detects a VoIP telephone and a PC and when these devices use the same cable for transmitting and receiving data.

Possible values:

- ▶ *trust* (default setting)
If voice traffic is present on the interface, then the data traffic uses the normal priority with this setting.
- ▶ *untrust*
If voice traffic is present and the *Voice VLAN mode* is set to *dot1p-priority*, then the data has the priority 0. If the interface only transmits data, then the data has the normal priority.

Status

Displays the status of the Voice VLAN on the port.

Possible values:

- ▶ *marked*
The Voice VLAN is enabled.
- ▶ *unmarked*
The Voice VLAN is disabled.

VLAN ID

Specifies the ID of the VLAN to which the table entry applies.

To forward traffic to this VLAN ID using this filter, select in the *Voice VLAN mode* column the value *vlan*.

Possible values:

- ▶ *0..4042*

Priority

Specifies the Voice VLAN Priority of the port.

Prerequisites:

- In the *Voice VLAN mode* column, you specify the value *dot1p-priority*.

Possible values:

- ▶ *0..7*
- ▶ *none*
Deactivates the Voice VLAN Priority of the port.

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 Port Authentication > Global* dialog, then set the *Port control* parameter for this port to the *multiClient* value before activating this function. You find the *Port control* parameter in the *Network Security > 802.1X Port Authentication > Global* dialog.

▶ *unmarked*

Buttons

You find the description of the standard buttons in section “Buttons” on page 17.

5.10 L2-Redundancy

[Switching > L2-Redundancy]

The menu contains the following dialogs:

- ▶ *MRP*
- ▶ *HIPER Ring*
- ▶ *Spanning Tree*
- ▶ *Link Aggregation*
- ▶ *Link Backup*
- ▶ *FuseNet*

5.10.1 MRP

[Switching > L2-Redundancy > MRP]

WARNING

UNINTENDED EQUIPMENT OPERATION

To help avoid loops during the configuration phase, configure each device of the *MRP* configuration individually. Before you connect the redundant lines, complete the configuration of the other devices of the ring configuration.

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

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

If a section is not operating, then the ring structure of an MRP ring changes back into a line structure. The maximum recovery time can be configured.

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

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

When you work with oversized Ethernet packets (the value in the *MTU* column for the port is > 1518, see the *Basic Settings > Port* dialog), the switching time of the MRP ring reconfiguration depends on the following parameters:

- ▶ Bandwidth of the ring line
- ▶ Size of the Ethernet packets
- ▶ Number of devices in the ring

Set the recovery time sufficiently large to help avoid delays in the MRP packages due to latencies in the devices. You can find the formula for calculating the switching time in IEC 62439-2, section 9.5.

Operation

Operation

Enables/disables the *MRP* function.

After you configured the parameters for the MRP ring, enable the function here.

Possible values:

- ▶ *On*
The *MRP* function is enabled.
After you configured the devices in the MRP ring, the redundancy is active.
- ▶ *Off* (default setting)
The *MRP* function is disabled.

Ring port 1/Ring port 2

Port

Specifies the number of the port that is operating as a ring port.

Possible values:

- ▶ *<Port number>*
Number of the ring port

Operation

Displays the operating status of the ring port.

Possible values:

- ▶ *forwarding*
The port is enabled, connection exists.
- ▶ *blocked*
The port is blocked, connection exists.
- ▶ *disabled*
The port is disabled.
- ▶ *not-connected*
No connection exists.

Fixed backup

Activates/deactivates the backup port function for the *Ring port 2*.

Note: The switch over to the primary port can exceed the maximum ring recovery time.

Possible values:

- ▶ *marked*
The *Ring port 2* backup function is active. When the ring is closed, the ring manager reverts back to the primary ring port.
- ▶ *unmarked* (default setting)
The *Ring port 2* backup function is inactive. When the ring is closed, the ring manager continues to send data on the secondary ring port.

Configuration

Ring manager

Enables/disables the *Ring manager* function.

If there is one device at each end of the line, then you activate this function.

Possible values:

- ▶ *On*
The *Ring manager* function is enabled.
The device operates as a ring manager.
- ▶ *Off* (default setting)
The *Ring manager* function is disabled.
The device operates as a ring client.

Advanced mode

Activates/deactivates the advanced mode for fast recovery times.

Possible values:

- ▶ *marked* (default setting)
Advanced mode active.
MRP-capable Schneider Electric devices support this mode.
- ▶ *unmarked*
Advanced mode inactive.
Select this setting if another device in the ring does not support this mode.

Ring recovery

Specifies the maximum recovery time in milliseconds for reconfiguration of the ring. This setting is effective if the device operates as a ring manager.

Possible values:

- ▶ *500ms*
- ▶ *200ms* (default setting)

Shorter switching times make greater demands on the response time of every individual device in the ring. Use values lower than *500ms* if the other devices in the ring also support this shorter recovery time.

When you are working with oversized Ethernet packets, the number of devices in the ring is limited. Note that the switching time depends on several parameters. See the description above.

VLAN ID

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

Possible values:

- ▶ 0 (default setting)
No VLAN assigned.
Assign in the *Switching > VLAN > Configuration* dialog to the ring ports for VLAN 1 the value \emptyset .
- ▶ 1..4042
VLAN assigned.
If you assign to the ring ports a non-existing VLAN, then the device creates this VLAN. In the *Switching > VLAN > Configuration* dialog, the device creates an entry in the table for the VLAN and assigns the value \mathbb{T} to the ring ports.

Information

Information

Displays messages for the redundancy configuration and the possible causes of detected errors.

When the device operates as a ring client or a ring manager, the following messages are possible:

- ▶ *Redundancy available*
The redundancy is set up. When a component of the ring is down, the redundant line takes over its function.
- ▶ *Configuration error: Error on ringport link.*
An error is detected in the cabling of the ring ports.

When the device operates as a ring manager, the following messages are possible:

- ▶ *Configuration error: Packets from another ring manager received.*
Another device exists in the ring that operates as the ring manager.
Enable the *Ring manager* function only on one device in the ring.
- ▶ *Configuration error: Ring link is connected to wrong port.*
A line in the ring is connected with a different port instead of with a ring port. The device only receives test data packets on one ring port.

Buttons

You find the description of the standard buttons in section “Buttons” on page 17.

Delete ring configuration

Disables the redundancy function and resets the settings in the dialog to the default setting.

5.10.2 HIPER Ring

[Switching > L2-Redundancy > HIPER Ring]

WARNING

UNINTENDED EQUIPMENT OPERATION

To help avoid loops during the configuration phase, configure each device of the *HIPER Ring* configuration individually. Before you connect the redundant lines, complete the configuration of the other devices of the ring configuration.

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

The concept of HIPER ring redundancy enables the construction of high-availability, ring-shaped networks. This device provides a HIPER ring client. This function lets you extend an existing HIPER ring or to replace a device already participating as a client in a HIPER ring.

A HIPER ring contains a Ring Manager (RM) which controls the ring. The RM sends watchdog packets into the ring on both the primary and secondary ports. When the RM receives the watchdog packets on both ports, the primary port remains in the forwarding state and the secondary port remains in the discarding state.

The device operates only in the ring client mode. This means that the device is able to recognize and forward the watchdog packets on the ring ports and can also forward the change in link status to the RM for example, LinkDown and LinkUp packets.

The device only supports Fast Ethernet and Gigabit Ethernet ports as ring ports. Furthermore, the device only supports HIPER ring in VLAN 1.

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

Note: Configure the devices of the HIPER ring individually. Before you connect the redundant link, complete the configuration of every device of the HIPER ring. You thus help avoid loops during the configuration phase.

Operation

Operation

Enables/disables the *HIPER Ring* client.

Possible values:

- ▶ *On*
The *HIPER Ring* client is enabled.
- ▶ *Off* (default setting)
The *HIPER Ring* client is disabled.

Ring port 1/Ring port 2

Port

Specifies the port number of the primary/secondary ring port.

Possible values:

- ▶ - (default setting)
No primary/secondary ring port selected.
- ▶ `<Port number>`
Number of the ring port

State

Displays the state of the primary/secondary ring port.

Possible values:

- ▶ `not-available`
The *HIPER Ring* client is disabled.
or
No primary or secondary ring port selected.
- ▶ `active`
The ring port is enabled and logically up.
- ▶ `inactive`
The ring port is logically down.
As soon as the link goes down on a ring port, the device sends a LinkDown packet to the Ring Manager on the other ring port.

Information

Mode

Displays that the device is able to operate in the ring client mode.

Buttons

You find the description of the standard buttons in section [“Buttons” on page 17](#).

5.10.3 Spanning Tree

[Switching > L2-Redundancy > Spanning Tree]

WARNING

UNINTENDED EQUIPMENT OPERATION

To help avoid loops during the configuration phase, configure each device of the *Spanning Tree* configuration individually. Before you connect the redundant lines, complete the configuration of the other devices of the *Spanning Tree* configuration.

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

The Spanning Tree Protocol (STP) is a protocol that deactivates redundant paths of a network in order to help avoid loops. If a network component becomes 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 Dual RSTP (MCSESM-E)*
- ▶ *Spanning Tree Port*

5.10.3.1 Spanning Tree Global

[Switching > L2-Redundancy > Spanning Tree > Global]

In this dialog you enable/disable the *Spanning Tree* function and specify the bridge settings.

Operation

Operation

Enables/disables the Spanning Tree function in the device.

Possible values:

▶ *On* (default setting)

▶ *Off*

The device behaves transparently. The device floods received Spanning Tree data packets like multicast data packets to the ports.

Variant

Variant

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

Possible values:

▶ *rstp*

The protocol *RSTP* is active.

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

Traps

Send trap

Activates/deactivates the sending of SNMP traps for the following events:

- Another bridge takes over the root bridge role.
- The topology changes. A port changes its *Port state* from *forwarding* into *discarding* or from *discarding* into *forwarding*.

Possible values:

▶ *marked*

The sending of SNMP traps is active.

▶ *unmarked* (default setting)

The sending of SNMP traps is inactive.

Bridge configuration

Bridge ID

Displays the bridge ID of the device.

The device with the lowest bridge ID numerical value takes over the role of the root bridge in the network.

Possible values:

- ▶ `<Bridge priority> / <MAC address>`
Value in the *Priority* field / MAC address of the device

Priority

Specifies the bridge priority of the device.

Possible values:

- ▶ `0..61440` in steps of 4096 (default setting: `32768`)

To make this device the root bridge, assign the lowest numeric priority value in the network to the device.

Hello time [s]

Specifies the time in seconds between the sending of two configuration messages (Hello data packets).

Possible values:

- ▶ `1..2` (default setting: `2`)

If the device takes over the role of the root bridge, then the other devices in the network use the value specified here.

Otherwise, the device uses the value specified by the root bridge. See the *Root information* frame.

Due to the interaction with the *Tx holds* parameter, we recommend that you do not change the default setting.

Forward delay [s]

Specifies the delay time for the status change in seconds.

Possible values:

- ▶ `4..30` (default setting: `15`)

If the device takes over the role of the root bridge, then the other devices in the network use the value specified here.

Otherwise, the device uses the value specified by the root bridge. See the *Root information* frame.

In the RSTP protocol, the bridges negotiate a status change without a specified delay.

The *Spanning Tree* protocol uses the parameter to delay the status change between the statuses *disabled*, *discarding*, *learning*, *forwarding*.

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

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

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 for example, the number of devices to the root bridge.

Possible values:

▶ 6..40 (default setting: 20)

If the device takes over the role of the root bridge, then the other devices in the network use the value specified here.

Otherwise, the device uses the value specified by the root bridge. See the *Root information* frame.

The *Spanning Tree* protocol uses the parameter to specify the validity of STP-BPDUs in seconds.

Tx holds

Limits the maximum transmission rate for sending BPDUs.

Possible values:

▶ 1..40 (default setting: 10)

When the device sends a BPDU, the device increments a counter on this port.

If the counter reaches the value specified here, then the port stops sending BPDUs. On the one hand, this reduces the load generated by RSTP, and on the other when the device does not receive BPDUs, a communication interruption can be caused.

The device decrements the counter by 1 every second. In the following second, the device sends a maximum of 1 new BPDU.

BPDU guard

Activates/deactivates the BPDU Guard function in the device.

With this function, the device helps protect your network from incorrect configurations, attacks with STP-BPDUs, and unwanted topology changes.

Possible values:

▶ *marked*

The *BPDU guard* is active.

- The device applies the function to manually specified edge ports. For these ports, in the *Switching > L2-Redundancy > Spanning Tree > Port* dialog, *CIST* tab the checkbox in the *Admin edge port* column is marked.
- If an edge port receives an STP-BPDU, then the device disables the port. For this port, in the *Basic Settings > Port* dialog, *Configuration* tab the checkbox in the *Port on* column is *unmarked*.

▶ *unmarked* (default setting)

The *BPDU guard* is inactive.

To reset the status of the port to the value *forwarding*, you proceed as follows:

- If the port is still receiving BPDUs, then:
 - In the *Switching > L2-Redundancy > Spanning Tree > Port* dialog, *CIST* tab unmark the checkbox in the *Admin edge port* column.
 - or
 - In the *Switching > L2-Redundancy > Spanning Tree > Global* dialog, unmark the *BPDU guard* checkbox.
- To re-enable the port again you use the *Auto-Disable* function. Alternatively, proceed as follows:
 - Open the *Basic Settings > Port* dialog, *Configuration* tab.
 - Mark the checkbox in the *Port on* column.

BPDU filter (all admin edge ports)

Activates/deactivates the STP-BPDU filter on every manually specified edge port. For these ports, in the *Switching > L2-Redundancy > Spanning Tree > Port* dialog, *CIST* tab the checkbox in the *Admin edge port* column is marked.

Possible values:

- ▶ *marked*
 - The BPDU filter is active on every edge port.
 - The function does not use these ports in *Spanning Tree* operations.
 - The device does not send STP-BPDUs on these ports.
 - The device drops any STP-BPDUs received on these ports.
- ▶ *unmarked* (default setting)
 - The global BPDU filter is inactive.
 - You have the option to explicitly activate the BPDU filter for single ports. See the *Port BPDU filter* column in the *Switching > L2-Redundancy > Spanning Tree > Port* dialog.

Auto-disable

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

Possible values:

- ▶ *marked*
 - The *Auto-Disable* function for the *BPDU guard* is active.
 - When the port receives an STP-BPDU, the device disables an edge port. The “Link status” LED for the port flashes 3× per period.
 - The *Diagnostics > Ports > Auto-Disable* dialog displays which ports are currently disabled due to the parameters being exceeded.
 - The *Auto-Disable* function reactivates the port 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

Bridge ID

Displays the bridge ID of the current root bridge.

Possible values:

▶ `<Bridge priority> / <MAC address>`

Priority

Displays the bridge priority of the current root bridge.

Possible values:

▶ `0..61440` in steps of 4096

Hello time [s]

Displays the time in seconds that the root bridge specifies between the sending of two configuration messages (Hello data packets).

Possible values:

▶ `1..2`

The device uses this specified value. See the *Bridge configuration* frame.

Forward delay [s]

Specifies the delay time in seconds set up by the root bridge for status changes.

Possible values:

▶ `4..30`

The device uses this specified value. See the *Bridge configuration* frame.

In the RSTP protocol, the bridges negotiate a status change without a specified delay.

The *Spanning Tree* protocol uses the parameter to delay the status change between the statuses *disabled*, *discarding*, *learning*, *forwarding*.

Max age

Specifies the maximum permitted branch length that the root bridge sets up for example, the number of devices to the root bridge.

Possible values:

▶ `6..40` (default setting: 20)

The *Spanning Tree* protocol uses the parameter to specify the validity of STP-BPDUs in seconds.

Topology information

Bridge is root

Displays if the device currently has the role of the root bridge.

Possible values:

- ▶ `marked`
The device currently has the role of the root bridge.
- ▶ `unmarked`
Another device currently has the role of the root bridge.

Root port

Displays the number of the port from which the current path leads to the root bridge.

If the device takes over the role of the root bridge, then the field displays the value `no Port`.

Root path cost

Specifies 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..200000000`
If the value `0` is specified, then the device takes over the role of the root bridge.

Topology changes

Displays how many times the device has put a port into the `forwarding` status using the `Spanning Tree` function since the `Spanning Tree` instance was started.

Time since topology change

Displays the time since the last topology change.

Possible values:

- ▶ `<days, hours:minutes:seconds>`

Buttons

You find the description of the standard buttons in section “Buttons” on page 17.

5.10.3.2 Spanning Tree Dual RSTP (MCSESM-E)

[Switching > L2-Redundancy > Spanning Tree > Dual RSTP]

WARNING

UNINTENDED EQUIPMENT OPERATION

To help avoid loops during the configuration phase, configure each device of the *RCP* and *Dual RSTP* configuration individually. Before you connect the redundant lines, complete the configuration of the other devices of the ring configuration.

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

In this dialog, you specify the bridge settings corresponding to the second *Spanning Tree* instance.

The *Dual RSTP* function is used together with the *RCP* function. Using the *RCP* function you have the option of coupling one or more RSTP rings to the RSTP instance in a primary ring. When coupling 2 *Spanning Tree* segments, the secondary ring represents a separate RSTP instance for which the settings of the *Dual RSTP* function apply. This *Dual RSTP* instance works independently of the RSTP instance of the primary ring and of the other secondary rings. When RSTP is the protocol used in only one of the rings to be coupled, you do not need the *Dual RSTP* function.

You specify the *RCP* function settings in the *Switching > L2-Redundancy > FuseNet > RCP* dialog.

Operation

Operation

Displays if the *Dual RSTP* function is enabled/disabled in the device.

Possible values:

- ▶ *On*
The *Dual RSTP* function is enabled in the device.
The device enables the *Dual RSTP* function itself if the following prerequisites are fulfilled:
 - In the *Switching > L2-Redundancy > FuseNet > RCP* dialog, you have specified the ports for the *Primary ring/network* and *Secondary ring/network* settings.
 - In the *Switching > L2-Redundancy > FuseNet > RCP* dialog, *Operation* frame, you have enabled the *RCP* function.
 - In the *Spanning Tree Global* dialog, *Operation* frame, you have enabled the *Spanning Tree* function.
 - There is no redundancy protocol configured in the secondary ring.
- ▶ *Off* (default setting)
The *Dual RSTP* function is disabled in the device.

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* to *discarding* or from *discarding* to *forwarding*.

Possible values:

- ▶ *marked* (default setting)
The sending of SNMP traps is active.
- ▶ *unmarked*
The sending of SNMP traps is inactive.

Bridge configuration

Bridge ID

Displays the bridge ID of the device.

The device with the lowest bridge ID numerical value takes over the role of the root bridge in the network.

Possible values:

- ▶ *<Bridge priority> / <MAC address>*
Value in the *Priority* field / MAC address of the device

Priority

Specifies the bridge priority of the device.

Possible values:

- ▶ *0..61440* in steps of 4096 (default setting: *32768*)

To make this device the root bridge, assign the lowest numeric priority value in the network to the device.

Hello time [s]

Specifies the time in seconds between the sending of two configuration messages (Hello data packets).

Possible values:

- ▶ *1..2* (default setting: *2*)

If the device takes over the role of the root bridge, then the other devices in the network use the value specified here.

Otherwise, the device uses the value 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 RSTP protocol, the bridges negotiate a status change without a specified delay.

The *Spanning Tree* protocol uses the parameter to delay the status change between the statuses *disabled*, *discarding*, *learning*, *forwarding*.

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

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

Max age

Specifies the maximum permitted number of devices in the path 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.

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 your network from incorrect configurations, attacks with STP-BPDUs, and unwanted topology changes.

Possible values:

- ▶ **marked**
The *BPDU guard* is active.
 - The device applies the function to manually specified edge ports. For these ports, in the *Switching > L2-Redundancy > Spanning Tree > Port* dialog, *CIST* tab the checkbox in the *Admin edge port* column is marked.
 - If an edge port receives an STP-BPDU, then the device disables the port. For this port, in the *Basic Settings > Port* dialog, *Configuration* tab the checkbox in the *Port on* column is **unmarked**.
- ▶ **unmarked** (default setting)
The *BPDU guard* is inactive.

To reset the status of the port to the value *forwarding*, you proceed as follows:

- If the port is still receiving BPDUs:
 - 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 > Dual RSTP* dialog, unmark the *BPDU guard* checkbox.
- To re-enable the port again, 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.

Root information

Root ID

Displays the bridge ID of the current root bridge.

Possible values:

▶ `<Bridge priority> / <MAC address>`

Priority

Displays the bridge priority of the current root bridge.

Possible values:

▶ `0..61440` in steps of 4096

Hello time [s]

Displays the time in seconds that the root bridge specifies between the sending of two configuration messages (Hello data packets).

Possible values:

▶ `1..2`

The device uses this specified value. See the *Bridge configuration* frame.

Forward delay [s]

Specifies the delay time in seconds set up by the root bridge for status changes.

Possible values:

▶ `4..30`

The device uses this specified value. See the *Bridge configuration* frame.

In the RSTP protocol, the bridges negotiate a status change without a specified delay.

The *Spanning Tree* protocol uses the parameter to delay the status change between the statuses *disabled*, *discarding*, *learning*, *forwarding*.

Max age

Specifies the maximum permitted branch length that the root bridge sets up for example, the number of devices to the root bridge.

Possible values:

▶ `6..40` (default setting: 20)

The *Spanning Tree* protocol uses the parameter to specify the validity of STP-BPDUs in seconds.

Topology information

Bridge is root

Displays if the device currently has the role of the root bridge.

Possible values:

- ▶ `marked`
The device currently has the role of the root bridge.
- ▶ `unmarked`
Another device currently has the role of the root bridge.

Root port

Displays the number of the port from which the current path leads to the root bridge.

If the device takes over the role of the root bridge, then the field displays the value `no Port`.

Root path cost

Specifies 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..200000000`
If the value `0` is specified, then the device takes over the role of the root bridge.

Topology changes

Displays how many times the device has put a port into the `forwarding` status using the `Spanning Tree` function since the `Spanning Tree` instance was started.

Time since topology change

Displays the time since the last topology change.

Possible values:

- ▶ `<days, hours:minutes:seconds>`

Buttons

You find the description of the standard buttons in section “Buttons” on page 17.

5.10.3.3 Spanning Tree Port

[Switching > L2-Redundancy > Spanning Tree > Port]

In this dialog you activate the Spanning Tree function on the ports, specify edge ports, and specify the settings for various protection functions.

The dialog contains the following tabs:

- ▶ [CIST]
- ▶ [Guards]

[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

Port

Displays the port number.

STP active

Activates/deactivates the Spanning Tree function on the port.

Possible values:

- ▶ *marked* (default setting)
The *Spanning Tree* function is active on the port.
- ▶ *unmarked*
The *Spanning Tree* function is inactive on the port.
If the *Spanning Tree* function is enabled in the device and inactive on the port, then the port does not send STP-BPDUs and drops any STP-BPDUs received.

Port state

Displays the transmission status of the port.

Possible values:

- ▶ *discarding*
The port is blocked and forwards only STP-BPDUs.
- ▶ *learning*
The port is blocked, but it learns the MAC addresses of received data packets.
- ▶ *forwarding*
The port forwards data packets.

- ▶ *disabled*
The port is inactive. See the *Basic Settings > Port* dialog, *Configuration* tab.
- ▶ *manualFwd*
The *Spanning Tree* function is disabled on the port. The port forwards STP-BPDUs.
- ▶ *notParticipate*
The port is not participating in STP.

Port role

Displays the current role of the port in CIST.

Possible values:

- ▶ *root*
Port with the cheapest path to the root bridge.
- ▶ *alternate*
Port with the alternative path to the root bridge (currently blocking).
- ▶ *designated*
Port for the side of the tree averted from the root bridge (currently blocking).
- ▶ *backup*
Port receives STP-BPDUs from its own device.
- ▶ *disabled*
The port is inactive. See the *Basic Settings > Port* dialog, *Configuration* tab.

Port path cost

Specifies the path costs of the port.

Possible values:

- ▶ *0..200000000* (default setting: *0*)

When the value is *0*, the device automatically calculates the path costs depending on the data rate of the port.

Port priority

Specifies the priority of the port.

Possible values:

- ▶ *16..240* in steps of 16 (default setting: *128*)

This value represents the first 4 bits of the port ID.

Received bridge ID

Displays the bridge ID of the device from which this port last received an STP-BPDU.

Possible values:

- ▶ For ports with the *designated* role, the device displays the information for the STP-BPDU last received by the port. This helps to diagnose the possible STP problems in the network.
- ▶ For the *alternate*, *backup*, *master*, and *root* port roles, in the stationary condition (static topology) this information is identical to the information of the *designated* port role.
- ▶ If a port has no connection or if it did not receive any STP-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 possible STP problems in the network.
- ▶ For the *alternate*, *backup*, *master*, and *root* port roles, in the stationary condition (static topology) this information is identical to the information of the *designated* port role.
- ▶ If a port has no connection or if it did not receive any STP-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 possible STP problems in the network.
- ▶ For the *alternate*, *backup*, *master*, and *root* port roles, in the stationary condition (static topology) this information is identical to the information of the *designated* port role.
- ▶ If a port has no connection or if it did not receive any STP-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* status without changing to the *learning* status beforehand.
 - If the port receives an STP-BPDU and the BPDU Guard function is active, then the device deactivates the port. See the *Switching > L2-Redundancy > Spanning Tree > Global* dialog.
- ▶ *unmarked* (default setting)
The *Admin edge port* mode is inactive.
The port is connected to another STP bridge.
After the connection is set up, the port changes to the *learning* status before changing to the *forwarding* status, if applicable.

Auto edge port

Activates/deactivates the automatic detection of whether you connect an end device to the port. The prerequisite is that the checkbox in the *Admin edge port* column is *unmarked*.

Possible values:

- ▶ *marked* (default setting)
The automatic detection is active.
After the installation of the connection and after $1.5 \times \textit{Hello time [s]}$, 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 via a direct full-duplex link.

Possible values:

- ▶ *marked*
The port is connected directly to an STP device via a full-duplex link. The direct, decentralized communication between 2 bridges enables short reconfiguration times.
- ▶ *unmarked*
The port is connected in another way, for example via a half-duplex link or via 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.

Buttons

You find the description of the standard buttons in section “Buttons” on page 17.

[Guards]

This tab lets you specify the settings for various protection functions on the ports.

Table

Port

Displays the port number.

Root guard

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

With this setting the device helps you protect your network from incorrect configurations or attacks with STP-BPDUs that try to change the topology. This setting is relevant only for ports with the STP role *designated*.

Possible values:

- ▶ **marked**
The monitoring of STP-BPDUs is active.
 - If the port receives an STP-BPDU with better path information to the root bridge, then the device discards the STP-BPDU and sets the status of the port to the value *discarding* instead of *root*.
 - If there are no STP-BPDUs with better path information to the root bridge, then the device resets the status of the port after $2 \times$ *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 your network from attacks with STP-BPDUs that try to change the topology.

Possible values:

- ▶ **marked**
The monitoring of "Topology Change Notifications" is enabled.
 - The port ignores the Topology Change flag in received STP-BPDUs.
 - If the received BPDU contains other information that causes a topology change, then the device processes the BPDU even if the TCN guard is enabled.
Example: The device receives better path information for the root bridge.
- ▶ **unmarked** (default setting)
The monitoring of "Topology Change Notifications" is disabled.
If the device receives STP-BPDUs with a Topology Change flag, then the device deletes the address table of the port and forwards the Topology Change Notifications.

Loop guard

Activates/deactivates the monitoring of loops on the port. The prerequisite is that the *Root guard* function is inactive.

With this setting the device helps prevent loops if the port does not receive any more STP-BPDUs. Use this setting only for ports with the STP role *alternate*, *backup* or *root*.

Possible values:

- ▶ **marked**
The monitoring of loops is active. This helps prevent loops for example, if you disable the Spanning Tree function on the remote device or if the connection is interrupted only in the receiving direction.
 - If the port does not receive any STP-BPDUs for a while, then the device sets the status of the port to the value *discarding* and marks the checkbox in the *Loop state* column.
 - If the port receives STP-BPDUs again, then the device sets the status of the port to a value according to *Port role* and unmarks the checkbox in the *Loop state* column.
- ▶ **unmarked** (default setting)
The monitoring of loops is inactive.
If the port does not receive any STP-BPDUs for a while, then the device sets the status of the port to the value *forwarding*.

Loop state

Displays if the loop state of the port is inconsistent.

Possible values:

▶ *marked*

The loop state of the port is inconsistent:

- The port is not receiving any STP-BPDUs and the *Loop guard* function is enabled.
- The device sets the state of the port to the value *discarding*. The device thus helps prevent any potential loops.

▶ *unmarked*

The loop state of the port is consistent. The port receives STP-BPDUs.

Trans. into loop

Displays how many times the loop state of the port became inconsistent (marked checkbox in the *Loop state* column).

Trans. out of loop

Displays how many times the loop state of the port became consistent (unmarked checkbox in the *Loop state* column).

BPDU guard effect

Displays if the port received an STP-BPDU as an edge port.

Prerequisite:

- The port is a manually specified edge port. In the *Port* dialog, the checkbox for this port in the *Admin edge port* column is *marked*.
- In the *Switching > L2-Redundancy > Spanning Tree > Global* dialog, the BPDU Guard function is active.

Possible values:

▶ *marked*

The port is an edge port and received an STP-BPDU.

The device deactivates the port. For this port, in the *Basic Settings > Port* dialog, *Configuration* tab the checkbox in the *Port on* column is *unmarked*.

▶ *unmarked*

The port is an edge port and has not received any STP-BPDUs, or the port is not an edge port.

To reset the status of the port to the value *forwarding*, you proceed as follows:

- If the port is still receiving BPDUs, then:
 - In the *CIST* tab, unmark the checkbox in the *Admin edge port* column.
 - or
 - In the *Switching > L2-Redundancy > Spanning Tree > Global* dialog, unmark the *BPDU guard* checkbox.
- To activate the port, proceed as follows:
 - Open the *Basic Settings > Port* dialog, *Configuration* tab.
 - Mark the checkbox in the *Port on* column.

Buttons

You find the description of the standard buttons in section “Buttons” on page 17.

5.10.4 Link Aggregation

[Switching > L2-Redundancy > Link Aggregation]

WARNING

UNINTENDED EQUIPMENT OPERATION

To help avoid loops during the configuration phase, configure each device of the *Link Aggregation* configuration individually. Before you connect the redundant lines, complete the configuration of the other devices of the *Link Aggregation* configuration.

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

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

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.
- ▶ *down* (lag/... row)
The LAG interface is down.
and
The number of operational physical ports assigned to the LAG interface is greater than or equal to the value specified in the *Active ports (min.)* column.
- ▶ *up*
The physical port is operational.
- ▶ *down* (lag/... row)
The LAG interface is down.
- ▶ *down*
The physical port is disabled.
or
No cable connected or no active link.

Active

Activates/deactivates the LAG interface.

Possible values:

- ▶ *marked* (default setting)
The LAG interface is active.
Consider that the following protocols do not work properly on the physical ports when you activate the LAG interface:
 - *PTP*
 - *802.1AS*
- ▶ *unmarked*
The LAG interface is inactive.

STP active

Activates/deactivates the *Spanning Tree* protocol on this LAG interface. The prerequisite is that you enable the *Spanning Tree* function globally in the *Switching > L2-Redundancy > Spanning Tree > Global* dialog.

You can also activate/deactivate the *Spanning Tree* protocol on the LAG interfaces in the *Switching > L2-Redundancy > Spanning Tree > Port* dialog.

Possible values:

- ▶ `marked` (default setting)
The *Spanning Tree* protocol is active on this LAG interface.
- ▶ `unmarked`
The *Spanning Tree* protocol is inactive on this LAG interface.

Static link aggregation

Activates/deactivates the *Static link aggregation* function on the LAG interface. The device aggregates the assigned physical ports to the LAG interface, even if the remote site does not support LACP.

Possible values:

- ▶ `marked`
The *Static link aggregation* function is active on this LAG interface. The device aggregates an assigned physical port to the LAG interface as soon as the physical port gets a link. The device does not send LACPDUs and discards received LACPDUs.
- ▶ `unmarked` (default setting)
The *Static link aggregation* function is inactive on this LAG interface. If the connection was successfully negotiated using LACP, then the device aggregates an assigned physical port to the LAG interface.

MTU

Specifies the maximum allowed size of Ethernet packets on the LAG interface in bytes. Any present VLAN tag is not taken into account.

This setting lets you increase the size of the Ethernet packets for specific applications.

Possible values:

- ▶ `1518..9720` (default setting: `1518`)
With the value `1518`, the LAG interface transmits the Ethernet packets up to the following size:
 - 1518 bytes without VLAN tag
(1514 bytes + 4 bytes CRC)
 - 1522 bytes with VLAN tag
(1518 bytes + 4 bytes CRC)

Active ports (min.)

Specifies the minimum number of physical ports to be active for the LAG interface to stay active. If the number of active physical ports is lower than the specified value, then the device deactivates the LAG interface.

If a redundancy function like *Spanning Tree* or *MRP* over LAG is active in the device, then you use this function to force the device to switch automatically to the redundant line.

Possible values:

- ▶ `1` (default setting)
- ▶ `2`
- ▶ Depending on the hardware:
 - `4`
 - `8`
 - `32`

Type

Displays if the LAG interface is based on the *Static link aggregation* function or on LACP.

Possible values:

- ▶ *static*
The LAG interface is based on the *Static link aggregation* function.
- ▶ *dynamic*
The LAG interface is based on LACP.

Send trap (Link up/down)

Activates/deactivates the sending of SNMP traps when the device detects a change in the link up/down status for this interface.

Possible values:

- ▶ *marked* (default setting)
The sending of SNMP traps is active.
If the device detects a link up/down status change, then the device sends an SNMP trap.
- ▶ *unmarked*
The sending of SNMP traps is inactive.

The prerequisite for sending SNMP traps is that you enable the function in the *Diagnostics > Status Configuration > Alarms (Traps)* dialog and specify at least one trap destination.

LACP admin key

Specifies the LAG interface key. The device uses this key to identify the ports that can be aggregated to the LAG interface.

Possible values:

- ▶ *0..65535*
You specify the corresponding value for the physical ports in the *LACP port actor admin key* column.

Port

Displays the physical ports number assigned to the LAG interface.

Aggregation port status

Displays if the LAG interface aggregates the physical port.

Possible values:

- ▶ *active*
The LAG interface aggregates the physical port.
- ▶ *inactive*
The LAG interface does not aggregate the physical port.

LACP active

Activates/deactivates LACP on the physical port.

Possible values:

- ▶ `marked` (default setting)
LACP is active on the physical port.
- ▶ `unmarked`
LACP is inactive on the physical port.

LACP port actor admin key

Specifies the physical port key. The device uses this key to identify the ports that can be aggregated to the LAG interface.

Possible values:

- ▶ `0`
The device ignores the key on this physical port when deciding to aggregate the port into the LAG interface.
- ▶ `1..65535`
If this value matches the value of the LAG interface specified in the *LACP admin key* column, then the device only aggregates this physical port to the LAG interface.

LACP actor admin state

Specifies the actor state values that the LAG interface transmits in the LACPDU. This lets you control the LACPDU parameters.

The device lets you mix the values. In the drop-down list, select one or more values.

Possible values:

- ▶ `ACT`
(*LACP_Activity* state)
When selected, the link transmits the LACPDUs cyclically, otherwise when requested.
- ▶ `STO`
(*LACP_Timeout* state)
When selected, the link transmits the LACPDUs cyclically using the short timeout, otherwise using the long timeout.
- ▶ `AGG`
(*Aggregation* state)
When selected, the device interprets the link as a candidate for aggregation, otherwise as an individual link.

For further information on the values, see the standard IEEE 802.1AX-2014.

LACP actor oper state

Displays the actor state values that the LAG interface transmits in the LACPDU.

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 LACPDU cyclically using the short timeout, otherwise using the long timeout.
- ▶ *AGG*
(Aggregation state)
When visible, the device interprets the link as a candidate for aggregation, otherwise as an individual link.
- ▶ *SYN*
(Synchronization state)
When visible, the device interprets the link as *IN_SYNC*, otherwise as *OUT_OF_SYNC*.
- ▶ *COL*
(Collecting state)
When visible, collection of incoming frames is enabled on this link, otherwise disabled.
- ▶ *DST*
(Distributing state)
When visible, distribution of outgoing frames is enabled on this link, otherwise disabled.
- ▶ *DFT*
(Defaulted state)
When visible, the link uses defaulted operational information, administratively specified for the Partner. Otherwise the link uses the operational information received from a LACPDU.
- ▶ *EXP*
(Expired state)
When visible, the link receiver is in the *EXPIRED* state.

LACP partner oper SysID

Displays the MAC address of the remote device connected to this physical port.

The LAG interface has received this information in a LACPDU from the partner.

LACP partner oper port

Displays the port number of the remote device connected to this physical port.

The LAG interface has received this information in a LACPDU from the partner.

LACP partner oper port state

Displays the partner state values that the LAG interface receives in the LACPDUs.

Possible values:

- ▶ *ACT*
- ▶ *STO*
- ▶ *AGG*
- ▶ *SYN*
- ▶ *COL*
- ▶ *DST*
- ▶ *DFT*
- ▶ *EXP*

For further information on the values, see the description of the *LACP actor oper state* column and the standard IEEE 802.1AX-2014.

Buttons

You find the description of the standard buttons in section “Buttons” on page 17.



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

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

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

5.10.5 Link Backup

[Switching > L2-Redundancy > Link Backup]

WARNING

UNINTENDED EQUIPMENT OPERATION

To help avoid loops during the configuration phase, configure each device of the *Link Backup* configuration individually. Before you connect the redundant lines, complete the configuration of the other devices of the *Link Backup* configuration.

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

With Link Backup, you configure pairs of redundant links. Each pair has a primary port and a backup port. The primary port forwards traffic until the device detects an error. If the device detects an error on the primary port, then the Link Backup function transfers traffic over to the backup port.

The dialog also lets you set a fail back option. If you enable the fail back function and the primary port returns to normal operation, then the device first blocks traffic on the backup port and then forwards traffic on the primary port. This process helps protect the device from causing loops in the network.

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

Primary port

Displays the primary port of the interface pair. When you enable the Link Backup function, this port is responsible for forwarding traffic.

Possible values:

- ▶ Physical ports

Backup port

Displays the backup port on which the device forwards traffic 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 traffic.
- ▶ *blocking*
The link is up, no shutdown, and blocking traffic.
- ▶ *down*
The port is either link down, cable unplugged, or disabled in software, shutdown.
- ▶ *unknown*
The Link Backup feature is globally disabled, or the port pair is inactive. Therefore, the device ignores the port pair settings.

Backup port status

Displays the status of the Backup port for this Link Backup pair.

Possible values:

- ▶ *forwarding*
The link is up, no shutdown, and forwarding traffic.
- ▶ *blocking*
The link is up, no shutdown, and blocking traffic.
- ▶ *down*
The port is either link down, cable unplugged, or disabled in the software, shutdown.
- ▶ *unknown*
The Link Backup feature is globally disabled, or the port pair is inactive. Therefore, the device ignores the port pair settings.

Fail back

Activates/deactivates the automatic fail back.

Possible values:

- ▶ `marked` (default setting)
The automatic fail back is active.
After the delay timer expires, the backup port changes to `blocking` and the primary port changes to `forwarding`.
- ▶ `unmarked`
The automatic fail back is inactive.
The backup port continues forwarding traffic even after the primary port re-establishes a link or you manually change the admin status of the primary port from `shutdown` to `no shutdown`.

Fail back delay [s]

Specifies the delay time in seconds that the device waits after the primary port re-establishes a link. Furthermore, this timer also applies when you manually set the admin status of the primary port from `shutdown` to `no shutdown`. After the delay timer expires, the backup port changes to `blocking` and the primary port changes to `forwarding`.

Possible values:

- ▶ `0..3600` (default setting: 30)
When set to 0, immediately after the primary port re-establishes a link, the backup port changes to `blocking` and the primary port changes to `forwarding`. Furthermore, immediately after you manually set the admin status of from `shutdown` to `no shutdown`, the backup port changes to `blocking` and the primary port changes to `forwarding`.

Active

Activates/deactivates the Link Back up pair configuration.

Possible values:

- ▶ `marked`
The Link Backup pair is active. The device senses the link and administration status and forwards traffic according to the pair configuration.
- ▶ `unmarked` (default setting)
The Link Backup pair is inactive. The ports forward traffic according to standard switching.

Buttons

You find the description of the standard buttons in section [“Buttons” on page 17](#).

Create

Primary port

Specifies the primary port of the backup interface pair. During normal operation this port is responsible for forwarding the traffic.

Possible values:

- ▶ Physical ports

Backup port

Specifies the backup port to which the device transfers the traffic 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.

5.10.6 FuseNet

[Switching > L2-Redundancy > FuseNet]

The *FuseNet* protocols let you couple rings that are operating with one of the following redundancy protocols:

- ▶ MRP
- ▶ HIPER Ring
- ▶ RSTP

Note: If you use the *Ring/Network Coupling* protocol to couple networks, then verify that the networks only contain Schneider Electric devices.

Use the following table to select the *FuseNet* coupling protocol to be used in your network:

Main Ring	Connected Network		
	MRP	HIPER ring	RSTP
MRP	<i>Sub Ring</i> ¹⁾	<i>Redundant Coupling Protocol</i> <i>Ring/Network Coupling</i>	<i>Redundant Coupling Protocol</i> <i>Ring/Network Coupling</i>
HIPER ring	<i>Sub Ring</i>	<i>Ring/Network Coupling</i>	<i>Redundant Coupling Protocol</i> <i>Ring/Network Coupling</i>
RSTP	<i>Redundant Coupling Protocol</i>	<i>Redundant Coupling Protocol</i>	<i>Dual RSTP</i>

– no suitable coupling protocol

1) with *MRP* configured on different VLANs

The menu contains the following dialogs:

- ▶ Sub Ring
- ▶ Ring/Network Coupling
- ▶ Redundant Coupling Protocol (MCSESM-E)

5.10.6.1 Sub Ring

[Switching > L2-Redundancy > FuseNet > Sub Ring]

WARNING

UNINTENDED EQUIPMENT OPERATION

To help avoid loops during the configuration phase, configure each device of the *Sub Ring* configuration individually. Before you connect the redundant lines, complete the configuration of the other devices of the ring configuration.

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

This dialog lets you set up the device as a subring manager.

The *Sub Ring* function enables you to easily couple network segments to existing redundancy rings. The subring manager (SRM) couples a subring to an existing ring (base ring).

In the subring you can use any devices that support MRP as ring participants. These devices do not require a subring manager function.

When setting up subrings, remember the following rules:

- ▶ The device supports *Link Aggregation* in the subring
- ▶ No spanning tree on subring ports
- ▶ Same *MRP domain* on devices within a subring
- ▶ Different VLANs for base ring and subring

Specify the VLAN settings as follows:

- ▶ VLAN *x* for base ring
 - on the ring ports of the base ring participants
 - on the base ring ports of the subring manager
- ▶ VLAN *y* for subring
 - on the ring ports of the subring participants
 - on the subring ports of the subring manager

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 subrings supported by the device.

Table

Sub ring ID

Displays the unique identifier of this subring.

Possible values:

- ▶ 1..8

Name

Specifies the optional name of the subring.

Possible values:

- ▶ Alphanumeric ASCII character string with 0..255 characters

Active

Activates/deactivates the subring.

Activate the subring when the configuration of every subring device is complete. Close the subring only after activating the *Sub Ring* function.

Possible values:

- ▶ *marked*
The subring is active.
- ▶ *unmarked* (default setting)
The subring is inactive.

Configuration status

Displays the operational state of the subring configuration.

Possible values:

- ▶ *noError*
The device detects an acceptable subring configuration.
- ▶ *ringPortLinkError*
 - The ring port has no link.
 - One of the subring lines is connected to one more port of the device. But the subring line is not connected to one of the ring ports of the device.
- ▶ *multipleSRM*
The subring manager receives packets from more than one subring manager in the subring.
- ▶ *noPartnerManager*
The subring manager receives its own frames.
- ▶ *concurrentVLAN*
The MRP protocol in the base ring uses the VLAN of the subring manager domain.

- ▶ *concurrentPort*
One more redundancy protocol uses the ring port of the subring manager domain.
- ▶ *concurrentRedundancy*
The subring manager domain is inactive because of one more active redundancy protocol.
- ▶ *trunkMember*
The ring port of the subring manager domain is member of a *Link Aggregation* connection.
- ▶ *sharedVLAN*
The subring manager domain is inactive because shared VLAN is active and the main ring also uses the MRP protocol.

Redundancy available

Displays the operational state of the ring redundancy in the subring.

Possible values:

- ▶ *redGuaranteed*
Redundancy reserve is available.
- ▶ *redNotGuaranteed*
Loss of redundancy reserve.

Port

Specifies the port that connects the device to the subring.

Possible values:

- ▶ *<Port number>*

SRM mode

Specifies the mode of the subring manager.

A subring has 2 managers simultaneously that couple the subring to the base ring. As long as the subring is physically closed, one manager blocks its subring port.

Possible values:

- ▶ *manager* (default setting)
The subring port forwards data packets.
When this value is set on both devices that couple the subring to the base ring, the device with the higher MAC address functions as the *redundantManager*.
- ▶ *redundantManager*
The subring port is blocked while the subring is physically closed. If the subring is interrupted, then the subring port transmits the data packets.
When this value is set on both devices that couple the subring to the base ring, the device with the higher MAC address functions as the *redundantManager*.
- ▶ *singleManager*
Use this value when the subring is coupled to the base ring via one single device. The prerequisite is that there are 2 instances of the subring in the table. Assign this value to both instances. The subring port of the instance with the higher port number is blocked while the subring is physically closed.

SRM status

Displays the current mode of the subring manager.

Possible values:

- ▶ *manager*
The subring port forwards data packets.
- ▶ *redundantManager*
The subring port is blocked while the subring is physically closed. If the subring is interrupted, then the subring port transmits the data packets.
- ▶ *singleManager*
The subring is coupled to the base ring via one single device. The subring port of the instance with the higher port number is blocked while the subring is physically closed.
- ▶ *disabled*
The subring is inactive.

Port status

Displays the connection status of the subring port.

Possible values:

- ▶ *forwarding*
The port is passing frames according to the forwarding behavior of IEEE 802.1D.
- ▶ *disabled*
The port is dropping every frame.
- ▶ *blocked*
The port is dropping every frame with the exception of the following cases:
 - The port passes frames used by the selected ring protocol specified to pass blocked ports.
 - The port passes frames from other protocols specified to pass blocked ports.
- ▶ *not-connected*
The port link is down.

VLAN

Specifies the VLAN to which this subring is assigned. If no VLAN exists under the VLAN ID entered, then the device automatically creates it.

Possible values:

- ▶ Available configured VLANs (default setting: 0)
If you do not want to use a separate VLAN for this subring, then you leave the entry as 0.

Partner MAC

Displays the MAC address of the subring manager at the other end of the subring.

MRP domain

Specifies the MRP domain of the subring manager. Assign the same MRP domain name to every member of a subring. If you only use Schneider Electric devices, then you use the default value for the MRP domain; otherwise adjust this value if necessary. With multiple subrings, the function lets you use the same MRP domain name for the subrings.

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:

- ▶ `iec-62439-mrp`

Buttons

You find the description of the standard buttons in section [“Buttons” on page 17](#).

5.10.6.2 Ring/Network Coupling

[Switching > L2-Redundancy > FuseNet > Ring/Network Coupling]

WARNING

UNINTENDED EQUIPMENT OPERATION

To help avoid loops during the configuration phase, configure each device of the *Ring/Network Coupling* configuration individually. Before you connect the redundant lines, complete the configuration of the other devices of the ring configuration.

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

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 Schneider Electric devices.

Note: With two-switch coupling, verify that you have configured a HIPER ring, MRP ring, or Fast HIPER ring before configuring the *Ring/Network Coupling* function.

In the *Ring/Network Coupling* dialog, you can perform the following tasks:

- ▶ display an overview of the existing *Ring/Network Coupling*
- ▶ configure a *Ring/Network Coupling*
- ▶ create a new *Ring/Network Coupling*
- ▶ delete *Ring/Network Coupling*
- ▶ enable/disable *Ring/Network Coupling*

When configuring the coupling ports, specify the following settings in the *Basic Settings > Port* dialog:

Port type	Bit rate	Port on	Automatic configuration	Manual configuration
TX	100 Mbit/s	marked	unmarked	100 Mbit/s FDX
TX	1 Gbit/s	marked	marked	–
Optical	100 Mbit/s	marked	unmarked	100 Mbit/s FDX
Optical	1 Gbit/s	marked	marked	–
Optical	2.5 Gbit/s	marked	–	2.5 Gbit/s FDX

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

If you configured VLANs, then note the VLAN configuration of the coupling and partner coupling ports. In the *Ring/Network Coupling* configuration, select the following values for the coupling and partner coupling ports:

- ▶ VLAN ID 1 and *Ingress filtering* disabled in the port table
- ▶ VLAN membership T in the *VLAN Configuration* table

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 the VLAN ID `1` and the highest VLAN priority `7`. If the forwarding port is a member in VLAN `1` and transmits the data packets without a VLAN tag, then the device also sends test packets.

Operation

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.

Mode

Type

Specifies the method used to couple the networks together.

Possible values:

- ▶ *one-switch coupling*
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, slave*
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 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 configured 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 disabled the coupling port, the *Port on* checkbox is unmarked in the *Basic Settings > Port* dialog, *Configuration* tab.

State

Displays the status of the selected port.

Possible values:

- ▶ *active*
The port is active.
- ▶ *standby*
The port is in stand-by mode.
- ▶ *not-connected*
The port is not connected.
- ▶ *not-applicable*
The port is incompatible with the configured control mode.

Partner coupling port

Port

Specifies the port on which you connect the partner port.

Possible values:

- ▶ -
No port selected.
- ▶ `<Port number>`

If you also have configured ring ports, then specify the coupling and ring ports on different ports.

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 configured control mode.

IP address

Displays the IP address of the partner, when the devices are connected.

The prerequisite is that you select a two-switch coupling method and enable the partner in the network.

Control port

Port

Displays the port on which you connect the control line.

Possible values:

- ▶ -
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 configured 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 down between the devices in the connected network, then the standby device keeps the redundant port in the standby mode.
- ▶ *extended redundancy*
The main line and the redundant line are active simultaneously. If the device detects a problem in the connection between the devices in the connected network, then the standby device forwards data on the redundant port. With the setting you can 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*
The device couples redundant rings. The device lets you couple rings that use the following redundancy protocols:
 - HIPER ring
 - Fast HIPER ring
 - MRP ring
- ▶ *network coupling*
The device couples network segments. The function lets you couple mesh and bus networks together.

Information

Redundancy available

Displays if the redundancy is available.

When a component of the ring is down, the redundant line takes over its function.

Possible values:

- ▶ *redGuaranteed*
The redundancy is available.
- ▶ *redNotGuaranteed*
The redundancy is unavailable.

Configuration failure

You have configured 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.

Buttons

You find the description of the standard buttons in section “Buttons” on page 17.

Reset

Disables the redundancy function and resets the parameters in the dialog to the default setting.

5.10.6.3 Redundant Coupling Protocol (MCSESM-E)

[Switching > L2-Redundancy > FuseNet > RCP]

WARNING

UNINTENDED EQUIPMENT OPERATION

To help avoid loops during the configuration phase, configure each device of the *RCP* configuration individually. Before you connect the redundant lines, complete the configuration of the other devices of the ring configuration.

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

WARNING

LOOP HAZARD

- ▶ Configure each device of the *RCP* and *Dual RSTP* configuration individually. Before you connect the redundant lines, complete the configuration of the other devices of the ring configuration.
- ▶ Configure the timeout in the *RCP* coupling configuration longer than the longest assumable interruption time for the faster instance of the redundancy protocol.
- ▶ In a topology with 2 coupling bridges, configure the coupling roles of the two devices only as *master*, *slave* or *auto*.
- ▶ Couple the primary and the secondary instance only by means of 1 *RCP* bridge (for a topology with 1 *RCP* bridge) or by means of 2 *RCP* bridges (for a topology with 2 *RCP* bridges). Keep the ports of the primary instance separated from the ports of each secondary instance.
- ▶ Activate the *Admin edge port* setting on a port only in cases where a terminal device is connected to the port.

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

A ring topology provides short transition times with a minimal use of resources. However, to couple these rings redundantly to a higher-level network is more of a challenge.

When you want to use a standard protocol such as MRP for the ring redundancy and RSTP to couple the rings together, the *Redundant Coupling Protocol* helps provide options for you.

Do not use the following redundancy protocols on the ports of the *RCP* primary ring and the *RCP* secondary rings:

- ▶ *Sub Ring*
- ▶ *Ring/Network Coupling*

If you want to use RSTP for the primary and secondary rings, then the *RCP* function assigns the ports of the secondary ring to the *Dual RSTP* instance. This creates two independent RSTP networks coupled by *RCP*. You specify the settings of the *Dual RSTP* function in the *Switching > L2-Redundancy* dialog.

If you configure the *RCP* function in a network and the configuration is not completed, it is possible that the devices temporarily disconnect the secondary ring and the primary ring. In this case, the device management of the *RCP* bridges cannot be reached from the secondary ring. During this configuration phase, connect your management station to the primary ring.

Operation

Operation

Enables/disables the *RCP* function.

Possible values:

- ▶ *On*
The *RCP* function is enabled.
- ▶ *off* (default setting)
The *RCP* function is disabled.

Primary ring/network / Secondary ring/network

If the device operates as slave (value in the *Role* field is *slave*), then do not activate the *Static query port* mode for the ports on the secondary ring/network.

Inner port

Specifies the inner port number in the primary ring/secondary ring. The port is directly connected to the partner bridge.

Possible values:

- ▶ - (default setting)
No port selected.
- ▶ <Port number>

Outer port

Specifies the outer port number in the primary ring/secondary ring.

Possible values:

- ▶ - (default setting)
No port selected.
- ▶ <Port number>

Primary Ring protocol/Secondary Ring protocol

Displays the protocol that is active on the redundant coupling port in the devices in the primary/secondary ring.

Coupler configuration

Role

Specifies the role of the local device.

Possible values:

- ▶ *master*
The device operates as master.

- ▶ *slave*
The device operates as slave.
- ▶ *single*
The device couples 2 RSTP networks with a *Dual RSTP* instance using one bridge.
- ▶ *auto* (default setting)
The device automatically selects its role as *master* or *slave*.

Current role

Displays the current role of the local device. The value can be different from the configured role:

- ▶ If you configured both partner bridges as *auto*, then the partner bridge that is currently coupling the instances takes the *master* role. The other partner bridge takes the *slave* role.
- ▶ If both partner bridges are configured as *master* or both as *slave*, then the partner bridge with the smaller Basis MAC address takes the *master* role. The other partner bridge takes the *slave* role.
- ▶ If the protocol is started and the partner bridge cannot be found for a bridge in the configured role *master*, *slave* or *auto*, then the bridge sets its own role to *listening*.
- ▶ If the device detects a configuration problem for example, the inner ring ports are connected crosswise, then the device sets its role to *error*.

Timeout [ms]

Specifies the maximum time, in milliseconds, during which the slave device waits for test packets from the master device on the outer ports before the slave device takes over the coupling. This only applies in the state in which both inner ports of the slave device have lost the connection to the master device.

Configure the timeout longer than the longest assumable interruption time for the redundancy protocol of the faster instance. Otherwise, loops can occur.

Possible values:

- ▶ *5..60000* (default setting: *45*)

Partner MAC address

Displays the basic MAC address of the partner device.

Partner IP address

Displays the IP address of the partner device.

Coupling state

Displays the coupling state of the local device.

Possible values:

- ▶ *forwarding*
The coupling state of the port is forwarding.
- ▶ *blocking*
The coupling state of the port is blocking.

Redundancy state

Displays if the redundancy is available.

For a master-slave configuration, both bridges display this information.

Possible values:

- ▶ *redAvailable*
The redundancy is available.
- ▶ *redNotAvailable*
The redundancy is unavailable.

Buttons

You find the description of the standard buttons in section [“Buttons” on page 17](#).

6 Diagnostics

The menu contains the following dialogs:

- ▶ Status Configuration
- ▶ System
- ▶ Email Notification
- ▶ Syslog
- ▶ Ports
- ▶ Loop Protection
- ▶ LLDP
- ▶ 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 in order to present its condition in graphic form.

The device displays its current status as *error* or *ok* in the *Device status* frame. The device determines this status from the individual monitoring results.

The device displays detected faults in the *Status* tab and also in the *Basic Settings > System* dialog, *Device Status* frame.

The dialog contains the following tabs:

- ▶ [Global]
- ▶ [Port]
- ▶ [Status]

[Global]

Device status

Device status

Displays the current status of the device. The device determines the status from the individual monitored parameters.

Possible values:

- ▶ *error*
The device displays this value to indicate a detected error in one of the monitored parameters.
- ▶ *ok*

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.
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.

The prerequisite for sending SNMP traps is that you enable the function in the *Diagnostics > Status Configuration > Alarms (Traps)* dialog and specify at least one trap destination.

Table

Temperature

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

Possible values:

- ▶ `marked` (default setting)
Monitoring is active.
If the temperature exceeds or falls below the specified limit, then in the *Device status* frame, the value changes to *error*.
- ▶ `unmarked`
Monitoring is inactive.

You specify the temperature thresholds in the *Basic Settings > System* dialog, *Upper temp. limit [°C]* field and *Lower temp. limit [°C]* field.

Ring redundancy

Activates/deactivates the monitoring of the ring redundancy.

Possible values:

- ▶ `marked`
Monitoring is active.
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.

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.

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.

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.

Buttons

You find the description of the standard buttons in section “Buttons” on page 17.

[Port]

Table

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.

Buttons

You find the description of the standard buttons in section “Buttons” on page 17.

[Status]

Table

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.

Buttons

You find the description of the standard buttons in section “Buttons” on page 17.

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:

- ▶ *error*
The device displays this value to indicate a detected error in one of the monitored parameters.
- ▶ *ok*

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.
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.

The prerequisite for sending SNMP traps is that you enable the function in the *Diagnostics > Status Configuration > Alarms (Traps)* dialog and specify at least one trap destination.

Table

Password default settings unchanged

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

Possible values:

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

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

Min. password length < 8

Activates/deactivates the monitoring of the `Min. password length` policy.

Possible values:

- ▶ `marked` (default setting)
Monitoring is active.
If the value for the `Min. password length` policy is less than 8, then in the `Security status` frame, the value changes to `error`.
- ▶ `unmarked`
Monitoring is inactive.

You specify the `Min. password length` policy in the `Device Security > User Management` dialog in the `Configuration` frame.

Password policy settings deactivated

Activates/deactivates the monitoring of the Password policies settings.

Possible values:

- ▶ `marked` (default setting)
Monitoring is active.
If the value for at least one of the following policies is less than 1, then in the `Security status` frame, the value changes to `error`.
 - `Upper-case characters (min.)`
 - `Lower-case characters (min.)`
 - `Digits (min.)`
 - `Special characters (min.)`
- ▶ `unmarked`
Monitoring is inactive.

You specify the policy settings in the `Device Security > User Management` dialog in the `Password policy` frame.

User account password policy check deactivated

Activates/deactivates the monitoring of the *Policy check* function.

Possible values:

▶ *marked*

Monitoring is active.

If the *Policy check* function is inactive for at least one user account, then in the *Security status* frame, the value changes to *error*.

▶ *unmarked* (default setting)

Monitoring is inactive.

You activate the *Policy check* function in the *Device Security > User Management* dialog.

Telnet server active

Activates/deactivates the monitoring of the Telnet server.

Possible values:

▶ *marked* (default setting)

Monitoring is active.

If you enable the Telnet server, then in the *Security status* frame, the value changes to *error*.

▶ *unmarked*

Monitoring is inactive.

You enable/disable the Telnet server in the *Device Security > Management Access > Server* dialog, *Telnet* tab.

HTTP server active

Activates/deactivates the monitoring of the HTTP server.

Possible values:

▶ *marked* (default setting)

Monitoring is active.

If you enable the HTTP server, then in the *Security status* frame, the value changes to *error*.

▶ *unmarked*

Monitoring is inactive.

You enable/disable the HTTP server in the *Device Security > Management Access > Server* dialog, *HTTP* tab.

SNMP unencrypted

Activates/deactivates the monitoring of the SNMP server.

Possible values:

▶ **marked** (default setting)

Monitoring is active.

If at least one of the following conditions applies, then in the *Security status* frame, the value changes to *error*:

- The *SNMPv1* function is enabled.
- The *SNMPv2* function is enabled.
- The encryption for SNMPv3 is disabled.

You enable the encryption in the *Device Security > User Management* dialog, in the *SNMP encryption type* column.

▶ **unmarked**

Monitoring is inactive.

You specify the settings for the SNMP agent in the *Device Security > Management Access > Server* dialog, *SNMP* tab.

Access to system monitor with serial interface possible

Activates/deactivates the monitoring of the system monitor.

When the system monitor is activated, you have the possibility to change to the system monitor via a serial connection.

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 Ethernet Switch Configurator possible

Activates/deactivates the monitoring of the Ethernet Switch Configurator function.

Possible values:

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

You enable/disable the Ethernet Switch Configurator function in the *Basic Settings > Network* 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 *Industrial Protocols > IEC61850-MMS* dialog, *Operation* frame.

Self-signed HTTPS certificate present

Activates/deactivates the monitoring of the HTTPS certificate.

Possible values:

- ▶ *marked* (default setting)

Monitoring is active.

If the HTTPS server uses a self-created digital certificate, then in the *Security status* frame, the value changes to *error*.

- ▶ *unmarked*

Monitoring is inactive.

Modbus TCP active

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

Possible values:

- ▶ *marked* (default setting)

Monitoring is active.

If you enable the *Modbus TCP* function, then in the *Security status* frame, the value changes to *error*.

- ▶ *unmarked*

Monitoring is inactive.

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

EtherNet/IP active

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

Possible values:

- ▶ *marked* (default setting)

Monitoring is active.

If you enable the *EtherNet/IP* function, then in the *Security status* frame, the value changes to *error*.

- ▶ *unmarked*

Monitoring is inactive.

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

Buttons

You find the description of the standard buttons in section “Buttons” on page 17.

[Port]

Table

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.

Buttons

You find the description of the standard buttons in section “Buttons” on page 17.

[Status]

Table

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.

Buttons

You find the description of the standard buttons in section [“Buttons” on page 17](#).

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 in the *Mode* drop-down list you select the *Manual setting* item.

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.
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.

The prerequisite for sending SNMP traps is that you enable the function in the *Diagnostics > Status Configuration > Alarms (Traps)* dialog and specify at least one trap destination.

Monitoring correct operation

In the table you specify the parameters that the device monitors. The device signals the occurrence of an event by opening the signal contact.

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 / falls below the threshold values, then the signal contact opens.
- ▶ **unmarked**
Monitoring is inactive.

You specify the temperature thresholds in the **Basic Settings > System** dialog, **Upper temp. limit [°C]** field and **Lower temp. limit [°C]** field.

Ring redundancy

Activates/deactivates the monitoring of the ring redundancy.

Possible values:

- ▶ **marked**
Monitoring is active.
The signal contact opens in the following situations:
 - The redundancy function becomes active (loss of redundancy reserve).
 - The device is a normal ring participant and detects an error in its settings.
- ▶ **unmarked** (default setting)
Monitoring is inactive.

External memory removed

Activates/deactivates the monitoring of the active external memory.

Possible values:

- ▶ **marked**
Monitoring is active.
If you remove the active external memory from the device, then the signal contact opens.
- ▶ **unmarked** (default setting)
Monitoring is inactive.

External memory not in sync with NVM

Activates/deactivates the monitoring of the configuration profile in the device and in the external memory.

Possible values:

- ▶ `marked`
Monitoring is active.
The signal contact opens in the following situations:
 - The configuration profile only exists in the device.
 - The configuration profile in the device differs from the configuration profile in the external memory.
- ▶ `unmarked` (default setting)
Monitoring is inactive.

Ethernet loops

Activates/deactivates the monitoring of layer 2 Ethernet loops. You specify the settings for the *Loop Protection* function in the *Diagnostics > Loop Protection* dialog.

Possible values:

- ▶ `marked`
Monitoring is active.
If the device has detected an Ethernet loop, then the signal contact opens.
- ▶ `unmarked` (default setting)
Monitoring is inactive.

Power supply

Activates/deactivates the monitoring of the power supply unit.

Possible values:

- ▶ `marked` (default setting)
Monitoring is active.
If the device has a detected power supply fault, then the signal contact opens.
- ▶ `unmarked`
Monitoring is inactive.

Buttons

You find the description of the standard buttons in section “Buttons” on page 17.

[Port]**Table**

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.

Buttons

You find the description of the standard buttons in section “Buttons” on page 17.

[Status]**Table**

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.

Buttons

You find the description of the standard buttons in section “Buttons” on page 17.

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. 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* (default setting: 30)

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

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.
- ▶ *unmarked* (default setting)
The *MAC Notification* function is inactive on the port.

The prerequisite for sending SNMP traps is that you enable the function in the *Diagnostics > Status Configuration > Alarms (Traps)* dialog and specify at least one trap destination.

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.

Buttons

You find the description of the standard buttons in section “Buttons” on page 17.

6.1.5 Alarms (Traps)

[Diagnostics > Status Configuration > Alarms (Traps)]

The device lets you send an SNMP trap as a reaction to specific events. In this dialog you specify the trap destinations to which the device sends the SNMP traps.

The events for which the device triggers an SNMP trap, you specify, for example, in the following dialogs:

- ▶ in the *Diagnostics > Status Configuration > Device Status* dialog
- ▶ in the *Diagnostics > Status Configuration > Security Status* dialog
- ▶ in the *Diagnostics > Status Configuration > MAC Notification* dialog

Operation

Operation

Enables/disables the sending of SNMP traps to the trap destinations.

Possible values:

- ▶ *On* (default setting)
The sending of SNMP traps is enabled.
- ▶ *Off*
The sending of SNMP traps is disabled.

Table

Name

Specifies the name of the trap destination.

Possible values:

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

Address

Specifies the IP address and the port number of the trap destination.

Possible values:

- ▶ `<Valid IPv4 address>:<port number>`

Active

Activates/deactivates the sending of SNMP traps to this trap destination.

Possible values:

- ▶ *marked* (default setting)
The sending of SNMP traps to this trap destination is active.
- ▶ *unmarked*
The sending of SNMP traps to this trap destination is inactive.

Buttons

You find the description of the standard buttons in section “Buttons” on page 17.



Opens the *Create* window to add a new entry to the table.

- ▶ In the *Name* field you specify a name for the trap destination.
- ▶ In the *Address* field you specify the IP address and the port number of the trap destination. If you choose not to enter a port number, then the device automatically adds the port number 162.

6.2 System

[Diagnostics > System]

The menu contains the following dialogs:

- ▶ System Information
- ▶ Hardware State
- ▶ IP Address Conflict Detection
- ▶ ARP
- ▶ Selftest

6.2.1 System Information

[Diagnostics > System > System Information]

This dialog displays the current operating condition of individual components in the device. The displayed values are a snapshot; they represent the operating condition at the time the dialog was loaded to the page.

Buttons

You find the description of the standard buttons in section [“Buttons” on page 17](#).

Save system information

Opens the HTML page in a new web browser window or tab. You can save the HTML page on your PC using the appropriate web browser command.

6.2.2 Hardware State

[Diagnostics > System > Hardware State]

This dialog provides information about the distribution and state of the flash memory of the device.

Information

Uptime

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

Flash region

Displays the name of the respective memory area.

Description

Displays a description of what the device uses the memory area for.

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.

Buttons

You find the description of the standard buttons in section [“Buttons” on page 17](#).

6.2.3 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.

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 traffic 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: 3)

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..5000 (default setting: 200)

Send trap

Activates/deactivates the sending of SNMP traps when the device detects an address conflict.

Possible values:

- ▶ `marked`
The sending of SNMP traps is active.
If the device detects an address conflict, then the device sends an SNMP trap.
- ▶ `unmarked` (default setting)
The sending of SNMP traps is inactive.

The prerequisite for sending SNMP traps is that you enable the function in the [Diagnostics > Status Configuration > Alarms \(Traps\)](#) dialog and specify at least one trap destination.

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.

Table

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.

Buttons

You find the description of the standard buttons in section [“Buttons” on page 17](#).

6.2.4 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 the IPv6 protocol, addresses of the neighboring devices are obtained with the use of the Neighbor Discovery Protocol (NDP).

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.

Buttons

You find the description of the standard buttons in section [“Buttons” on page 17](#).

Reset ARP table

Removes the dynamically set up addresses from the ARP table.

6.2.5 Selftest

[Diagnostics > System > Selftest]

This dialog lets you do the following:

- ▶ Activate/deactivate the RAM test when the device is being started.
- ▶ Enable/disable the option of entering the system monitor upon the system start.
- ▶ Specify how the device behaves in the case of a detected error.

Configuration

If the device does not detect any readable configuration profile when restarting, then the following settings block your access to the device permanently.

- ▶ *SysMon1 is available* checkbox is *unmarked*.
- ▶ *Load default config on error* checkbox is *unmarked*.

This is the case, for example, if the password of the configuration profile that you are loading differs from the password set in the device. To have the device unlocked again, contact your sales partner.

RAM test

Activates/deactivates the RAM memory check during the restart.

Possible values:

- ▶ *marked* (default setting)
The RAM memory check is activated. During the restart, the device checks the RAM memory.
- ▶ *unmarked*
The RAM memory check is deactivated. This shortens the start time for the device.

SysMon1 is available

Activates/deactivates the access to the system monitor during the restart.

Possible values:

- ▶ *marked* (default setting)
The device lets you open the system monitor during the restart.
- ▶ *unmarked*
The device starts without the option of opening 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. Upon restart, the device loads the default settings.

Table

In this table you specify how the device behaves in the case of a detected error.

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:

- ▶ `reboot` (default setting)
The device triggers a restart.
- ▶ `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 for sending SNMP traps is that you enable the function in the [Diagnostics > Status Configuration > Alarms \(Traps\)](#) dialog and specify at least one trap destination.

Buttons

You find the description of the standard buttons in section “Buttons” on page 17.

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.

Certificate

The device can send messages to a server over unsecured networks. To help deny a “man in the middle” attack, request that the Certificate Authority creates a certificate for the server. Configure the server to use the certificate. Transfer the certificate onto the device.

If you specify the settings for the mail servers, then use the IP address or DNS name provided as *Common Name* or *Subject Alternative Name* in the certificate. Otherwise the certificate validation will be unsuccessful.

URL


Specifies the path and file name of the certificate.

The device accepts certificates with the following properties:

- X.509 format
- .PEM file name extension
- Base64-coded, enclosed by
-----BEGIN CERTIFICATE-----
and
-----END CERTIFICATE-----

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

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

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

▶ Import from a TFTP server

When the certificate is on a TFTP server, specify the URL for the file in the following form:

`tftp://<IP address>/<path>/<file name>`

▶ Import from an SCP or SFTP server

When the certificate is on an SCP or SFTP server, you specify the URL for the file in the following form:

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

When you click the *Start* button, the device displays the *Credentials* window. There you enter *User name* and *Password*, to log in to the server.

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

Start

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

Sender

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

Notification immediate

Here you specify the settings for emails which the device sends immediately.

Severity

Specifies the minimum severity of events for which the device immediately sends an email. If an event of this severity occurs, or of a more urgent severity, then the device sends an email to the recipients.

Possible values:

- ▶ *emergency*
- ▶ *alert* (default setting)
- ▶ *critical*
- ▶ *error*
- ▶ *warning*
- ▶ *notice*
- ▶ *informational*
- ▶ *debug*

Subject

Specifies the subject of the email.

Possible values:

- ▶ Alphanumeric ASCII character string with 0..255 characters

Notification periodic

Here you specify the settings for emails which the device sends periodically.

Severity

Specifies the minimum severity of events for which the device periodically sends an email. If an event of this severity occurs, or of a more urgent severity, then the device registers the event in the buffer. The device sends the buffer content periodically or when the buffer overflows.

If an event of a less urgent severity occurs, then the device does not register the event in the buffer.

Possible values:

- ▶ *emergency*
- ▶ *alert*
- ▶ *critical*
- ▶ *error*
- ▶ *warning* (default setting)
- ▶ *notice*
- ▶ *informational*
- ▶ *debug*

Subject

Specifies the subject of the email.

Possible values:

- ▶ Alphanumeric ASCII character string with 0..255 characters

Sending interval [min]

Specifies the send interval in minutes.

If the device has registered at least one event, then the device sends an email with the log file after the time expires.

Possible values:

- ▶ *30..1440* (default setting: *30*)

Send

Sends an email immediately with the buffer content and clears the buffer.

Information

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.

Buttons

You find the description of the standard buttons in section [“Buttons” on page 17](#).

Clear email notification statistics

Resets the counters in the *Information* frame to 0.

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	Informal 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

Index

Displays the index number to which the table entry relates.

Notification type

Specifies if the device sends the emails to this recipient immediately or periodically.

Possible values:

- ▶ *immediate*
The device sends the emails to this recipient immediately.
- ▶ *periodic*
The device sends the emails to this recipient periodically.

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* (default setting)
The informing of the recipient is active.
- ▶ *unmarked*
The informing of the recipient is inactive.

Buttons

You find the description of the standard buttons in section [“Buttons” on page 17](#).

6.3.3 Email Notification Mail Server

[Diagnostics > Email Notification > Mail Server]

In this dialog you specify the settings for the mail servers. The device supports encrypted and unencrypted connections to the mail server.

Table

Index

Displays the index number to which the table entry relates.

Description

Specifies the name of the server.

Possible values:

- ▶ Alphanumeric ASCII character string with 0..255 characters

IP address

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

Possible values:

- ▶ Valid IPv4 address (default setting: 0.0.0.0)
- ▶ DNS name in the format `domain.tld` or `host.domain.tld`
If you specify a DNS name, then also enable the *Client* function in the *Advanced > DNS > Client > Global* dialog.
If you establish encrypted connections using the certificate, then verify that the DNS name is equal to the server DNS name mentioned in the certificate.

Destination TCP port

Specifies the TCP port of the server.

Possible values:

- ▶ 1..65535 (default setting: 25)
Exception: Port 2222 is reserved for internal functions.

Frequently used TCP-Ports:

- SMTP 25
- Message Submission 587

Encryption

Specifies the protocol which encrypts the connection between the device and the mail server.

Possible values:

- ▶ none (default setting)
The device establishes an 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.

Buttons

You find the description of the standard buttons in section “Buttons” on page 17.

Connection test

Opens the *Connection test* dialog to send a test email.

If the mail server settings are correct, then the selected recipients receive a test email.

- ▶ In the *Recipient* field, you specify to which recipients the device sends the test email:
 - *immediate*
The device sends the test email to the recipients to which the device sends emails immediately.
 - *periodic*
The device sends the test email to the recipients to which the device sends emails periodically.
- ▶ In the *Message text* field, you specify the text of the test email.

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.

Certificate

The device can send messages to a server over unsecured networks. To help deny a “man in the middle” attack, request that the Certificate Authority creates a certificate for the server. Configure the server to use the certificate. Transfer the certificate onto the device.

If you specify the parameters on the server, then verify that you specify the IP address and DNS name provided in the certificate as the Common Name or Subject Alternative Name. Otherwise the certificate validation will be unsuccessful.

Note: In order for the changes to take effect after loading a new certificate, restart the *Syslog* function.

URL


Specifies the path and file name of the certificate.

The device accepts certificates with the following properties:

- X.509 format
- .PEM file name extension
- Base64-coded, enclosed by
-----BEGIN CERTIFICATE-----
and
-----END CERTIFICATE-----

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

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

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

Start

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

Table

Index

Displays the index number to which the table entry relates.

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

Possible values:

- ▶ 1..8

IP address

Specifies the IP address of the syslog server.

Possible values:

- ▶ Valid IPv4 address (default setting: 0.0.0.0)
- ▶ Valid IPv6 address
- ▶ Hostname

Destination UDP port

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

Possible values:

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

Transport type

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

Possible values:

- ▶ `udp` (default setting)
The device sends the events over the UDP port specified in the *Destination UDP port* column.
- ▶ `tls`
The device sends the events over TLS on the TCP port specified in the *Destination UDP port* column.

Min. severity

Specifies the minimum severity of the events. The device sends a log entry for events with this severity and with more urgent severities to the syslog server.

Possible values:

- ▶ `emergency`
- ▶ `alert`
- ▶ `critical`
- ▶ `error`
- ▶ `warning` (default setting)
- ▶ `notice`
- ▶ `informational`
- ▶ `debug`

Type

Specifies the type of the log entry transmitted by the device.

Possible values:

- ▶ `systemlog` (default setting)
- ▶ `audittrail`

Active

Activates/deactivates the transmission of events to the syslog server:

- ▶ `marked`
The device sends events to the syslog server.
- ▶ `unmarked` (default setting)
The transmission of events to the syslog server is deactivated.

Buttons

You find the description of the standard buttons in section [“Buttons” on page 17.](#)

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.

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.

Buttons

You find the description of the standard buttons in section [“Buttons”](#) on page 17.

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 an open circuit in the cable, it also displays the estimated distance to the problem.

To receive dependable results, use the *TP cable diagnosis* function for twisted pair cables with a minimum length of 3 meters.

Note: This test interrupts traffic on the port.

Information


Port

Displays the port number.

Status

Status of the Virtual Cable Tester.

Possible values:

- ▶ *active*
Cable testing is in progress.
To start the test, click the  button and then the *Start cable diagnosis...* item. This action opens the *Select port* dialog.
- ▶ *success*
The device displays this entry after performing a successful test.
- ▶ *failure*
The device displays this entry after an interruption in the test.
- ▶ *uninitialized*
The device displays this entry while in standby.

Table

Cable pair

Displays the cable pair to which this entry 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 deactivated, 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.

Buttons

You find the description of the standard buttons in section “Buttons” on page 17.

Start cable diagnosis...

Opens the *Select port* dialog.

In 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.

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 *Operation* function in the *Port Monitor* 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

Port

Displays the port number.

Link flap on

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

Possible values:

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

CRC/Fragments on

Activates/deactivates the monitoring of CRC/fragment errors detected on the port.

Possible values:

- ▶ `marked`
Monitoring is active.
 - The *Port Monitor* function monitors CRC/fragment errors detected on the port.
 - If the device detects too many CRC/fragment errors, then the device executes the action specified in the *Action* column.
 - On the *CRC/Fragments* tab, specify the parameters to be monitored.
- ▶ `unmarked` (default setting)
Monitoring is inactive.

Duplex mismatch detection active

Activates/deactivates the monitoring of duplex mismatches on the port.

Possible values:

- ▶ `marked`
Monitoring is active.
 - The *Port Monitor* function monitors duplex mismatches on the port.
 - If the device detects a duplex mismatch, then the device executes the action specified in the *Action* column.
- ▶ `unmarked` (default setting)
Monitoring is inactive.

Overload detection on

Activates/deactivates the overload detection on the port.

Possible values:

- ▶ *marked*
Monitoring is active.
 - The *Port Monitor* function monitors the data load on the port.
 - If the device detects a data overload on the port, then the device executes the action specified in the *Action* column.
 - On the *Overload detection* tab, specify the parameters to be monitored.
- ▶ *unmarked* (default setting)
Monitoring is inactive.

Link speed/Duplex mode detection on

Activates/deactivates the monitoring of the link speed and duplex mode on the port.




Possible values:

- ▶ *marked*
Monitoring is active.
 - The *Port Monitor* function monitors the link speed and duplex mode on the port.
 - If the device detects an unpermitted combination of link speed and duplex mode, then the device executes the action specified in the *Action* column.
 - On the *Link speed/Duplex mode detection* tab, specify the parameters to be monitored.
- ▶ *unmarked* (default setting)
Monitoring is inactive.

Active condition

Displays the monitored parameter that led to the action on the port.


Possible values:

- ▶ -
No monitored parameter.
The device does not carry out any action.
- ▶ *Link flap*
Too many link changes during the observed period. 
- ▶ *CRC/Fragments*
Too many CRC/fragment errors detected during the observed period. 
- ▶ *Duplex mismatch*
Duplex mismatch detected.
- ▶ *Overload detection*
Overload detected during the observed period. 
- ▶ *Link speed/Duplex mode detection*
Impermissible combination of speed and duplex mode detected.

Action

Specifies the action that the device carries out if the *Port Monitor* function detects that the parameters have been exceeded.

Possible values:

- ▶ *disable port*
The device disables the port and sends an SNMP trap.
The “Link status” LED for the port flashes 3× per period.
 - To re-enable the port, highlight the port and click the  button and then the *Reset* item.
 - 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 for sending SNMP traps is that you enable the function in the *Diagnostics > Status Configuration > Alarms (Traps)* dialog and specify at least one trap destination.
- ▶ *auto-disable* (default setting)
The device disables the port and sends an SNMP trap.
The “Link status” LED for the port flashes 3× per period.
The prerequisite is that on the *Auto-disable* tab the checkbox for the monitored parameter is marked.
 - The *Diagnostics > Ports > Auto-Disable* dialog displays which ports are currently disabled due to the parameters being exceeded.
 - The *Auto-Disable* function reactivates the port automatically. For this you go to the *Diagnostics > Ports > Auto-Disable* dialog and specify a waiting period for the relevant port in the *Reset timer [s]* column.

Port status

Displays the operating state of the port.

Possible values:

- ▶ *up*
The port is enabled.
- ▶ *down*
The port is disabled.
- ▶ *notPresent*
Physical port unavailable.

Buttons

You find the description of the standard buttons in section “Buttons” on page 17.

Reset

Enables the port highlighted in the table again and resets its counter to 0. 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

[Auto-disable]

In this tab you activate the *Auto-Disable* function for the parameters monitored by the *Port Monitor* function.

Table

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.

Buttons

You find the description of the standard buttons in section “Buttons” on page 17.

Reset

Enables the port highlighted in the table again and resets its counter to 0. 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

[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

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.

Buttons

You find the description of the standard buttons in section “Buttons” on page 17.

Reset

Enables the port highlighted in the table again and resets its counter to 0. 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

[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

Port

Displays the port number.

Sampling interval [s]

Specifies in seconds, the period during which the *Port Monitor* function monitors a parameter to detect discrepancies.

Possible values:

- ▶ 5..180 (default setting: 10)

CRC/Fragments count [ppm]

Specifies the detected fragment error rate (in parts per million).

If the *Port Monitor* function detects this fragment error rate in the monitored period, then the device performs the specified action.

Possible values:

- ▶ 1..1000000 (default setting: 1000)

Last active interval [ppm]

Displays the fragment error rate that the device has detected during the period that has elapsed.

Total [ppm]

Displays the fragment error rate that the device has detected since the port was enabled.

Buttons

You find the description of the standard buttons in section “Buttons” on page 17.

Reset

Enables the port highlighted in the table again and resets its counter to 0. 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

[Overload detection]

In this tab you specify individually for every port the following settings:

- ▶ The load threshold values.
- ▶ The period during which the *Port Monitor* function monitors a parameter to detect discrepancies.

You also see the number of data packets that the device has detected up to now.

The *Port Monitor* function monitors those ports for which the checkbox in the *Overload detection on* column is marked on the *Global* tab.

The *Port Monitor* function does not monitor any ports that are members of a link aggregation group.

Table

Port

Displays the port number.

Traffic type

Specifies the type of data packets that the device considers when monitoring the load on the port.

Possible values:

- ▶ *all*
The *Port Monitor* function monitors Broadcast, Multicast and Unicast packets.
- ▶ *bc* (default setting)
The *Port Monitor* function monitors only Broadcast packets.
- ▶ *bc-mc*
The *Port Monitor* function monitors only Broadcast and Multicast packets.

Threshold type

Specifies the unit for the data rate.

Possible values:

▶ `pps` (default setting)
packets per second

▶ `kbps`
kbit per second

The prerequisite is that the value in the *Traffic type* column = `all`.

Lower threshold

Specifies the lower threshold value for the data rate.

The *Auto-Disable* function enables the port again only when the load on the port is lower than the value specified here.

Possible values:

▶ `0..10000000` (default setting: `0`)

Upper threshold

Specifies the upper threshold value for the data rate.

If the *Port Monitor* function detects this load in the monitored period, then the device performs the specified action.

Possible values:

▶ `0..10000000` (default setting: `0`)

Interval [s]

Specifies in seconds, the period that the *Port Monitor* function observes a parameter to detect that a parameter is being exceeded.

Possible values:

▶ `1..20` (default setting: `1`)

Packets

Displays the number of Broadcast, Multicast and Unicast packets that the device has detected during the period that has elapsed.

Broadcast packets

Displays the number of Broadcast packets that the device has detected during the period that has elapsed.

Multicast packets

Displays the number of Multicast packets that the device has detected during the period that has elapsed.

Kbit/s

Displays the data rate in Kbits per second that the device has detected during the period that has elapsed.

Buttons

You find the description of the standard buttons in section “Buttons” on page 17.

Reset

Enables the port highlighted in the table again and resets its counter to 0. 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

[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

Port

Displays the port number.

10 Mbit/s HDX

Activates/deactivates the port monitor to accept a half-duplex and 10 Mbit/s data rate combination on the port.

Possible values:

- ▶ *marked*
The port monitor takes into consideration the speed and duplex combination.
- ▶ *unmarked*
If the port monitor detects the speed and duplex combination on the port, then the device executes the action specified in the *Global* tab.

10 Mbit/s FDX

Activates/deactivates the port monitor to accept a full-duplex and 10 Mbit/s data rate combination on the port.

Possible values:

- ▶ `marked`
The port monitor takes into consideration the speed and duplex combination.
- ▶ `unmarked`
If the port monitor detects the speed and duplex combination on the port, then the device executes the action specified in the *Global* tab.

100 Mbit/s HDX

Activates/deactivates the port monitor to accept a half-duplex and 100 Mbit/s data rate combination on the port.

Possible values:

- ▶ `marked`
The port monitor takes into consideration the speed and duplex combination.
- ▶ `unmarked`
If the port monitor detects the speed and duplex combination on the port, then the device executes the action specified in the *Global* tab.

100 Mbit/s FDX

Activates/deactivates the port monitor to accept a full-duplex and 100 Mbit/s data rate combination on the port.

Possible values:

- ▶ `marked`
The port monitor takes into consideration the speed and duplex combination.
- ▶ `unmarked`
If the port monitor detects the speed and duplex combination on the port, then the device executes the action specified in the *Global* tab.

1,000 Mbit/s FDX

Activates/deactivates the port monitor to accept a full-duplex and 1 Gbit/s data rate combination on the port.

Possible values:

- ▶ `marked`
The port monitor takes into consideration the speed and duplex combination.
- ▶ `unmarked`
If the port monitor detects the speed and duplex combination on the port, then the device executes the action specified in the *Global* tab.

2.5 Gbit/s FDX

Activates/deactivates the port monitor to accept a full-duplex and 2.5 Gbit/s data rate combination on the port.

Possible values:

- ▶ *marked*
The port monitor takes into consideration the speed and duplex combination.
- ▶ *unmarked*
If the port monitor detects the speed and duplex combination on the port, then the device executes the action specified in the *Global* tab.

Buttons

You find the description of the standard buttons in section “Buttons” on page 17.

Reset

Enables the port highlighted in the table again and resets its counter to 0. 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

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

Port

Displays the port number.

Reset timer [s]

Specifies the waiting period in seconds, after which the *Auto-Disable* function enables the port again.

Possible values:

- ▶ 0 (default setting)
The timer is inactive. The port remains disabled.
- ▶ 30..4294967295
If the parameters are no longer being exceeded, then the *Auto-Disable* function enables the port again after the waiting period specified here.

Error time

Displays when the device disabled the port due to the parameters being exceeded.

Remaining time [s]

Displays the remaining time in seconds, until the *Auto-Disable* function enables the port again.

Component

Displays the software component in the device that disabled the port.

Possible values:

- ▶ `PORT_MON`
Port Monitor
See the *Diagnostics > Ports > Port Monitor* dialog.
- ▶ `PORT_ML`
Port Security
See the *Network Security > Port Security* dialog.
- ▶ `DHCP_SNP`
DHCP Snooping
See the *Network Security > DHCP Snooping* dialog.
- ▶ `DOT1S`
BPDU guard
See the *Switching > L2-Redundancy > Spanning Tree > Global* dialog.
- ▶ `DAI`
Dynamic ARP Inspection
See the *Network Security > Dynamic ARP Inspection* dialog.

Reason

Displays the monitored parameter that led to the port being disabled.

Possible values:

- ▶ `none`
No monitored parameter.
The port is enabled.
- ▶ `link-flap`
Too many link changes. See the *Diagnostics > Ports > Port Monitor* dialog, *Link flap* tab.
- ▶ `crc-error`
Too many CRC/fragment errors are detected. See the *Diagnostics > Ports > Port Monitor* dialog, *CRC/Fragments* tab.
- ▶ `duplex-mismatch`
Duplex mismatch detected. See the *Diagnostics > Ports > Port Monitor* dialog, *Global* tab.
- ▶ `dhcp-snooping`
Too many DHCP packages from untrusted sources. See the *Network Security > DHCP Snooping > Configuration* dialog, *Port* tab.
- ▶ `arp-rate`
Too many ARP packages from untrusted sources. See the *Network Security > Dynamic ARP Inspection > Configuration* dialog, *Port* tab.
- ▶ `bpdud-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.

Buttons

You find the description of the standard buttons in section “Buttons” on page 17.

[Status]

This tab displays the monitored parameters for which the *Auto-Disable* function is activated.

Table

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 > Port > Port Monitor* menu.
- ▶ `network-security`
The parameter belongs to the functions in the *Network Security* menu.
- ▶ `l2-redundancy`
The parameter belongs to the functions in the *Switching > L2-Redundancy* menu.

Auto-disable

Displays if the *Auto-Disable* function is activated/deactivated 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.

Buttons

You find the description of the standard buttons in section “Buttons” on page 17.

Reset

Enables the port highlighted in the table again and resets its counter to 0. 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

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

Operation

Enables/disables the *Port Mirroring* function.

Possible values:

- ▶ *On*
The *Port Mirroring* function is enabled.
The device copies the data packets from the selected source ports to the destination port.
- ▶ *Off* (default setting)
The *Port Mirroring* function is disabled.

Destination port

Primary port

Specifies the destination port.

Suitable ports are those ports that are not used for the following purposes:

- Source port
- L2 redundancy protocols

Possible values:

- ▶ *no Port* (default setting)
No destination port selected.
- ▶ *<Port number>*
Number of the destination port. The device copies the data packets from the source ports to this port.

On the destination port, the device adds a VLAN tag to the data packets that the source port transmits. The destination port transmits unmodified the data packets that the source port receives.

Note: The destination port needs sufficient bandwidth to absorb the data stream. If the copied data stream exceeds the bandwidth of the destination port, then the device discards surplus data packets on the destination port.

Secondary port

Specifies a second destination port. The prerequisite is that you have specified a primary port.

Possible values:

- ▶ `no Port` (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

Source port

Specifies the port number.

Possible values:

- ▶ `<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 transmits. The destination port transmits unmodified the data packets that the source port receives.

Possible values:

- ▶ `none` (default setting)
No data packets.
- ▶ `tx`
Data packets that the source port transmits.
- ▶ `rx`
Data packets that the source port receives.
- ▶ `txrx`
Data packets that the source port transmits and receives.

Note: With the `txrx` setting the device copies transmitted and received data packets. The destination ports needs at least a bandwidth that corresponds to the sum of the send and receive channel of the source ports. For example, for similar ports the destination port is at 100 % capacity when the send and receive channel of a source port are at 50 % capacity respectively.

Buttons

You find the description of the standard buttons in section “Buttons” on page 17.

Reset config

Resets the settings in the dialog to the default settings and transfers the changes to the volatile memory of the device (`RAM`).

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 enables a network management station to map the structure of your network.

This menu lets you configure the topology discovery and to display the information received in table form.

The menu contains the following dialogs:

- ▶ `LLDP Configuration`
- ▶ `LLDP Topology Discovery`

6.6.1 LLDP Configuration

[Diagnostics > LLDP > Configuration]

This dialog lets you configure 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 transmits LLDP data packets.

Possible values:

- ▶ 5..32768 (default setting: 30)

Transmit interval multiplier

Specifies the factor for determining the time-to-live value for the LLDP data packets.

Possible values:

- ▶ 2..10 (default setting: 4)

The time-to-live value coded in the LLDP header results from multiplying this value with the value in the *Transmit interval [s]* field.

Reinit delay [s]

Specifies the delay in seconds for the reinitialization of a port.

Possible values:

- ▶ 1..10 (default setting: 2)

If in the *Operation* column the value *Off* is specified, then the device tries to reinitialize the port after the time specified here has elapsed.

Transmit delay [s]

Specifies the delay in seconds for transmitting successive LLDP data packets after configuration changes in the device occur.

Possible values:

- ▶ 1..8192 (default setting: 2)

The recommended value is between a minimum of 1 and a maximum of a quarter of the value in the *Transmit interval [s]* field.

Notification interval [s]

Specifies the interval in seconds for transmitting LLDP notifications.

Possible values:

- ▶ 5..3600 (default setting: 5)

After transmitting a notification trap, the device waits for a minimum of the time specified here before transmitting the next notification trap.

Table

Port

Displays the port number.

Operation

Specifies if the port transmits and receives LLDP data packets.

Possible values:

- ▶ *transmit*
The port transmits LLDP data packets but does not save any information about neighboring devices.
- ▶ *receive*
The port receives LLDP data packets but does not transmit any information to neighboring devices.
- ▶ *receive and transmit* (default setting)
The port transmits LLDP data packets and saves information about neighboring devices.
- ▶ *disabled*
The port does not transmit LLDP data packets and does not save information about neighboring devices.

Notification

Activates/deactivates the LLDP notifications on the port.

Possible values:

- ▶ *marked*
LLDP notifications are active on the port.
- ▶ *unmarked* (default setting)
LLDP notifications are inactive on the port.

Transmit port description

Activates/deactivates the transmitting of a TLV (Type Length Value) with the port description.

Possible values:

- ▶ `marked` (default setting)
The transmitting of the TLV is active.
The device transmits the TLV with the port description.
- ▶ `unmarked`
The transmitting of the TLV is inactive.
The device does not transmit a TLV with the port description.

Transmit system name

Activates/deactivates the transmitting of a TLV (Type Length Value) with the device name.

Possible values:

- ▶ `marked` (default setting)
The transmitting of the TLV is active.
The device transmits the TLV with the device name.
- ▶ `unmarked`
The transmitting of the TLV is inactive.
The device does not transmit a TLV with the device name.

Transmit system description

Activates/deactivates the transmitting of the TLV (Type Length Value) with the system description.

Possible values:

- ▶ `marked` (default setting)
The transmitting of the TLV is active.
The device transmits the TLV with the system description.
- ▶ `unmarked`
The transmitting of the TLV is inactive.
The device does not transmit a TLV with the system description.

Transmit system capabilities

Activates/deactivates the transmitting of the TLV (Type Length Value) with the system capabilities.

Possible values:

- ▶ `marked` (default setting)
The transmitting of the TLV is active.
The device transmits the TLV with the system capabilities.
- ▶ `unmarked`
The transmitting of the TLV is inactive.
The device does not transmit a TLV with the system capabilities.

Neighbors (max.)

Limits the number of neighboring devices to be recorded for this port.

Possible values:

- ▶ `1..50` (default setting: 10)

FDB mode

Specifies which function the device uses to record neighboring devices on this port.

Possible values:

- ▶ `lldpOnly`
The device uses only LLDP data packets to record neighboring devices on this port.
- ▶ `macOnly`
The device uses learned MAC addresses to record neighboring devices on this port. The device uses the MAC address only if there is no other entry in the address table (FDB, Forwarding Database) for this port.
- ▶ `both`
The device uses LLDP data packets and learned MAC addresses to record neighboring devices on this port.
- ▶ `autoDetect` (default setting)
If the device receives LLDP data packets at this port, then the device operates the same as with the `lldpOnly` setting. Otherwise, the device operates the same as with the `macOnly` setting.

Buttons

You find the description of the standard buttons in section [“Buttons” on page 17](#).

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 via LLDPDU are useful for many reasons. Thus the device detects which devices in the network are neighbors and via 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 enables a network management station to map the structure of your network.

When devices both with and without an active topology discovery function are connected to a port, the topology table hides the devices without active topology discovery.

When only devices without active topology discovery are connected to a port, the table contains one line for this port to represent every device. This line contains the number of connected devices.

The Forwarding Database (FDB) address table contains MAC addresses of devices that the topology table hides for the sake of clarity.

When you use one port to connect several devices, for example via a hub, the table contains one line for each connected device.

Table

Port

Displays the port number.

Neighbor identifier

Displays the chassis ID of the neighboring device. This can be the basis MAC address of the neighboring device, for example.

FDB

Displays if the connected device has active LLDP support.

Possible values:

- ▶ `marked`
The connected device does not have active LLDP support.
The device uses information from its address table (FDB, Forwarding Database)
- ▶ `unmarked` (default setting)
The connected device has active LLDP support.

Neighbor IP address

Displays the IP address with which the access to the neighboring device management is possible.

Neighbor port description

Displays a description for the port of the neighboring device.

Neighbor system name

Displays the device name of the neighboring device.

Neighbor system description

Displays a description for the neighboring device.

Port ID

Displays the ID of the port through which the neighboring device is connected to the device.

Autonegotiation supported

Displays if the port of the neighboring device supports autonegotiation.

Autonegotiation

Displays if autonegotiation is enabled 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 enabled on the port of the neighboring device.

Buttons

You find the description of the standard buttons in section [“Buttons” on page 17](#).

[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

Port

Displays the port number.

Device class

Displays the device class of the remotely connected device.

- ▶ A value of `notDefined` indicates that the device has capabilities not covered by any of the *LLDP-MED* classes.
- ▶ A value of `endpointClass1..3` indicates that the device has "endpoint class 1..3" capabilities.
- ▶ A value of `networkConnectivity` indicates that the device has network connectivity device capabilities.

VLAN ID

Displays the extension of the VLAN Identifier for the remote system connected to this port, as defined in IEEE 802.3.

- ▶ The device uses a value from 1 through 4042 to specify a valid Port VLAN ID.
- ▶ The device displays the value 0 for priority tagged packets. This means that only the 802.1D priority is significant and the device uses the default VLAN ID of the ingress port.

Priority

Displays the value of the 802.1D priority which is associated with the remote system connected to the port.

DSCP

Displays the value of the Differentiated Service Code Point (DSCP) which is associated with the remote system connected to the port.

Unknown bit status

Displays the unknown bit status of incoming traffic.

- ▶ A value of `true` indicates that the network policy for the specified application type is currently unknown. In this case, the VLAN ID ignores the Layer 2 priority and value of the *DSCP* field.
- ▶ A value of `false` indicates a specified network policy.

Tagged bit status

Displays the tagged bit status.

- ▶ A value of `true` indicates that the application uses a tagged VLAN.
- ▶ A value of `false` indicates that 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, 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.

Buttons

You find the description of the standard buttons in section [“Buttons” on page 17](#).

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.

Global

Transmit interval

Specifies the interval in seconds at which the device sends *loop detection* packets if the *Loop Protection* function is active on the port.

Possible values:

▶ 1..10

Receive threshold

Specifies the threshold value for the number of *loop detection* packets received in a row. If the number reaches or exceeds this threshold, then the device will perform the action specified in the *Action* column.

Possible values:

▶ 1..50

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 the *auto-disable* or the *all* action is specified in the *Action* column.

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.

Table

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*
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*
The device disables the port using the *Auto-Disable* function.
The prerequisite for disabling the port is that the *Auto-disable* checkbox in the *Configuration* frame 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 the *Auto-disable* checkbox in the *Configuration* frame 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 the VLAN is already configured and that the port is a member of the VLAN. See the *Switching > VLAN > Port* dialog.

Loop detected

Displays if the device has detected a layer 2 network loop on the port.

Possible values:

- ▶ *yes*
The device has detected a layer 2 network loop on the port.
After the loop has ended and the port is enabled again, the device resets the value to *no*.
- ▶ *no*
The device has not detected a layer 2 network loop on the port.

Loop count

Displays the number of loops the device has detected on the port since the last port statistics reset or since the last restart of the device.

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 you synchronize the system time of the device with the appropriate reference time. See the [Time > Basic Settings](#) dialog.

Sent frames

Displays the number of *loop detection* packets sent on the port since the last port statistics reset or since the last restart of the device.

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 restart of the device.

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.

Buttons

You find the description of the standard buttons in section [“Buttons” on page 17](#).

Clear port statistics

Resets the values in the following columns:

- *Loop count*
- *Sent frames*
- *Received frames*

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 system information on your PC.

Console logging

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.

The device outputs the messages on the serial interface.

Possible values:

- ▶ *emergency*
- ▶ *alert*
- ▶ *critical*
- ▶ *error*
- ▶ *warning* (default setting)
- ▶ *notice*
- ▶ *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.

Possible values:

- ▶ `emergency`
- ▶ `alert`
- ▶ `critical`
- ▶ `error`
- ▶ `warning` (default setting)
- ▶ `notice`
- ▶ `informational`
- ▶ `debug`

SNMP logging

When you enable the logging of SNMP requests, the device sends these as events with the preset severity `notice` to the list of syslog servers. The preset minimum severity for a syslog server entry is `critical`.

To send SNMP requests to a syslog server, you have a number of options to change the default settings. Select the ones that meet your requirements best.

- Set the severity for which the device creates SNMP requests as events to `warning` or `error`. Change the minimum severity for a syslog entry for one or more syslog servers to the same value.
You also have the option of creating a separate syslog server entry for this.
- Set only the severity for SNMP requests to `critical` or higher. The device then sends SNMP requests as events with the severity `critical` or higher to the syslog servers.
- Set only the minimum severity for one or more syslog server entries to `notice` or lower. Then it is possible that the device sends many events to the syslog servers.

Log SNMP get request

Enables/disables the logging of SNMP Get requests.

Possible values:

- ▶ `On`
The logging is enabled.
The device registers SNMP Get requests as events in the syslog.
In the *Severity get request* drop-down list, you select the severity for this event.
- ▶ `Off` (default setting)
The logging is disabled.

Log SNMP set request

Enables/disables the logging of SNMP Set requests.

Possible values:

- ▶ *On*
The logging is enabled.
The device registers SNMP Set requests as events in the syslog.
In the *Severity set request* drop-down list, you select the severity for this event.
- ▶ *Off* (default setting)
The logging is disabled.

Severity get request

Specifies the severity of the event that the device registers for SNMP Get requests.

Possible values:

- ▶ emergency
- ▶ alert
- ▶ critical
- ▶ error
- ▶ warning
- ▶ notice (default setting)
- ▶ informational
- ▶ debug

Severity set request

Specifies the severity of the event that the device registers for SNMP Set requests.

Possible values:

- ▶ emergency
- ▶ alert
- ▶ critical
- ▶ error
- ▶ warning
- ▶ notice (default setting)
- ▶ 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.

Buttons

You find the description of the standard buttons in section “Buttons” on page 17.

Download support information

Generates a ZIP archive which the web browser lets you download from the device.

The ZIP archive contains system information about the device. You will find an explanation of the files contained in the ZIP archive in the following section.

Support Information: Files contained in ZIP archive

File name	Format	Comments
audittrail.html	HTML	Contains the chronological recording of the system events and saved user changes in the Audit Trail.
defaultconfig.xml	XML	Contains the configuration profile with the default settings.
script	TEXT	Contains the output of the command <code>show running-config script</code> .
runningconfig.xml	XML	Contains the configuration profile with the current operating settings.
supportinfo.html	TEXT	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 <i>Diagnostics > Report > System Log</i> dialog.

Meaning of the event severities

Severity	Meaning
<i>emergency</i>	Device not ready for operation
<i>alert</i>	Immediate user intervention required
<i>critical</i>	Critical status

Severity	Meaning
error	Error status
warning	Warning
notice	Significant, normal status
informational	Informal 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 created file.

In the table the device displays you the log files held in the external memory. As soon as the specified maximum number of files has been attained, the device deletes the oldest file and renames the remaining files. This helps ensure that there is enough memory space in the external memory.

Note: Verify that an external memory is connected. To verify if an external memory is connected, see the *Status* column in the *Basic Settings > External Memory* dialog. We recommend to monitor the external memory connection using the *Device Status* function, see the *External memory removal* parameter in the *Diagnostics > Status Configuration > Device Status* dialog.

Operation

Operation

Enables/disables the *Persistent Logging* function.

Only activate this function if the external memory is available in the device.

Possible values:

- ▶ *On* (default setting)
The *Persistent Logging* function is enabled.
The device saves the log entries in a file in the external memory.
- ▶ *Off*
The *Persistent Logging* function is disabled.

Configuration

Max. file size [kbyte]

Specifies the maximum size of the log file in KBytes. When the log file reaches the specified size, the device archives this file and saves the following log entries in a newly created file.

Possible values:

- ▶ *0..4096* (default setting: *1024*)

The value *0* deactivates saving of log entries in the log file.

Files (max.)

Specifies the number of log files that the device keeps in the external memory.

As soon as the specified maximum number of files has been attained, the device deletes the oldest file and renames the remaining files.

Possible values:

- ▶ 0..25 (default setting: 4)

The value 0 deactivates saving of log entries in the log file.

Severity

Specifies the minimum severity of the events. The device saves the log entry for events with this severity and with more urgent severities in the log file in the external memory.

Possible values:

- ▶ emergency
- ▶ alert
- ▶ critical
- ▶ error
- ▶ warning (default setting)
- ▶ notice
- ▶ informational
- ▶ debug

Log file target

Specifies the external memory device for logging.

Possible values:

- ▶ usb
External USB memory (EAM)

Table

Index

Displays the index number to which the table entry 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.

Buttons

You find the description of the standard buttons in section [“Buttons” on page 17](#).

Delete persistent log file

Removes the log files from the external memory.

6.8.3 System Log

[Diagnostics > Report > System Log]

The device logs device-internal events in a log file (System Log).

This dialog displays the log file (System Log). The dialog lets you save the log file in HTML format on your PC.

In order to search the log file for search terms, use the search function of your web browser.

The log file is kept until a restart is performed in the device. After the restart the device creates the file again.

Buttons

You find the description of the standard buttons in section [“Buttons” on page 17](#).

Save log file

Opens the HTML page in a new web browser window or tab. You can save the HTML page on your PC using the appropriate web browser command.

Delete log file

Removes the logged events from the log file.

6.8.4 Audit Trail

[Diagnostics > Report > Audit Trail]

This dialog displays the log file (Audit Trail). The dialog lets you save the log file as an HTML file on your PC.

In order to search the log file for search terms, use the search function of your web browser.

The device logs system events and writing user actions in the device. This lets you keep track of WHO changes WHAT in the device and WHEN. The prerequisite is that the user role `auditor` or `administrator` is assigned to your user account.

The device logs the following user actions, among others:

- ▶ A user logging in with the Command Line Interface (local or remote)
- ▶ A user logging off manually
- ▶ Automatic logging off of a user in the Command Line Interface after a specified period of inactivity
- ▶ Device restart
- ▶ Locking of a user account due to too many unsuccessful login attempts
- ▶ Locking of the access to the device management due to unsuccessful login attempts
- ▶ Commands executed in the Command Line Interface, apart from `show` commands
- ▶ Changes to configuration variables
- ▶ Changes to the system time
- ▶ File transfer operations, including firmware updates
- ▶ Configuration changes via Ethernet Switch Configurator
- ▶ Firmware updates and automatic configuration of the device via the external memory
- ▶ Opening and closing of SNMP via an HTTPS tunnel

The device does not log passwords. The logged entries are write-protected and remain saved in the device after a restart.

During the restart, 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.

WARNING

UNINTENDED EQUIPMENT OPERATION

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.

Failure to follow these instructions can result in death, serious injury, or equipment damage.

Buttons

You find the description of the standard buttons in section [“Buttons” on page 17](#).

Save audit trail file

Opens the HTML page in a new web browser window or tab. You can save the HTML page on your PC using the appropriate web browser command.

7 Advanced


The menu contains the following dialogs:

- ▶ DHCP L2 Relay
- ▶ DHCP Server
- ▶ DNS
- ▶ Industrial Protocols
- ▶ Digital IO Module
- ▶ Command Line Interface

7.1 DHCP L2 Relay

[Advanced > DHCP L2 Relay]

On the front panel of the device you find the following hazard message:

 WARNING
UNINTENDED OPERATION
Do not change cable positions if DHCP Option 82 is enabled. Check the user manual before servicing.
Failure to follow these instructions can result in death, serious injury, or equipment damage.

A network administrator uses the DHCP L2 *Relay Agent* to add DHCP client information. L3 *Relay Agents* and DHCP servers need the DHCP client information to assign an IP address and a configuration to the clients.

When active, the relay adds *Option 82* information configured in this dialog to the packets before it relays DHCP requests from the clients to the server. The *Option 82* fields provide unique information about the client and relay. This unique identifier consists of a *Circuit ID* for the client and a *Remote ID* for the relay.

In addition to the type, length, and multicast fields, the *Circuit ID* includes the VLAN ID, unit number, slot number, and port number for the connected client.

The *Remote ID* consists of a type and length field and either a MAC address, IP address, client identifier, or a user-defined device description. A client identifier is the user-defined system name for the device.

For the DHCPv6 protocol, the device uses a *Relay Agent* to add *Relay Agent* options to DHCPv6 packets exchanged between a client and a DHCPv6 server. The Lightweight DHCPv6 Relay Agent (LDRA) is described in RFC 6221.

The LDRA processes 2 types of messages:

▶ *Relay-Forward* messages

The *Relay Agent* forwards *Relay-Forward* messages that contain unique information about the client. The client information includes the peer-address, meaning the IPv6 link-local address of the client and the *Interface-ID* information. The *Interface-ID* information, also known as *Option 18*, provides information that identifies the interface on which the client request was sent.

▶ *Relay-Reply* messages

The DHCPv6 server sends *Relay-Reply* messages. The *Relay Agent* validates the messages to include the information encapsulated in the initial *Relay-Forward* message. If the information is valid, then the *Relay Agent* forwards the packet to the client.

The menu contains the following dialogs:

▶ DHCP L2 Relay Configuration

▶ DHCP L2 Relay Statistics

7.1.1 DHCP L2 Relay Configuration

[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

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.

Buttons

You find the description of the standard buttons in section “Buttons” on page 17.

[VLAN ID]

Table

VLAN ID

VLAN to which the table entry relates.

Active

Activates/deactivates the *DHCP L2 Relay* function on the VLAN.

The prerequisite is that you enable the function globally.

Possible values:

- ▶ **marked**
The *DHCP L2 Relay* function is active.
- ▶ **unmarked** (default setting)
The *DHCP L2 Relay* function is inactive.

Circuit ID

Activates or deactivates the addition of the *Circuit ID* to the *Option 82* information.

Possible values:

- ▶ `marked` (default setting)
Enables *Circuit ID* and *Remote ID* to be sent together.
- ▶ `unmarked`
The device sends only the *Remote ID*.

Remote ID type

Specifies the components of the *Remote ID* for this VLAN.

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 use this value, enter in the *Remote ID* column user-defined information.

Remote ID

Displays the *Remote ID* for the VLAN.

When you specify the value `other` in the *Remote ID type* column, specify the identifier.

Buttons

You find the description of the standard buttons in section “Buttons” on page 17.

7.1.2 DHCP L2 Relay Statistics

[Advanced > DHCP L2 Relay > Statistics]

The device monitors the traffic on the ports and displays the results in tabular form.

This table is divided into various categories to aid you in traffic analysis.

The DHCPv6 relay options are not displayed in the statistics table.

Table

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.

Buttons

You find the description of the standard buttons in section [“Buttons” on page 17](#).

Reset

Resets the entire table.

7.2 DHCP Server

[Advanced > DHCP Server]

With the DHCP server, you manage a database of available IP addresses and configuration information. When the device receives a request from a client, the DHCP server validates the DHCP client network, and then leases an IP address. When activated, the DHCP server also allocates configuration information appropriate for that client. The configuration information specifies, for example, which IP address, DNS server and the default route a client uses.

The DHCP server assigns an IP address to a client for a user-defined interval. The DHCP client is responsible for renewing the IP address before the interval expires. When the DHCP client is unable to renew the address, the address returns to the pool for reassignment.

The menu contains the following dialogs:

- ▶ DHCP Server Global
- ▶ DHCP Server Pool
- ▶ DHCP Server Lease Table

7.2.1 DHCP Server Global

[Advanced > DHCP Server > Global]

Activate the 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 server uses an *ICMP Echo* request to check whether this IP address is already in use on the network.

Possible values:

- ▶ *marked* (default setting)
The *IP Probe* function is active.
- ▶ *unmarked*
The *IP Probe* function is inactive.

Table

Port

Displays the port number.

DHCP server active

Activates/deactivates the DHCP server function on this port.

The prerequisite is that you enable the function globally.

Possible values:

- ▶ *marked* (default setting)
The DHCP server function is active.
- ▶ *unmarked*
The DHCP server function is inactive.

Buttons

You find the description of the standard buttons in section [“Buttons”](#) on page 17.

7.2.2 DHCP Server Pool


[Advanced > DHCP Server > Pool]

Assign an IP address to an end device or switch connected to a port or included in a VLAN.

The DHCP server provides IP address pools from which it allocates IP addresses to clients. A pool consists of a list of entries. Specify an entry as static to a specific IP address, or as dynamic to an IP address range. The device holds a maximum of 128 pools. The pools together hold a maximum of 1000 entries.

With static allocation, the DHCP server assigns an IP address to a specific client. The DHCP server identifies the client using a unique hardware ID. A static address entry contains one IP address. You apply this IP address to every port or to a specific port of the device. For static allocation, enter an IP address for allocation in the *IP address* field, and leave the *Last IP address* column empty. Enter a hardware ID with which the DHCP server uniquely identifies the client. This ID is either a MAC address, a Client ID, a Remote ID, or a Circuit ID. When a client contacts the device with a known hardware ID, the DHCP server allocates the static IP address.

In dynamic allocation, when a DHCP client makes contact on a port, the DHCP server assigns an available IP address from a pool for this port. For dynamic allocation, create a pool for the ports by assigning an IP address range. Specify the first and last IP addresses for the IP address range. Leave the *MAC address*, *Client ID*, *Remote ID* and *Circuit ID* fields empty. You have the option of creating multiple pool entries. This lets you create an IP address range that contains gaps.

This dialog displays the different information that is required for the assignment of an IP address for a port or a VLAN. Use the  button to add an entry. The device adds a writable and readable entry.

Table

Index

Displays the index number to which the table entry relates.

Active

Activates/deactivates the DHCP server function on this port.

Possible values:

- ▶ *marked*
The DHCP server function is active.
- ▶ *unmarked* (default setting)
The DHCP server function is inactive.

IP address

Specifies the IP address for static IP address assignment. When using dynamic IP address assignment, this value specifies the start of the IP address range.

Possible values:

- ▶ Valid IPv4 address

Last IP address

When using dynamic IP address assignment, this value specifies the end of the IP address range.

Possible values:

- ▶ Valid IPv4 address

Port

Displays the port number.

VLAN ID

Displays the VLAN to which the table entry relates.

A value of 1 corresponds to the default device management VLAN.

Possible values:

- ▶ 1..4042

MAC address

Specifies the MAC address of the device leasing the IP address.

Possible values:

- ▶ Valid Unicast MAC address
Specify the value with a colon separator, for example 00:11:22:33:44:55.
- ▶ -
For the IP address assignment, the server ignores this variable.

DHCP relay

Specifies the IP address of the DHCP relay through which the clients transmit their requests to the DHCP server. When the DHCP server receives the client's request through another DHCP relay, it ignores this request.

Possible values:

- ▶ Valid IPv4 address
IP address of the DHCP relay.
- ▶ -
Between the client and the DHCP server there is no DHCP relay.

Client ID

Specifies the identification of the client device leasing the IP address.

Possible values:

▶ 1..80 bytes (format `XX XX .. XX`)

▶ -

For the IP address assignment, the server ignores this variable.

Remote ID

Specifies the identification of the remote device leasing the IP address.

Possible values:

▶ 1..80 bytes (format `XX XX .. XX`)

▶ -

For the IP address assignment, the server ignores this variable.

Circuit ID

Specifies the Circuit ID of the device leasing the IP address.

Possible values:

▶ 1..80 bytes (format `XX XX .. XX`)

▶ -

For the IP address assignment, the server ignores this variable.

Schneider Electric device

Activates/deactivates Schneider Electric multicasts.

If the device in this IP address range serves only Schneider Electric devices, then activate this function.

Possible values:

▶ `marked`

In this IP address range, the device serves only Schneider Electric devices. Schneider Electric multicasts are activated.

▶ `unmarked` (default setting)

In this IP address range, the device serves the devices of different manufacturers. Schneider Electric multicasts are deactivated.

Configuration URL

Specifies the protocol to be used as well as the name and path of the configuration file.

Possible values:

▶ Alphanumeric ASCII character string with 0..70 characters

Example: `tftp://192.9.200.1/cfg/config.xml`

When you leave this field blank, the device leaves this option field blank in the DHCP message.

Lease time [s]

Specifies the lease time in seconds.

Possible values:

▶ 60..220752000 (default setting: 86400)

▶ 4294967295

Use this value for assignments unlimited in time and for assignments via 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

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

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

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

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

Buttons

You find the description of the standard buttons in section [“Buttons” on page 17](#).

7.2.3 DHCP Server Lease Table

[Advanced > DHCP Server > Lease Table]

This dialog displays the status of IP address leasing on a per port basis.

Table

Port

Displays the port number to which the address is currently being leased.

IP address

Displays the leased IP address to which the entry refers.

Status

Displays the lease phase.

According to the standard for DHCP operations, there are 4 phases to leasing an IP address: Discovery, Offer, Request, and Acknowledgement.

Possible values:

- ▶ `bootp`
A DHCP client is attempting to discover a DHCP server for IP address allocation.
- ▶ `offering`
The DHCP server is validating that the IP address is suitable for the client.
- ▶ `requesting`
A DHCP client is acquiring the offered IP address.
- ▶ `bound`
The DHCP server is leasing the IP address to a client.
- ▶ `renewing`
The DHCP client is requesting an extension to the lease.
- ▶ `rebinding`
The DHCP server is assigning the IP address to the client after a successful renewal.
- ▶ `declined`
The DHCP server denied the request for the IP address.
- ▶ `released`
The IP address is available for other clients.

Remaining lifetime

Displays the time remaining on the leased IP address.

Leased MAC address

Displays the MAC address of the device leasing the IP address.

Gateway

Displays the Gateway IP address of the device leasing the IP address.

Client ID

Displays the client identifier of the device leasing the IP address.

Remote ID

Displays the remote identifier of the device leasing the IP address.

Circuit ID

Displays the Circuit ID of the device leasing the IP address.

Buttons

You find the description of the standard buttons in section [“Buttons” on page 17](#).

7.3 DNS

[Advanced > DNS]

The menu contains the following dialogs:

- ▶ [DNS Client](#)

7.3.1 DNS Client

[Advanced > DNS > Client]

DNS (Domain Name System) is a service in the network that translates host names into IP addresses. This name resolution lets you contact other devices using their host names instead of their IP addresses.

The *Client* function enables the device to send 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

Cache

Enables/disables the *Cache* function.

Possible values:

- ▶ *On* (default setting)
The *Cache* function is enabled.
The device temporarily saves up to 128 DNS server responses (hostname and corresponding IP address) in the cache. When the cache contains a matching entry, the host name of a new request the device resolves itself. This makes sending a new query to the DNS server unnecessary.
- ▶ *Off*
The *Cache* function is disabled.

Buttons

You find the description of the standard buttons in section “Buttons” on page 17.

Flush cache

Removes every entry from the DNS cache.

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

Index

Displays the sequential number of the DNS server.

Address

Displays the IP address of the DNS server. The device forwards requests for resolving host names in IP addresses to the DNS server with this IP address.

Buttons

You find the description of the standard buttons in section [“Buttons” on page 17](#).

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 host names in IP addresses.

The device lets you specify up to 4 IP addresses yourself or to transfer the IP addresses from a DHCP server.

Configuration

Configuration source

Specifies the source from which the device obtains the IP address of DNS servers to which the device addresses requests.

Possible values:

- ▶ `user`
The device uses the IP addresses specified in the table.
- ▶ `mgmt-dhcp` (default setting)
The device uses the IP addresses which the DHCP server delivers to the device.

Domain name

Specifies the domain name according to 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, you specify a value >0.

Possible values:

- ▶ 0..100 (default setting: 2)

Table

Index

Displays the sequential number of the DNS server.

The device lets you specify up to 4 DNS servers.

Address

Specifies the IP address of the DNS server.

Possible values:

- ▶ Valid IPv4 address (default setting: 0.0.0.0)
- ▶ Valid IPv6 address

Active

Activates/deactivates the table entry.

The device sends requests to the DNS server configured in the first active table entry. When the device does not receive a response from this server, it sends requests to the DNS server configured in the next active table entry.

Possible values:

- ▶ `marked`
The DNS client sends requests to this DNS server.
Prerequisites:
 - Enable the DNS-client function in the *Advanced > DNS > Global* dialog.
 - Select in the *Configuration* frame, *Configuration source* drop-down-list the value `user`.
- ▶ `unmarked` (default setting)
The device does not send requests to this DNS server.

Buttons

You find the description of the standard buttons in section “Buttons” on page 17.

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

Index

Displays the index number to which the table entry relates.

Possible values:

▶ 1..64

Name

Specifies the hostname.

Possible values:

▶ Alphanumeric ASCII character string with 0..255 characters

IP address

Specifies the IP address under which the host is reachable.

Possible values:

▶ Valid IPv4 address

Active

Activates/deactivates the table entry.

Possible values:

▶ `marked`

The device resolves a request for the host name for this entry.

▶ `unmarked`

After receiving a request for this host name, the device sends a request to one of the configured name servers for resolution.

Buttons

You find the description of the standard buttons in section [“Buttons” on page 17](#).

7.4 Industrial Protocols

[Advanced > Industrial Protocols]

The menu contains the following dialogs:

- ▶ IEC61850-MMS
- ▶ Modbus TCP
- ▶ EtherNet/IP

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. This in turn can result in an incorrect configuration of the device and to potential issues in the network.

Activate the write access only if you have taken additional measures (for example Firewall, VPN, etc.) to reduce possible unauthorized access.

This dialog lets you specify the following MMS server settings:

- ▶ Activates/deactivates the MMS server.
- ▶ Activates/deactivates the write access to the MMS server.
- ▶ The MMS server TCP Port.
- ▶ The maximum number of MMS server sessions.

Operation

Operation

Enables/disables the *IEC61850-MMS* server.

Possible values:

- ▶ *On*
The *IEC61850-MMS* server is enabled.
- ▶ *OFF* (default setting)
The *IEC61850-MMS* server is disabled.
The IEC61850 MIBs stay accessible.

Configuration

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 following characters are allowed:
 - `0..9`
 - `a..z`
 - `A..Z` (default setting: `KEY`)

To get the MMS server to use the IED name, click the button and restart the MMS server. The connection to connected clients is then interrupted.

TCP port

Specifies TCP port for MMS server access.

Possible values:

- ▶ `1..65535` (default setting: `102`)
Exception: Port `2222` is reserved for internal functions.

Note: The server restarts automatically after you change the port. In the process, the device terminates open connections to the server.

Sessions (max.)

Specifies the maximum number of MMS server connections.

Possible values:

- ▶ 1..15 (default setting: 5)

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.

Buttons

You find the description of the standard buttons in section [“Buttons” on page 17](#).

Download ICD file

Copies the ICD file to your PC.

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 Human-Machine Interface (HMI) software and the memory mapping table. Refer to the tables located in the “Configuration” user manual for the supported objects and memory mapping.

The dialog lets you enable the function, activate the write access, control which TCP port the Human-Machine Interface (HMI) polls for data. You can also specify the number of sessions allowed to be open at the same time.

Note: Activating the *Modbus TCP* write-access can cause an unavoidable security risk, because the protocol does not authenticate user access.

To help minimize the unavoidable security risks, specify the IP address range located in the *Device Security > Management Access* dialog. Enter only the IP addresses assigned to your devices before enabling the function. Furthermore, the default setting for monitoring function activation in the *Diagnostics > Status Configuration > Security Status* dialog, *Global* tab, is active.

Operation

Operation

Enables/disables the *Modbus TCP* server in the device.

Possible values:

- ▶ *On*
The *Modbus TCP* server is enabled.
- ▶ *OFF* (default setting)
The *Modbus TCP* server is disabled.

Configuration

Write access

Activates/deactivates the write access to the *Modbus TCP* parameters.

Note: Activating the *Modbus TCP* write-access can cause an unavoidable security risk, because the protocol does not authenticate user access.

Possible values:

- ▶ `marked` (default setting)
The *Modbus TCP* server read/write access is active. This lets you change the device configuration using the *Modbus TCP* protocol.
- ▶ `unmarked`
The *Modbus TCP* server read-only access is active.

TCP port

Specifies the TCP port number that the *Modbus TCP* server uses for communication.

Possible values:

- ▶ `<TCP Port number>` (default setting: 502)
Specifying 0 is not allowed.

Sessions (max.)

Specifies the maximum number of concurrent sessions that the *Modbus TCP* server maintains.

Possible values:

- ▶ `1..5` (default setting: 5)

Buttons

You find the description of the standard buttons in section “Buttons” on page 17.

7.4.3 EtherNet/IP

[Advanced > Industrial Protocols > EtherNet/IP]

This dialog lets you specify the *EtherNet/IP* settings. You have the following options:

- ▶ Enable/disable the *EtherNet/IP* function in the device.
- ▶ Specify a VLAN which forwards the *EtherNet/IP* packets exclusively.
- ▶ Activate/deactivate the read/write capability of the *EtherNet/IP* protocol.
- ▶ Download the Electronic Data Sheet (EDS) file from the device.

Operation

Operation

Enables/disables the *EtherNet/IP* function in the device.

Possible values:

- ▶ *On*
The *EtherNet/IP* function is enabled.
- ▶ *Off* (default setting)
The *EtherNet/IP* function is disabled.

VLAN Configuration

Advantages of setting up a VLAN:

- Reduced flooding of *EtherNet/IP* packets. The device forwards the *EtherNet/IP* packets in the VLAN you assign.
- Improved network security and privacy.

VLAN ID

Specifies a VLAN in which the device forwards the *EtherNet/IP* packets.

Possible values:

- ▶ *mgmt* (default setting)
The device forwards the *EtherNet/IP* packets in the VLAN in which the device management is accessible through the network. You specify this VLAN in the *Basic Settings > Network > Global* dialog, *Management interface* frame, *VLAN ID* field.
- ▶ *1..4042*
In the drop-down list, select one item. The device forwards the *EtherNet/IP* packets in this VLAN.
Prerequisites:
 - The VLAN is already set up in the device.
See the *Switching > VLAN > Configuration* dialog.
 - The port over which the device forwards the *EtherNet/IP* packets is a member of the VLAN you assign and transmits the data packets with a VLAN tag.
See the *Switching > VLAN > Configuration* dialog.
 - The *IP Access Restriction* function is enabled.
See the *Device Security > Management Access > IP Access Restriction* dialog.

Configuration

Write access

Activates/deactivates the read/write capability of the *EtherNet/IP* protocol.

Possible values:

- ▶ *marked*
The *EtherNet/IP* protocol accepts set/get requests.
- ▶ *unmarked* (default setting)
The *EtherNet/IP* protocol accepts only get requests.

Buttons

You find the description of the standard buttons in section “Buttons” on page 17.

Download EDS file

Copies the following information in a zip file onto your PC:

- ▶ Electronic Data Sheet (EDS) with device related information
- ▶ device icon

7.5 Digital IO Module

[Advanced > Digital IO Module]

The digital inputs allow you to capture and forward signals from digital sensors. The digital outputs allow you to apply the signal, relayed from the inputs, to the actuators. The 24 VDC output voltage lets you operate actuators such as indicator lights.

The device transmits sensor signals throughout the network to activate the appropriate actuators. The module captures signals via the input connections and forwards them to the outputs. Based on the location of the actuators, the device forwards signals to outputs located on the same module, on a different module within the same device or on another device.

When the device maps the digital input ports to the digital output ports, there is a 1:N relationship. The device mirrors the data stream of one digital input port to any number of digital outputs ports.

When the device maps the digital output ports to the digital input ports, there is a 1:1 relationship. One digital output port mirrors the data stream of one digital input port.

The dialog contains the following tabs:

▶ [IO input]

[IO input]

This tab enables you to:

- ▶ activate/deactivate the querying of the digital inputs globally
- ▶ configure the interval at which the device queries the values of the digital inputs
- ▶ activate/deactivate logging an event
- ▶ activate/deactivate the sending of SNMP traps

Operation

Operation

Enables/disables the cyclical queries from the digital inputs (IO Input).

Possible values:

- ▶ *On*
Enables you to query the input values.
- ▶ *Off* (default setting)

Configuration

Refresh interval [ms]

Specifies the time interval in milliseconds in which the device queries the values from the digital inputs.

Possible values:

- ▶ `1000..10000` (default setting: `1000`)

Table

Input ID

Displays the slot number of the module (x) and number of the digital input (i) that applies to this entry.

Notation: `x.i`

Possible values:

- ▶ `x = 0..7`
The value `0` equals the main unit (MU).
- ▶ `i = 1..4`

Value

Specifies the digital input level.

Possible values:

- ▶ `low`
The input voltage on the digital input is 0 V.
- ▶ `high`
The input voltage on the digital input is +24 VDC.
- ▶ `not-available`
The input voltage on the digital input has another value than 0 V or +24 VDC. Verify that the module is present and seated properly.

Log event

Activates/deactivates the logging in the log file. See the [Diagnostics > Report > System Log](#) dialog.

Possible values:

- ▶ `marked`
Logging is activated.
The device checks the status of the digital inputs in accordance with the time interval specified in the [Configuration](#) frame, [Refresh interval \[ms\]](#) field.
When changes on the digital inputs occur, the device logs an entry in the System Log log file.
- ▶ `unmarked` (default setting)
Logging is deactivated.

Send trap

Activates/deactivates the sending of SNMP traps when the device detects a change on the digital inputs.

The device checks the status of the digital inputs in accordance with the time interval specified in the *Configuration* frame, *Refresh interval [ms]* field.

Possible values:

- ▶ *marked*
The sending of SNMP traps is active.
When the device detects changes on the digital inputs, the device sends an SNMP trap.
- ▶ *unmarked* (default setting)
The sending of SNMP traps is inactive.

The prerequisite for sending SNMP traps is that you enable the function in the *Diagnostics > Status Configuration > Alarms (Traps)* dialog and specify at least one trap destination.

Buttons

You find the description of the standard buttons in section “Buttons” on page 17.

7.6 Command Line Interface

[Advanced > CLI]

This dialog lets you access the device using the Command Line Interface.

The prerequisites are:

- In the device, enable the SSH server in the *Device Security > Management Access > Server* dialog, tab *SSH*.
- On your workstation, install a SSH-capable client application which registers a handler for URLs starting with `ssh://` in your operating system.

Buttons

You find the description of the standard buttons in section “Buttons” on page 17.

Open SSH connection

Opens the SSH-capable client application.

When you click the button, the web application passes the URL of the device starting with `ssh://` and the user name of the currently logged in user.

If the web browser finds a SSH-capable client application, then the SSH-capable client establishes a connection to the device using the SSH protocol.

A Index

0-9	
802.1D/p mapping	274
802.1X	117, 164
A	
Access control	164
Access control lists	217
Access restriction	143
ACL	217
Address conflict detection	368
Aging time	227, 372
Alarms	363
ARP	368
ARP inspection	208
ARP table	372
Audit trail	434
Authentication history	178
Authentication list	117
Auto disable	158, 197, 211, 213, 299, 305, 395, 396, 404, 420
B	
Boundary clock	83
Bridge	296
C	
Cable diagnosis	390
Certificate	21, 48, 122, 140, 141, 353, 377, 384
CLI	148
Command line interface	148
Community names	151
Configuration profile	15, 38
ConneXium Network Manager	11, 131
Context menu	15
Counter reset	66
D	
Daylight saving time	70
Device software	35
Device software backup	35
Device status	19, 344
DHCP L2 relay	437
DHCP server	443
DHCP snooping	195
DHCPv6 L2 Relay	437
Digital input	466
DNS	452
DNS cache	453
DNS client	453
Domain name system	452
DoS	191
Download EDS for EtherNet/IP	464
DSCP	276
Duplicate Address Detection	30
Dynamic ARP inspection	208

E	
EAPOL	176
Egress rate limiter	229
Email notification	376
Encryption	38
ENVM	36, 38, 43, 49, 345, 351, 358, 431
Ethernet Switch Configurator	24, 352, 434
EtherNet/IP	353, 464
EtherNet/IP, Download EDS	464
EtherNet/IP, Read/write capability	464
EtherNet/IP, VLAN	464
Event severity	380, 428
External memory	36, 38, 43, 49, 431
F	
FDB	232
Filter MAC addresses	232
Fingerprint	135, 139
Flash memory	36, 367
Flow control	227
Forwarding database	232
G	
GARP	266
GMRP	267
Guards	312
GVRP	269
H	
Hardware clock	69
Hardware state	367
HIPER ring	293
Host key	137
HTML	366, 433
HTTP	137
HTTP server	350
HTTPS	138
I	
IAS	117, 180
IEC61850-MMS	353, 459
IEEE 802.1X	117
IGMP snooping	234
Ingress filtering	285
Ingress rate limiter	229
Integrated authentication server	117, 180
IO input	466
IP access restriction	143
IP address conflict detection	368
IP DSCP mapping	276
IP source guard	204
IPv4 rule	218

L	
L2 relay	437
LDAP	117
Link aggregation	315
Link backup	322
LLDP	410
Load/save	38
Log file	66, 433
Login banner	149, 152
Loop protection	359
Loops	295
M	
MAC address table	232
MAC flood	157
MAC rule	221
MAC spoof	157
Mail notification	376
Management access	24, 29, 143
Management VLAN	24
Manufacturing message specification	459
Media redundancy protocol	289
Menu	15
MMRP	258
MMS	459
Modbus TCP	353, 462
MRP	289
MRP-IEEE	256
MVRP	263
N	
Network load	57
NVM	14, 16, 22, 36, 43
O	
Out-of-band management port	33
P	
Password	112, 349
Password length	112, 349
Persistent logging	430
PoE	59
Port clients	174
Port configuration	168, 272
Port mirroring	408
Port monitor	404
Port priority	272
Port security	157
Port statistics	176
Port VLAN	284
Port-based access control	164
Power over Ethernet	59
Power supply	21, 346, 359
Pre-Login banner	152
Priority queue	271
Q	
Queue management	278
Queues	271

R	
RADIUS	117, 181
RAM	42
RAM test	374
Rate limiter	229
RCP	338
Read/write capability for EtherNet/IP	464
Reboot	66
Redundant coupling protocol	338
Relay	437
Request interval	75
Ring structure	289
Ring/Network coupling	332
RNC	332
Root bridge	296
RSTP	295, 296
S	
Secure shell	134
Security status	20, 348
Self-test	374
Serial interface	351
Settings	38
Severity	380, 428
SFP module	388
Signal contact	20, 355
SNMP server	131, 351
SNMP traps	55, 60, 62, 160, 296, 303, 318, 344, 348, 357, 363, 370, 395, 468
SNMPv1/v2	151
SNTP	73
SNTP client	74
SNTP server	78
Software backup	35
Software update	35
Source guard	204
Spanning tree protocol	295
SSH server	134
Subring	327
Switch dump	428
Syslog	384
System information	366
System log	433
System monitor	374
System time	69
T	
Telnet server	132, 350
Temperature	22, 345, 358
Threshold values network load	229
Time-Sensitive Networking	249
Topology discovery	415
Transparent clock	93
Trap destination	363
Traps	55, 60, 62, 160, 296, 303, 318, 344, 348, 357, 363, 370, 395, 468
Trust mode	272
TSN Configuration	249
TSN Gate Control List	252, 255
Twisted pair	390

U	
USB network interface	33
User administration	111
Utilization	57
V	
Virtual local area network	279
VLAN	24, 279, 421
VLAN configuration	282
VLAN for EtherNet/IP	464
VLAN ports	284
W	
Watchdog	38, 42
Web server	137, 138
Z	
ZIP archive	428

