Modicon MCSESM, MCSESP Series Managed Switch

Graphic User Interface

User Guide

Original instructions

QGH59084.03
02/2026

www.se.com

Legal Information

The information provided in this document contains general descriptions, technical characteristics and/or recommendations related to products/solutions.

This document is not intended as a substitute for a detailed study or operational and site-specific development or schematic plan. It is not to be used for determining suitability or reliability of the products/solutions for specific user applications. It is the duty of any such user to perform or have any professional expert of its choice (integrator, specifier or the like) perform the appropriate and comprehensive risk analysis, evaluation and testing of the products/solutions with respect to the relevant specific application or use thereof.

The Schneider Electric brand and any trademarks of Schneider Electric SE and its subsidiaries referred to in this document are the property of Schneider Electric SE or its subsidiaries. All other brands may be trademarks of their respective owner.

Schneider Electric does not grant any right or license for commercial use of the document or its content, except for a non-exclusive and personal license to consult it on an "as is" basis.

Schneider Electric reserves the right to make changes or updates with respect to or in the content of this document or the format thereof, at any time without notice.

To the extent permitted by applicable law, no responsibility or liability is assumed by Schneider Electric and its subsidiaries for any errors or omissions in the informational content of this document, as well as any non-intended use or misuse of the content thereof.

Table of Contents

Safety Information 15
Before You Begin 15
Start-up and Test 16
Operation and Adjustments 17
About the Document 18
Notes on the Graphical User Interface 22
Banner 22
Menu Pane 22
Icon Toolbar 22
Menu Tree 23
Dialog Area 23
Control Elements 23
Modification Mark 24
Standard Buttons 24
Saving the Settings 24
Updating the Display 25
Working with Tables 25
Basic Settings 26
System 26
Device Status 26
Security Status 27
Signal Contact Status 27
System Data 28
LED Status 29
Port Status 29
Network 30
Global 30
Management Interface 30
Ethernet Switch Configurator Protocol V1/V2 30
IPv4 31
Configuration 31
Management Interface 31
IP Parameter 32
BOOTP/DHCP 33
IPv6 33
Operation 33
Configuration 34
Management Interface 34
DHCP 34
IP Parameter 35
Duplicate Address Detection 35
IPv6 Addresses 35
Out-of-Band over USB 36
Operation 37
Management Interface 37
IP Parameter 37
Software 38
Version 38

Software Update 38
File System Table 39
Load/Save 40
Load/Save Table 40
External Memory 44
Configuration Encryption 45
Undo Configuration Modifications 46
Information 46
Backup Config on a Remote Server when Saving 47
External Memory 47
External Memory Table 47
Port 49
Port Configuration Table 49
Statistics 52
Ingress Utilization Table 52
Power over Ethernet (MCSESP) 53
PoE Global 53
Operation 54
Configuration 54
System Power 54
PoE Global Table 54
PoE Port 55
PoE Port Table 55
Restart 57
Restart 57
Buttons 58
Time 59
Basic Settings 59
Global 59
Daylight Saving Time 60
Time Profile 62
Table 63
SNTP 65
SNTP Client 66
Operation 66
State 66
Configuration 67
Table 67
SNTP Server 69
Operation 70
State 70
Configuration 71
PTP 72
PTP Global 72
Operation IEEE1588/PTP 73
Configuration IEEE1588/PTP 73
Status 74
PTP Boundary Clock 74
PTP Boundary Clock Global 74
Operation IEEE1588/PTPv2 BC 75
Status IEEE1588/PTPv2 BC 76

Grandmaster 76
Local Time Properties 78
Identities 78
PTP Boundary Clock Port 79
Table 79
PTP Transparent Clock 82
PTP Transparent Clock Global 82
Operation IEEE1588/PTPv2 TC 83
Local Synchronization 85
Status IEEE1588/PTPv2 TC 85
PTP Transparent Clock Port 86
Table 86
802.1AS 87
802.1AS Global 87
Operation 87
Configuration 88
Status 88
Grandmaster 88
Parent 89
802.1AS Port 90
Instance 90
802.1AS Statistics 96
Instance 97
Device Security 98
User Management 98
Configuration 98
Password policy 99
Table 100
Authentication List 102
Table 103
LDAP 105
LDAP Configuration 105
Operation 106
Configuration 107
Certificates/CRLs 107
Table 109
LDAP Role Mapping 111
Configuration 112
Table 112
Management Access 114
Server 114
Information 114
SNMP 116
Telnet 118
SSH 119
HTTP 122
HTTPS 123
IP Access Restriction 127
Operation 127
Table 127
Web 129

Configuration 130
Command Line Interface 130
Global 130
Login Banner 131
SNMPv1/v2 Community 132
Table 132
Configuration 133
Pre-Login Banner 133
Operation 134
Banner Text 134
SSH Known Hosts 134
Table 134
Network Security 137
Network Security Overview 137
Port Security 137
Operation 138
Mode 139
Configuration 139
Table 139
Wizard: Port Security 141
802.1X 143
802.1X Global 144
Operation 144
Configuration 145
MAC Authentication Bypass Format Options 146
Information 147
802.1X Port Configuration 147
Table 147
802.1X Port Clients 151
Table 151
802.1X EAPOL Port Statistics 152
Table 152
802.1X Port Authentication History 153
Table 153
802.1X Integrated Authentication Server (IAS) 154
Table 154
RADIUS 155
RADIUS Global 156
RADIUS Configuration 156
RADIUS Authentication Server 157
Table 157
RADIUS Accounting Server 159
Table 159
RADIUS Authentication Statistics 160
Table 160
RADIUS Accounting Statistics 160
Table 161
DoS 161
DoS Global 161
TCP/UDP 161
IP 163

ICMP 163
Information 164
DHCP Snooping 164
DHCP Snooping Global 165
Operation 165
Configuration 166
Binding Database 166
DHCP Snooping Configuration 166
Port 167
VLAN ID 169
DHCP Snooping Statistics 169
Table 169
DHCP Snooping Bindings 170
Table 170
IP Source Guard 171
IP Source Guard Port 172
Table 172
IP Source Guard Bindings 173
Table 173
Dynamic ARP Inspection 174
Dynamic ARP Inspection Global 175
Configuration 176
Dynamic ARP Inspection Configuration 177
Port 177
VLAN ID 178
Dynamic ARP Inspection ARP Rules 179
Table 180
Dynamic ARP Inspection Statistics 180
Table 180
ACL 181
ACL IPv4 Rule 182
Table 182
ACL MAC Rule 189
Table 189
ACL Assignment 193
Table 193
Switching 195
Switching Global 195
Configuration 196
Rate Limiter 196
Ingress 196
Egress 198
Filter for MAC Addresses 198
Table 198
IGMP Snooping 200
IGMP Snooping Global 201
Operation 201
Information 202
IGMP Snooping Configuration 202
VLAN ID 202
Port 204

IGMP Snooping Enhancements 206
Table 206
Wizard: IGMP Snooping Enhancements 209
IGMP Snooping Querier 209
Operation 210
Configuration 210
Table 210
IGMP Snooping Multicasts 211
Configuration 212
Table 212
Time-Sensitive Networking 212
TSN Configuration 212
Operation 213
Base Time 213
Configuration 214
Table 214
TSN Gate Control List 215
TSN Configured Gate Control List 216
<Port number> 216
TSN Current Gate Control List 217
<Port number> 218
MRP-IEEE 218
MRP-IEEE Configuration 218
Table 219
MRP-IEEE Multiple MAC Registration Protocol 219
Configuration 219
Service requirement 221
Statistics 221
MRP-IEEE Multiple VLAN Registration Protocol 222
Configuration 223
Statistics 224
GARP 225
GMRP 225
Operation 226
Multicasts 226
Table 226
GVRP 227
Operation 227
Table 227
QoS/Priority 227
QoS/Priority Global 228
Configuration 228
QoS/Priority Port Configuration 229
Table 229
802.1D/p Mapping 229
Table 230
Default Assignment of the VLAN Priority to *Traffic Classes* 230
IP DSCP Mapping 231
Table 231
Default Assignment of the DSCP Values to *Traffic Classes* 232
Queue Management 232

Table....232
VLAN....234
VLAN Global....234
Configuration....235
VLAN Configuration....235
Table....235
VLAN Port....237
Table....238
VLAN Voice....238
Operation....239
Table....239
Private VLAN....241
VLAN Type....241
VLAN Association....242
Port Association....242
L2-Redundancy....244
MRP....244
Operation....245
Ring Port 1/Ring Port 2....245
Configuration....246
Information....247
HIPER Ring....247
Operation....248
Ring Port 1/Ring Port 2....249
Information....249
Spanning Tree....249
Spanning Tree Global....250
Operation....250
Variant....250
Traps....251
Bridge Configuration....252
Root Information....255
Topology Information....256
Spanning Tree MSTP....256
MST Region Identifier....257
Global CIST Parameter....258
Table....259
Spanning Tree Port....261
CIST....261
Guards....265
MSTI <MSTI>....267
Link Aggregation....269
Configuration....270
Table....270
Link Backup....276
Operation....276
Table....276
Create....278
FuseNet....278
Sub Ring....279
Operation....280

Information 280
Table 280
Ring/Network Coupling 283
Operation 285
Information 286
Mode 287
Coupling Port 287
Partner Coupling Port 288
Control Port 288
Configuration 289
Redundant Coupling Protocol 289
Operation 290
Primary Ring/Network / Secondary Ring/Network 290
Coupler Configuration 291
Diagnostics 292
Status Configuration 292
Device Status 292
Global 293
Port 295
Status 295
Security Status 296
Global 296
Port 301
Status 302
Signal Contact 302
Signal Contact 1 / Signal Contact 2 302
Global 303
Port 306
Status 306
MAC Notification 307
Operation 307
Configuration 307
Table 307
Alarms (Traps) 308
Trap V3 User Management 308
Table 309
Trap Destinations 311
Operation 311
SNMPv1/v2 Trap Community 311
Table 311
System 313
System Information 313
Hardware State 313
Information 314
Table 314
IP Address Conflict Detection 314
Operation 314
Information 315
Configuration 316
Table 317
ARP 317

Table....317
Selftest....318
Configuration....318
Table....319
Email Notification....320
Email Notification Global....320
Operation....321
Information....321
Certificates/CRLs....321
Sender....323
Notification Urgent....323
Notification Non-Urgent....323
Meaning of the Event Severities....324
Email Notification Recipients....324
Table....325
Email Notification Mail Server....325
Table....325
Syslog....327
Operation....327
Certificates/CRLs....327
Table....329
Ports....331
SFP....331
Table....331
TP Cable Diagnosis....332
Information....332
Table....332
Port Monitor....333
Global....334
Auto-Disable....337
Link Flap....338
CRC/Fragments....339
Overload Detection....339
Link speed/Duplex Mode Detection....340
Auto-Disable....343
Port....343
Status....345
Port Mirroring....346
Operation....346
Destination Port....347
Table....347
RSPAN....349
Operation....349
Role....349
Source Switch....350
Destination Switch....351
LLDP....352
LLDP Configuration....352
Operation....352
Configuration....353
Table....353

LLDP Topology Discovery 355
LLDP 355
LLDP-MED 356
Loop Protection 358
Operation 358
Configuration 359
Global 359
Table 359
SFlow 361
SFlow Configuration 361
Global 362
Sampler 362
Poller 362
SFlow Receiver 363
Table 363
Report 364
Report Global 364
Console Logging 365
SNMP Logging 365
Buffered Logging 366
CLI Logging 367
Support Information: Files in ZIP archive 367
Meaning of the Event Severities 368
Persistent Logging 368
Operation 368
Configuration 369
Table 369
System Log 370
Audit Trail 370
Advanced 372
DHCP 372
DHCP Server 372
DHCP Server Global 372
Operation 372
Configuration 373
Table 373
DHCP Server Pool 373
Table 375
DHCP Server Lease Table 378
Table 379
DHCP L2 Relay 380
DHCP L2 Relay Configuration 380
Operation 381
Interface 381
VLAN ID 382
DHCP L2 Relay Statistics 383
Table 383
DNS 383
DNS Client 383
DNS Client Global 384
Operation 384

Cache 384
DNS Client Current 384
Table 385
DNS Client Static 385
Configuration 385
Table 386
DNS Client Static Hosts 386
Table 387
Industrial Protocols 388
IEC 61850-MMS 388
Operation 388
Information 389
Configuration 390
Modbus TCP 390
Operation 391
Configuration 391
EtherNet/IP 392
Operation 392
Configuration 392
VLAN Configuration 393
OPC UA Server 393
Operation 393
Configuration 394
Table 395
Service Discovery 396
ITxPT Module Inventory 396
Operation 397
Table 398
Tracking 398
Tracking Configuration 399
Table 400
Tracking Applications 402
Table 403
Digital IO Module 403
IO input Tab 403
Command Line Interface 406
Button 406
Index 407

Safety Information

Important Information

Read these instructions carefully, and look at the equipment to become familiar with the device before trying to install, operate, service, 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 a hazardous situation which, if not avoided, **will result in** death or serious injury.

⚠ WARNING

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

⚠ CAUTION

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

NOTICE

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

Please 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.

Before You Begin

Do not use this product on machinery lacking effective point-of-operation guarding. Lack of effective point-of-operation guarding on a machine can result in serious injury to the operator of that machine.

⚠WARNING

UNGUARDED EQUIPMENT

- Do not use this software and related automation equipment on equipment which does not have point-of-operation protection.
- Do not reach into machinery during operation.

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

This automation equipment and related software is used to control a variety of industrial processes. The type or model of automation equipment suitable for each application will vary depending on factors such as the control function required, degree of protection required, production methods, unusual conditions, government regulations, etc. In some applications, more than one processor may be required, as when backup redundancy is needed.

Only you, the user, machine builder or system integrator can be aware of all the conditions and factors present during setup, operation, and maintenance of the machine and, therefore, can determine the automation equipment and the related safeties and interlocks which can be properly used. When selecting automation and control equipment and related software for a particular application, you should refer to the applicable local and national standards and regulations. The National Safety Council's Accident Prevention Manual (nationally recognized in the United States of America) also provides much useful information.

In some applications, such as packaging machinery, additional operator protection such as point-of-operation guarding must be provided. This is necessary if the operator's hands and other parts of the body are free to enter the pinch points or other hazardous areas and serious injury can occur. Software products alone cannot protect an operator from injury. For this reason the software cannot be substituted for or take the place of point-of-operation protection.

Ensure that appropriate safeties and mechanical/electrical interlocks related to point-of-operation protection have been installed and are operational before placing the equipment into service. All interlocks and safeties related to point-of-operation protection must be coordinated with the related automation equipment and software programming.

NOTE: Coordination of safeties and mechanical/electrical interlocks for point-of-operation protection is outside the scope of the Function Block Library, System User Guide, or other implementation referenced in this documentation.

Start-up and Test

Before using electrical control and automation equipment for regular operation after installation, the system should be given a start-up test by qualified personnel to verify correct operation of the equipment. It is important that arrangements for such a check are made and that enough time is allowed to perform complete and satisfactory testing.

⚠WARNING

EQUIPMENT OPERATION HAZARD

- Verify that all installation and set up procedures have been completed.
- Before operational tests are performed, remove all blocks or other temporary holding means used for shipment from all component devices.
- Remove tools, meters, and debris from equipment.

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

Follow all start-up tests recommended in the equipment documentation. Store all equipment documentation for future references.

Software testing must be done in both simulated and real environments.

Verify that the completed system is free from all short circuits and temporary grounds that are not installed according to local regulations (according to the National Electrical Code in the U.S.A, for instance). If high-potential voltage testing is necessary, follow recommendations in equipment documentation to prevent accidental equipment damage.

Before energizing equipment:

- Remove tools, meters, and debris from equipment.
- Close the equipment enclosure door.
- Remove all temporary grounds from incoming power lines.
- Perform all start-up tests recommended by the manufacturer.

Operation and Adjustments

The following precautions are from the NEMA Standards Publication ICS 7.1-1995:

(In case of divergence or contradiction between any translation and the English original, the original text in the English language will prevail.)

- Regardless of the care exercised in the design and manufacture of equipment or in the selection and ratings of components, there are hazards that can be encountered if such equipment is improperly operated.
- It is sometimes possible to misadjust the equipment and thus produce unsatisfactory or unsafe operation. Always use the manufacturer’s instructions as a guide for functional adjustments. Personnel who have access to these adjustments should be familiar with the equipment manufacturer’s instructions and the machinery used with the electrical equipment.
- Only those operational adjustments required by the operator should be accessible to the operator. Access to other controls should be restricted to prevent unauthorized changes in operating characteristics.

About the Document

Document Scope

This document describes how to use the graphical user interface to operate the individual functions of the the Modicon MCSESM, MCSESP series managed switches.

Validity Note

The characteristics of the products described in this document are intended to match the characteristics that are available on www.se.com. As part of our corporate strategy for constant improvement, we may revise the content over time to enhance clarity and accuracy. If you see a difference between the characteristics in this document and the characteristics on www.se.com, consider www.se.com to contain the latest information.

Product Related Information

⚠WARNING

LOSS OF CONTROL

- Perform a Failure Mode and Effects Analysis (FMEA) or equivalent risk analysis of your application and apply preventive and detective controls before implementation.
- Provide a fallback state for undesired control events or sequences.
- Provide separate or redundant control paths wherever required.
- Supply appropriate parameters, particularly for limits.
- Review the implications of transmission delays and take actions to mitigate them.
- Review the implications of communication link interruptions and take actions to mitigate them.
- Provide independent paths for control functions (for example, emergency stop, over-limit conditions, and error conditions) according to your risk assessment, and applicable codes and regulations.
- Apply local accident prevention and safety regulations and guidelines.[1]
- Test each implementation of a system for proper operation before placing it into service.

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

[1] For additional information, refer to NEMA ICS 1.1 (latest edition), Safety Guidelines for the Application, Installation, and Maintenance of Solid State Control and to NEMA ICS 7.1 (latest edition), Safety Standards for Construction and Guide for Selection, Installation and Operation of Adjustable-Speed Drive.

⚠WARNING

UNINTENDED EQUIPMENT OPERATION

- Only use software approved by Schneider Electric for use with this equipment.
- Update your application program every time you change the physical hardware configuration.

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

General Cybersecurity Information

In recent years, the growing number of networked machines and production plants has seen a corresponding increase in the potential for cyber threats, such as unauthorized access, data breaches, and operational disruptions. You must, therefore, consider all possible cybersecurity measures to help protect assets and systems against such threats.

To help keep your Schneider Electric products secure and protected, it is in your best interest to implement the cybersecurity best practices as described in the Cybersecurity Best Practices document.

Schneider Electric provides additional information and assistance:

- Subscribe to the Schneider Electric security newsletter.
- Visit the Cybersecurity Support Portal web page to:

  Find security notifications.

  Report vulnerabilities and incidents.
- Visit the Schneider Electric Cybersecurity and Data Protection Posture web page to:

  Access the cybersecurity posture.

  Learn more about cybersecurity in the cybersecurity academy.

  Explore the cybersecurity services from Schneider Electric.

Environmental Data

For product compliance and environmental information, refer to the Schneider Electric Environmental Data Program.

Available Languages of the Document

Language	Reference number
English	QGH59084
French	QGH59087
German	QGH59086
Italian	QGH59089
Spanish	QGH59088
Chinese	QGH59090

Related Documents

Title of documentation	Reference number
Modicon MCSESM, MCSESP Series Managed Switch Installation Guide	QGH59091 (EN) QGH59094 (FR) QGH59093 (DE) QGH59096 (IT) QGH59095 (ES) QGH59097 (CN)
Modicon MCSESM, MCSESP Series Managed Switch Configuration Guide	QGH59056 (EN) QGH59080 (FR) QGH59058 (DE) QGH59082 (IT) QGH59081 (ES) QGH59083 (CN)
Modicon MCSESM, MCSESP Series Managed Switch Command Line Interface User Guide	QGH59098 (EN)
Modicon MCSESM, MCSESP Series Managed Switch Security User Guide	EIO0000005492 (EN) EIO0000005493 (FR) EIO0000005494 (DE) EIO0000005495 (IT) EIO0000005496 (ES) EIO0000005497 (CN)

To find documents online, visit the Schneider Electric download center (www.se.com/ww/en/download/).

Terminology Derived from Standards

The technical terms, terminology, symbols and the corresponding descriptions in the information contained herein, or that appear in or on the products themselves, are generally derived from the terms or definitions of international standards.

In the area of functional safety systems, drives and general automation, this may include, but is not limited to, terms such as *safety*, *safety function*, *safe state*, *fault*, *fault reset*, *malfunction*, *failure*, *error*, *error message*, *dangerous*, etc.

Among others, these standards include:

Standard	Description
IEC 61131-2:2007	Programmable controllers Part 2: Equipment requirements and tests.
ISO 13849-1:2023	Safety of machinery: Safety related parts of control systems. General principles for design.
EN 61496-1:2020	Safety of machinery: Electro-sensitive protective equipment. Part 1: General requirements and tests.
ISO 12100:2010	Safety of machinery - General principles for design - Risk assessment and risk reduction
EN 60204-1:2006	Safety of machinery - Electrical equipment of machines - Part 1: General requirements
ISO 14119:2013	Safety of machinery - Interlocking devices associated with guards - Principles for design and selection
ISO 13850:2015	Safety of machinery - Emergency stop - Principles for design
IEC 62061:2021	Safety of machinery - Functional safety of safety-related electrical, electronic, and electronic programmable control systems
IEC 61508-1:2010	Functional safety of electrical/electronic/programmable electronic safety-related systems: General requirements.

Standard	Description
IEC 61508-2:2010	Functional safety of electrical/electronic/programmable electronic safety-related systems: Requirements for electrical/electronic/ programmable electronic safety-related systems.
IEC 61508-3:2010	Functional safety of electrical/electronic/programmable electronic safety-related systems: Software requirements.
IEC 61784-3:2021	Industrial communication networks - Profiles - Part 3: Functional safety fieldbuses - General rules and profile definitions.
2006/42/EC	Machinery Directive
2014/30/EU	Electromagnetic Compatibility Directive
2014/35/EU	Low Voltage Directive

In addition, terms used in the present document may tangentially be used as they are derived from other standards such as:

Standard	Description
IEC 60034 series	Rotating electrical machines
IEC 61800 series	Adjustable speed electrical power drive systems
IEC 61158 series	Digital data communications for measurement and control – Fieldbus for use in industrial control systems

Finally, the term *zone of operation* may be used in conjunction with the description of specific hazards, and is defined as it is for a *hazard zone* or *danger zone* in the *Machinery Directive* (*2006/42/EC*) and *ISO 12100:2010*.

NOTE: The aforementioned standards may or may not apply to the specific products cited in the present documentation. For more information concerning the individual standards applicable to the products described herein, see the characteristics tables for those product references.

Information on Non-Inclusive or Insensitive Terminology

As a responsible, inclusive company, Schneider Electric is constantly updating its communications and products that contain non-inclusive or insensitive terminology. However, despite these efforts, our content may still contain terms that are deemed inappropriate by some customers.

Trademarks

QR Code is a registered trademark of DENSO WAVE INCORPORATED in Japan and other countries.

Notes on the Graphical User Interface

The use of the GUI (graphical user interface) requires a web browser with HTML5 support.

The GUI automatically adapts to the size of your screen.

The GUI has the following sections:

- Banner, page 22
- Menu pane, page 22
- Dialog area, page 23

Banner

The banner displays the following information:

Icon	Description
	Displays or hides the menu pane.
Brand logo	Select the brand logo to open the device manufacturer website in a new window.
Dialog name	Displays the name of the dialog currently displayed.
	States the web browser cannot contact the device. The connection to the device is interrupted.
	Displays if the settings in the volatile memory (**RAM**) differ from the settings of the **Selected** configuration profile in the non-volatile memory (**NVM**). The banner displays the icon if you have applied the settings, but not yet saved them in the non-volatile memory (**NVM**).
	Select the button to open the online help in a new window.
	Select the button to display a tool tip that provides the following information: • The summary of the **Device status** frame. See the **Basic Settings > System** dialog. • The summary of the **Security status** frame. See the **Basic Settings > System** dialog. A red dot next to the icon means that at least one of the values is greater than **0**.
	Select the button to open a submenu with the following menu items: • User account name • Logout button

Menu Pane

To display or hide the menu pane, select the  button in the banner. The menu pane displays the following:

- Icons bar, page 22
- Menu tree, page 23

Icon Toolbar

The icon toolbar displays the following information:

Icon	Description
Device software	Displays the version number of the software that the device loaded during the last system startup.
	Displays a text field to search.
	The menu tree displays a menu item only for those dialogs in which at least one parameter differs from the default setting (diff to default). To display the complete menu tree, select the  button.
	Expands the menu tree. To display the collapsed menu tree, select the  button.

Menu Tree

The menu tree contains one item for each dialog in the GUI. You can change the view of the menu tree by selecting the buttons in the icons bar at the top. You can also change the view of the menu tree by selecting the following buttons:

Icon	Description
	Expands the menu item to display the menu items of the next lower level. The menu tree displays the button next to each collapsed menu item that contains menu items on the next lower level.
	Collapses the menu item to hide the menu items of the lower levels. The menu tree displays the button next to each expanded menu item.

Dialog Area

In the dialog area, you can monitor and change the settings of the device depending on your access role. The following information describes how to use the dialogs.

- Control elements, page 23
- Modification mark, page 24
- Standard buttons, page 24
- Saving the settings, page 24
- Updating the display, page 25
- Working with tables, page 25

Control Elements

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

The control elements have the following properties:

- Read-only control elements

  Medium-dark border

  Light background (check boxes, radio buttons)

  Shaded background (input fields)
- Editable control elements

  Dark border

  Light background

Modification Mark

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

Standard Buttons

The special dialog-specific buttons are described in the corresponding dialog help text.

Icon	Description
	Applies the settings you modified to the device. For more Information on how the device retains the modified settings even after a reboot, see the Saving the settings, page 24 topic.
	Undoes the unsaved changes in the present dialog. Resets the values in the fields to the settings applied to the device.

Saving the Settings

When applying settings, the device temporarily stores the modified settings. To do this, perform the following step:

- Select the  button.

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

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

- Open the **Basic Settings > Load/Save** dialog.
- In the table, mark the far left check box in the table row.
- When the check box in the **Selected** column is unmarked, select the  button and then the **Select** item.
- Select the  button to save your changes.

Updating the Display

If a dialog remains open, the values in the device have possibly changed. To update the display in the dialog, select the  button. Unsaved information in the dialog is lost.

Working with Tables

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

The following sections describe how to use the tables:

- Filtering table rows, page 25
- Sorting table rows, page 25
- Selecting multiple table rows, page 25

Filtering Table Rows

The filter allows you to reduce the number of displayed table rows:

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

Sorting Table Rows

When you select the table header, an icon displays the sorting status so you can change the order of the table rows, if desired.

Icon	Description
	The table rows are sorted in descending order based on the entries of the corresponding column. Select the icon to sort the table rows in ascending order based on the entries of the corresponding column. You can restore the initial sorting in the table only after logging out and logging in.
	The table rows are sorted in ascending order based on the entries of the corresponding column. Select the icon to sort the table rows in descending order based on the entries of the corresponding column. You can restore the initial sorting in the table only after logging out and logging in.

Selecting Multiple Table Rows

You can select multiple table rows and apply an action to the selection.

- To select individual table rows, mark the left check box in the table row..
- To select all table rows, mark the left check box in the table header.

You can now apply an action to each of these table rows simultaneously, for example:

- Enter or change the values in one table column
- Remove multiple table rows

Basic Settings

The menu contains the following dialogs:

- System, page 26
- Network, page 30
- Out-of-band over USB, page 36
- Software, page 38
- Load/save, page 40
- External memory, page 47
- Port, page 49
- Power over Ethernet (MCSESP), page 53
- Restart, page 57

System

This dialog **Basic Setting > System** displays information about the operating status of the device.

Device Status

The following table presents the device status:

Icon	Description
 Device status	Displays the device status and alarms. When at least one alarm is present, the background color isred. Otherwise, the background color remains green. Specify the parameters that you want the device to monitor in the **Diagnostics > Status Configuration > Device Status** dialog. If a monitored parameter differs from the desired status, then the device triggers an alarm. A tooltip displays the cause of the alarms and the time at which the device triggered each alarm. To display the tooltip, hover the mouse over or tap the field. In the **Diagnostics > Status Configuration > Device Status** dialog, the **Status** tab displays an overview of the alarms. **NOTE:** If you connect only one power supply module to a device that supports two redundant power supply modules, the device triggers an alarm. To help avoid this alarm, deactivate the monitoring of the missing power supply modules in the **Diagnostics > Status Configuration > Device Status** dialog.

Security Status

The following table presents the security status:

Icon	Description
 Security status	Displays the security status and alarms. When at least one alarm is present, the background color is red. Otherwise, the background color remains green. Specify the parameters that you want the device to monitor in the **Diagnostics > Status Configuration > Security Status** dialog. If a monitored parameter differs from the desired status, the device triggers an alarm. A tooltip displays the cause of the alarms and the time at which the device triggered each alarm. To display the tooltip, hover the mouse pointer over or tap the field. In the **Diagnostics > Status Configuration > Security Status** dialog, the **Status** tab displays an overview of the alarms.

Signal Contact Status

The device can contain several signal contacts.

Icon	Description
 Signal contact status	Displays the signal contact status and alarms. When at least one alarm is present, the background color is red. Otherwise, the background color remains green. Specify the parameters that you want the device to monitor in the **Diagnostics > Status Configuration > Signal Contact > Signal Contact 1**/**Diagnostics > Status Configuration > Signal Contact > Signal Contact 2** dialog. If a monitored parameter differs from the desired status, the device triggers an alarm. A tooltip displays the cause of the alarms and the time at which the device triggered each alarm. To display the tooltip, hover the mouse pointer over or tap the field. In the **Diagnostics > Status Configuration > Signal Contact > Signal Contact 1**/**Diagnostics > Status Configuration > Signal Contact > Signal Contact 2** dialog, the **Status** tab displays an overview of the alarms.

System Data

These fields display operating data and information on the location of the device.

Icon	Description
System name	Specifies the name by which the device is defined in the network. Possible values are alphanumeric ASCII character strings with 0..255 characters, of which the following are acceptable: • **0..9** • **a..z** • **A..Z** • **!#$%&'()*+,-./:;<=>?@[\\]^_`{}~** • **<device type name>-<MAC address>** (default setting) When generating a digital certificate, the application uses the specified value as the domain name and common name. The following functions use the specified value as a hostname or fully qualified domain name (FQDN). For compatibility reasons, use only lowercase letters, as some systems differentiate uppercase from lowercase in the FQDN. Verify that the name is unique in the entire network. • DHCP client • Syslog • IEC 61850-MMS
Location	Specifies the present or planned location. Possible values are alphanumeric ASCII character stringd with 0..255 characters.
Contact person	Specifies the contact person for this device. Possible values are alphanumeric ASCII character stringd with 0..255 characters.
Device type	Displays the product name of the device.
Power supply module 1 / power supply module 2	Displays the status of the power supply module at the respective voltage supply connector. Possible values: • **present** • **defective** • **not installed** • **unknown**
Uptime	Displays the time that has elapsed since the device was last restarted. Possible values are time strings in the format **day(s), ...h ...m ...s**
Temperature [°C]	Displays the present temperature in the device in °C. Monitor the temperature threshold values in the **Diagnostics > Status Configuration > Device Status** dialog.
Upper temp. limit [°C]	Specifies the upper temperature threshold value in °C. Possible values are **-99..99** (integer). If the temperature in the device exceeds the specified value, the device displays an alarm.
Lower temp. limit [°C]	Specifies the lower temperature threshold value in °C. Possible values are **-99..99** (integer). If the temperature in the device falls below the specified value, then the device displays an alarm.
Humidity [%]	Displays the humidity in the device as a percentage. Monitor the humidity threshold values in the **Diagnostics > Status Configuration > Device Status** dialog.

Icon	Description
Upper humidity limit [%]	Specifies the upper humidity threshold value as a percentage. Possible values are **0..100** (default setting: **95**). If the humidity in the device exceeds the specified value, the device displays an alarm.
Lower humidity limit [%]	Specifies the lower humidity threshold value as a percentage. Possible values are **0..100** (default setting: **5**). If the humidity in the device falls below the specified value, the device displays an alarm.

LED Status

For further information about the device status LEDs, see the *Modicon MCSESM, MCSESP Series Managed Switch Installation User Guide*.

The following table describes the LED indicators, their colors, and their corresponding status meanings:

LED	Color	Description
Status		There is no device status alarm. The device status is OK. There is at least one device status alarm. For details, see the **Device status** dialog.
Power		Device that supports two redundant power supply modules. Only one supply voltage is active. Device that supports one power supply module. The supply voltage is active. Device that supports two redundant power supply modules. Both supply voltages are active.
EAM		No external memory (**ENVM**) is connected. The external memory (**ENVM**) is connected but not ready for operation. The external memory (**ENVM**) is connected and ready for operation.

Port Status

This frame displays the ports at the time of the last display update.

The frame displays only ports with an active link. When you select the button, the frame displays every port.

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

The following table presents the LED colors and their descriptions:

LED	Description
Green background color	Port with an active link
Gray background color	Port with an inactive link
Yellow background color	Port on which the device detected an unsupported SFP transceiver or an unsupported data rate.
Dashed border	Port in a *blocking* state due to a redundancy function.

Network

The menu **Basic Settings > Network** contains the following dialogs:

- Global, page 30
- IPv4, page 31
- IPv6, page 33

Global

This dialog **Basic Settings > Network > Global** allows you to specify the VLAN and Ethernet Switch Configurator settings required for the access to the device management through the network.

Management Interface

You can specify the VLAN in which the device management can be accessed.

Setting	Description
MAC address	Displays the MAC address of the device. The device management is accessible through the network using the MAC address.
MAC address conflict detection	Enables/disables the MAC address conflict detection function. Possible values: • **marked** The MAC address conflict detection function is enabled. The device verifies that its MAC address is unique in the network. • **unmarked** (default setting) The MAC address conflict detection function is disabled.

Ethernet Switch Configurator Protocol V1/V2

You can specify settings for 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 configurator function is enabled. You can access these devices even if they have invalid or no IP parameters assigned. You can assign or change the IP parameters in the device using the configurator protocol.

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.

The following table presents the Ethernet switch configurator protocol:

Setting	Description
Operation	Enables/disables the Ethernet switch configurator function in the device. Possible values: • **On** (default setting): The Ethernet switch configurator function is enabled. You can use the Ethernet switch configurator software to access the device from your PC. • **Off** : The Ethernet switch configurator function is disabled.
Access	Enables/disables write access to the device using the Ethernet switch configurator function. Possible values: • **ReadWrite** (default setting): The Ethernet switch configurator function has write access to the device. You can change the IP parameters in the device. • **ReadOnly** : The Ethernet switch configurator function has read-only access to the device. You can view the IP parameters in the device. Change the setting of the **ReadOnly** value only after putting the device into operation. :
Signal	Activates/deactivates the flashing of the port LEDs. You can identify the device in the field. Possible values: • **marked** The port LEDs are flashing. The port LEDs flash until you disable the function. • **unmarked** (default setting) The port LEDs are flashing.

IPv4

This dialog **Basic Settings > Network > IPv4** allows you to specify the IPv4 settings required to access the device management through the network.

Configuration

The following table presents the IPv4 configuration:

Setting	Description
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. Specify the settings 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 provides the addresses of the DNS servers, the device displays these addresses in the **Advanced > DNS > Client > Current** dialog. **NOTE:** If there is no response from the BOOTP or DHCP server, the device sets the IP address to **0.0.0.0** and tries to obtain a valid IP address.

Management Interface

The following table presents the management interface:

Setting	Description
VLAN ID	Specifies the VLAN in which the device management is accessible through the network. The device management is accessible through ports that are members of this VLAN. Possible values: • **1..4042** (default setting: **1**): The prerequisite is that in the **Switching > VLAN > Configuration** dialog, the VLAN is already set up. When you select the  button after changing the value, the Information window opens. Select the port, over which you connect to the device. After selecting 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. The device is reachable over the new port in the new device management VLAN.

IP Parameter

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

The following table presents the IP parameter settings:

Setting	Description
IP address	Specifies the IP address under which the device management can be accessed through the network. The possible value is valid IPv4 adress.
Netmask	Specifies the netmask. The possible value is valid IPv4 netmask.
Gateway address	Specifies the IP address of a router through which the device accesses other devices outside of its own network. The possible value is valid IPv4 address.

BOOTP/DHCP

The following table presents the BOOTP/DHCP settings:

Setting	Descritpion
Client ID	Displays the DHCP client ID that the device sends to the BOOTP or DHCP server. If the server is set up accordingly, it reserves an IP address for DHCP client ID. Therefore, the device receives the same IP from the server every time it requests it. The DHCP client ID that the device sends is the device name specified in the **System** name field in the **Basic Settings > System** dialog.
Lease time(s)	Displays the remaining time in seconds before the IP address, assigned to the device management by the DHCP server, expires. To update the display, select the button.
DHCP option 66/67/4/42	Enables/disables the DHCP option 66/67/4/42 function in the device. The possible values are: • **On** (default setting). The DHCP option 66/67/4/42 function is enabled. The device loads the configuration profile and receives the time server information using the following DHCP options: **Option 66: TFTP server name** **Option 67: Boot file name** The device automatically loads the configuration profile from the DHCP server into the volatile memory (**RAM**) using the trivial file transfer protocol (TFTP). The device uses the settings of the imported configuration profile in the **running-config**. **Option 4: Time server** **Option 42: Network time protocol servers** The device receives the time server information from the DHCP server. • **Off**: The DHCP option 66/67/4/42 function is disabled. The device does not load a configuration profile using DHCP Options 66/67. The device does not receive time server information using DHCP Options 4/42.

IPv6

This dialog **Basic Settings > Network > IPv6** allows you to specify the IPv6 settings required to access to the device management through the network.

Operation

The following table presents the operation setting:

Setting	Description
Operation	Enables/disables the IPv6 protocol in the device. You can operate IPv4 and IPv6 simultaneously in the device with dual IP layer technique, also referred to as dual stack. Possible values are: • **On** (default setting): IPv6 is enabled. • **Off**: IPv6 is disabled. If you want the device to operate using only IPv4, then disable IPv6 in the device.

Configuration

The following table presents the IPv6 configuration:

Setting	Description
Dynamic IP address assign-ment	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 four 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. It receives a maximum of two IPv6 addresses. An example here is the router advertisement daemon (RADVD). The RADVD uses *router solicitation* and *router advertisement* messages to automatically set up an IPv6 address. The *router solicitation* and *router advertisement* messages are described in RFC 4861. • **DHCPv6**: The device receives its IPv6 parameters from a DHCPv6 server. • **All** If you select the **All** radio button, the device receives its IPv6 parameters using alternatives for both dynamic and manual assignments.

Management Interface

The following table presents the management interface setting:

Setting	Description
VLAN ID	Specifies the VLAN in which the device management is accessible through the network. The device management is accessible through ports that are members of this VLAN. Possible values: • **1..4042** (default setting: **1**): The prerequisite is that in the **Switching > VLAN > Configuration** dialog the VLAN is already set up. When you select the  button after changing the value, the Information window opens. Select the port, through which you connect to the device. After you select the **OK** button, the new device management VLAN settings are assigned to the port. • The port is now a member of the VLAN and transmits 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. The device is reachable over the new port in the new device management VLAN.

DHCP

The following table presents the DHCP setting:

Setting	Description
Client ID	Displays the DHCPv6 client ID that the device sends to the DHCPv6 server. If the server is set up accordingly, the client device receives an IPv6 address for this DHCPv6 client ID. The IPv6 address received from the DHCPv6 server has the PrefixLength value **128**. According to RFC 8415, a DHCPv6 server cannot be used to supply gateway address or PrefixLength information. The device can receive only one IPv6 address from the DHCPv6 server.

IP Parameter

The following table presents the IP parameter setting:

Setting	Description
Gateway address	Specifies the IPv6 address of a router through which the device accesses other devices outside its own network. Possible value is a valid IPv6 address (except loopback and multicast addresses). **NOTE:** If the auto radio button is selected and you use an RADVD, the device automatically receives a link-local type gateway address with a greater metric than the manually-set gateway address.

Duplicate Address Detection

You can specify the number of consecutive *neighbor solicitation* messages that the device sends for the duplicate address detection function, which is used to determine the uniqueness of an IPv6 unicast address.

Setting	Description
Number of neighbor solicitations	Specifies the number of *neighbor solicitation* messages that the device sends for the duplicate address detection function. Possible values are: • **0**(The function is disabled.) • **1..5** (The default setting is **1**.) If the duplicate address detection function discovers that an IPv6 address is not unique on a link, the device does not log this event in the log file.

IPv6 Addresses

The following table lists the IPv6 addresses set up for device management.

For information on how to customize the appearance of the table, see Working with Tables, page 25.

The following table presents the IPv6 addresses types:

Address type	Description
Prefix	Displays the prefix of the IPv6 address in a compressed format. The prefix indicates the network part of the address.
PrefixLength	Displays the prefix length of the IPv6 address. Unlike an IPv4 address, an IPv6 address does not use a subnet mask to identify the subnet part of the address. This role is performed in IPv6 by the prefix length. The possible value is **0..128**.
IP address	Displays the full IPv6 address in a compressed format, which is automatically applied to every IPv6 address regardless of the source from which the device management receives its IPv6 parameters. The possible value is a valid IPv6 address. To use an IPv6 address in a URL, use the following URL syntax: **https://[<ipv6_address>]**. For more IPv6 compression rules and address types, see the *Modicon MCSESM MCSESP Series Managed Switch Configuration Guide*.
EUI option	Specifies whether the EUI option function is applied to the IPv6 address. When you mark this check box, the Interface ID of the IPv6 address is automatically specified. The device uses the MAC address of its interface with the values **ff** and **fe** added between byte 3 and byte 4 to generate a 64–bit Interface ID. You can only select this option for IPv6 addresses that have a prefix length equal to **64**. The possible values are: • **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. The possible values are: • **Autoconf**: The device received the IPv6 address dynamically if the auto radio button is selected. • **Manual**: The device received the IPv6 address manually. • **DHCP**: The device received the IPv6 address from a DHCPv6 server. • **Linklayer**: The device automatically sets up a link-local type IPv6 address, which cannot be changed.
Status	Displays the status of the IPv6 address. The Possible values are: • **active**: The IPv6 address is active. • **notInService**: The IPv6 address is inactive. • **notReady**: The IPv6 address is specified but not currently active because some configuration parameters are still missing. **NOTE:** When the IPv6 address is manually specified, you can manually change between **active** and **notInService** states.

Out-of-Band over USB

Basic Settings > Out-of-Band over USB

The USB port provides access to the device management out-of-band when there is a high in-band load on the switching ports. Access to the device management through the USB port uses the following protocols:

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

Accessing the device management has the following limitations:

- The management station is directly connected to the USB port.
- The USB port does not support the following features:

  Priority-tagged packets

  Packets including a VLAN tag

  DHCP L2 Relay

  LLDP

  DiffServ

  ACL

  Industrial protocols

You can change the IP parameters and disable the USB port if needed.

Operation

The following table presents the operation setting:

Setting	Description
Operation	Enables/disables the USB port. The possible values are: • **On** (default setting): You can access the device management through the USB port. • **Off**: You cannot access the device management through the USB port.

Management Interface

The following table presents the management interface settings:

Setting	Description
Device MAC address	Displays the MAC address of the USB port.
Host MAC address	Displays the MAC address of the connected management station.

IP Parameter

Verify that the IP subnet of the USB port does not overlap with a subnet connected to another device port.

Setting	Description
IP address	Specifies the IP address of the device management access through the USB port. The possible value is a valid IPv4 address. • Default setting: **91.0.0.100** • The device assigns this IP address, increased by 1, to the management station that is connected to the device. • Example: **91.0.0.100** for the USB port, **91.0.0.101** for the management station.
Netmask	Specifies the netmask. The possible value is a valid IPv4 netmask with a default setting of **255.255.255.0**.

Software

This dialog **Basic Settings > Software** displays information about the device software, which you can update.

You can restore a backup of the device software.

NOTE: Before you update the device software, follow the version-specific notes in the **Read Me** text file.

Version

The following table presents the version settings:

Setting	Description
Stored version	Displays the version number and creation date of the device software stored in the flash memory. The device loads the software during the next system startup.
Running version	Displays the version number and creation date of the device software that was loaded during the last system startup.
Backup version	Displays the version number and creation date of the device software saved as a backup in the flash memory. The device copied this software into the backup memory during the last software update or after you selected the **Restore** button.
Restore	The device swaps the software images and the values displayed in the **Stored** version and **Backup** version fields. During the next system startup, the device loads the software displayed in the **Stored** version field.
Boot-code	Displays the version number and creation date of the boot code.

Software Update

You can update the device if a suitable software image is available outside the device. If a suitable software image is saved on the selected external memory (**ENVM**), use the table in the **File system** tab.

The following table presents the software update settings:

Setting	Description
URL	Specifies the path and the file name of the device software image. You can update the software using the following options: • Software update from the PC Drag and drop the file into the area from your PC or network drive. • Software update from an FTP server Do not use this method if you transmit data over untrusted networks. If the file is on an FTP server, specify the URL in the following form: ftp://<user>:<password>@<IP address>[:port]/<file name> • Software update from a TFTP server Do not use this method if you transmit data over untrusted networks. If the file is on a TFTP server, specify the URL in the following form: tftp://<IP address>/<path>/<file name> • Software update from an SCP or SFTP server If the file is on an SCP or SFTP server, then specify the URL in one of the following forms: scp:// or sftp://<IP address>/<path>/<file name> Select the **Start** button to open the **Credentials** window. Enter the **User name** and **Password** to log into the server: scp:// or sftp://<user>:<password>@<IP address>/<path>/<file name> Remember to set up the SCP or SFTP server as an SSH known host before the device accesses the server for the first time. See the **Device Security > SSH Known Hosts** dialog.
Start	Updates the device software. • To remain logged into the device management during the software update, move the mouse pointer occasionally. Or, before you start the software update, specify a sufficiently high value in the **Web interface session timeout [min]** field of the **Device Security > Management Access > Web** dialog. • The device transfers the previously used software to the backup memory. • The device transfers the selected file to the flash memory, replacing the previously used software. During the next startup, the device boots with the software that you transferred.
Allow upload of unsigned device software	Activates/deactivates the upload of unsigned device software. The purpose of this setting is to enable the upload of a software that does not have a cryptographic signature. Possible values are: • **marked**: You can upload an unsigned device software. Uploading an unsigned device software can be a security risk. If you trust the originator, you can upload the unsigned software. • **unmarked**(default setting): You cannot upload a unsigned device software.
Secure Boot enabled	Activates a mode in which the device only boots with a device software image that has a valid cryptographic signature. Possible values are: • **marked**: During system startup, the device only boots with a device software image that has a valid cryptographic signature. Once activated, you cannot deactivate the mode. The check box is permanently grayed out. You cannot downgrade to a software version earlier than 10.0.00. The **Allow upload** of unsigned device software check box is permanently hidden. • **unmarked** (default setting): During system startup, the device boots with any device software image, whether the software image is cryptographically signed or not. The signature of a cryptographically signed software image, must be valid.

File System Table

To customize the appearance of the file system table, see Working with Tables, page 25.

The following table presents the file system table settings:

Setting	Description
Buttons	(Update firmware): Updates the device software if a suitable software image is saved on the external memory (**ENVM**). The prerequisite is that a table row is selected for which the file location column displays the value **usb**. • To remain logged in to the device management during the software update, move the mouse pointer occasionally. Or, before you start the software update, specify a sufficiently high value in the **Web interface session timeout [min]** field of the **Device Security > Management Access > Web** dialog. • The device transfers the previously used software to the backup memory. • The device transfers the selected file to the flash memory, replacing the previously used software. During the next startup, the device boots with the software that you transferred.
File location	Displays the storage location of the device software. The possible values are: • **ram**: Volatile memory of the device • **flash**: Non-volatile memory (**NVM**) • **usb**: External USB memory (EAM)
Index	Displays the index of the device software. The index numbers are as follows: • **1**: During the next system startup, the device loads this software. • **2**: The device copied this 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.

Load/Save

This dialog **Basic Settings > Load/Save** allows you to 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 can also import 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, the device saves both the present 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, the device loads the configuration profile saved in the non-volatile memory (**NVM**) after the specified time.

Load/Save Table

To customize the appearance of the Load/Save table, see Working with Tables, page 25.

The following table presents the load/save table:

Setting	Buttons	Description
Buttons	(Remove)	Removes the configuration profile selected in the table from the non-volatile memory (**NVM**) or from the external memory (**ENVM**). If the configuration profile is designated as **Selected**, the device helps prevent you from removing the configuration profile.

Setting	Buttons	Description
	(Save)	Saves the temporarily applied settings in the configuration profile designated as **Selected** in the non-volatile memory (**NVM**). Within the **Basic Settings > External Memory** dialog, if the check box in the **Backup config when saving** column is marked, the device saves a copy of the configuration profile in the external memory (**ENVM**).
		Displays a context menu with functions for the corresponding dialog.
	Save as...	Opens the **Save as...** window to copy the configuration profile selected in the table and saves it with a user-specified name in the non-volatile memory (**NVM**). • Select the **Profile name** drop-down list and enter the name for saving the configuration profile (maximum 32 characters) in the search box. To overwrite an existing configuration profile, select the desired item from the search results. To save the configuration profile with a new name, select the **Create** link below the search box. Within the **Basic Settings > External Memory** dialog, if the check box in the **Backup config when saving** column is marked, the device designates the configuration profile of the same name in the external memory as **Selected**. **NOTE:** Before adding additional configuration profiles, decide for or against permanently activated configuration encryption in the device. Save additional configuration profiles either unencrypted or encrypted with the same password.
	Activate	Loads the settings of the configuration profile selected in the table to the volatile memory (**RAM**). • The device terminates the connection to the GUI. To access the device management again, perform the following steps: Reload the GUI. Log in again. • The device immediately uses the settings of the configuration profile. Enable the **Undo configuration modifications** function before you activate another configuration profile. If the connection is lost afterwards, 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, the device loads an unencrypted configuration profile. If the configuration encryption is active and the password matches the password stored in the device, 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 the software version. The device sets the values of new functions to their default value.
	Select	Designates the configuration profile selected in the table as **Selected**. In the **Selected** column, the check box is **marked**. When applying the **Undo configuration modifications** function or during the system startup, the device loads the settings of this configuration profile to the volatile memory (**RAM**). • If the configuration encryption in the device is disabled, 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, 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. In this case, specify in the **Diagnostics > System > Selftest** dialog whether the device starts with the factory settings or terminates the restart and stops. **NOTE:** Only mark the configuration profiles saved in the non-volatile memory (**NVM**). Within the **Basic Settings > External Memory** dialog, if the check box in the **Backup config when saving** column is marked, 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 exported the configuration profile using the **Export...** button or the link in the **Profile name** column. From the **Select source** drop-down list, select from where the device imports the configuration profile. • **PC/URL**: The device imports the configuration profile from the local PC or a remote server. When **PC/URL** is selected, specify the configuration profile file to be imported in the **Import profile from PC/URL** frame. In the **Destination** frame, specify where the device saves the imported configuration profile. In the **Profile name** field, specify the name under which the device saves the configuration profile. In the **Storage** field, specify the storage location for the configuration profile. The prerequisite is that from the **Select source** drop-down list, the **PC/URL** item is selected. **Import from the PC**: When the file is located on your PC or a network drive, drag and drop it onto the area. • **Import from an FTP server**: Do not use this method if you transmit data over untrusted networks. If the file is on an FTP server, then specify the URL in the following form: ftp://<user>:<password>@<IP address>[:port]/<file name> • **Import from a TFTP server**: Do not use this method if you transmit data over untrusted networks. If the file is on a TFTP server, then specify the URL in the following form: tftp://<IP address>/<path>/<file name>

Setting	Buttons	Description
		• **Import from an SCP or SFTP server**: If the file is on an SCP or SFTP server, specify the URL in one of the following forms: scp:// or sftp://<IP address>/<path>/<file name> Click the **Start** button to open the **Credentials** window. Enter the **User name** and **Password** to log into the server. Remember to set up the SCP or SFTP server as an SSH known host before the device accesses the server for the first time. See the **Device Security > SSH Known Hosts** dialog. **External memory**: The device imports the configuration profile from the external memory (**ENVM**). When **External memory** is selected above, in the **Import profile from external memory** frame, specify the configuration profile file to be imported. From the **Profile name** drop-down list, select the name of the configuration profile to be imported. **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 an identically equipped device, the device takes over the settings completely. • If the configuration profile was exported on an other device, the device takes over the settings that can be interpreted 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, see the **Configuration encryption** frame. The device imports a configuration profile under the following conditions: • The configuration encryption of the device is inactive. The configuration profile is unencrypted. • The configuration encryption of the device is active. The configuration profile is encrypted with the same password that the device currently uses.
	Export...	Exports the configuration profile selected in the table and saves it as an XML file on a remote server. To save the file on your PC, select the link in the **Profile name** column to select the storage location and specify the file name. Exporting a configuration profile has the following options: • **Export to an FTP server**: Do not use this method if you transmit data over untrusted networks. To save the file on an FTP server, specify the URL for the file in the following form: ftp://<user>:<password>@<IP address>[:port]/<file name> • **Export to a TFTP server**: Do not use this method if you transmit data over untrusted networks. To save the file on a TFTP server, specify the URL for the file in the following form: tftp://<IP address>/<path>/<file name> • **Export 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> Select the **OK** button to open the **Credentials** window. Enter the **User name** and **Password** to log into the server. Remember to set up the SCP or SFTP server as an SSH known host before the device accesses the server for the first time. See the **Device Security > SSH Known Hosts** dialog.
	Save running-config as script	Saves the **running config** configuration profile as a script file on the local PC. You can back up your device settings or use them on various devices.
	Load running-config from script	Imports a script file which modifies the **running config** configuration profile. See the previous **Import...** to import a script file.
	Back to factory...	Resets the device settings to the default values. • The device deletes the saved configuration profiles from the volatile memory (**RAM**) and from the non-volatile memory (**NVM**). • The device deletes the digital certificate used by the web server in the device. • The device deletes the RSA key (host key) used by the SSH server in the device. • When an external memory (**ENVM**) is connected, the device deletes the configuration profiles saved in the external memory. • The device then reboots and uses the default settings.
	Back to default	**Back to default**: Deletes the operating (**running config**) settings from the volatile memory (**RAM**).
Storage		Displays the storage location of the configuration profile. The possible values are: • **RAM** (volatile memory of the device): In the volatile memory, the device stores the settings for the present operation. • **NVM** (non-volatile memory of the device): When applying the **Undo configuration modifications** function or during the system startup, the device loads the **Selected** configuration profile from the non-volatile memory. The non-volatile memory provides space for multiple configuration profiles, depending on the number of settings saved in the configuration profile. The device manages a maximum of 20 configuration profiles in the non-volatile memory. You can load a configuration profile into the volatile memory (**RAM**). To do this, perform the following steps:

Setting	Buttons	Description
		Select the table row of the configuration profile. Select the ☰ button and then **Activate**. • **ENVM** (external memory) In the external memory, the device saves a backup copy of the “Selected” configuration profile. The prerequisite is that in the **Basic Settings > External Memory** dialog the Backup configuration when saving checkbox is marked.
Profile name		Displays the name of the configuration profile. The possible values are: • **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: Save a configuration profile with a user-specified name. To do this, select the table row of an existing configuration profile in the table, click the ☰ button and then **Save as...** . To export the configuration profile as an XML file on your PC, select the link. Then select the storage location and specify the file name. To save the file on a remote server, select the ☰ button and then **Export...** .
Last modified (UTC)		Displays the Universal Time Coordinated (UTC) time last saved in the configuration profile.
Selected		Displays whether the configuration profile is designated as **Selected**. Designate another configuration profile as **Selected**. To do this, select the desired configuration profile in the table, select the ☰ button, and then **Activate**. The possible values are: • **marked**: The configuration profile is designated as **Selected**. When applying the **Undo configuration modifications** function or during the system startup, the device loads the configuration profile into the volatile memory (**RAM**). When you select the 💾 button, the device saves the temporarily applied settings in this configuration profile. • **unmarked**: Another configuration profile is designated as **Selected**.
Encryption		Displays if the configuration profile is encrypted. The possible values are: • **marked**: The configuration profile is encrypted. • **unmarked**: The configuration profile is unencrypted. Activate/deactivate the encryption of the configuration profile in the **Configuration encryption** frame.
Verified		Displays if the password of the encrypted configuration profile matches the password stored in the device. The possible values are: • **marked**: The passwords match. The device can unencrypt the configuration profile. • **unmarked**: The passwords are different. The device cannot unencrypt the configuration profile. **NOTE:** The device applies script files additionally to the present settings. Verify that the script file does not contain any parts that conflict with the present settings.
Software version		Displays the version number of the device software that the device ran while saving the configuration profile.
Fingerprint		Displays the checksum saved in the configuration profile. When saving the settings, the device calculates the checksum and inserts it into the configuration profile.
Verified		Displays if the checksum saved in the configuration profile is valid. The device calculates the checksum of the configuration profile marked as **Selected** and compares it with the checksum saved in this configuration profile. The possible values are: • **marked**: The calculated and the saved checksum match. The saved settings are consistent. • **unmarked**: For the configuration profile marked as **Selected**, the calculated and the saved checksum are different. The configuration profile contains modified settings. The possible causes are: The file is damaged. The file system in the external memory is inconsistent. The configuration profile has been exported and the XML file has been changed 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 **NOTE:** This function identifies changes to the settings in the configuration profile. The function does not provide protection against operating the device with modified settings.

External Memory

The following table presents the external memory settings:

Setting	Description
Selected external memory	Displays the type of the external memory (**ENVM**). The possible value is **usb** external USB memory (EAM).
Status	Displays the operating state of the external memory (**ENVM**). The possible values are: • **notPresent**: No external memory (**ENVM**) is connected. • **removed**: Someone has removed the external memory (**ENVM**) from the device during operation. • **ok**: The external memory (**ENVM**) is connected and ready for operation. • **outOfMemory**: The memory space is occupied in the external memory (**ENVM**). • **genericErr**: The device has detected an error.

Configuration Encryption

The following table presents the configuration encryption settings:

Setting	Description
Active	Displays whether the configuration encryption is active/inactive in the device. The possible values are: • **marked**: The configuration encryption is active. If the configuration profile is encrypted and the password matches the password stored in the device, the device loads a configuration profile from the non-volatile memory (**NVM**). • **unmarked**: The configuration encryption is inactive. If the configuration profile is unencrypted, 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, the **Security status** frame in the **Basic Settings > System** dialog displays an alarm. In the **Global** tab of the **Diagnostics > Status Configuration > Security Status** dialog, specify whether the device monitors the load unencrypted configuration from external memory parameter in the **Monitor** column.
Set password	Opens the **Set password** window 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** check box. • In the **New password** field, enter the password. To display the password in plain text instead of ***** (asterisks), mark the **Display content** check box. • Mark the **Save configuration afterwards** check box to use encryption for the **Selected** configuration profile in the non-volatile memory (**NVM**) and in the external memory (**ENVM**). **NOTE:** If a maximum of one configuration profile is stored in the non-volatile memory (**NVM**) of the device, use this function only. Before adding additional configuration profiles, decide for or against permanently activated configuration encryption in the device. Save additional configuration profiles either unencrypted or encrypted with the same password. If you are replacing a device with an encrypted configuration profile, for example due to an inoperable device, perform the following steps: • Restart the new device and assign the IP parameters. • Open the **Basic Settings > Load/Save** dialog on the new device. • Encrypt the configuration profile in the new device (see above). Enter the same password you used in the inoperable device. • Install the external memory (**ENVM**) from the inoperable device in the new device. • Restart the new device. During the next system startup, the device loads the configuration profile with the settings of the inoperable device from the external memory (**ENVM**). The device copies the settings into the volatile memory (**RAM**) and into the non-volatile memory (**NVM**).
Delete	Opens the **Delete** window 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** check box. • Mark the **Save configuration afterwards** check box to remove the encryption for the **Selected** configuration profile in the non-volatile memory (**NVM**) and in the external memory (**ENVM**). **NOTE:** If you keep additional encrypted configuration profiles in the memory, the device helps prevent you from activating or designating these configuration profiles as **Selected**.

Undo Configuration Modifications

The following table presents the undo configuration modifications settings:

Setting	Description
Operation	Enables/disables **the Undo configuration modifications** function. The device continuously checks if it can still be reached from the IP address of your PC. If the connection is lost, the device loads the **Selected** configuration profile from the non-volatile memory (**NVM**). The device can be accessed again. The possible values are: • **On**: The function is enabled. 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 GUI to 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.
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. The possible value is **30..600** (default setting: **600**). Specify a sufficiently large value. Consider the time when you view the dialogs of the GUI without changing or updating them.
Watchdog IP address	Displays the IP address of the PC on which you have enabled the function. The possible value is IPv4 address (default setting: **0.0.0.0**).

Information

The following table presents the information settings:

Setting	Description
NVM in sync with running config	Displays whether the settings in the volatile memory (**RAM**) differ from the settings of the **Selected** configuration profile in the non-volatile memory (**NVM**). The possible values are: • **marked**: The settings match. • **unmarked**: The settings differ. Additionally, the Banner displays the icon  .
External memory in sync with NVM	Displays whether the settings of the **Selected** configuration profile in the external memory (**ENVM**) differ from the settings of the **Selected** configuration profile in the non-volatile memory (**NVM**). The possible values are: • **marked**: The settings match. • **unmarked**: The settings differ. The possible causes are: No external memory (**ENVM**) is connected to the device. In the **Basic Settings > External Memory** dialog, the **Backup config when saving** function is disabled.

Backup Config on a Remote Server when Saving

The following table presents the settings of the backup configuration on a remote server when saving:

Setting	Description
Operation	Enables/disables the **Backup config on a remote server when saving** function. The possible values are: • **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. The possible values are: • 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 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** check box. 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** check box. Possible values: Alphanumeric ASCII character string with 6..64 characters The device accepts the following characters: **a..z** **A..Z** **0..9** **!#$%&'()*+,-./:;<=>?@[\\]^_`{}~**

External Memory

This dialog **Basic Settings > External Memory** allows you to 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.

External Memory Table

To customize the appearance of the table, see Working with Tables, page 25.

The following table presents the exeternal memory table settings:

Setting	Description
Type	Displays the type of the external memory (**ENVM**). The possible value is **usb** external USB memory (EAM).
Status	Displays the operating state of the external memory (**ENVM**). The possible values are: • **notPresent**: No external memory (**ENVM**) is connected. • **removed**: The external memory (**ENVM**) has been removed from the device during operation. • **ok**: The external memory (**ENVM**) is connected and ready for operation. • **outOfMemory**: The memory space is occupied in the external memory (**ENVM**). • **genericErr**: The device has detected an error.
Writable	Displays whether the device has write access to the external memory (**ENVM**). The possible values are: • **marked**: The device has write access to the external memory (**ENVM**). • **unmarked**: The device has read-only access to the external memory (**ENVM**). The write protection may be activated in the external memory.
Software auto update	Activates/deactivates the automatic device software update during the system startup. The possible values are • **marked** (default setting): The device updates the device software when the following files are located in the external memory (**ENVM**): the device software image file a startup.txt file with the `autoUpdate=<software_image_file_name>.bin` content. • **unmarked**: No automatic device software update during the system startup.
SSH key auto upload	Activates/deactivates the loading of the RSA key from an external memory (**ENVM**) during the system startup. The possible values are: • **marked** (default setting): The loading of the RSA key is activated. During the system startup, the device loads the RSA key from the external memory (**ENVM**) when the following files are located in the external memory: SSH RSA key file a startup.txt file with the `autoUpdateRSA=<filename_of_the_SSH_RSA_key>` content. 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. The possible values are: • **disable**: The device loads the configuration profile from the non-volatile memory (**NVM**). • **first**: The device loads the configuration profile from the external memory (**ENVM**). When the device does not find a configuration profile in the external memory (**ENVM**), it loads the configuration profile from the non-volatile memory (**NVM**). **NOTE:** When loading the configuration profile from the external memory (**ENVM**), the device overwrites the settings of the **Selected** configuration profile in the non-volatile memory (**NVM**). If the **Config priority** column has the value **first** and the configuration profile is unencrypted, then the **Security status** frame in the **Basic Settings > System** dialog displays an alarm. In the **Global** tab of the **Diagnostics > Status Configuration > Security Status** dialog, you can specify whether the device monitors the load unencrypted configuration from external memory parameter in the **Monitor** column.

Setting	Description
Backup config when saving	Activates/deactivates saving a copy of the configuration profile in the external memory (**ENVM**). The possible values are: • **marked** (default setting): Saving a copy is activated. When you select the  button in the **Basic Settings > Load/Save** dialog, the device saves a copy of the configuration profile on the active external memory (**ENVM**). • **unmarked**: Saving a copy is deactivated. The device does not save a copy of the configuration profile.
Manufacturer ID	Displays the name of the memory manufacturer.
Revision	Displays the revision number specified by the memory manufacturer.
Version	Displays the version number specified by the memory manufacturer.
Name	Displays the product name specified by the memory manufacturer.
Serial number	Displays the serial number specified by the memory manufacturer.

Port

This dialog **Basic Settings > Port** allows you to specify settings for the individual ports. The dialog displays the operating mode, connection status, bit rate, and duplex mode for every port. The dialog contains the following tabs:

- Configuration
- Statistics, page 52
- Ingress Utilization

Port Configuration Table

To customize the appearance of the table, see Working with Tables, page 25.

The following table presents the port configuration table settings:

Setting	Description
Port	Displays the port number.
Name	Name of the port. The possible values are: • Alphanumeric ASCII character string with 0..64 characters The device accepts the following characters: ◦ **<space>** ◦ **0..9** ◦ **a..z** ◦ **A..Z** ◦ **!#$%&'()*+,-./:;<=>?@[\\]^_`{}~**
Port on	Activates/deactivates the port. The possible values are: • **marked** (default setting): The port is active. • **unmarked**: The port is inactive. The port does not send or receive any data.
State	Displays whether the port is currently physically enabled or disabled. The possible values are: • **marked**: The port is physically enabled. • **unmarked**: The port is physically disabled. If the port is disabled even though the **Port on** check box is marked, the port was disabled by another function, for example **Auto-Disable** or **Port Monitor**. Specify the settings of the **Auto-Disable** function in the **Diagnostics > Ports > Auto-Disable** dialog. Specify the settings of the **Port Monitor** function in the **Diagnostics > Ports > Port Monitor** dialog.
Autoneg	Activates/deactivates the automatic selection of the operating mode for the port. The possible values are: • **marked** (default setting for twisted-pair ports): The automatic selection of the operating mode is active. The port negotiates the operating mode independently using auto-negotiation and automatically detects the assignment of the twisted-pair port connectors (auto cable crossing). This setting has priority over the manual setting of the port. Several seconds elapse until the port has set the operating mode. • **unmarked**: The automatic selection of the operating mode is inactive. The port operates with the values you specify in the **Manual configuration** column and in the **Manual cable crossing** column. • Grayed-out display (default setting for optical ports with port speeds > **1G**): No automatic selection of the operating mode.
Manual configuration	Specifies the operating mode of the ports when the **Autoneg** function is disabled. The possible values are: • **10M HDX**: Half-duplex connection. Applies to device variants with 20 or more ports. Refer to the *Modicon MCSESM MCSESP Series Managed Switch Installation Guide* for information on whether the port supports half-duplex. • **10M FDX**: Full-duplex connection • **100M HDX**: Half-duplex connection. Applies to device variants with 20 or more ports. Refer to the *Modicon MCSESM MCSESP Series Managed Switch Installation Guide* for information on whether the port supports half-duplex. • **100M FDX**: Full-duplex connection • **1G FDX**: Full-duplex connection • **2.5G FDX**: Full-duplex connection **NOTE:** The operating modes of the available ports depend on the device hardware.
Link/current settings	Displays the operating mode which the port currently uses. The possible values are: • **–**: No cable connected, no link. • **10M HDX**: Half-duplex connection • **10M FDX**: Full-duplex connection • **100M HDX**: Half-duplex connection • **100M FDX**: Full-duplex connection • **1G FDX**: Full-duplex connection • **2.5G FDX**: Full-duplex connection **NOTE:** The operating modes of the available ports depend on the device hardware.

Setting	Description
Manual cable crossing	Specifies the devices connected to a twisted-pair port. The prerequisite is that the **Autoneg** function is disabled. The possible values are: • **mdi**: The device interchanges the send- and receive-line pairs on the port. • **mdix** (default setting on twisted-pair ports): The device helps prevent the interchange of the send- and receive-line pairs on the port. • **auto-mdix**: The device detects the send and receive line pairs of the connected device and automatically adapts to them. Example: When you connect an end device over a crossed cable, the device automatically resets the port from **mdix** to **mdi**. • **unsupported** (default setting on optical ports or twisted-pair SFP ports): The port does not support this function.
Flow control	Activates/deactivates the **Flow control** on the port. The possible values are: • **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** on the port of the device that is connected to this port. On an uplink port, activating the **Flow control** can possibly cause unexpected interruptions in the upper-level network segment (wandering backpressure). • **unmarked**: The Flow control on the port is inactive. If you are using a redundancy function, deactivate the **Flow control** on the participating ports. If the **Flow control** and the **redundancy** function are active at the same time, the redundancy function may operate differently than expected.
Send trap	Activates/deactivates sending SNMP traps when the device detects a change in the link up/down status on the port. The possible values are: • **marked** (default setting): Sending SNMP traps is active. The prerequisite is that in the **Diagnostics > Status Configuration > Alarms (Traps)** dialog, the **Alarms** (traps) function is enabled and at least one trap destination is specified. When the device detects a link up/down status change, the device sends an SNMP trap. • **unmarked**: Sending SNMP traps is inactive.
MTU	Specifies the maximum allowed size of Ethernet packets on the port in bytes. The possible values are: • **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 increase the maximum 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, you may require an MTU that is larger than 4 bytes. On other interfaces, specify the maximum permissible size of the Ethernet packets as follows: Link Aggregation interfaces (**MTU** column in the **Switching > L2-Redundancy > Link Aggregation** dialog)
Power state	Specifies whether the port is physically enabled or disabled after you deactivated the port in the **Port on** column. The possible values are: • **marked**: The device keeps the port physically enabled when the Port on checkbox is unmarked. A device connected to this port continues to detect the link status as active. • **unmarked** (default setting): The port is physically disabled. The physical status of the port is controlled only by the setting in the Port on column.
Track name	Specifies the name of the tracking object to which the device links the physical port. The prerequisite is that in the **Advanced > Tracking > Configuration** dialog, the **Track name** field is already set up. The possible value is: • **<Track name>** (default setting: **-**): The device automatically activates or deactivates the link status of a physical port depending on the selected tracking object from the drop-down list.
Power save	Specifies how the port behaves when no cable is connected. The possible values are: • **no-power-save** (default setting): The port remains activated. • **auto-power-down**: The port changes to the energy-saving mode. • **unsupported**: The port does not support this function and remains activated.
Signal	Activates/deactivates the port LED flashing. This function identify the port in the field. The possible values are: • **marked**: The flashing of the port LED is active. The port LED flashes until you disable the function. • **unmarked** (default setting): The flashing of the port LED is inactive.

Statistics

The **Statistics** tab displays the following information per port:

- Number of data packets/bytes received by the device:
  - Received packets
  - Received octets
  - Received unicasts
  - Received multicasts
  - Received broadcasts
- Number of data packets/bytes sent or forwarded by the device:
  - Transmitted packets
  - Transmitted octets
  - Transmitted unicasts
  - Transmitted multicasts
  - Transmitted broadcasts
- Number of errors detected by the device:
  - Received fragments
  - Detected CRC errors
  - Detected collisions
- Number of data packets per size category received by the device:
  - Packets 64 bytes
  - Packets 65 to 127 bytes
  - Packets 128 to 255 bytes
  - Packets 256 to 511 bytes
  - Packets 512 to 1023 bytes
  - Packets 1024 to 1518 bytes
- Number of data packets discarded by the device:
  - Received discards
  - Transmitted discards

To sort the table by specific criteria, select the header of the corresponding column.

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

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

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

Ingress Utilization Table

To customize the appearance of the table, see Working with Tables, page 25.

The following table presents the ingress utilization table settings:

Setting	Description
Port	Displays the port number.
Utilization [%]	Displays the utilization in percentage in relation to the time interval specified in the Control interval [s] column. The utilization is the relationship between the received data quantity and the maximum possible data quantity at the set data rate.
Lower threshold [%]	Specifies the lower notification threshold value for the network load. If the network load on the port falls below this value, the status of the check box in the **Alarm** column changes to **marked**. The possible value is **0.00..100.00** (default setting: **0.00**). The value **0** or **0.00** deactivates the lower notification threshold value.
Upper threshold [%]	Specifies the upper notification threshold value for the network load. If the network load on the port exceeds this value, the status of the check box in the **Alarm** column changes to **marked**. The possible value is **0.00..100.00** (default setting: **0.00**). The value **0** or **0.00** deactivates the upper notification threshold value.
Control interval [s]	Specifies the interval in seconds by which the device determines and possibly limits the network load. The possible value is **1..3600** (default setting: **30**).
Alarm	Displays the utilization alarm status. The possible values are: • **marked**: The network load on the port is below the value specified in the **Lower threshold [%]** column or above the value specified in the **Upper threshold [%]** column. The device sends an SNMP trap. The prerequisite is that in the **Diagnostics > Status Configuration > Alarms (Traps)** dialog, the **Alarms** (traps) function is enabled and at least one trap destination is specified. • **unmarked**: The network load on the port is between the lower and the upper notification threshold values.

Power over Ethernet (MCSESP)

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 PoE. The PoE ports of the device support PoE 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.

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

This menu **Basic Settings > Power over Ethernet** contains the following dialogs:

- PoE Global, page 53
- PoE Port, page 55

PoE Global

Basic Settings > Power over Etherne > Global

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

Operation

The following table presents the operation setting:

Setting	Description
Operation	Enables/disables the PoE function. The possible values are: • **On** (default setting): The PoE function is enabled. • **Off**: The PoE function is disabled.

Configuration

The following table presents the configuration settings:

Setting	Description
Send trap	Activates/deactivates sending SNMP traps. If the power consumption exceeds the user-specified threshold value, the device sends an SNMP trap. The possible values are: • **marked** (default setting): The device sends SNMP traps. The prerequisite is that in the **Diagnostics > Status Configuration > Alarms (Traps)** dialog, the **Alarms** (traps) function is enabled and at least one trap destination is specified. • **unmarked**: The device does not send any SNMP traps.
Threshold [%]	Specifies the threshold value for the power consumption in percentage. If the power output exceeds this threshold value, then the device measures the total output power and sends an SNMP trap. The possible value is **0..99** (default setting: **90**).

System Power

The following table presents the system power settings:

Setting	Description
Max. Budget [W]	Displays the maximum available global power budget.
Reserved [W]	Displays the global reserved power. The device reserves power according to the detected classes of connected powered devices. Reserved power is equal to or less than the actual delivered power.
Delivered [W]	Displays the actual power delivered to the modules in watts.
Delivered [mA]	Displays the actual current delivered to the modules in milliamperes.

PoE Global Table

To customize the appearance of the table, see Working with Tables, page 25.

The following table presents the PoE global table settings:

Setting	Description
Module	Device module to which the table rows relate.
Configured power budget [W]	Specifies the power of the modules for the distribution at the ports. The possible value is **0..n** (default setting: n, where n = 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. The possible values are: • **internal**: Internal power source • **external**: External power source
Threshold [%]	Specifies the threshold value for the power consumption of the module in percentage. If the power output exceeds the threshold value, the device measures the total output power and sends an SNMP trap. The possible value is **0..99** (default setting: **90**)
Send trap	Activates/deactivates sending SNMP traps if the device detects that the threshold value for the power consumption exceeds. The possible values are: • **marked** (default setting): Sending SNMP traps is active. The prerequisite is that in the **Diagnostics > Status Configuration > Alarms (Traps)** dialog, the **Alarms** (traps) function is enabled and at least one trap destination is specified. If the power consumption of the module exceeds the user-defined threshold value, then the device sends an SNMP trap. • **unmarked**: Sending SNMP traps is inactive.

PoE Port

Basic Settings > Power over Ethernet > Port

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

PoE Port Table

To customize the appearance of the table, see Working with Tables, page 25.

The following table presents the PoE port table settings:

Setting	Description
Port	Displays the port number.
PoE enable	Activates/deactivates the PoE power provided to the port. When the device activates or deactivates the function, the device logs an event. The possible values are: • **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 PoE **Fast Startup** function on the port. The prerequisite is that the check box in the PoE enable column is marked. The possible values are: • **marked**: The **Fast Startup** function is active. The device sends power to the PD immediately after turning on the power to the device. • **unmarked** (default setting): The **Fast Startup** function is inactive. The device sends power to the 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 the device disabling the ports supplying necessary devices, specify a high priority for these ports. The possible values are: • **critical** • **high** • **low** (default setting)
Status	Displays the status of the port PD detection. The possible values are: • **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. The possible values are: • **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. The possible values are: • **marked** (default setting) • **unmarked**
Consumption [W]	Displays the current power consumption of the port in watts. The possible value is **0,0..30,0**.
Consumption [mA]	Displays the current delivered to the port in milliamperes. The possible value is **0..600**.
Power limit [W]	Specifies the maximum power in watts that the port outputs. This function distributes 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 undefined, 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. The possible value is **0,0..30,0** (default setting: **0**).

Setting	Description
Max. consumption [W]	Displays the maximum power in watts that the device has consumed so far. 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. The possible value is alphanumeric ASCII character string with 0..32 characters.
Auto-shutdown power	Activates/deactivates the **Auto-shutdown power** function according to the settings. The possible values are: • **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. The possible value is **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. The possible value is **00:00..23:59** (default setting: **00:00**).

Restart

This dialog **Basic Settings > Restart** allows you to restart the device, reset port counters and the MAC address table (forwarding database), and delete log files.

Restart

The following table presents the restart settings:

Setting	Description
Cold start...	Opens the **Restart** window to initiate an immediate or delayed restart of the device. If the configuration profile in the volatile memory (**RAM**) and the **Selected** configuration profile in the non-volatile memory (**NVM**) differ, the device displays the **Warning** window. • To permanently save the settings, select the **Yes** button in the **Warning** window. • To discard the changed settings, select the **No** button in the **Warning** window. • In the **Restart** field, specify the delay time for the delayed restart. The possible value is **00:00:00..596:31:23** (default setting: **00:00:00**) Hour:Minute:Second When the delay time elapses, the device restarts and goes through the following phases: • If you activate the function in the **Diagnostics > System > Selftest** dialog, the device performs the RAM self-test. • The device starts the device software that the **Stored version** field displays in the **Basic Settings > Software** dialog. • The device loads the settings from the **Selected** configuration profile. See the **Basic Settings > Load/Save** dialog. **NOTE:** During the restart, the device does not transfer any data. During this time, the device cannot be accessed by the GUI or other management systems.
Restart in	Displays the remaining time in days, hours, minutes, seconds until the device restarts. To update the display of the remaining time, select the  button.
Cancel	Aborts a delayed restart.

Buttons

The following table presents the buttons settings:

Setting	Description
Clear FDB	Removes the MAC addresses from the forwarding table that has the value **Learned** in the **Status** column in the **Switching > Filter for MAC Addresses** dialog.
Clear ARP table	Removes the dynamically set up addresses from the ARP table. See the **Diagnostics > System > ARP** dialog.
Clear port statistics	Resets the counter for the port statistics to **0**. See the **Statistics** tab in the **Basic Settings > Port** dialog.
Clear management access statistics	Resets the counters for the device management access statistics to **0**. See the **Used Management Ports** table in the **Diagnostics > System > System Information** dialog.
Clear IGMP snooping data	Removes the IGMP Snooping entries and resets the counter in the Information frame to **0**. See the **Switching > IGMP Snooping > Global** dialog.
Clear log file	Removes the logged events from the log file. See the **Diagnostics > Report > System Log** dialog.
Clear persistent log file	Removes the log files from the external memory (**ENVM**). See the **Diagnostics > Report > Persistent Logging** dialog.
Clear email notification statistics	Resets the counters in the Information frame to **0**. See the **Diagnostics > Email Notification > Global** dialog.

Time

The menu contains the following dialogs:

- Basic Settings, page 59
- Time Profile, page 62
- SNTP, page 65
- PTP, page 72
- 802.1AS, page 87

Basic Settings

The device is equipped with a buffered hardware clock. This clock keeps the correct time if the power supply becomes inoperable or you disconnect the device from the power supply. The hardware clock bridges a power supply downtime of three hours. The power supply of the device must be connected continuously for at least five minutes beforehand. In this dialog, Specify time-related settings independently of the time synchronization protocol specified.

The dialog **Time > Basic Settings**contains the following tabs:

- Global, page 59
- Daylight saving time, page 60

Global

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

Time Configuration

Specify the system time and time zone on the **Global** time tab.

Setting	Description
System time (UTC)	Displays the date and time in Universal Time Coordinated (UTC) format.
Set time from PC	The device takes over the time from your computer as the system time.
System time	Displays the local date and time: System time = System time (UTC) + Local offset [min] + Daylight saving time
Time source	Displays the time source from which the device obtains the time information. The device automatically selects the available time source with the greatest accuracy. Possible values: • **local** System clock of the device. • **sntp** The SNTP client is enabled, and the device is synchronized by an SNTP server. See the **Time > SNTP** dialog. • **ptp** The PTP function is enabled, and the device clock is synchronized with a *PTP master clock*. See the **Time > PTP** dialog.
Local offset [min]	Specifies the difference in minutes between Universal Time Coordinated (UTC) and local time: Local offset [min] = System time − System time (UTC) Possible values: • **-780..840** (default setting: **60**)

Daylight Saving Time

In this tab, you enable/disable the Daylight saving time function. You specify the start and end of summer time using a pre-defined profile. As an alternative, you specify these settings individually. During the summer time, the device advances the local time by one hour.

Operation

The following table presents the operation settings:

Setting	Description
Daylight saving time	Enables/disables the Daylight saving time mode. Possible values: • **On** The Daylight saving time mode is enabled. The device automatically sets the clock forward to summer time and back again. • **Off** (default setting) The Daylight saving time mode is disabled. You specify the daylight saving time settings in the Summertime begin and Summertime end frames.
Profile...	Opens the Profile... window to select a pre-defined profile for the start and end of summer time. Selecting a profile overwrites the settings specified in the Summertime begin and Summertime end frames. Possible values: • **EU** Daylight saving time settings as applicable in the European Union. • **USA** Daylight saving time settings as applicable in the United States.

Summertime Begin

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

The following table presents the summertime begin settings:

Setting	Description
Week	Specifies the week of the month. Possible values: • **-** (default setting) • **first** • **second** • **third** • **fourth** • **last**
Day	Specifies the day of the week. Possible values: • **-** (default setting) • **Sunday** • **Monday** • **Tuesday** • **Wednesday** • **Thursday** • **Friday** • **Saturday**
Month	Specifies the month. Possible values: • **-** (default setting) • **January** • **February** • **March** • **April** • **May** • **June** • **July** • **August** • **September** • **October** • **November** • **December**
System time	Specifies the time at which the device sets the clock forward to summer time. Possible values: • **<HH:MM>** (default setting: **00:00**)

Summertime End

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

The following table presents the summertime end settings:

Setting	Description
Week	Specifies the week of the month. Possible values: • **-** (default setting) • **first** • **second** • **third** • **fourth** • **last**
Day	Specifies the day of the week. Possible values: • **-** (default setting) • **Sunday** • **Monday** • **Tuesday** • **Wednesday** • **Thursday** • **Friday** • **Saturday**
Month	Specifies the month. Possible values: • **-** (default setting) • **January** • **February** • **March** • **April** • **May** • **June** • **July** • **August** • **September** • **October** • **November** • **December**
System time	Specifies the time at which the device resets the clock to standard time. Possible values: • **<HH:MM>** (default setting: **00:00**)

Time Profile

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

You can set up to 100 time profiles.

- If a time profile is assigned to a rule, the device applies the rule during the times specified within the time profile.
- If no time profile is assigned to a rule, the device applies the rule permanently.

Each time profile can contain:

- One Absolute time period and up to 9 Periodic time periods

  or

- Up to 10 Periodic time periods

Table

For information on how to customize the appearance of the table, see Working with tables, page 25.

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

Buttons

The following table presents the button icons:

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

Profil Name

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

Operational Status

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

Index

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

Type

Displays the time profile type.

Possible values:

- **Absolute**

  The device applies the rule once. For more information, refer to columns Start date to End time.

- **Periodic**

  The device applies the rule recurrently. For more information, refer to columns Start days to End time.

Absolute

The following table presents the absolute settings:

Setting	Description
Start date	Specifies the date at which the device starts to apply the one-time rule. Possible values: • **<Day of the week, date>** (depending on the language and region settings of your computer)
Start time	Specifies the time at which the device starts to apply the one-time rule. Possible values: • **hh:mm AM/PM** Hour:Minute
End date	Specifies the date at which the device terminates the one-time rule. Possible values: • **<Day of the week, date>** (depending on the language and region settings of your computer) The device also allows you to specify time periods that span several days. Example: • Start date: Sat • Start time: **12:00 PM** • End date: Sun • End time: **11:00 AM**
End time	Specifies the time at which the device terminates the one-time rule. Possible values: • **hh:mm AM/PM** Hour:Minute

Periodic

The following table presents the periodic settings:

Setting	Description
Start days	Specifies the days of the week on which the device periodically starts to apply the rule. The device allows you to specify multiple values in the Start days column, for example a list of the weekdays Mon,Tue,Wed,Thu,Fri. In this case, verify that the Start days and End days fields contain identical values. The device then applies the rule every weekday at the times specified in the Start time and End time fields. Possible values: • **Sun** • **Mon** • **Tue** • **Wed** • **Thu** • **Fri** • **Sat**
Start time	Specifies the time at which the device periodically starts to apply the rule. Possible values: • **hh:mm AM/PM** Hour:Minute
End days	Specifies the days of the week on which the device periodically terminates the rule. The device allows you to specify multiple values in the End days column, for example a list of the weekdays Mon,Tue,Wed,Thu,Fri. In this case, verify that the Start days and End days fields contain identical values. The device then applies the rule every weekday at the times specified in the Start time and End time fields. The device also allows you to specify time periods that span several days. In this case, verify that the Start days and End days fields each contain a single value. Example: Start days: Sat, Start time: **12:00 PM**, End days: Sun, End time: **11:00 AM** Possible values: • **Sun** • **Mon** • **Tue** • **Wed** • **Thu** • **Fri** • **Sat**
End time	Specifies the time at which the device periodically terminates the rule. Possible values: • **hh:mm AM/PM** Hour:Minute

SNTP

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

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

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

The menu **Time > SNTP** contains the following dialogs:

- SNTP Client, page 66
- SNTP Server, page 69

SNTP Client

In this dialog **Time > SNTP > Client**, you specify the settings with which the device operates as an SNTP client. As an SNTP client, the device obtains time information from an external NTP or SNTP servers and synchronizes the local system clock with the time from the time server.

Operation

The following table presents the operation setting:

Setting	Description
Operation	Enables/disables the Client function in the device. Note the setting in the Disable client after successful sync checkbox in the Configuration frame. Possible values: • **On** The Client function is enabled. The device operates as an SNTP client. • **Off** (default setting) The Client function is disabled.

State

The following table presents the state setting:

Setting	Description
State	Displays the status of the Client function. Possible values: • **disabled** The SNTP client is not operating. • **notSynchronized** The SNTP client is operating. The local system clock is not in sync with an external NTP or SNTP server. • **synchronizedToRemoteServer** The SNTP client is not operating. The local system clock is in sync with an external NTP or SNTP server.

Configuration

The following table presents the configuration settings:

Setting	Description
Mode	Specifies if the device actively requests the time information from an external NTP or SNTP server set up in the device (unicast mode) or passively waits for the time information from a random NTP or SNTP server (**broadcast** mode). Possible values: • **unicast** (default setting) The device takes the time information only from one of the set-up NTP or SNTP servers. The device sends Unicast requests to the external SNTP or NTP server and evaluates the response of the server. • **broadcast** The device obtains the time information from a random NTP or SNTP server. The device evaluates the Broadcasts or Multicasts from this server.
Request interval [s]	Specifies the interval in seconds at which the device requests time information from the external NTP or SNTP server. Possible values: • **5..3600** (default setting: **30**)
Broadcast recv timeout [s]	Specifies the time in seconds the device operating in broadcast mode waits before changing the value in the State field from **syncToRemoteServer** to **notSynchronized** when it does not receive Broadcast packets. See the State frame. Possible values: • **128..2048** (default setting: **320**)
Disable client after successful sync	Activates/deactivates the automatic disabling of the SNTP Client function after the device has successfully synchronized its local system clock. Possible values: • **marked** The automatic disabling of the SNTP Client function is active. The device disables the SNTP Client function after it has successfully synchronized its local system clock. • **unmarked** (default setting) The automatic disabling of the SNTP Client function is inactive. The device keeps the SNTP Client function enabled after it has successfully synchronized its local system clock.

Table

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

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

For information on how to customize the appearance of the table, see Working with tables, page 25.

The following table presents the table settings:

Setting	Description
Buttons	 Add: Adds a table row.  Remove: Removes the selected table row.
Index	Displays the index number to which the table row relates. The device automatically assigns the value when you add a table row. When you delete a table row, this leaves a gap in the numbering. When you add a table row, the device fills the first gap.
Name	Specifies a name for the external NTP or SNTP server. Possible values: • Alphanumeric ASCII character string with 1..32 characters
IP address	Specifies the IP address of the external NTP or SNTP server. Possible values: • Valid IPv4 address (default setting: **0.0.0.0**) • Valid IPv6 address • Hostname
Destination UDP port	Specifies the UDP port on which the external NTP or SNTP server listens for requests. Possible values: • **1..65535 (2^{16}-1)** (default setting: **123**) Exception: Port **2222** is reserved for internal functions.

Setting	Description
Status	Displays the connection status between the device and the external NTP or SNTP server. Possible values: • **success** The device has successfully synchronized the local system clock with the external NTP or SNTP server. • **badDateEncoded** Synchronization was unsuccessful. The time information received contains protocol detected errors. • **other** Synchronization was unsuccessful. ◦ The IP address **0.0.0.0** is specified for the external NTP or SNTP server. or ◦ The device is using a different external NTP or SNTP server. • **requestTimedOut** Synchronization was unsuccessful. The device has not received a response from the external NTP or SNTP server. • **serverKissOfDeath** Synchronization was unsuccessful. The external NTP or SNTP server is overloaded. The device is requested to synchronize its system clock with another NTP or SNTP server. When no other NTP or SNTP server is available, the device checks at intervals longer than the value in the Request interval [s] field, if the server is still overloaded. • **serverUnsychronized** Synchronization was unsuccessful. The external NTP or SNTP server is not in sync with a reference time source. • **versionNotSupported** Synchronization was unsuccessful. The SNTP versions of the client and server are incompatible.
Active	Activates/deactivates the connection to the external NTP or SNTP server. Possible values: • **marked** The connection to the external NTP or SNTP server is activated. The device has the option to access to the server. • **unmarked** (default setting) The connection to the external NTP or SNTP server is deactivated. The device does not have the option to access to the server.

SNTP Server

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

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

Operation

The following table presents the operation setting:

Setting	Description
Operation	Enables/disables the Server function in the device. Note the setting in the Disable server at local time source checkbox in the Configuration frame. Possible values: • **On** The Server function is enabled. The device operates as an SNTP server. • **Off** (default setting) The Server function is disabled.

State

The following table presents the state setting:

Setting	Description
State	Displays the state of the Server function on the device. Possible values: • **disabled** The SNTP server is not operating. • **notSynchronized** The SNTP server is operating. The local system clock is not in sync with a reference time source. • **syncToLocal** The SNTP server is operating. The local system clock is in sync with the hardware clock of the device. • **syncToRefclock** The SNTP server is operating. The local system clock is in sync with an external reference time source, like a PTP clock. • **syncToRemoteServer** The SNTP server is operating. The local system clock is in sync with an external NTP or SNTP server which is superordinate to the device in a cascade.

Configuration

The following table presents the configuration settings:

Setting	Description
UDP port	Specifies the UDP port on which the device listens for requests. Possible values: • **1..65535 (2^{16}-1)** (default setting: **123**) Exception: Port **2222** is reserved for internal functions.
Broadcast admin mode	Activates/deactivates the Broadcast mode. Possible values: • **marked** The device sends SNTP packets as Broadcasts or Multicasts. The device also responds to SNTP requests in unicast mode. • **unmarked** (default setting) The device responds to SNTP requests in unicast mode, but sends no Broadcast packets on its own.
Broadcast destination address	Specifies the destination IP address to which the device sends the SNTP packets in Broadcast mode. Possible values: • Valid IPv4 address (default setting: **0.0.0.0**) Broadcast and Multicast addresses are permitted.
Broadcast UDP port	Specifies the UDP port on which the device sends the SNTP packets in Broadcast mode. Possible values: • **1..65535 (2^{16}-1)** (default setting: **123**) Exception: Port **2222** is reserved for internal functions.
Broadcast VLAN ID	Specifies the VLAN to which the device sends the SNTP packets in Broadcast mode. Possible values: • **0** The device sends the SNTP packets in the same VLAN in which the device management access occurs. See the **Basic Settings > Network > Global** dialog. • **1..4042** (default setting: **1**)
Broadcast send interval [s]	Specifies the interval in seconds at which the device broadcasts SNTP packets. Possible values: • **64..1024** (default setting: **128**)
Disable server at local time source	Activates/deactivates the automatic disabling of the SNTP Server function if the local system clock is not in sync with another external time reference. Possible values: • **marked** The automatic disabling of the SNTP Server function is active. If the device has synchronized its local system clock to an external time reference, like a PTP clock, then it keeps the SNTP Server function enabled. Otherwise, the device disables the SNTP Server function. • **unmarked** (default setting) The automatic disabling of the SNTP Server function is inactive. The device keeps the SNTP Server function enabled, regardless of whether it has synchronized its local system clock to an external time reference. If the local system clock is not in sync with an external time reference, then in the SNTP packet, the device informs the client that its system clock is synchronized locally.

PTP

The menu **Time > PTP** contains the following dialogs:

- PTP Global, page 72
- PTP Boundary Clock, page 74
- PTP Transparent Clock, page 82

PTP Global

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

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

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

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

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

The protocol differentiates between the following clocks:

- *Boundary Clock (BC)*

  This clock has any number of PTP ports and operates as both PTP master and PTP slave. In its respective network segment, the clock operates as an Ordinary Clock.

  - As PTP slave, the clock synchronizes itself with a PTP master that is greater than the device in the cascade.
  - As PTP master, the clock forwards the time information through the network to PTP slaves that are greater 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

The following table presents the operation IEEE1588/PTP setting:

Setting	Description
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

The following table presents the configuration IEEE1588/PTP settings:

Setting	Description
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 device considers its local clock to be synchronized. Possible values: • **1..999999999 (10^9-1)** (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 device considers its local clock to be unsynchronized. Possible values: • **31..1000000000 (10^9)** (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

The following table presents the status settings:

Setting	Description
Is synchronized	Displays if the local system clock is synchronized with the reference time source (*Grandmaster*). If the path difference between the local clock and the reference time source (*Grandmaster*) falls below the synchronization lower threshold value one time, then the device considers its local clock to be synchronized. The device keeps this status until the path difference exceeds the synchronization upper threshold value one time. You specify the synchronization threshold values in the Configuration IEEE1588/PTP frame.
Max. offset absolute [ns]	Displays the maximum path difference in nanoseconds that has occurred since the local system clock was synchronized with the reference time source (*Grandmaster*).
PTP time	Displays the date and time for the PTP time scale when the local clock is synchronized with the reference time source (*Grandmaster*). Format: **Month Day, Year hh:mm:ss AM/PM**

PTP Boundary Clock

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

The menu **Time > PTP > Boundary Clock** contains the following dialogs:

- PTP Boundary Clock Global, page 74
- PTP Boundary Clock Port, page 79

PTP Boundary Clock Global

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

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

Operation IEEE1588/PTPv2 BC

The following table presents the operation IEEE1588/PTPv2 BC settings:

Setting	Description
Priority 1	Specifies the *priority 1* value for the device. Possible values: • **0..255** (default setting: **128**) The *Best Master Clock* algorithm first evaluates the *priority 1* value among the participating devices to determine the reference time source (*Grandmaster*). The lower you set this value, the more probable it is that the device becomes the reference time source (*Grandmaster*). See the Grandmaster frame.
Priority 2	Specifies the *priority 2* value for the device. Possible values: • **0..255** (default setting: **128**) When the previously evaluated criteria are the same for multiple devices, the *Best Master Clock* algorithm evaluates the *priority 2* value of the participating devices. The lower you set this value, the more probable it is that the device becomes the reference time source (*Grandmaster*). See the Grandmaster frame.
Domain number	Assigns the device to a PTP domain. Possible values: • **0..255** (default setting: **0**) The device transmits time information from and to devices only in the same domain.

Status IEEE1588/PTPv2 BC

The following table presents the status IEEE1588/PTPv2 BC settings:

Setting	Description
Two step	Displays that the clock is operating in Two-Step mode.
Steps removed	Displays the number of communication paths passed through between the local clock of the device and the reference time source (*Grandmaster*). For a PTP slave, the value **1** means that the clock is connected with the reference time source (*Grandmaster*) directly through one communication path.
Offset to master [ns]	Displays the measured difference (offset) between the local clock and the reference time source (*Grandmaster*) in nanoseconds. The PTP slave calculates the difference from the time information received. In Two-Step mode the time information consists of 2 PTP synchronization messages each, which the PTP master sends cyclically: • The first synchronization message (sync message) contains an estimated value for the exact sending time of the message. • The second synchronization message (follow-up message) contains the exact sending time of the first message. The PTP slave uses the two PTP synchronization messages to calculate the difference (offset) from the master and corrects its clock by this difference. Here the PTP slave also considers the Delay to master [ns] value.
Delay to master [ns]	Displays the delay when transmitting the PTP synchronization messages from the PTP master to the PTP slave in nanoseconds. The PTP slave sends a “Delay Request” packet to the PTP master and thus determines the exact sending time of the packet. When it receives the packet, the PTP master generates a time stamp and sends this in a “Delay Response” packet back to the PTP slave. The PTP slave uses the two packets to calculate the delay, and considers this starting from the next offset measurement. The prerequisite is that in the **Time > PTP > Boundary Clock > Port** dialog, Delay mechanism column, the value **e2e** is specified for the slave ports.

Grandmaster

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

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

The device allows you to 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.

The following table presents the grandmaster settings:

Setting	Description
Priority 1	Displays the *priority 1* value for the device that is currently the reference time source (*Grandmaster*).
Clock class	Displays the class of the reference time source (*Grandmaster*). Parameter for the *Best Master Clock* algorithm.
Clock accuracy	Displays the estimated accuracy of the reference time source (*Grandmaster*). Parameter for the *Best Master Clock* algorithm.
Clock variance	Displays the variance of the reference time source (*Grandmaster*), also defined as the *Offset scaled log variance*. Parameter for the *Best Master Clock* algorithm.
Priority 2	Displays the *priority 2* value for the device that is currently the reference time source (*Grandmaster*).

Local Time Properties

The following table presents the local time properties settings:

Setting	Description
Time source	Specifies the time source from which the local clock gets its time information. Possible values: • **atomicClock** • **gps** • **terrestrialRadio** • **ptp** • **ntp** • **handSet** • **other** • **internalOscillator** (default setting)
UTC offset [s]	Specifies the difference between the PTP time scale and the Universal Time Coordinated (UTC). See the PTP timescale checkbox. Possible values: • **-32768..32767 (2^{15}-1)** **NOTE:** The default setting is the value valid on the creation date of the device software. For further information, see the "Bulletin C" of the Earth Rotation and Reference Systems Service (IERS):
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 obtains the time from a primary UTC reference, for example from an NTP server. Possible values: • **marked** • **unmarked**
Frequency traceable	Displays if the device obtains 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 Universal Time Coordinated (UTC), TAI does not use leap seconds. As of July 1, 2020, the TAI time is 37 s ahead of the Universal Time Coordinated (UTC).

Identities

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

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

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

The following table presents the identities settings:

Setting	Description
Clock identity	Displays the identification number (UUID) of the device.
Parent port identity	Displays the port identification number (UUID) of the directly superior master device.
Grandmaster identity	Displays the identification number (UUID) of the reference time source (*Grandmaster*) device.

PTP Boundary Clock Port

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

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

Table

For information on how to customize the appearance of the table, see Working with tables, page 25.

The following table presents the table settings:

Setting	Description
Port	Displays the port number.
PTP enable	Activates/deactivates transmitting PTP synchronization messages on the port. Possible values: • **marked** (default setting) The transmission is activated. The port forwards and receives PTP synchronization messages. • **unmarked** The transmission is deactivated. The port blocks PTP synchronization messages.
PTP status	Displays the status of the port. Possible values: • **initializing** Initialization phase • **faulty** Error in the Precision Time Protocol (PTP). • **disabled** PTP is disabled on the port. • **listening** The port is waiting for PTP synchronization messages. • **pre-master** PTP pre-master mode • **master** PTP master mode • **passive** PTP passive mode • **uncalibrated** PTP uncalibrated mode • **slave** PTP slave mode
Network protocol	Specifies which protocol the port uses to transmit the PTP synchronization messages. Possible values: • **802.3** (default setting) • **UDP/IPv4**
Announce interval [s]	Specifies the interval in seconds at which the port transmits messages for the PTP topology discovery. Assign the same value to every device of a PTP domain. Possible values: • **1** • **2** (default setting) • **4** • **8** • **16**
Announce timeout	Specifies the number of announce intervals. Example: For the default setting (Announce interval [s] = **2** and Announce timeout = **3**), the timeout is $3 \times 2\ s = 6\ s$. Possible values: • **2..10** (default setting: **3**) Assign the same value to every device of a PTP domain.

Setting	Description
Sync interval [s]	Specifies the interval in seconds at which the port transmits PTP synchronization messages. Possible values: • **0.25** • **0.5** • **1** (default setting) • **2**
Delay mechanism	Specifies the mechanism with which the device measures the delay for transmitting the PTP synchronization messages. Possible values: • **disabled** The measurement of the delay for the PTP synchronization messages for the connected PTP devices is inactive. • **e2e** (default setting) End-to-End: As the PTP slave, the port measures the delay for the PTP synchronization messages to the PTP master. The device displays the measured value in the **Time > PTP > Boundary Clock > Global** dialog. • **p2p** Peer-to-Peer: The device measures the delay for the PTP synchronization messages for the connected PTP devices, provided that these devices support P2P. This mechanism spares the device from having to determine the delay again in the case of a reconfiguration.
P2P delay	Displays the measured Peer-to-Peer delay for the PTP synchronization messages. The prerequisite is that in the Delay mechanism column the value **p2p** is specified.
P2P delay interval [s]	Specifies the interval in seconds at which the port measures the Peer-to-Peer delay. The prerequisite is that in the Delay mechanism column the value **p2p** is specified for this port and for the port of the remote device. Possible values: • **1** (default setting) • **2** • **4** • **8** • **16** • **32**
E2E delay interval [s]	Displays the interval in seconds at which the port measures the End-to-End delay. Possible values: • When the port is operating as the PTP master, the device assigns to the port the value **8**. • When the port is operating as the PTP slave, the value is specified by the PTP master connected to the port.
Asymmetry	Corrects the measured delay value corrupted by asymmetrical transmission paths. Possible values: • **-2000000000..2000000000** (default setting: **0**) The value represents the delay symmetry in nanoseconds. A measured delay value of `y ns` corresponds to an asymmetry of `y × 2 ns`. The value is positive if the delay from the PTP master to the PTP slave is longer than in the opposite direction.

Setting	Description
VLAN	Specifies the VLAN ID that the device uses to tag the received PTP synchronization messages on this port. Possible values: • **none** (default setting) The device transmits PTP synchronization messages without a VLAN tag. • **0..4042** You specify VLANs that you have already set up in the device from the list. Verify that the port is a member of the VLAN. See the **Switching > VLAN > Configuration** dialog.
VLAN priority	Specifies the priority with which the device transmits the PTP synchronization messages marked with a VLAN ID (Layer 2, IEEE 802.1D). Possible values: • **0..7** (default setting: **6**) If you specified in the VLAN column the value **none**, then the device ignores the VLAN priority.

PTP Transparent Clock

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

The menu **Time > PTP > Transparent Clock** contains the following dialogs:

- PTP Transparent Clock Global, page 82
- PTP Transparent Clock Port, page 86

PTP Transparent Clock Global

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

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

Operation IEEE1588/PTPv2 TC

The following table presents the operation IEEE1588/PTPv2 TC settings:

Setting	Description
Delay mechanism	Specifies the mechanism with which the device measures the delay for transmitting the PTP synchronization messages. Possible values: • **e2e** (default setting) As the PTP slave, the port measures the delay for the PTP synchronization messages to the PTP master. The device displays the measured value in the **Time > PTP > Transparent Clock > Global** dialog. • **p2p** The device measures the delay for the PTP synchronization messages for every connected PTP device, provided that the device supports P2P. This mechanism spares the device from having to determine the delay again in the case of a reconfiguration. If you specify this value, then the value **802.3** is only available in the Network protocol column. • **e2e-optimized** Like **e2e**, with the following special characteristics: ◦ The device transmits the delay requests of the PTP slaves only to the PTP master, even though these requests are multicast messages. The device thus spares the other devices from unnecessary multicast requests. ◦ If the master-slave topology changes, then the device relearns the port for the PTP master as soon as it receives a synchronization message from another PTP master. ◦ If the device does not know a PTP master, then the device transmits delay requests to the ports. • **disabled** The delay measuring is disabled on the port. The device discards messages for the delay measuring.
Primary domain	Assigns the device to a PTP domain. Possible values: • **0..255** (default setting: **0**) The device transmits time information from and to devices only in the same domain.
Network protocol	Specifies which protocol the port uses to transmit the PTP synchronization messages. Possible values: • **ieee8023** (default setting) • **udpIpv4**
Multi domain mode	Activates/deactivates the PTP synchronization message correction in every PTP domain. Possible values: • **marked** The device corrects PTP synchronization messages in every PTP domain. • **unmarked** (default setting) The device corrects PTP synchronization messages only in the primary PTP domain. See the Primary domain field.

Setting	Description
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

The following table presents the local synchronization settings:

Setting	Description
Syntonize	Activates/deactivates the frequency synchronization of the *Transparent Clock* with the PTP master. Possible values: • **marked** (default setting) The frequency synchronization is active. The device synchronizes the frequency. • **unmarked** The frequency synchronization is inactive. The frequency remains constant.
Synchronize local clock	Activates/deactivates the synchronization of the local system time. Possible values: • **marked** The synchronization is active. The device synchronizes the local system time with the time received using PTP. The prerequisite is that the Syntonize checkbox is marked. • **unmarked** (default setting) The synchronization is inactive. The local system time remains constant.
Current master	Displays the port identification number (UUID) of the directly superior master device on which the device synchronizes its frequency. If the value contains only zeros, this is because: • The Syntonize function is disabled. or • The device cannot find a PTP master.
Offset to master [ns]	Displays the measured difference (offset) between the local clock and the PTP master in nanoseconds. The device calculates the difference from the time information received. The prerequisite is that the Synchronize local clock function is enabled.
Delay to master [ns]	Displays the delay when transmitting the PTP synchronization messages from the PTP master to the PTP slave in nanoseconds. Prerequisites: • The Synchronize local clock function is enabled. • In the Delay mechanism field, the value **e2e** is selected.

Status IEEE1588/PTPv2 TC

The following table presents the status IEEE1588/PTPv2 TC settings:

Setting	Description
Clock identity	Displays the identification number (UUID) of the device. The device displays the identities as byte sequences in hexadecimal notation. The device identification number consists of the MAC address of the device, with the values **ff** and **fe** added between byte 3 and byte 4.

PTP Transparent Clock Port

In this dialog **Time > PTP > Transparent Clock > Port**, specify the *Transparent Clock (TC)* settings on each individual port.

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

Table

For information on how to customize the appearance of the table, see Working with tables, page 25.

The following table presents the table settings:

Setting	Description
Port	Displays the port number.
PTP enable	Activates/deactivates transmitting PTP synchronization messages on the port. Possible values: • **marked** (default setting) The transmitting is active. The port forwards and receives PTP synchronization messages. • **unmarked** The transmitting is inactive. The port blocks PTP synchronization messages.
P2P delay interval [s]	Specifies the interval in seconds at which the port measures the Peer-to-Peer delay. The prerequisite is that in the **Time > PTP > Transparent Clock > Global** dialog, Delay mechanism option list, the radio button **p2p** is selected for this port and for the port of the remote device. Possible values: • **1** (default setting) • **2** • **4** • **8** • **16** • **32**
P2P delay	Displays the measured Peer-to-Peer delay for the PTP synchronization messages. The prerequisite is that in the **Time > PTP > Transparent Clock > Global** dialog, Delay mechanism option list, the radio button **p2p** is selected.
Asymmetry	Corrects the measured delay value corrupted by asymmetrical transmission paths. Possible values: • **-2000000000..2000000000 (2 × 10⁹)** (default setting: **0**) The value represents the delay symmetry in nanoseconds. A measured delay value of `y ns` corresponds to an asymmetry of `y × 2 ns`. The value is positive if the delay from the PTP master to the PTP slave is longer than in the opposite direction.

802.1AS

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

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

The 802.1AS function has the following specifications:

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

The menu **Time > 802.1AS** contains the following dialogs:

- 802.1AS Global, page 87
- 802.1AS Port, page 90
- 802.1AS Statistics, page 96

802.1AS Global

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

Operation

The following table presents the operation setting:

Setting	Description
Operation	Enables/disables the 802.1AS function. Possible values: • **On** The 802.1AS function is enabled. The device synchronizes its clock using the 802.1AS function. Consider activating the 802.1AS function for each instance and also on the individual ports. • **Off** (default setting) The 802.1AS function is disabled. When disabling the 802.1AS function globally, you disable time synchronization for both instances and for the respective ports allocated to them. This disables time synchronization on the instance and port levels even if the 802.1AS function is enabled on the instances and on the individual ports.

Configuration

The following table presents the configuration settings:

Setting	Description
Sync lower bound [ns]	Specifies the lower threshold value in nanoseconds for the measured time difference between the local clock and the reference time source (*Grandmaster*). If the measured time difference falls below this value, then the device considers its local clock to be synchronized. Possible values: • **0..999999999 (10^9-1)** (default setting: **30**)
Sync upper bound [ns]	Specifies the upper threshold value in nanoseconds for the measured time difference between the local clock and the reference time source (*Grandmaster*). If the measured time difference exceeds this value, then the device considers its local clock to be unsynchronized. Possible values: • **31..1000000000 (10^9)** (default setting: **5000**)

Status

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

The following table presents the status settings:

Setting	Description
Offset to master [ns]	Displays the measured difference (offset) between the local clock and the reference time source (*Grandmaster*) in nanoseconds. The device calculates the difference from the received time information.
Steps removed	Displays the number of communication paths passed through between the local clock of the device and the reference time source (*Grandmaster*). When the device operates in the Slave role, the value **1** means that the device is connected with the reference time source (*Grandmaster*) directly through one communication path.
Clock identity	Displays the clock identification number of the device. The device displays the identification number as a byte sequence in hexadecimal notation. The device identification number consists of the MAC address of the device followed by: • **00:01** for *Instance 0* • **00:02** for *Instance 1*
Max. offset absolute [ns]	Displays the maximum measured time difference in nanoseconds that has occurred since the device synchronized its local clock with the reference time source (*Grandmaster*).
Is synchronized	Displays if the local clock is synchronized with the reference time source (*Grandmaster*). If the measured time difference between the local clock and the reference time source (*Grandmaster*) falls below the synchronization lower threshold value, then the device considers its local clock to be synchronized. The device keeps this status until the measured time difference exceeds the synchronization upper threshold value. You specify the synchronization threshold values in the Configuration frame.

Grandmaster

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

The algorithm first evaluates the value in the Priority 1 field of the participating devices. The device with the numerically lowest value in the Priority 1 field is designated as the reference time source (*Grandmaster*). If the value is the same for multiple devices, then the algorithm takes the next criterion. If this is also the same, then the algorithm takes the next criterion after this one. If these values are the same for multiple devices, then the numerically lowest value in the Clock identity field determines which device is designated as the reference time source (*Grandmaster*). The value in the Clock identity field is based on the device MAC address which is supposed to be globally unique. The value in the Clock identity field serves as the final tie-break for the algorithm.

The device allows you to influence which device in the network is designated as the reference time source (*Grandmaster*). To do this, modify the value in the Priority 1 field or the Priority 2 field in the **Time > 802.1AS > Global** frame.

The following table presents the grandmaster settings:

Setting	Description
Priority 1	Displays the *priority 1* value for the device that is currently the reference time source (*Grandmaster*).
Clock class	Displays the class of the reference time source (*Grandmaster*). This is a parameter used by the *Best Master Clock* algorithm.
Clock accuracy	Displays the estimated accuracy of the reference time source (*Grandmaster*). This is a parameter used by the *Best Master Clock* algorithm.
Clock variance	Displays the variance of the reference time source (*Grandmaster*), also defined as the *Offset scaled log variance*. This is a parameter used by the *Best Master Clock* algorithm.
Priority 2	Displays the *priority 2* value for the device that is currently the reference time source (*Grandmaster*).
Clock identity	Displays the identification number of the reference time source (*Grandmaster*) device. The device identification number consists of the MAC address of the device followed by: • **00:01** for *Instance 0* • **00:02** for *Instance 1*

Parent

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

The following table presents the parent settings:

Setting	Description
Clock identity	Displays the port identification number of the directly superior master device. The device identification number consists of the MAC address of the device followed by: • **00:01** for *Instance 0* • **00:02** for *Instance 1*
Port	Displays the port number of the directly superior master device.
Cumulative rate ratio [ppm]	Displays the measured frequency difference of the local clock in ppm (parts per million) relative to the reference time source (*Grandmaster*).

802.1AS Port

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

Instance

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

You set up each instance separately:

- *Instance 0*

  for synchronizing device clocks and transmitting time synchronization messages
- *Instance 1*

  only for transmitting time synchronization messages

Operation

The following table presents the operation setting:

Setting	Description
Operation	Enables/disables the 802.1AS function for the respective instance. Possible values: • **On** The 802.1AS function is enabled. The device synchronizes its local clock using the 802.1AS function. Consider activating the 802.1AS function on the individual ports. • **Off** (default setting) The 802.1AS function is disabled.

Configuration

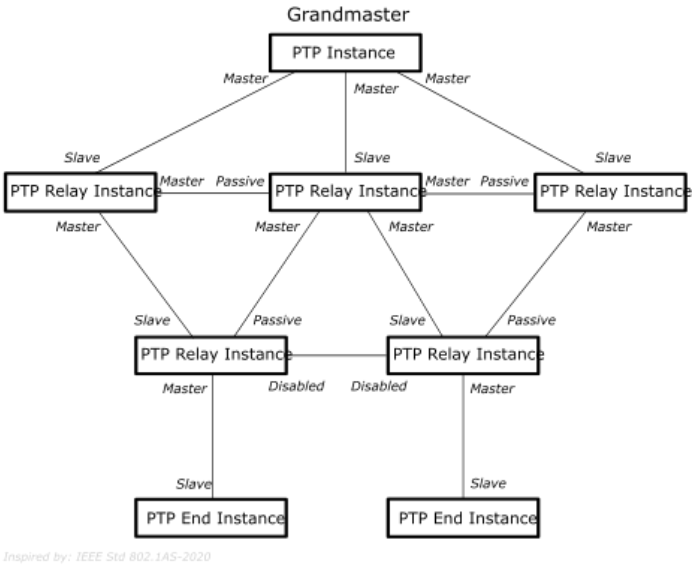
The following table presents the configuration settings:

Setting	Description
Priority 1	Specifies the *priority 1* value for the instance. Possible values: • **0..255** (default setting: **248**) Verify that you use the value **255** for a *PTP instance* that is not Grandmaster-capable.
Priority 2	Specifies the *priority 2* value for the instance. Possible values: • **0..255** (default setting: **247**) Verify that you use the value **255** for a *PTP instance* that is not Grandmaster-capable.
Domain number	Specifies the domain number. If a port is part of the same domain for both *Instance 0* and *Instance 1*, then the dialog displays an diagnostic message. Possible values: • **0..127** (default settings: **0** for *Instance 0* and **1** for *Instance 1*)
External port configuration	Activates/deactivates the manual setup of the port roles. Possible values: • **marked** Manual setup is active. You can select the desired port roles from the Desired Role drop-down list. • **unmarked** (default setting) Manual setup is inactive. The device auto-negotiates port roles.

Table

For information on how to customize the appearance of the table, see Working with tables, page 25.

The following table presents the table settings:

Setting	Description
Port	Displays the port number.
Active	Activates/deactivates the 802.1AS function on the port. Possible values: • **marked** (default setting) The 802.1AS function is active on the port. On the port, the device synchronizes its clock using the 802.1AS function. The prerequisite is that none of the following protocols are active on the port: ◦ Link Aggregation • **unmarked** The 802.1AS function is inactive on the port.
Role	Displays the role that the port operates in within the 802.1AS domain. Possible values: • **Disabled** The port is not 802.1AS-capable. • **Master** The port operates in the **Master** role. • **Passive** The port operates in the **Passive** role. • **Slave** The port operates in the **Slave** role. 
Desired Role	Specifies the desired role for the port. If the checkbox in the External port configuration column is marked, then auto-negotiation of port roles is disabled. You can then manually set the desired port role. Possible values: • **Disabled** The port is not 802.1AS-capable. • **Master** The port operates in the **Master** role. • **Passive** The port operates in the **Passive** role. • **Slave** The port operates in the **Slave** role.

Setting	Description
AS capable	Displays if the port of the device and the port of the neighboring device are both 802.1AS-capable and have the 802.1AS function enabled. Possible values: • **marked** The connected ports are 802.1AS-capable and have the 802.1AS function enabled. The prerequisites are: ◦ The checkbox in the Measuring delay column is marked. The device measures the delay (*Peer delay*) on the port. ◦ The value you specify in the Peer delay threshold [ns] column is greater than the value in the Peer delay [ns] column. • **unmarked** (default setting) At least one of the connected ports is not 802.1AS-capable or does not have the 802.1AS function enabled.
Initial announce interval [s]	Specifies the interval in seconds at which the port, in the **Master** role, sends *Announce* messages for 802.1AS topology discovery. Possible values: • **1..2** (default setting: **1**) Assign the same value to every device of an 802.1AS domain. • **–** The port does not send *Announce* messages.
Settable announce interval [s]	Specifies the interval in seconds at which the port, in the **Master** role, sends *Announce* messages for 802.1AS topology discovery. If the checkbox in the Use settable announce interval column is marked, then the device uses this value instead of the value specified in the Initial announce interval [s] column. During the first synchronization, the device uses the value in the Initial announce interval [s] column even if the Use settable announce interval checkbox is marked. Possible values: • **1..2** (default setting: **1**) Assign the same value to every device of an 802.1AS domain. • **–** The port does not transmit *Announce* messages.
Use settable announce interval	Activates/deactivates the use of the interval specified in the Settable announce interval [s] column for sending *Announce* messages. The device sends *Announce* messages for 802.1AS topology discovery. Possible values: • **marked** (default setting) The device sends *Announce* messages in the interval specified in the Settable announce interval [s] column. • **unmarked** The device sends *Announce* messages in the interval specified in the Initial announce interval [s] column.
Announce timeout	Specifies the number of *Announce* intervals that the device waits for to receive an *Announce* message on this port from the neighboring port. Example: In the default setting, where Settable announce interval [s] **= 1** and Announce timeout **= 3**, the total timeout in seconds is `1 s × 3 = 3 s`. When the specified interval elapses without receiving an *Announce* message, the device tries to find a new path to the reference time source (*Grandmaster*) using the *Best Master Clock* algorithm. If the device finds a reference time source (*Grandmaster*), then it assigns the **Slave** role to the port through which the new path leads. If the device does not find a reference time source (*Grandmaster*), the device itself becomes the reference time source (*Grandmaster*) and assigns the **Master** role to its ports. Possible values: • **2..10** (default setting: **3**) Assign the same value to each port that belongs to the same 802.1AS domain.

Setting	Description
Initial sync interval [s]	Specifies the interval in seconds at which the port, in the **Master** role, sends *Sync* messages for time synchronization. Possible values: • **0.125** (default setting) • **0.250** • **0.5** • **1** • **–** The port does not send *Sync* messages.
Settable sync interval [s]	Specifies the interval in seconds at which the port, in the **Master** role, sends *Sync* messages for time synchronization. If the checkbox in the Use settable sync interval column is marked, then the device uses this value instead of the value specified in the Initial sync interval [s] column. During the first synchronization, the device uses the value in the Initial sync interval [s] column even if the Use settable sync interval checkbox is marked. Possible values: • **0.125** (default setting) • **0.250** • **0.5** • **1** • **–** The port does not send *Sync* messages.
Use settable sync interval	Activates/deactivates the use of the value in the Settable sync interval [s] column for sending *Sync* messages. Possible values: • **marked** (default setting) The device sends *Sync* messages in the interval specified in the Settable sync interval [s] column. • **unmarked** The device sends *Sync* messages in the interval specified in the Initial sync interval [s] column.
Sync timeout	Specifies the number of *Sync* intervals the device waits for to receive a *Sync* message on this port from the neighboring port. Example: In the default setting, whereSettable sync interval [s] = **0.125** andSync timeout = **3**, the total timeout in seconds is `0.125 s × 3 = 0.375 s`. When the number of intervals elapses without receiving a *Sync* message, the device tries to find a new path to the reference time source using the *Best Master Clock* algorithm. If the device finds a reference time source (*Grandmaster*), then it assigns the **Slave** role to the port through which the new path leads. Otherwise, the device itself becomes the reference time source (*Grandmaster*) and assigns the **Master** role to its ports. Possible values: • **2..10** (default setting: **3**) Assign the same value to each port that belongs to the same 802.1AS domain.
Initial pdelay interval [s]	Specifies the interval in seconds at which the port sends a *Peer delay request* message to the neighboring port to measure the *Peer delay*. Possible values: • **1** (default setting) • **2** • **4** • **8** • **–** The port does not send *Peer delay request* messages.

Setting	Description
Settable pdelay interval [s]	Specifies the interval in seconds at which the port sends a *Peer delay request* message to the neighboring port to measure the *Peer delay*. If the checkbox in the Use settable pdelay interval column is marked, then the devices uses this value instead of the value specified in the Initial pdelay interval [s] column. During the first synchronization, the device uses the value in the Initial pdelay interval [s] column even if the Use settable pdelay interval checkbox is marked. Possible values: • **1** (default setting) • **2** • **4** • **8** • **–** The port does not send *Peer delay request* messages.
Use settable pdelay interval	Activates/deactivates the use of the value in the Settable pdelay interval [s] column for sending *Peer delay request* messages. Possible values: • **marked** The device sends *Peer delay request* messages in the interval specified in the Settable pdelay interval [s] column. • **unmarked** (default setting) The device sends *Peer delay request* messages in the interval specified in the Initial pdelay interval [s] column.
Initial GptpCapable interval [s]	Specifies the interval in seconds at which the port sends a message to the neighboring port about the device capability for time synchronization. Possible values: • **1** (default setting) • **2** • **4** • **8** • **–** The port does not send *gPTP-capable* messages.
Settable GptpCapable interval [s]	Specifies the interval in seconds at which the port sends a message to the neighboring port about the device capability for time synchronization. If the checkbox in theUse settable GptpCapable interval column is marked, the device uses this value instead of the value specified in the Initial GptpCapable interval [s] column. During the first synchronization, the device uses the value in the Initial GptpCapable interval [s] column even if the Use settable GptpCapable interval checkbox is marked. Possible values: • **1** (default setting) • **2** • **4** • **8** • **–** The port does not send *gPTP-capable* messages.
Use settable GptpCapable interval	Activates/deactivates the use of the value in the Settable GptpCapable interval [s] column for sending messages that contain *gPTP-capable* information. Possible values: • **marked** The device sends *gPTP-capable* messages in the interval specified in the Settable GptpCapable interval [s] column. • **unmarked** (default setting) The device sends *gPTP-capable* messages in the interval specified in the Initial GptpCapable interval [s] column.

Setting	Description
GptpCapable timeout	Specifies the number of *gPTP-capable* intervals that the device waits for to receive a *gPTP-capable* message on this port from the neighboring port. When the number of intervals elapses without receiving a *gPTP-capable* message, the device assigns the **Disabled** role to the port. The port is no longer *gPTP-capable*. Possible values: • **1..255** (default setting: **9**)
Peer delay timeout	Specifies the number of *Peer delay* intervals that the device waits for to receive a *Peer delay* message from the neighboring port. When the number of intervals elapses without receiving a *Peer delay* message, the device assigns the **Disabled** role to the port. The port is no longer 802.1AS-capable. See the AS capable column. Possible values: • **1..255** (default setting: **9**)
Allowed faults	Specifies the number of detected faults above which the device no longer considers the port as 802.1AS-capable. The device assigns the **Disabled** role to the port. Examples of such detected faults are: • The Peer delay threshold [ns] value exceeds the upper threshold. • The calculated Neighbor rate ratio [ppm] is invalid. Possible values: • **1..255** (default setting: **9**)
Peer delay threshold [ns]	Specifies the upper threshold value for the *Peer delay* in nanoseconds. If the value in the Peer delay [ns] column is greater than this value, then the device assigns the **Disabled** role to the port. The port is no longer 802.1AS-capable. See the AS capable column. Possible values: • **0..1000000 (10^6)** (default setting: **10000**)
Measuring delay	Displays if the device measures the delay (*Peer delay*) on the port. Possible values: • **marked** The device measures the delay (*Peer delay*) on the port. You find the measured value in the Peer delay [ns] column. • **unmarked** The device does not measure the delay (*Peer delay*) on the port.
Peer delay [ns]	Displays the *Peer delay* value in nanoseconds the device measured. The prerequisite is that the checkbox in the Measuring delay column is marked.
Asymmetry	Specifies the time difference in nanoseconds between the mean link delay value (`Peer delay [ns] / 2`) and the propagation time from the port to its neighbor. Possible values: • **-10000000000..10000000000 (10^{10})** (default setting: **0**)
Neighbor rate ratio [ppm]	Displays the measured frequency difference of the local clock in parts per million relative to the clock in the adjacent device.

802.1AS Statistics

This dialog **Time > 802.1AS > Statistics** displays information about the number of messages received, sent, or discarded on the ports. The dialog also displays counters that increment every time a timeout event occurred.

Instance

The device displays information for each instance separately.

Table

For information on how to customize the appearance of the table, see Working with tables, page 25.

The following table presents the table settings:

Setting	Description
Port	Displays the port number.
Received messages	Displays the counters for messages received on the ports: • **Sync**: Displays the number of *Sync* messages. • **Sync follow-up**: Displays the number of *Sync follow-up* messages. • **Delay request**: Displays the number of *Peer delay request* messages. • **Delay response**: Displays the number of *Peer delay response* messages. • **Delay response follow-up**: Displays the number of *Peer delay response follow-up* messages. • **Announce**: Displays the number of *Announce* messages. • **Discarded**: Displays the number of *Sync* messages that the device discarded on this port. The device discards a *Sync* message for example, in cases where the port does not receive a *Sync follow-up* message for a corresponding *Sync* message. • **Sync timeout**: Displays the number of times that a Sync timeout event occurred on the port. See the Sync timeout column in the **Time > 802.1AS > Port** dialog. • **Announce timeout**: Displays the number of times that the Announce timeout event occurred on this port. See the Announce timeout column in the **Time > 802.1AS > Port** dialog. • **Delay timeout**: Displays the number of times that the Peer delay timeout event occurred on this port. See the Peer delay timeout column in the **Time > 802.1AS > Port** dialog.
Transmitted messages	Displays the counters for messages transmitted on the ports: • **Sync**: Displays the number of *Sync* messages. • **Sync follow-up**: Displays the number of *Sync follow-up* messages. • **Delay request**: Displays the number of *Peer delay request* messages. • **Delay response**: Displays the number of *Peer delay response* messages. • **Delay response follow-up**: Displays the number of *Peer delay response follow-up* messages. • **Announce**: Displays the number of *Announce* messages.

Device Security

The menu contains the following dialogs:

- User Management, page 98
- Authentication List, page 102
- LDAP, page 105
- Management Access, page 114
- Pre-login Banner, page 133
- SSH Known Hosts, page 134

User Management

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

In this dialog **Device Security > User Management**, 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 specify settings for the login.

Setting	Description
Login attempts	Specifies the number of possible consecutive unsuccessful login attempts when the user accesses the device management using the Graphical User Interface or the Command Line Interface. **NOTE:** When accessing the device management using the Command Line Interface through the serial connection, the number of unsuccessful login attempts is unlimited. Possible values: • **0..5** (default setting: **0**) If the user makes one more consecutive unsuccessful login attempt, then the device locks access for the user. The device allows only users with the **administrator** authorization remove the lock. The value **0** deactivates the lock. The user has unlimited attempts to log into the device management.
Min. password length	The device accepts the password if it contains at least the number of characters specified here. The device checks the password according to this setting, regardless of the setting for the Policy check checkbox. Possible values: • **1..64** (default setting: **6**)
Login attempts period (min.)	Displays the time period before the device resets the counter in the Login attempts field. Possible values: • **0..60** (default setting: **0**)

Password policy

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

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

The following table presens the password policy settings:

Setting	Description
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 allows you to set up and manage user accounts. To change settings, click the desired parameter in the table and modify the value.

For information on how to customize the appearance of the table, see Working with tables, page 25.

Setting	Description
Buttons	The following list presents the buttons descriptions: • Add: Opens the Create window to add a table row. In the User name field, you specify the name of the user account. Possible values: Alphanumeric ASCII character string with 1..32 characters. • Remove: Removes the selected table row.
User name	Displays the name of the user account. To add a user account, click the button.
Active	Activates/deactivates the user account. Possible values: • **marked** The user account is active. The device accepts the login of a user, to the device management, with this user name. • **unmarked** (default setting) The user account is inactive. The device rejects the login of a user, to the device management, with this user name. When one user account exists with the access role **administrator**, this user account is constantly active.
Password	Specifies the password that the user applies to access the device management using the Graphical User Interface or Command Line Interface. Displays ***** (asterisks) instead of the password with which the user logs into the device management. To change the password, click the relevant field. When you specify the password for the first time, the device uses the same password in the SNMP auth password and SNMP encryption password columns. • Specify different passwords in the SNMP auth password and SNMP encryption password columns. • If you change the password in the column, then the device also changes the passwords for the SNMP auth password and SNMP encryption password columns, but only if they are not individually specified previously. Possible values: • Alphanumeric ASCII character string with 6..64 characters The device accepts the following characters: ◦ **a..z** ◦ **A..Z** ◦ **0..9** ◦ **!#$%&'()*+,-./:;<=>?@[\]^_`{}~** The minimum length of the password is specified in the Configuration frame. The device differentiates between upper and lower case. If the checkbox in the Policy check column is marked, then the device checks the password according to the policy specified in the Password policy frame. The device constantly checks the minimum length of the password, even if the checkbox in the Policy check column is **unmarked**.

Setting	Description
Role	Specifies the access role that regulates the access of the user to the individual functions of the device. Possible values: • **unauthorized** The user is blocked, and the device rejects the user login to the device management. Assign this value to temporarily lock the user account. If the device detects an error when another access role is being assigned, then the device assigns this access role to the user account. • **guest** (default setting) The user is authorized to monitor the device. • **auditor** The user is authorized to monitor the device and to save the log file in the **Diagnostics > Report > Audit Trail** dialog. • **operator** The user is authorized to monitor the device and to change the settings – with the exception of security settings for device access. • **administrator** The user is authorized to monitor the device and to change the settings. The device assigns the Service Type transferred in the response of a RADIUS server as follows to an access role: • **Administrative-User**: **administrator** • **Login-User**: **operator** • **NAS-Prompt-User**: **guest**
User locked	Unlocks the user account. Possible values: • **marked** The user account is locked. The user has no access to the device management. If the user makes too many consecutive unsuccessful login attempts, then the device automatically locks the user. • **unmarked** (grayed out) (default setting) The user account is unlocked. The user has access to the device management.
Policy check	Activates/deactivates the password check. Possible values: • **marked** The password verification 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 verification is deactivated.
SNMP auth type	Specifies the authentication protocol that the device applies for user access using SNMPv3. Possible values: • **hmacmd5** (default setting) For this user account, the device uses protocol HMACMD5. • **hmacsha** For this user account, the device uses protocol HMACSHA.

Setting	Description
SNMP auth password	Specifies the password that the device applies for user access using SNMPv3. Displays ***** (asterisks) instead of the password with which the user logs into the device management. To change the password, click the relevant field. By default, the device uses the same password that you specify in the Password column. • For the present column, 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 column, but only if it is not individually specified. Possible values: • Alphanumeric ASCII character string with 6..64 characters The device accepts the following characters: ◦ **a..z** ◦ **A..Z** ◦ **0..9** ◦ **!#$%&'()*+,-./:;<=>?@[\]^_`{}~**
SNMP encryption type	Specifies the encryption protocol that the device applies for user access using SNMPv3. Possible values: • **none** No encryption. • **des** (default setting) DES encryption • **aesCfb128** AES128 encryption
SNMP encryption password	Specifies the password that the device applies to encrypt user access using SNMPv3. Displays ***** (asterisks) instead of the password with which the user logs into the device management. To change the password, click the relevant field. By default, the device uses the same password that you specify in the Password column. • For the present column, 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 column, but only if it is not individually specified. Possible values: • Alphanumeric ASCII character string with 6..64 characters The device accepts the following characters: ◦ **a..z** ◦ **A..Z** ◦ **0..9** ◦ **!#$%&'()*+,-./:;<=>?@[\]^_`{}~**

Authentication List

In this dialog **Device Security > Authentication List**, 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 allows 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 allows them have access to the network. The device authenticates the end devices using the following methods:

- RADIUS
- IAS (Integrated Authentication Server)

In the default setting the following authentication lists are available:

- **defaultDot1x8021AuthList**
- **defaultLoginAuthList**
- **defaultV24AuthList**

Table

For information on how to customize the appearance of the table, see Working with tables, page 25.

NOTE:

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

The following table presents the table settings:

Setting	Description
Buttons	The following list presents the icon descriptions: • Add: Opens the Create window to add a table row. In the Name field, you specify the name of the list. Possible values: Alphanumeric ASCII character string with 1..32 characters. • Remove: Removes the selected table row. • Allocate applications: Opens the Allocate applications window. The window displays the applications that you can designate to the selected list. ◦ Click and select an item to designate it to the currently selected list. An application that is already designated to a different list the device designates to the currently selected list, after you click the Ok button. ◦ Click and deselect an item to undo its designation to the currently selected list. If you deselect the application **WebInterface**, then the connection to the device is lost, after you click the Ok button.
Name	Displays the name of the list. To add a list, click the button.
Policy 1 **Policy 2** **Policy 3** **Policy 4** **Policy 5**	Specifies the authentication policy that the device uses for access using the application specified in the Dedicated applications column. The device gives you the option of a fall-back solution. For this, you specify another policy in each of the policy fields. If the authentication with the specified policy is unsuccessful, then the device can use the next policy, depending on the order of the values entered in each policy. Possible values: • **local** (default setting) The device authenticates the users by using the local user management. See the **Device Security > User Management** dialog. You cannot assign this value to the authentication list **defaultDot1x8021AuthList**. • **radius** The device authenticates the users with a RADIUS server in the network. You specify the RADIUS server in the **Network Security > RADIUS > Authentication Server** dialog. • **reject** The device accepts or rejects the user logging into the device management depending on which policy you try first. The following list contains authentication scenarios: ◦ If the first policy in the authentication list is **local** and the device accepts the login credentials of the user, then it logs the user into the device management without attempting the other polices. ◦ If the first policy in the authentication list is **local** and the device denies the login credentials of the user, then it attempts to log the user into the device management using the other polices in the order specified. ◦ If the first policy in the authentication list is **radius** or **ldap** and the device rejects a login, then the login is immediately rejected without attempting to log in the user using another policy. If there is no response from the RADIUS or LDAP server, then the device attempts to authenticate the user with the next policy. ◦ If the first policy in the authentication list is **reject**, then the devices immediately rejects the user login without attempting another policy. ◦ Verify that the authentication list **defaultV24AuthList** contains at least one policy different from **reject**. • **ias** The device authenticates the end devices logging in using 802.1X with the integrated authentication server (IAS). The integrated authentication server manages the login data in a separate database. See the **Network Security > 802.1X > IAS** dialog. You can only assign this value to the authentication list **defaultDot1x8021AuthList**. • **ldap** The device authenticates the users with authentication data and access role saved in a central location. You specify the Active Directory server that the device uses in the **Device Security > LDAP > Configuration** dialog.

Setting	Description
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. Assign each application to exactly one list.
Active	Activates/deactivates the list. Possible values: • **marked** (default setting) The list is activated. The device uses the policies in this list when users access the device with the relevant application. • **unmarked** The list is deactivated.

LDAP

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

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

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

The menu **Device Security > LDAP** contains the following dialogs:

- LDAP Configuration, page 105
- LDAP Role Mapping, page 111

LDAP Configuration

This dialog **Device Security > LDAP > Configuration** allows you to 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

The following table presents the operation setting:

Setting	Description
Operation	Enables/disables the LDAP client. If in the **Device Security > Authentication List** dialog you specify the value **ldap** in one of the columns Policy 1 to Policy 5, then the device uses the LDAP client. Prior to this, specify in the **Device Security > LDAP > Role Mapping** dialog at least one mapping for this access role **administrator**. This provides you access to the device as administrator after logging into the device management through LDAP. Possible values: • **On** The LDAP client is enabled. • **Off** (default setting) The LDAP client is disabled.

Configuration

The following table presents the configuration settings:

Setting	Description
Buttons	Flush cache: Deletes the cached login data of the successfully logged in users.
Client cache timeout [min]	Specifies for how many minutes after successfully logging into the device management the login data of a user remain valid. When a user logs in again within this time, no complex LDAP search operation is necessary. The login process is much faster. Possible values: • **1..1440** (default setting: **10**)
Bind user	Specifies the user ID in the form of the “Distinguished Name” (DN) with which the device logs into the LDAP server. If the LDAP server requires a user ID in the form of the “Distinguished Name” (DN) for the login, then this information is necessary. In Active Directory environments, this information is unnecessary. The device attempts to authenticate on the LDAP server with the user ID to find the “Distinguished Name” (DN) for the users logging into the device management. The device conducts the search according to the settings in the Base DN and User name attribute fields. Possible values: • Alphanumeric ASCII character string with 0..64 characters
Bind user password	Specifies the password which the device uses together with the user ID specified in the Bind user field when logging into the LDAP server. Possible values: • Alphanumeric ASCII character string with 0..64 characters
Base DN	Specifies the starting point for the search in the directory tree in the form of the “Distinguished Name” (DN). Possible values: • Alphanumeric ASCII character string with 0..255 characters
User name attribute	Specifies the LDAP attribute which contains a biunique user name. Afterwards, the user uses the user name contained in this attribute to log into the device management. Often the LDAP attributes **userPrincipalName**, **mail**, **sAMAccountName** and **uid** contain a unique user name. The device adds the character string specified in the Default domain field to the user name under the following condition: • The user name contained in the attribute does not contain the @ character. • In the Default domain field, a domain name is specified. Possible values: • Alphanumeric ASCII character string with 0..64 characters (default setting: **userPrincipalName**)
Default domain	Specifies the character string which the device adds to the user name of the users logging in if the user name does not contain the @ character. Possible values: • Alphanumeric ASCII character string with 0..64 characters

Certificates/CRLs

To establish a secure connection, the device requires to obtain a valid digital certificate to verify the identity of the server. The prerequisite is that you have transferred the public certificate of the server onto the device. Ask the server

administrator for a digital certificate in X.509 format. For security reasons, using only digital certificates signed by a Certification Authority (CA).

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

Setting	Description
Buttons	Clear all Certificates/CRLs: Deletes the digital certificates and CRLs transferred onto the device from the non-volatile memory (**NVM**).
URL	Specifies the path and file name of the digital certificate or CRL. The device accepts digital certificates and CRLs with the following properties: • X.509 format • .PEM file name extension • Base64-coded and enclosed by the lines -----BEGIN CERTIFICATE----- … -----END CERTIFICATE----- or -----BEGIN CRL----- … -----END CRL----- The device gives you the following options for transferring the file onto the device: • Import from the PC When the file is located on your PC or on a network drive, drag and drop it onto the area. As an alternative, click in the area to select the file. • Import from an FTP server Do not use this method if you transmit data over untrusted networks. When the file is on an FTP server, specify the URL for the file in the following form: ftp://<user>:<password>@<IP address>[:port]/<path>/<file name> • Import from a TFTP server Do not use this method if you transmit data over untrusted networks. When the file is on a TFTP server, specify the URL for the file in the following form: tftp://<IP address>/<path>/<file name> • Import from an SCP or SFTP server When the file is on an SCP or SFTP server, specify the URL for the file in the following form: ◦ scp:// or sftp://<IP address>/<path>/<file name> Click the Start button to open the Credentials window. In this window, you enter the User name and Password to log into the server. ◦ scp:// or sftp://<user>:<password>@<IP address>/<path>/<file name> Remember to set up the SCP or SFTP server as an SSH known host before the device accesses the server for the first time. See the **Device Security > SSH Known Hosts** dialog.
Start	Transfers the file specified in the URL field onto the device. In this dialog, you can transfer a maximum of 16 digital certificates and additionally a maximum of 16 CRLs onto the device. For the changes to take effect after transferring a digital certificate or a CRL into the device, disable and re-enable the LDAP function. See the Operation frame.

Table

For information on how to customize the appearance of the table, see Working with tables, page 25.

The following table presents the table settings:

Setting	Description
Buttons	The following list presents the icon descriptions: • Add: Adds a table row. • Remove: Removes the selected table row.
Index	Displays the index number to which the table row relates. The device automatically assigns the value when you add a table row.
Description	Specifies the description. You have the option to describe here the authentication server or note additional information. Possible values: • Alphanumeric ASCII character string with 0..255 characters
Address	Specifies the IP address or the DNS name of the server. If in the Connection security column a value other than **none** is specified and the digital certificate contains only DNS names of the server, then specify a DNS name. Possible values: • Valid IPv4 address (default setting: **0.0.0.0**) • Valid IPv6 address • DNS name in the format **<domain>.<tld>** or **<host>.<domain>.<tld>** The prerequisite is that you also enable the Client function in the **Advanced > DNS > Client > Global** dialog. To establish an encrypted connection using a digital certificate, verify that the `Common Name` or `Subject Alternative Name` information in the digital certificate that you have transferred onto the device matches the value you specify here. Otherwise, the device will not be able to verify the identity of the server. • **_ldap._tcp.<domain>.<tld>** Using this DNS name, the device queries the LDAP server list (SRV Resource Record) from the DNS server.
Destination TCP port	Specifies the TCP Port on which the server expects the requests. If you have specified the value **_ldap._tcp.domain.tld** in the Address column, then the device ignores this value. Possible values: • **0..65535 (2^{16}-1)** (default setting: **389**) Exception: Port **2222** is reserved for internal functions. Frequently used TCP-Ports: • **LDAP**: **389** • **LDAP over SSL**: **636** • **Active Directory Global Catalogue**: **3268** • **Active Directory Global Catalogue SSL**: **3269**

Setting	Description
Connection security	Specifies the protocol which encrypts the communication between the device and the authentication server. Possible values: • **none** No encryption. The device establishes an LDAP connection to the server and transmits the communication including the passwords in clear text. • **ssl** Encryption with SSL. The device establishes a TLS connection to the server and tunnels the LDAP communication over it. • **startTLS** (default setting) Encryption with startTLS extension. The device establishes an LDAP connection to the server and encrypts the communication. The prerequisite for encrypted communication is that the device uses the correct time. If the digital certificate contains only the DNS names, then you specify the DNS name of the server in the Address column. Enable the Client function in the **Advanced > DNS > Client > Global** dialog. If the digital certificate contains the IP address of the server in the *Subject Alternative Name* field, then the device is able to verify the identity of the server without the DNS setting.
Server status	Displays the connection status and the authentication with the authentication server. Possible values: • **ok** The server is reachable. If in the Connection security column a value other than **none** is specified, then the device has verified the digital certificate of the server. • **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.

LDAP Role Mapping

This dialog **Device Security > LDAP > Role Mapping** allows you to set up to 64 mappings to assign an access role to users.

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

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

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

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

On this basis, the device checks any mapping.

- Does the user object contain the required attribute?

  or

- Is the user member of the group?

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

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

Configuration

The following table presents the configuration setting:

Setting	Description
Matching policy	Specifies which access role the device applies if more than one mapping applies to a user. Possible values: • **highest** (default setting) The device applies the access role with more extensive authorizations. • **first** The device applies the rule which has the lower value in the Index column to the user.

Table

For information on how to customize the appearance of the table, see Working with tables, page 25.

The following table presents the table settings:

Setting	Description
Buttons	The following list presents the icon descriptions: • Opens the Create window to add a table row. In the Index field, you specify the index number. Possible values: **1..64** •  Remove: Removes the selected table row.
Index	Displays the index number to which the table row relates. You specify the index number when you add a table row.
Role	Specifies the access role that regulates the access of the user to the individual functions of the device. Possible values: • **unauthorized** (default setting) The user is blocked, and the device rejects the user login. Assign this value to temporarily lock the user account. If an error is detected when another role is being assigned, then the device assigns this access role to the user account. • **guest** The user is authorized to monitor the device. • **auditor** The user is authorized to monitor the device and to save the log file in the **Diagnostics > Report > Audit Trail** dialog. • **operator** The user is authorized to monitor the device and to change the settings – with the exception of security settings for device access. • **administrator** The user is authorized to monitor the device and to change the settings.
Type	Specifies if a group or an attribute with an attribute value is specified in the Parameter column. Possible values: • **attribute** (default setting) The Parameter column contains an attribute with an attribute value. • **group** The Parameter column contains the “Distinguished Name” (DN) of a group.
Parameter	Specifies a group or an attribute with an attribute value, depending on the setting in the Type column. Possible values: • Alphanumeric ASCII character string with 0..255 characters The device differentiates between upper and lower case. ◦ If in the Type column the value **attribute** is specified, then you specify the attribute in the form of **Attribute_name=Attribute_value**. Example: **l=Germany** ◦ If in the Type column the value **group** is specified, then you specify the “Distinguished Name” (DN) of a group. Example: **CN=admin-users,OU=Groups,DC=example,DC=com**
Active	Activates/deactivates the role mapping. Possible values: • **marked** The role mapping is active. • **unmarked** (default setting) The role mapping is inactive.

Management Access

The Management Access menu **Device Security > Management Access**contains the following dialogs:

- Server, page 114
- IP Access Restriction, page 127
- Web, page 129
- Command Line Interface, page 130
- SNMPv1/v2 Community, page 132

Server

This dialog **Device Security > Management Access > Server** allows you to set up the server services which enable users or applications to access the management of the device.

The dialog contains the following tabs:

- Information, page 114
- SNMP, page 116
- Telnet, page 118
- SSH, page 119
- HTTP, page 122
- HTTPS, page 123

Information

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

Table

For information on how to customize the appearance of the table, see Working with tables, page 25.

The following table presents the table settings:

Setting	Description
SNMPv1	Displays if the server service is active or inactive, which authorizes access to the device using SNMP version 1. See the SNMP tab. Possible values: • **marked** Server service is active. • **unmarked** Server service is inactive.
SNMPv2	Displays if the server service is active or inactive, which authorizes access to the device using SNMP version 2. See the SNMP tab. Possible values: • **marked** Server service is active. • **unmarked** Server service is inactive.
SNMPv3	Displays if the server service is active or inactive, which authorizes access to the device using SNMP version 3. See the SNMP tab. Possible values: • **marked** Server service is active. • **unmarked** Server service is inactive.
Telnet server	Displays if the server service is active or inactive, which authorizes access to the device using Telnet. See the Telnet tab. Possible values: • **marked** Server service is active. • **unmarked** Server service is inactive.
SSH server	Displays if the server service is active or inactive, which authorizes access to the device using Secure Shell (SSH). See the SSH tab. Possible values: • **marked** Server service is active. • **unmarked** Server service is inactive.
HTTP server	Displays if the server service is active or inactive, which authorizes access to the device using the Graphical User Interface through HTTP. See the HTTP tab. Possible values: • **marked** Server service is active. • **unmarked** Server service is inactive.
HTTPS server	Displays if the server service is active or inactive, which authorizes access to the device using the Graphical User Interface through HTTPS. See the HTTPS tab. Possible values: • **marked** Server service is active. • **unmarked** Server service is inactive.

SNMP

This tab 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

The following table presents the configuration settings:

Setting	Description
SNMPv1	Activates/deactivates the access to the device with SNMP version 1. Possible values: • **marked** SNMP version 1 access is active. ◦ You specify the community names in the **Device Security > Management Access > SNMPv1/v2 Community** dialog. ◦ You activate/deactivate the write access for the *read and write* authorization in the **Device Security > Management Access > SNMPv1/v2 Community** dialog. • **unmarked** (default setting) SNMP version 1 access is inactive.
SNMPv2	Activates/deactivates the access to the device with SNMP version 2. Possible values: • **marked** SNMP version 2 access is active. ◦ You specify the community names in the **Device Security > Management Access > SNMPv1/v2 Community** dialog. ◦ You activate/deactivate the write access for the *read and write* authorization in the **Device Security > Management Access > SNMPv1/v2 Community** dialog. • **unmarked** (default setting) SNMP version 2 access is inactive.
SNMPv3	Activates/deactivates the access to the device with SNMP version 3. Possible values: • **marked** (default setting) Access is activated. • **unmarked** Access is deactivated. Network management systems like 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 (2^{16}-1)** (default setting: **161**) Exception: Port **2222** is reserved for internal functions. To enable the SNMP agent to use the new port after a change, you proceed as follows: • Click the  button. • Select in the **Basic Settings > Load/Save** dialog the active configuration profile. • Click the  button to save the updated settings. • Restart the device.
SNMPover802	Activates/deactivates the access to the device through SNMP over IEEE 802. Possible values: • **marked** Access is activated. • **unmarked** (default setting) Access is deactivated.

Telnet

This tab allows you to 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

The following table presents the operation setting:

Setting	Description
Telnet server	Enables/disables the Telnet server. Possible values: • **On** The Telnet server is enabled. The access to the device management is possible through the Command Line Interface using an unencrypted Telnet connection. • **Off** (default setting) The Telnet server is disabled. **NOTE:** If the SSH server is disabled and you also disable the Telnet server, then access to the device management is only possible using the Command Line Interface through the serial connection.

Configuration

The following table presents the configuration settings:

Settings	Description
TCP port	Specifies the number of the TCP port on which the device receives Telnet requests from clients. Possible values: • **1..65535 (2^{16}-1)** (default setting: **23**) Exception: Port **2222** is reserved for internal functions. The server restarts automatically after the port is changed. Existing connections remain in place.
Connections	Displays how many Telnet connections are currently established to the device.
Connections (max.)	Specifies the maximum number of Telnet connections to the device that can be set up simultaneously. Possible values: • **1..5** (default setting: **5**)
Session timeout [min]	Specifies the timeout in minutes. After the device has been inactive for this time, it ends the session for the user logged into the device management. A change in the value takes effect the next time a user logs into the device management. Possible values: • **0** Deactivates the function. The connection remains established in the case of inactivity. • **1..160** (default setting: **5**)

SSH

This tab allows you to 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 verify. When you make this character sequence available to the users through a reliable channel, they have the option to compare both fingerprints. If the character sequences match, then the client is connected to the correct server.

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

Furthermore, the device can load an RSA *Host Key*, which is stored on the external memory (**ENVM**), during system startup. You activate this function in the **Basic Settings > External Memory** dialog, SSH key auto upload column.

Operation

The following table presents the operation setting:

Setting	Description
SSH server	Enables/disables the SSH server. Possible values: • **On** (default setting) The SSH server is enabled. The access to the device management is possible through the Command Line Interface using an encrypted SSH connection. You can start the server only if there is an RSA signature in the device. • **Off** The SSH server is disabled. When you disable the SSH server, the existing connections remain established. However, the device helps prevent new connections from being set up. **NOTE:** If the Telnet server is disabled and you also disable the SSH server, then access to the device management is only possible using the Command Line Interface through the serial connection.

Configuration

The following table presents the configuration settings:

Setting	Description
TCP port	Specifies the number of the TCP port on which the device receives SSH requests from clients. Possible values: • **1..65535 (2^{16}-1)** (default setting: **22**) Exception: Port **2222** is reserved for internal functions. The server restarts automatically after the port is changed. Existing connections remain in place.
Sessions	Displays how many SSH connections are currently established to the device.
Sessions (max.)	Specifies the maximum number of SSH connections to the device that can be set up simultaneously. Possible values: • **1..5** (default setting: **5**)
Session timeout [min]	Specifies the timeout in minutes. After the user logged into the device management has been inactive for this time, the device ends the connection. A change in the value takes effect the next time a user logs into the device management. Possible values: • **0** Deactivates the function. The connection remains established in the case of inactivity. • **1..160** (default setting: **5**)

Signature

The following table presents the signature settings:

Setting	Description
RSA present	Displays if an RSA *host key* is present in the device. Possible values: • **marked** The RSA *host key* is present. • **unmarked** The RSA *host key* is not present.
Create	Generates a RSA *host key* in the device. The prerequisite is that the SSH server is disabled. Length of the key generated: • 2048 bit (RSA) To get the SSH server to use the generated RSA *host key*, restart the SSH server. As an alternative, you can transfer your own private RSA key in PEM format onto the device. See the Key import frame.
Delete	Deletes the RSA *host key* from the device. The prerequisite is that the SSH server is disabled.
Oper status	Displays if the device currently generates a RSA *host key*. It is possible that another user triggered this action. Possible values: • **rsa** The device currently generates an RSA *host key*. • **none** The device does not generate an RSA *host key*.

Fingerprint

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

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

Setting	Description
Fingerprint type	Specifies which fingerprint the RSA fingerprint field displays. Possible values: • **md5** The RSA fingerprint field displays the fingerprint as hexadecimal MD5 hash. • **sha256** (default setting) The RSA fingerprint field displays the fingerprint as Base64-coded SHA256 hash.
RSA fingerprint	Displays the fingerprint of the RSA *host key* of the SSH server. When you change the settings in the Fingerprint type field, click afterwards the  button and then the  button to update the display.

Key Import

The following table presents the key import settings:

Setting	Description
URL	Specifies the path and file name of your own private RSA key. The device accepts the key if it has a length of 2048 bits. The device gives you the following options for transferring the file onto the device: • Import from the PC When the file is located on your PC or on a network drive, drag and drop it onto the area. As an alternative, click in the area to select the file. • Import from an FTP server Do not use this method if you transmit data over untrusted networks. When the file is on an FTP server, specify the URL for the file in the following form: ftp://<user>:<password>@<IP address>[:port]/<file name> • Import from a TFTP server Do not use this method if you transmit data over untrusted networks. When the file is on a TFTP server, specify the URL for the file in the following form: tftp://<IP address>/<path>/<file name> • Import from an SCP or SFTP server When the file is on an SCP or SFTP server, specify the URL for the file in the following form: ◦ scp:// or sftp://<IP address>/<path>/<file name> Click the Start button to open the Credentials window. In this window, you enter the User name and Password to log into the server. ◦ scp:// or sftp://<user>:<password>@<IP address>/<path>/<file name> Remember to set up the SCP or SFTP server as an SSH known host before the device accesses the server for the first time. See the **Device Security > SSH Known Hosts** dialog.
Start	Transfers the file specified in the URL field onto the device. For the changes to take effect after transferring a digital certificate onto the device, disable and re-enable the SSH server function. See the Operation frame.

HTTP

Enable/disable the Hypertext Transfer Protocol (HTTP) for the web server and specify the settings required for HTTP.

The web server provides the Graphical User Interface through an unencrypted HTTP connection. For security reasons, disable the Hypertext Transfer Protocol (HTTP) and use the Hypertext Transfer Protocol Secure (HTTPS) instead.

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

NOTE:

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

Operation

The following table presents the operation setting:

Setting	Description
HTTP server	Enables/disables the HTTP function for the web server. Possible values: • **On** (default setting) The HTTP function is enabled. The access to the device management is possible through an unencrypted HTTP connection. When the HTTPS function is also enabled, the device automatically redirects the request for a HTTP connection to an encrypted HTTPS connection. • **Off** The HTTP function is disabled. When the HTTPS function is enabled, the access to the device management is possible through an encrypted HTTPS connection. **NOTE:** If the HTTP and HTTPS functions are disabled, then you can enable the HTTP function using the Command Line Interface command `http server` to get to the Graphical User Interface.

Configuration

The following table presents the configuration setting:

Setting	Description
TCP port	Specifies the number of the TCP port on which the web server receives HTTP requests from clients. Possible values: • **1..65535 (2^{16}-1)** (default setting: **80**) Exception: Port **2222** is reserved for internal functions.

HTTPS

Enable/disable the Hypertext Transfer Protocol Secure(HTTPS) for the web server and specify the settings required for HTTPS.

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

A digital certificate is required for the encryption of the HTTP connection. The device allows you to generate this digital certificate yourself or to transfer an existing digital certificate onto the device.

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

NOTE:

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

Operation

The following table presents the operation setting:

Setting	Description
HTTPS server	Enables/disables the HTTPS function for the web server. Possible values: • **On** (default setting) The HTTPS function is enabled. The access to the device management is possible through an encrypted HTTPS connection. When there is no digital certificate present, the device generates a digital certificate before it enables the HTTPS function. • **Off** The HTTPS function is disabled. When the HTTP function is enabled, the access to the device management is possible through an unencrypted HTTP connection. **NOTE:** If the HTTP and HTTPS functions are disabled, then you can enable the HTTPS function using the Command Line Interface command `https server` to get to the Graphical User Interface.

Configuration

The following table presents the configuration setting:

Setting	Description
TCP port	Specifies the number of the TCP port on which the web server receives HTTPS requests from clients. Possible values: • **1..65535 (2^{16}-1)** (default setting: **443**) Exception: Port **2222** is reserved for internal functions.

Certificate

If the device uses a digital certificate not signed by a Certification Authority (CA) defined by the web browser, then the web browser may display a notification before loading the Graphical User Interface.

To address the notification, you have the following possibilities:

- Transfer a digital certificate onto the device whose Certification Authority (CA) is defined by your web browser. This may additionally require you to make the Certification Authority (CA) defined by your web browser or operating system.
- As a workaround, you can also add an exception rule for the existing device certificate in your web browser.

The following table presents the certificate settings:

Setting	Description
Present	Displays if a digital certificate is present in the device. Possible values: • **marked** A digital certificate is present. • **unmarked** The digital certificate has been removed.
Create	Generates a digital certificate in the device. Until restarting the web server uses the previous certificate. To get the web server to use the newly generated digital certificate, restart the web server. Restarting the web server is possible only through the Command Line Interface. You can transfer a digital certificate onto the device. See the Certificate import frame.
Delete	Deletes the digital certificate. Until restarting the web server uses the previous certificate.
Oper status	Displays if the device currently generates or deletes a digital certificate. It is possible that another user has triggered the action. Possible values: • **none** The device does currently not generate or delete a digital certificate. • **delete** The device currently deletes a digital certificate. • **generate** The device currently generates a digital certificate.

Fingerprint

The fingerprint is an easily verified hexadecimal number sequence that uniquely identifies the digital certificate of the HTTPS server.

After importing a new digital certificate, the device displays the fingerprint until you restart the server.

The following table presents the fingerprint settings:

Setting	Description
Fingerprint type	Specifies which fingerprint the Fingerprint field displays. Possible values: • **sha1** The Fingerprint field displays the SHA1 fingerprint of the digital certificate. • **sha256** (default setting) The Fingerprint field displays the SHA256 fingerprint of the digital certificate.
Fingerprint	Hexadecimal character sequence of the digital certificate used by the server. When you change the settings in the Fingerprint type field, click afterwards the  button and then the  button to update the display.

Certificate import

The following table presents the certificate import settings:

Setting	Description

URL	Specifies the path and file name of the digital certificate.
	
	The device accepts digital certificates with the following properties:
	• X.509 format
	• .PEM file name extension
	• Base64-coded and enclosed by the lines
	◦ `-----BEGIN PRIVATE KEY-----`
	…
	`-----END PRIVATE KEY-----`
	or
	◦ `-----BEGIN CERTIFICATE-----`
	…
	`-----END CERTIFICATE-----`
	• RSA key with 2048 bit length
	The device gives you the following options for transferring the file onto the device:
	• Import from the PC
	When the file is located on your PC or on a network drive, drag and drop it onto the area. As an alternative, click in the area to select the file.
	• Import from an FTP server
	Do not use this method if you transmit data over untrusted networks.
	When the file is on an FTP server, specify the URL for the file in the following form:
	ftp://<user>:<password>@<IP address>[:port]/<path>/<file name>
	• Import from a TFTP server
	Do not use this method if you transmit data over untrusted networks.
	When the file is on a TFTP server, specify the URL for the file in the following form:
	tftp://<IP address>/<path>/<file name>
	• Import from an SCP or SFTP server
	When the file is on an SCP or SFTP server, specify the URL for the file in the following form:
	◦ scp:// or sftp://<IP address>[:port]/<path>/<file name>
	Click the Start button to open the Credentials window. In this window, you enter the User name and Password to log into the server.
	◦ scp:// or sftp://<user>:<password>@<IP address>[:port]/<path>/<file name>
	Remember to set up the SCP or SFTP server as an SSH known host before the device accesses the server for the first time. See the **Device Security > SSH Known Hosts** dialog.

Start	Transfers the file specified in the URL field onto the device. For the changes to take effect after transferring a digital certificate onto the device, disable and re-enable the HTTPS server function. See the Operation frame.

IP Access Restriction

This dialog **Device Security > Management Access > IP Access Restriction** allows you to restrict access to the device management from a specific IP address range for selected applications.

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

    and
  - You access the device with a permitted application from a permitted IP address range specified in the rule.

Operation

The following table presents the operation setting:

Setting	Description
Operation	Enables/disables the IP Access Restriction function. Possible values: • **On** The IP Access Restriction function is enabled. The access to the device management is restricted. **NOTE:** Before you enable the function, verify that the table contains at least one active rule that grants you access to the device management. Otherwise, access to the device management is only possible using the Command Line Interface through the serial connection. • **Off** (default setting) The IP Access Restriction function is disabled.

Table

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

For information on how to customize the appearance of the table, see Working with tables, page 25.

The following table presents the table settings:

Setting	Description
Buttons	The following list presents the icon descriptions: • Add: Adds a table row. • Remove: Removes the selected table row.
Index	Displays the index number to which the table row relates. The device automatically assigns the value when you add a table row. When you delete a table row, this leaves a gap in the numbering. When you add a table row, the device fills the first gap. Possible values: • **1..16**
Address	Specifies the IP address of the network from which you allow the access to the device management. You specify the network range in the Netmask column. Possible values: • Valid IPv4 address (default setting: **0.0.0.0**)
Netmask	Specifies the range of the network specified in the Address column. Possible values: • Valid netmask (default setting: **0.0.0.0**) Example: To restrict access from a single IP address, specify the value as **255.255.255.255**.
HTTP	Activates/deactivates the HTTP access. Possible values: • **marked** (default setting) HTTP access is active. Access is possible from the adjacent IP address range. • **unmarked** HTTP access is inactive.
HTTPS	Activates/deactivates the HTTPS access. Possible values: • **marked** (default setting) HTTPS access is active. Access is possible from the adjacent IP address range. • **unmarked** HTTPS access is inactive.
SNMP	Activates/deactivates the SNMP access. Possible values: • **marked** (default setting) SNMP access is active. Access is possible from the adjacent IP address range. • **unmarked** SNMP access is inactive.
Telnet	Activates/deactivates the Telnet access. Possible values: • **marked** (default setting) Telnet access is active. Access is possible from the adjacent IP address range. • **unmarked** Telnet access is inactive.

Setting	Description
SSH	Activates/deactivates the SSH access. Possible values: • **marked** (default setting) SSH access is active. Access is possible from the adjacent IP address range. • **unmarked** SSH access is inactive.
IEC 61850-MMS	Activates/deactivates the access to the MMS server. Possible values: • **marked** (default setting) IEC61850-MMS access is active. Access is possible from the adjacent IP address range. • **unmarked** IEC61850-MMS access is inactive.
Modbus TCP	Activates/deactivates the access to the Modbus TCP server. Possible values: • **marked** (default setting) Modbus TCP access is active. Access is possible from the adjacent IP address range. • **unmarked** Modbus TCP access is inactive.
EtherNet/IP	Activates/deactivates the access to the EtherNet/IP server. Possible values: • **marked** (default setting) Ethernet/IP access is active. Access is possible from the adjacent IP address range. • **unmarked** Ethernet/IP access is inactive.
Active	Activates/deactivates the table row. Possible values: • **marked** (default setting) The table row is active. The device restricts the access to the device management from the specified IP address range for the selected applications. • **unmarked** The table row is inactive. The device does not restrict access to the device management from the specified IP address range for the selected applications.

Web

In this dialog **Device Security > Management Access > Web**, you specify settings for the Graphical User Interface.

Configuration

The following table presents the configuration setting:

Setting	Description
Web interface session timeout [min]	Specifies the timeout in minutes. After the device has been inactive for this time, it ends the session for the user logged into the device management. Possible values: • **0..160** (default setting: **5**) The value **0** deactivates the function, and the user remains logged in when inactive.

Command Line Interface

In this dialog **Device Security > Management Access > CLI**, you specify settings for the Command Line Interface. For further information about the Command Line Interface, see the “Command Line Interface” reference manual.

The dialog contains the following tabs:

- Global, page 130
- Login banner, page 131

Global

Change the prompt in the Command Line Interface and to activate automatic closing of inactive Command Line Interface sessions through the serial connection.

You can access the device management using the Command Line Interface in the following ways:

- Through a serial connection over the USB-C interface
- Through SSH over Ethernet

Configuration

The following table presents the configuration settings:

Setting	Description
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 spacebar characters Wildcards ◦ **%d** date ◦ **%i** IP address ◦ **%m** MAC address ◦ **%p** product name ◦ **%s** short product name ◦ **%t** time Default setting: **(MCSESM)** Changes to this setting are immediately effective in the active Command Line Interface session.
Serial interface timeout [min]	Specifies the time in minutes after which the device automatically closes the session of an inactive user logged into the device management using the Command Line Interface through the serial connection. Possible values: • **0..160** (default setting: **5**) The value **0** deactivates the function, and the user remains logged into the device management when inactive. A change in the value takes effect the next time a user logs into the device management. For the Telnet server and the SSH server, you specify the timeout in the **Device Security > Management Access > Server** dialog.

Login Banner

In this tab you replace the start screen of the Command Line Interface with your own text.

In the default setting, the start screen displays information about the device, such as the software version and the device settings. With the function in this tab, you deactivate this information and replace it with an individually specified text.

To display your own text in the Command Line Interface and in the Graphical User Interface before the login, you use the **Device Security > Pre-login Banner** dialog.

Operation

The following table presents the operation setting:

Setting	Description
Operation	Enables/disables the Login banner function. Possible values: • **On** The Login banner function is enabled. The device displays the text information specified in the Banner text field to the users that log into the device management through the Command Line Interface. • **Off** (default setting) The Login banner function is disabled. The start screen displays information about the device. The text information in the Banner text field is kept.

Banner text

The following table presents the banner text setting:

Setting	Description
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 spacebar characters • **<Tab>** • **<Line break>**

SNMPv1/v2 Community

In this dialog **Device Security > Management Access > SNMPv1/v2 Community**, you specify the community name for SNMPv1/v2 applications and activate/deactivate the write access for the *read and write* authorization.

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

You activate the access to the device using SNMPv1/v2 in the **Device Security > Management Access > Server** dialog.

Table

For information on how to customize the appearance of the table, see Working with tables, page 25.

The following table presents the table settings:

Setting	Description
Community	Displays the authorization for SNMPv1/v2 access to the device. Possible values: • **Write** For requests with the community name entered, the application receives *read and write* authorization. If the SNMP V1/V2 readOnly checkbox is marked, then the application receives *read-only* authorization. • **Read** For requests with the community name entered, the application receives *read-only* authorization.
Name	Specifies the community name for the adjacent authorization. Possible values: • Alphanumeric ASCII character string with 0..64 characters The device accepts the following characters: ◦ **<space>** ◦ **0..9** ◦ **a..z** ◦ **A..Z** ◦ **!"#$%&'()*+,-./:;<=>?@[\]^_`{|}~** **admin** (default setting for *read and write* authorization) **user** (default setting for *read-only* authorization)

Configuration

The following table presents the configuration setting:

Setting	Description
SNMP V1/V2 readOnly	Activates/deactivates the write access for the **Write** community. Possible values: • **marked** The write access for the **Write** community is inactive. For requests with the community name entered, the application receives *read-only* authorization. • **unmarked** (default setting) The write access for the **Write** community is active. For requests with the community name entered, the application receives *read and write* authorization.

Pre-Login Banner

This dialog **Device Security > Pre-login Banner** allows you to display a greeting or information text to users before they log into the device management.

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

To display the text only in the Command Line Interface, use the settings in the **Device Security > Management Access > CLI** dialog.

Operation

The following table presents the operation setting:

Setting	Description
Operation	Enables/disables the Pre-login Banner function. Using the Pre-login Banner function, the device displays a greeting or information text in the login dialog of the Graphical User Interface and of the Command Line Interface. Possible values: • **On** The Pre-login Banner function is enabled. The device displays the text specified in the Banner text field in the login dialog. • **Off** (default setting) The Pre-login Banner function is disabled. The device does not display a text in the login dialog. When you enter a text in the Banner text field, the device saves this text.

Banner Text

The following table presents the banner text setting:

Setting	Description
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 spacebar characters • **<Tab>** • **<Line break>**

SSH Known Hosts

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

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

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

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

Table

For information on how to customize the appearance of the table, see Working with tables, page 25.

The following table presents the table settings:

Setting	Description
Buttons	The following list presents the icon descriptions: • Add: Opens the Create window to add a table row. ◦ In the Index field, you specify the index number. Possible values: **1..50** (specify up to 50 defined hosts.) ◦ In the Address field, you specify the address of the server. If the server can be accessed using both an IP address and a DNS name, then add a separate table row for each address type. Possible values: – Valid IPv4 address – Valid IPv6 address – DNS hostname ◦ In the Key fingerprint field, you specify the public key fingerprint of the server. You can find out the public key fingerprint of the server, for example, as follows: – From the administrator of a defined SSH server. – From the diagnostic message following an unsuccessful software update in the Software dialog due to the mismatch between the public key fingerprint stored in the device and the fingerprint calculated from the public key which the remote server actually sent. Do not use this method if you transmit data over untrusted networks. Possible values: Base64-coded SHA256 hash sequence with a length of 43 or 44 characters. ◦ In the Key type field, you specify the algorithm that was used for generating the public key of the server. You can find out the Key type value simultaneously and through the same method you used to obtain the public key fingerprint. If you accidentally select a different algorithm, then the device cannot identify the public key using the public key fingerprint. Possible values: – **dsa** – **rsa** – **ecdsa** – **ed25519**
Index	Displays the index number to which the table row relates. You specify the index number when you add a table row.
Address	Displays the address of the server. Possible values: • Valid IPv4 address • Valid IPv6 address • DNS hostname
Key fingerprint	Specifies the public key fingerprint of the server. Possible values: • Base64-coded SHA256 hash sequence with a length of 43 or 44 characters To modify the public key fingerprint, first unmark the checkbox in the Active column.

Setting	Description
Key type	Displays the algorithm that was used for generating the public key of the server. Possible values: • **dsa** • **rsa** • **ecdsa** • **ed25519**
Active	Activates/deactivates the table row. Possible values: • **marked** (default setting) The table row is active. The device considers the server set up in this table row to be defined. When you transfer a file from an external server onto the device or vice versa, the device verifies the identity of the external server based on this public key fingerprint. • **unmarked** The table row is inactive. The device considers the server set up in this table row to be undefined. When you transfer a file from an external server onto the device or vice versa, the device terminates the connection to this server.

Network Security

The menu contains the following dialogs:

- Network Security Overview, page 137
- Port Security, page 137
- 802.1X, page 143
- RADIUS, page 155
- DoS, page 161
- DHCP Snooping, page 164
- IP Source Guard, page 171
- Dynamic ARP Inspection, page 174
- ACL, page 181

Network Security Overview

This dialog **Network Security > Overview** displays an overview over the network security rules used in the device.

The following table presents the network security overview settings:

Setting	Description
Overview	The top level displays: • The ports to which a network security rule is assigned • The VLANs to which a network security rule is assigned The subordinate levels display: • The set-up ACL rules See the **Network Security > ACL** dialog.
Buttons	The following list presents the icon descriptions: • : Displays a text field to search for a keyword. When you enter a character or string, the overview displays only items related to this keyword. • : Expands the levels. The overview then displays every level of the items. To collapse the levels again, click the button. The overview then displays only the first level of the items. • : Expands the item and displays the items of the next lower level. • : Collapses the item and hides the items of the underlying levels.

Port Security

Forward only data packets from desired senders on a port. When the Port Security function is enabled, the device verifies the VLAN ID and MAC address or IP address of the sender before it forwards a data packet. The device discards data packets from not desired senders and logs this event.

The device also offers the function to verify the IP address of the sender before it forwards a data packet.

NOTE: The following note explains how the device manages IP and MAC addresses when the IP mode is selected.:

- If in the Mode frame the IP radio button is selected, the Port Security function indirectly operates on Layer 2. When you set up a desired 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 a desired IP address is that the connected device is reachable and responds to ARP requests.
- If a connected device sends data packets with a desired 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 desired. After this step, the device uses the new associated MAC address.

In this dialog **Network Security > Port Security**, a Wizard window helps you associate the ports with the address of one or more desired senders. In the device, these addresses are defined as *static entries*. To view the specified static addresses, select the relevant port and click the  button.

To simplify the setup process, the device allows you to record the address of the desired senders automatically. The device “learns” the addresses by evaluating the received data packets. In the device, these addresses are defined as *dynamic entries*. When a user-defined upper limit has been reached (Dynamic limit), the device stops the “learning” on the relevant port. The device forwards only the data packets of the senders already registered on the port. When you adapt the upper limit to the number of expected senders, you thus make *MAC Flooding* attacks more difficult.

NOTE: With the automatic recording of the *dynamic entries*, the device constantly discards the first data packet from undefined senders. Using this first data packet, the device checks if the upper limit has been reached. The device records the addresses until the upper limit is reached. Afterwards, the device forwards data packets that it receives on the relevant port from this sender.

Operation

The following table presents the operation setting:

Setting	Description
Operation	Enables/disables the Port Security function in the device. Possible values: • **On** The Port Security function is enabled. The device checks the VLAN ID and the source MAC address before it forwards a data packet. The device forwards a received data packet only if the VLAN and the source MAC address of the data packet are desired on the relevant port. For this setting to take effect, you also activate the Port Security function on the relevant ports. • **Off** (default setting) The Port Security function is disabled. The device forwards every received data packet without checking the source address. **NOTE:** If in the Mode frame the MAC radio button is selected, then the device checks the source MAC address against the desired source MAC addresses. If the IP radio button is selected, the device checks the source MAC address against the MAC addresses associated with the desired source IP addresses.

Mode

The following table presents the mode setting:

Setting	Description
Mode	Specifies if the Port Security function uses either the desired MAC addresses or the desired IP addresses to verify a received packet. Possible values: • **MAC** (default setting) The Port Security function uses the desired source MAC addresses. The device checks the VLAN ID and the source MAC address against the desired source MAC addresses before it forwards a data packet. • **IP** The Port Security function uses the desired source IP addresses. The device checks the VLAN ID and the source MAC address against the MAC addresses associated with the desired source IP addresses before it forwards a data packet

Configuration

The following table presents the configuration setting:

Setting	Description
Auto-disable	Activates/deactivates the Auto-Disable function for Port Security in the device. Possible values: • **marked** The Auto-Disable function for Port Security is active. Also mark the checkbox in the Auto-disable column for the relevant ports. The device disables the port and optionally sends an SNMP trap when one of the following events occurs: ◦ The device registers at least one address of a sender that is not desired on the port. ◦ The device registers more addresses than specified in the Dynamic limit column. • **unmarked** (default setting) The Auto-Disable function for Port Security is inactive.

Table

For information on how to customize the appearance of the table, see Working with tables, page 25.

The following table presents the table settings:

Setting	Description
Buttons	 Wizard: Opens the Wizard window that helps you associate the ports with the address of one or more desired senders. See Wizard: Port security, page 141.
Port	Displays the port number.
Active	Activates/deactivates the Port Security function on the port. Possible values: • **marked** The device checks every data packet received on the port and forwards it only if the source address of the data packet is desired. Also enable the Port Security function in the Operation frame. • **unmarked** (default setting) The device forwards every data packet received on the port without checking the source address. **NOTE:** When you operate the device as an active participant within an MRP ring or HIPER Ring, unmark the checkbox for the ring ports. **NOTE:** When you operate the device as an active participant of a Ring/Network Coupling or RCP, unmark the checkbox for the relevant coupling ports.
Auto-disable	Activates/deactivates the Auto-Disable function for Port Security on the port. Possible values: • **marked** (default setting) The Auto-Disable function is active on the port. The device disables the port and optionally sends an SNMP trap when one of the following events occurs: ◦ The device registers at least one address of a sender that is not desired on the port. ◦ The device registers more addresses than specified in the Dynamic limit column. The ***Link status*** LED for the port flashes 3 × per period. This restriction makes *MAC Spoofing* attacks more difficult. The prerequisite is that in the Configuration frame the Auto-disable checkbox is marked. ◦ The **Diagnostics > Ports > Auto-Disable** dialog displays which ports are currently disabled due to the parameters being exceeded. ◦ After a waiting period, the Auto-Disable function enables the port again automatically. For this you go to the **Diagnostics > Ports > Auto-Disable** dialog and specify a waiting period for the relevant port in the Reset timer [s] column. • **unmarked** The Auto-Disable function is inactive on the port.
Send trap	Activates/deactivates the sending of SNMP traps when the device discards a data packet from an undesired sender on the port. Possible values: • **marked** The sending of SNMP traps is active. The prerequisite is that in the **Diagnostics > Status Configuration > Alarms (Traps)** dialog the Alarms (Traps) function is enabled and at least one trap destination is specified. If the device discards data packets from a sender that is not desired on the port, then the device sends an SNMP trap. • **unmarked** (default setting) The sending of SNMP traps is inactive.
Trap interval [s]	Specifies the delay time in seconds that the device waits after sending an SNMP trap before sending the next SNMP trap. Possible values: • **0..3600** (default setting: **0**) The value **0** deactivates the delay time.

Setting	Description
Dynamic limit	Specifies the upper limit for the number of automatically registered addresses (*dynamic entries*). When the upper limit is reached, the device stops “learning” on this port. Adjust the value to the number of expected senders. If the port registers more addresses than specified here, then the Auto-Disable function disables the port. The prerequisite is that you mark the checkbox in the Auto-disable column and the Auto-disable checkbox in the Configuration frame. Possible values: • **0** No automatic registering of addresses on this port. • **1..600** (default setting: **600**)
Static limit	Specifies the upper limit for the number of addresses associated with the port using the Wizard window (*static entries*). Possible values: • **0** No association possible between the port and a desired sender. Only specify this value if you specify a value > 0 in the Dynamic limit column. • **1..64** (default setting: **64**)
Dynamic entries	Displays the number of addresses that the device has automatically registered. 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 MAC addresses associated with the port.
Static IP entries	Displays the number of IP addresses associated with the port.
Last violating VLAN ID/MAC	Displays the VLAN ID and MAC address of an undesired sender whose data packets the device last discarded on this port.
Sent traps	Displays the number of discarded data packets on this port that caused the device to send an SNMP trap.

Wizard: Port Security

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

The Wizard window guides you through the following steps:

- Select port, page 141
- MAC addresses, page 142
- IP addresses, page 143

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

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

Select Port

The following table presents the select port setting:

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

MAC Addresses

The following table presents the MAC addresses settings:

Setting	Description
Static entries (x/y)	Displays the number of addresses associated with the port using the Wizard window and the upper limit for *static entries*. The lower part of the Wizard window displays the entries in detail, if any.  : Deletes the entries in the lower part of the Wizard window. The device removes the respective association between a port and the desired senders.
VLAN ID	Specifies the VLAN ID of the desired sender. Possible values: **1..4042**
MAC address	Specifies the MAC address of the desired sender. Possible values: Valid Unicast MAC address. Specify the value with a colon separator, for example **00:11:22:33:44:55**. **NOTE:** You can assign a MAC address to only one port.
Add	Adds a *static entry* based on the values specified in the VLAN ID and MAC address fields. As a result, you find a new entry in the lower part of the Wizard window.
Entries in the lower part of the window	The lower part of the Wizard window displays the VLAN ID and MAC address of desired senders on this port. In the following list you find a description of the icon specific to these entries. The following list presents the icon descriptions: •  : *Static entry*: When you click the icon, the device removes the *static entry* and the respective association between the port and the desired senders. •  : *Dynamic entry*: When you click the icon, the icon changes to  . The device converts the *dynamic entry* to a *static entry* when you close the Wizard window. To undo this change, click the icon again before you close the Wizard window.

IP Addresses

The following table presents the IP addresses settings:

Setting	Description
Static entries (x/y)	Displays the number of senders associated with the port and the upper limit for *static entries*. The lower part of the Wizard window displays the entries in detail, if any.  : Deletes the entries in the lower part of the Wizard window. The device removes the respective association between a port and the desired senders.
VLAN ID	Specifies the VLAN ID of the desired sender. Possible values: **1..4042** **NOTE:** Assign the VLAN ID of the management VLAN.
IP address	Specifies the IP address of the desired source. Possible values: Valid IPv4 address.
Add	Adds a *static entry* based on the values specified in the VLAN ID and IP address fields. As a result, you find a new entry in the lower part of the Wizard window.
Entries in the lower part of the window	The lower part of the Wizard window displays the VLAN ID and IP address of desired senders on this port. In the following list you find a description of the icons specific to these entries.  : *Static entry*: When you click the icon, the device removes the *static entry* and the respective association between the port and the desired senders.

802.1X

With the port-based access control according to IEEE 802.1X, the device monitors the access to the network from connected end devices. The device (authenticator) allows an end device (supplicant) have access to the network if it logs in with valid login data. The authenticator and the end devices communicate using the EAPoL (Extensible Authentication Protocol over LANs) authentication protocol.

The device supports the following methods to authenticate end devices:

- **radius**

  A RADIUS server in the network authenticates the end devices.

- **ias**

  The Integrated Authentication Server (IAS) implemented in the device authenticates the end devices. Compared to RADIUS, the IAS provides only basic functions.

The 802.1X menu **Network Security > 802.1X** contains the following dialogs:

- 802.1X Global, page 144
- 802.1X Port Configuration, page 147
- 802.1X Port Clients, page 151
- 802.1X EAPOL Port Statistics, page 152
- 802.1X Port Authentication History, page 153
- 802.1X Integrated Authentication Server (IAS), page 154

802.1X Global

This dialog **Network Security > 802.1X > Global** allows you to specify basic settings for the port-based access control.

Operation

The following table presents the operation setting:

Setting	Description
Operation	Enables/disables the 802.1X function. Possible values: • **On** The 802.1X function is enabled. The device checks the access to the network from connected end devices. The port-based access control is enabled. • **Off** (default setting) The 802.1X function is disabled. The port-based access control is disabled.

Configuration

The following table presents the configuration settings:

Setting	Description
VLAN assignment	Activates/deactivates the assigning of the relevant port to a VLAN. This function provide selected services to the connected end device in this VLAN. Possible values: • **marked** The assigning is active. If the end device successfully authenticates itself, then the device assigns to the relevant port the VLAN ID transferred by the RADIUS authentication server. • **unmarked** (default setting) The assigning is inactive. The relevant port is assigned to the VLAN specified in the **Network Security > 802.1X > Port Configuration** dialog, Assigned VLAN ID column.
Dynamic VLAN creation	Activates/deactivates the automatic creation of the VLAN assigned by the RADIUS authentication server if the VLAN does not exist. Possible values: • **marked** The automatic VLAN creation is active. The device sets up the VLAN if it does not exist. • **unmarked** (default setting) The automatic VLAN creation is inactive. If the assigned VLAN does not exist, then the port remains assigned to the original VLAN.
Monitor mode	Activates/deactivates the monitor mode. Possible values: • **marked** The monitor mode is active. The device monitors the authentication and helps with diagnosing detected errors. If an end device has not logged in successfully, then the device gives the end device access to the network. • **unmarked** (default setting) The monitor mode is inactive.

MAC Authentication Bypass Format Options

The following table presents the MAC authentication bypass format options settings:

Setting	Description
Group size	Specifies the size of the MAC address groups. The device splits the MAC address for authentication into groups. The size of the groups is specified in half bytes, each of which is represented as one character. Possible values: • **1** The device splits the MAC address into 12 groups of one character. Example: **A-A-B-B-C-C-D-D-E-E-F-F** • **2** The device splits the MAC address into 6 groups of 2 characters. Example: **AA-BB-CC-DD-EE-FF** • **4** The device splits the MAC address into 3 groups of 4 characters. Example: **AABB-CCDD-EEFF** • **12** (default setting) The device formats the MAC address as one group of 12 characters. Example: **AABBCCDDEEFF**
Group separator	Specifies the character which separates the groups. Possible values: • **-** (default setting) dash • **:** colon • **.** dot
Upper or lower case	Specifies if the device formats the authentication data in lowercase or uppercase letters. Possible values: • **lower-case** • **upper-case** (default setting)
Password	Specifies the optional password for the clients which use the authentication bypass. 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

The following table presents the information settings:

Setting	Description
Monitor mode clients	Displays to how many end devices the device gave network access even though they did not log in successfully. The prerequisite is that in the Configuration frame the Monitor mode function is active.
Non monitor mode clients	Displays the number of end devices to which the device gave network access after successful login.
Policy 1	Displays the method that the device currently uses to authenticate the end devices using the protocol 802.1X. You specify the method used in the **Device Security > Authentication List** dialog. • To authenticate the end devices through a RADIUS server, you assign the **radius** policy to the **8021x** list. • To authenticate the end devices through the Integrated Authentication Server (IAS) you assign the **ias** policy to the **8021x** list.

802.1X Port Configuration

This dialog **Network Security > 802.1X > Port Configuration** allows you to specify the access settings for every port.

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

Table

For information on how to customize the appearance of the table, see Working with tables, page 25.

The following table presents the table settings:

Setting	Description
Port	Displays the port number.
Port control	Specifies how the device grants access to the network (**Port control mode**). Possible values: • **forceUnauthorized** The device blocks the access to the network. You use this setting if an end device is connected to the port that does not receive access to the network. • **auto** The device grants access to the network if the end device logged in successfully. You use this setting if an end device is connected to the port that logs in at the authenticator. **NOTE:** If other end devices are connected through the same port, then they get access to the network without additional authentication. • **forceAuthorized** (default setting) When end devices do not support IEEE 802.1X, the device grants access to the network. You use this setting if an end device is connected to the port that receives access to the network without logging in. • **multiClient** The device grants access to the network if the end device logs in successfully. If the end device does not send any EAPOL data packets, then the device grants or denies access to the network individually depending on the MAC address of the end device. See the MAC authorized bypass column. You use this setting if multiple end devices are connected to the port or if the MAC authorized bypass function is required.
Authentication state	Displays the status of the authentication on the port (**Controlled Port Status**). Possible values: • **authorized** The end device is logged in successfully. • **unauthorized** The end device is not logged in.
Assigned VLAN ID	Displays the VLAN that the authenticator assigned to the port. This value applies only on ports in which the Port control column contains the value **auto**. Possible values: • **0..4042** (default setting: **0**) You find the VLAN that the authenticator assigned to the ports in the **Network Security > 802.1X > Port Clients** dialog. For the ports in which the Port control column contains the value **multiClient**, the device assigns the VLAN tag based on the MAC address of the end device when receiving data packets without a VLAN tag.
Reason	Displays the reason for the assignment of the VLAN. This value applies only on ports in which the Port control column contains the value **auto**. Possible values: • **notAssigned** (default setting) • **radius** • **guestVlan** • **unauthenticatedVlan** You find the VLAN that the authenticator assigned to the ports for a supplicant in the **Network Security > 802.1X > Port Clients** dialog.

Setting	Description
Guest VLAN ID	Specifies the VLAN that the authenticator assigns to the port if the end device does not log in during the time period specified in the Guest VLAN period column. This value applies only on ports in which the Port control column contains the value **auto** or **multiClient**. This function grant end devices, without IEEE 802.1X support, access to selected services in the network. Possible values: • **0** (default setting) The authenticator does not assign a Guest VLAN to the port. • **1..4042** **NOTE:** The MAC authorized bypass function and the Guest VLAN ID function cannot be in use simultaneously.
Unauthenticated VLAN ID	Specifies the VLAN that the authenticator assigns to the port if the end device does not log in successfully. This value applies only on ports in which the Port control column contains the value **auto**. This function 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 authenticate end devices without IEEE 802.1X support on the basis of their MAC address. Possible values: • **marked** The MAC-based authentication is active. The device sends the MAC address of the end device to the RADIUS authentication server. The device assigns the end device to the respective VLAN based on its MAC address, as if the end device had authenticated directly using the 802.1X protocol. • **unmarked** (default setting) The MAC-based authentication is inactive.
Periodic reauthentication	Activates/deactivates periodic reauthentication requests. Possible values: • **marked** The periodic reauthentication requests are active. The device periodically requests the end device to log in again. You specify this time period in the Reauthentication period [s] column. If the authenticator assigned a Voice VLAN, Unauthenticated VLAN or Guest VLAN to the end device, then this setting becomes ineffective. • **unmarked** (default setting) The periodic reauthentication requests are inactive. The device keeps the end device logged in.
Reauthentication period [s]	Specifies the period in seconds after which the authenticator periodically requests the end device to log in again. Possible values: • **1..65535 (2^{16}-1)** (default setting: **3600**)
Users (max.)	Specifies the upper limit for the number of end devices that the device authenticates on this port at the same time. This upper limit applies only to ports in which the Port control column contains the value **multiClient**. Possible values: • **1..16** (default setting: **16**)
Quiet period [s]	Specifies the time period in seconds in which the authenticator does not accept any more logins from the end device after an unsuccessful login attempt (**Quiet period [s]**). Possible values: • **0..65535 (2^{16}-1)** (default setting: **60**)

Setting	Description
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 (2^{16}-1)** (default setting: **30**)
Supplicant timeout [s]	Specifies the period in seconds for which the authenticator waits for the login of the end device. Possible values: • **1..65535 (2^{16}-1)** (default setting: **30**)
Server timeout [s]	Specifies the period in seconds for which the authenticator waits for the response from the authentication server (RADIUS or IAS). Possible values: • **1..65535 (2^{16}-1)** (default setting: **30**)
Requests (max.)	Specifies how many times the authenticator requests the end device to log in until the time specified in the Supplicant timeout [s] column has elapsed. The device sends an EAP request/identity data packet to the end device as often as specified here. Possible values: • **0..10** (default setting: **2**)
Guest VLAN period	Displays the period in seconds for which the authenticator waits for EAPOL data packets after the end device is connected. If this period elapses, then the authenticator grants the end device access to the network and assigns the port to the Guest VLAN specified in the Guest VLAN ID column. The value in this column is the triple of the value specified in the Transmit period [s] column.
Status	Displays the status of the Authenticator (**Authenticator PAE state**). Possible values: • **initialize** • **disconnected** • **connecting** • **authenticating** • **authenticated** • **aborting** • **held** • **forceAuth** • **forceUnauth**
Backend authentication state	Displays the status of the connection to the authentication server (**Backend Authentication state**). Possible values: • **request** • **response** • **success** • **fail** • **timeout** • **idle** • **initialize**

Setting	Description
Initialize port	Activates/deactivates the port initialization to activate the access control on the port or reset it to its initial state. Use this function only on ports in which the Port control column contains the value **auto** or **multiClient**. Possible values: • **marked** The port initialization is active. When the initialization is complete, the device changes the value to **unmarked** again. • **unmarked** (default setting) The port initialization is inactive. The device keeps the present port status.
Reauthenticate	Activates/deactivates the one-time reauthentication request. Use this function only on ports in which the Port control column contains the value **auto** or **multiClient**. The device also allows you to 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.

802.1X Port Clients

This dialog **Network Security > 802.1X > Port Clients** displays information on the connected end devices.

Table

For information on how to customize the appearance of the table, see Working with tables, page 25.

The following table presents the table settings:

Setting	Description
Port	Displays the port number.
User name	Displays the user name with which the end device logged in.
MAC address	Displays the MAC address of the end device.
Filter ID	Displays the name of the filter list that the RADIUS authentication server assigned to the end device after successful authentication. The authentication server transfers the filter ID attributes in the Access Accept data packet.
Assigned VLAN ID	Displays the VLAN that the authenticator assigned to the port after the successful authentication of the end device. If for the port in the **Network Security > 802.1X > Port Configuration** dialog, Port control column the value **multiClient** is specified, then the device assigns the VLAN tag based on the MAC address of the end device when receiving data packets without a VLAN tag.
VLAN assignment reason	Displays the reason for the assignment of the VLAN. Possible values: • **default** • **radius** • **unauthenticatedVlan** • **guestVlan** • **monitorVlan** • **invalid** The field only displays a valid value as long as the client is authenticated.
Session timeout	Displays the remaining time in seconds until the login of the end device expires. This value applies only if for the port in the **Network Security > 802.1X > Port Configuration** dialog, Port control column the value **auto** or **multiClient** is specified. The authentication server assigns the timeout period to the device through RADIUS. The value **0** means that the authentication server has not assigned a timeout.
Termination action	Displays the action performed by the device when the login has elapsed. Possible values: • **default** • **reauthenticate**

802.1X EAPOL Port Statistics

This dialog **Network Security > 802.1X > Statistics** displays which EAPOL data packets the end device has sent and received for the authentication of the end devices.

Table

For information on how to customize the appearance of the table, see Working with tables, page 25.

The following table presents table settings:

Setting	Description
Buttons	Remove: Removes the selected table row.
Port	Displays the port number.
Received	Displays the total number of EAPOL data packets that the device received on the port.
Transmitted	Displays the total number of EAPOL data packets that the device sent on the port.
Start	Displays the number of EAPOL start data packets that the device received on the port.
Logoff	Displays the number of EAPOL logoff data packets that the device received on the port.
Response/ID	Displays the number of EAP response/identity data packets that the device received on the port.
Response	Displays the number of valid EAP response data packets that the device received on the port (without EAP response/identity data packets).
Request/ID	Displays the number of EAP request/identity data packets that the device received on the port.
Request	Displays the number of valid EAP request data packets that the device received on the port (without EAP request/identity data packets).
Invalid	Displays the number of EAPOL data packets with an undefined frame type that the device received on the port.
Received error	Displays the number of EAPOL data packets with an invalid packet body length field that the device received on the port.
Packet version	Displays the protocol version number of the EAPOL data packet that the device last received on the port.
Source of last received packet	Displays the sender MAC address of the EAPOL data packet that the device last received on the port. The value **00:00:00:00:00:00** means that the port has not received any EAPOL data packets yet.

802.1X Port Authentication History

The device registers the authentication process of the end devices that are connected to its ports. This dialog **Network Security > 802.1X > Port Authentication History** displays the information recorded during the authentication.

Table

For information on how to customize the appearance of the table, see Working with tables, page 25.

The following table presents the table settings:

Setting	Description
Buttons	Remove: Removes the selected table row.
Port	Displays the port number.
Time	Displays the time at which the authenticator authenticated the end device.
Present for	Displays the time that has elapsed since the device generated this log entry.
MAC address	Displays the MAC address of the end device.
VLAN ID	Displays the ID of the VLAN that was assigned to the end device before the login.
Status	Displays the status of the authentication on the port. Possible values: • **success** The authentication was successful. • **failure** The authentication did not succeed.
Access	Displays if the device grants the end device access to the network. Possible values: • **granted** The device grants the end device access to the network. • **denied** The device denies the end device access to the network.
Assigned VLAN ID	Displays the ID of the VLAN that the authenticator assigned to the port.
VLAN type	Displays the type of the VLAN that the authenticator assigned to the port. Possible values: • **default** • **radius** • **unauthenticatedVlan** • **guestVlan** • **monitorVlan** • **notAssigned**
Reason	Displays the reason for assigning the VLAN and the VLAN type.

802.1X Integrated Authentication Server (IAS)

The Integrated Authentication Server (IAS) allows you to authenticate end devices using the protocol 802.1X. Compared to RADIUS, the IAS has a very limited range of functions. The authentication is based only on the user name and the password.

In this dialog **Network Security > 802.1X > IAS**, you manage the login data of the end devices. The device allows you to set up to 100 sets of login data.

To authenticate the end devices through the Integrated Authentication Server you assign in the **Device Security > Authentication List** dialog the **ias** policy to the 8021x list.

Table

For information on how to customize the appearance of the table, see Working with tables, page 25.

The following table presents table settings:

Setting	Description
Buttons	The following list presents the icon descriptions: •  Add: Opens the Create window to add a table row. In the User name field, you specify the name of the user account on the end device. •  Remove: Removes the selected table row.
User name	Displays the name of the user account on the end device. To add a user account, click the  button.
Password	Specifies the password with which the user authenticates. Possible values: Alphanumeric ASCII character string with 0..64 characters The device differentiates between upper and lower case.
Active	Activates/deactivates the login data. Possible values: • **marked** The login data is active. An end device has the option of logging in with this login data using the protocol 802.1X. • **unmarked** (default setting) The login data is inactive.

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) allows you to 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 allows 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 login data of the users to the primary authentication server. The authentication server determines if the login data is valid and transfers the authorizations of the users to the device.

The device assigns the Service Type transferred in the response of a RADIUS server as follows to an access role existing in the device:

- **Administrative-User**: **administrator**
- **Login-User**: **operator**

- **NAS-Prompt-User**: **guest**

The device also allwos you to 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 RADIUS **Network Security > RADIUS** menu contains the following dialogs:

- RADIUS Global, page 156
- RADIUS Authentication Server, page 157
- RADIUS Accounting Server, page 159
- RADIUS Authentication Statistics, page 160
- RADIUS Accounting Statistics, page 160

RADIUS Global

This dialog **Network Security > RADIUS > Global** specify basic settings for RADIUS.

RADIUS Configuration

The following table presents the RADIUS configuration settings:

Setting	Description
Buttons	Reset: Deletes the statistics in the **Network Security > RADIUS > Authentication Statistics** dialog and in the **Network Security > RADIUS > Accounting Statistics** dialog.
Retransmits (max.)	Specifies how many times the device retransmits an unanswered request to the authentication server before the device sends the request to an alternative authentication server. Possible values: **1..15** (default setting: **4**)
Timeout [s]	Specifies how many seconds the device waits for a response after a request to an authentication server before it retransmits the request. Possible values: • **1..30** (default setting: **5**)
Accounting	Activates/deactivates the accounting. Possible values: • **marked** Accounting is active. The device sends the traffic data to an accounting server specified in the **Network Security > RADIUS > Accounting Server** dialog. • **unmarked** (default setting) Accounting is inactive.
NAS IP address (attribute 4)	Specifies the IP address that the device transfers to the authentication server as attribute 4. Specify the IP address of the device or another available address. **NOTE:** The device only includes the attribute 4 if the packet was triggered by the *802.1X* authentication request of an end device (supplicant). Possible values: Valid IPv4 address (default setting: **0.0.0.0**) In many cases, there is a firewall between the device and the authentication server. In the Network Address Translation (NAT) in the firewall changes the original IP address, and the authentication server receives the translated IP address of the device. The device transfers the IP address in this field unchanged across the Network Address Translation (NAT).

RADIUS Authentication Server

This dialog **Network Security > RADIUS > Authentication Server** allows you to specify up to 8 authentication servers. An authentication server authenticates and authorizes the users when the device forwards the login data to the server.

The device sends the login data to the specified primary authentication server. When the server does not respond, the device contacts the specified authentication server that is highest in the table. When no response comes from this server either, the device contacts the next server in the table.

Table

For information on how to customize the appearance of the table, see Working with tables, page 25.

The following table presents the tables settings:

Setting	Description
Buttons	The following list presents the icon descriptions: • Add: Opens the Create window to add a table row. ◦ In the Index field, you specify the index number. ◦ In the Address field, you specify the IP address of the server. • Remove: Removes the selected table row.
Index	Displays the index number to which the table row relates. You specify the index number when you add a table row.
Name	Displays the name of the server. To change the value, click the relevant field. Possible values: • Alphanumeric ASCII character string with 1..32 characters (default setting: **Default-RADIUS-Server**) You can specify the same name for several servers. When several servers have the same name, the setting in the Primary server column applies.
Address	Specifies the IP address of the server. Possible values: • Valid IPv4 address
Destination UDP port	Specifies the number of the UDP port on which the server receives requests. Possible values: • **0..65535 (2^{16}-1)** (default setting: **1812**) Exception: Port **2222** is reserved for internal functions.
Secret	Displays ****** (asterisks) when you specify a password with which the device logs into the server. To change the password, click the relevant field. Possible values: • Alphanumeric ASCII character string with 1..64 characters You get the password from the administrator of the authentication server.
Primary server	Specifies the authentication server as primary or secondary. Possible values: • **marked** The server is specified as the primary authentication server. The device sends the login data for authenticating the users to this authentication server. This setting applies only if more than one server in the table has the same value in the Name column. • **unmarked** (default setting) The server is the secondary authentication server. When the device does not receive a response from the primary authentication server, the device sends the login data to the secondary authentication server.
Active	Activates/deactivates the connection to the server. The device uses the server, if you specify in the **Device Security > Authentication List** dialog the value **radius** in one of the columns Policy 1 to Policy 5. Possible values: • **marked** (default setting) The connection is active. The device sends the login data for authenticating the users to this server if the preceding preconditions named are fulfilled. • **unmarked** The connection is inactive. The device does not send any login data to this server.

RADIUS Accounting Server

This dialog **Network Security > RADIUS > Accounting Server** allows you to specify up to 8 accounting servers. An accounting server records the traffic data that has occurred during the port authentication according to IEEE 802.1X. The prerequisite is that in the **Network Security > RADIUS > Global** dialog the Accounting function is active.

The device sends the traffic data to the first accounting server that can be reached. When the accounting server does not respond, the device contacts the next server in the table.

Table

For information on how to customize the appearance of the table, see Working with tables, page 25.

The following table presents the table settings:

Setting	Description
Buttons	The following list presents the icon descriptions: • Add: Opens the Create window to add a table row. ◦ In the Index field, you specify the index number. ◦ In the Address field, you specify the IP address of the server. • Remove: Removes the selected table row.
Index	Displays the index number to which the table row relates. You specify the index number when you add a table row. Possible values: **1..8**
Name	Displays the name of the server. To change the value, click the relevant field. Possible values: • Alphanumeric ASCII character string with 1..32 characters (default setting: **Default-RADIUS-Server**)
Address	Specifies the IP address of the server. Possible values: Valid IPv4 address.
Destination UDP port	Specifies the number of the UDP port on which the server receives requests. Possible values: • **0..65535 (2^{16}-1)** (default setting: **1813**) Exception: Port **2222** is reserved for internal functions.
Secret	Displays ****** (asterisks) when you specify a password with which the device logs into the server. To change the password, click the relevant field. Possible values: Alphanumeric ASCII character string with 1..16 characters. You get the password from the administrator of the authentication server.
Active	Activates/deactivates the connection to the server. Possible values: • **marked** (default setting) The connection is active. The device sends traffic data to this server if the preceding preconditions named are fulfilled. • **unmarked** The connection is inactive. The device does not send any traffic data to this server.

RADIUS Authentication Statistics

This dialog **Network Security > RADIUS > Authentication Statistics** displays information about the communication between the device and the authentication server. The table displays the information for each server in a separate table row.

To delete the statistic, click in the **Network Security > RADIUS > Global** dialog the button.

Table

For information on how to customize the appearance of the table, see Working with tables, page 25.

The following table presents the table settings:

Setting	Description
Name	Displays the name of the server.
IP address	Displays the IP address of the server.
Round trip time	Displays the time interval in hundredths of a second between the last response received from the server (Access Reply/Access Challenge) and the corresponding data packet sent (Access Request).
Access requests	Displays the number of access data packets that the device sent to the server. This value does not take repetitions into account.
Retransmitted access requests	Displays the number of access data packets that the device retransmitted to the server.
Access accepts	Displays the number of access accept data packets that the device received from the server.
Access rejects	Displays the number of access reject data packets that the device received from the server.
Access challenges	Displays the number of access challenge data packets that the device received from the server.
Malformed access responses	Displays the number of malformed access response data packets that the device received from the server (including data packets with an invalid length).
Bad authenticators	Displays the number of access response data packets with an invalid authenticator that the device received from the server.
Pending requests	Displays the number of access request data packets that the device sent to the server to which it has not yet received a response from the server.
Timeouts	Displays how many times no response to the server was received before the specified waiting time elapsed.
Unknown types	Displays the number data packets with an undefined 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.

RADIUS Accounting Statistics

This dialog **Network Security > RADIUS > Accounting Statistics** displays information about the communication between the device and the accounting server. The table displays the information for each server in a separate table row.

To delete the statistic, click in the **Network Security > RADIUS > Global** dialog the button.

Table

For information on how to customize the appearance of the table, see Working with tables, page 25.

The following table presents the table settings:

Setting	Description
Name	Displays the name of the server.
IP address	Displays the IP address of the server.
Round trip time	Displays the time interval in hundredths of a second between the last response received from the server (Accounting Response) and the corresponding data packet sent (Accounting Request).
Accounting requests	Displays the number of accounting request data packets that the device sent to the server. This value does not take repetitions into account.
Retransmitted accounting requests	Displays the number of accounting request data packets that the device retransmitted to the server.
Received packets	Displays the number of accounting response data packets that the device received from the server.
Malformed packets	Displays the number of malformed accounting response data packets that the device received from the server (including data packets with an invalid length).
Bad authenticators	Displays the number of accounting response data packets with an invalid authenticator that the device received from the server.
Pending requests	Displays the number of accounting request data packets that the device sent to the server to which it has not yet received a response from the server.
Timeouts	Displays how many times no response to the server was received before the specified waiting time elapsed.
Unknown types	Displays the number data packets with an undefined 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.

DoS

Denial of Service (DoS) is a cyberattack that aims to make certain services or devices unusable. In this dialog, you can set up several filters to help protect the device itself and other devices in the network from DoS attacks.

The DoS menu **Network Security > DoS**contains the following dialogs:

- DoS Global, page 161

DoS Global

In this dialog **Network Security > DoS > Global**, you specify the DoS settings for the TCP/UDP, IP and ICMP protocols.

NOTE: Activate the filters to increase the level of security of the device.

TCP/UDP

A scanner uses port scans to prepare network attacks. The scanner uses different techniques to determine running devices and open ports. This frame allows you to activate filters for specific scanning techniques.

The following table presents the TCP/UDP settings:

Setting	Description
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.

Setting	Description
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

The following table presents the IP setting:

Setting	Description
Land Attack filter	Activates/deactivates the *Land Attack* filter. With the *Land Attack* method, the attacking station sends data packets whose source and destination addresses are identical to the IP address of the recipient. Possible values: • **marked** The filter is active. The device discards data packets whose source and destination addresses are identical. • **unmarked** (default setting) The filter is inactive.

ICMP

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

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

The following table presents the ICMP settings:

Setting	Description
Fragmented packets filter	Activates/deactivates the filter for fragmented ICMP packets. The filter detects fragmented ICMP packets and discards them. Possible values: • **marked** The filter is active. • **unmarked** (default setting) The filter is inactive.
Packet size filter	Activates/deactivates the filter for incoming ICMP packets. The filter detects ICMP packets whose payload size exceeds the size specified in the Allowed payload size [byte] field and discards them. Possible values: • **marked** The filter is active. • **unmarked** (default setting) The filter is inactive.
Allowed payload size [byte]	Specifies the maximum allowed payload size of ICMP packets in bytes. Mark the Packet size filter checkbox if you want the device to discard incoming data packets whose payload size exceeds the maximum allowed size for ICMP packets. Possible values: • **0..1472** (default setting: **512**)
Drop broadcast ping	Activates/deactivates the filter for Broadcast Pings. Broadcast Pings are a defined 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

The following table presents the information setting:

Setting	Description
Packets dropped	Displays the number of data packets that the device has discarded.

DHCP Snooping

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

In this dialog, you set up and monitor the following device behavior:

- Validate DHCP packets from untrusted sources and filter out invalid packets.
- Limit the amount of DHCP data packets from trusted and untrusted sources.
- Set up and update the DHCP Snooping binding database. This database contains the MAC address, IP address, VLAN and port of DHCP clients at untrusted ports.

- Validate follow-up requests from untrusted hosts on the basis of the DHCP Snooping binding database.

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

The DHCP Snooping menu **Network Security > DHCP Snooping** contains the following dialogs:

- DHCP Snooping Global, page 165
- DHCP Snooping Configuration, page 166
- DHCP Snooping Statistics, page 169
- DHCP Snooping Bindings, page 170

DHCP Snooping Global

This dialog **Network Security > DHCP Snooping > Global** allows you to set up the global DHCP Snooping parameters for your device:

- Activate/deactivate DHCP Snooping globally.
- Activate/deactivate Auto-Disable globally.
- Enable/disable the checking of the source MAC address.
- Specify the name, storage location and storing interval for the binding database.

Operation

The following table presents operation setting:

Setting	Description
Operation	Enables/disables the DHCP Snooping function globally. Possible values: • **On** • **Off** (default setting)

Configuration

The following table presents the configuration settings:

Setting	Description
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

The following table presents the binding database settings:

Setting	Description
Remote file name	Specifies the name of the file in which the device saves the DHCP Snooping binding database. **NOTE:** The device saves only dynamic bindings in the persistent binding database. The device saves static bindings in the configuration profile.
Remote IP address	Specifies the remote IP address under which the device saves the persistent DHCP Snooping binding database. With the value **0.0.0.0** the device saves the binding database locally. Possible values: • Valid IPv4 address • **0.0.0.0** (default setting) The device saves the DHCP Snooping binding database locally.
Store interval [s]	Specifies the time delay in seconds after which the device saves the DHCP Snooping binding database when the device identifies a change in the database. Possible values: • **15..86400 (1 d)** (default setting: **300**)

DHCP Snooping Configuration

This dialog **Network Security > DHCP Snooping > Configuration** allows you to set up DHCP Snooping for individual ports and for individual VLANs.

The dialog contains the following tabs:

- Port, page 167
- VLAN ID, page 169

Port

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

- Set up a port as trusted/untrusted.
- Activate/deactivate the logging of invalid packets for individual ports.
- Limit the amount of DHCP packets.
- Deactivate a port automatically if the amount of DHCP data packets exceeds the threshold value.

Table

For information on how to customize the appearance of the table, see Working with tables, page 25.

The following table presents the table settings:

Setting	Description
Port	Displays the port number.
Trust	Activates/deactivates the security status (trusted, untrusted) of the port. Possible values: • **marked** The port is set up as trusted. DHCP Snooping forwards permissible client packets through trusted ports. Typically, you have connected the trusted port to a DHCP server. • **unmarked** (default setting) The port is set up as untrusted. On untrusted ports, the device compares the receiver port with the client port in the binding database.
Log	Activates/deactivates the logging of invalid packets that the device determines on this port. Possible values: • **marked** The logging of invalid packets is active. • **unmarked** (default setting) The logging of invalid packets is inactive.
Rate limit	Specifies the maximum number of DHCP packets per burst interval on the port. If the number of incoming DHCP packets is currently exceeding the specified limit in a burst interval, then the device discards the additional incoming DHCP packets. Possible values: • **-1** (default setting) Deactivates the limitation of the number of DHCP packets per burst interval on this port. • **0..150**packets per interval Limits the maximum number of DHCP packets per burst interval on this port. You specify the burst interval in the Burst interval column. If you activate the auto-disable function, then the device also disables the port. You find the auto-disable function in the Auto-disable column.
Burst interval	Specifies the length of the burst interval in seconds on this port. The burst interval is relevant for the rate limiting function. You specify the maximum number of DHCP packets per burst interval in the Rate limit column. Possible values: • **1..15** (default setting: **1**)
Auto-disable	Activates/deactivates the Auto-Disable function for the parameters that the DHCP Snooping function is monitoring on the port. Possible values: • **marked** (default setting) The Auto-Disable function is active on the port. The prerequisite is that in the **Network Security > DHCP Snooping > Global** dialog, in the Configuration frame the Auto-disable checkbox is marked. ◦ If the port receives more DHCP packets than specified in the Rate limit field in the time specified in the Burst interval column, then the device disables the port. The ***Link status*** LED for the port flashes 3 × per period. ◦ The **Diagnostics > Ports > Auto-Disable** dialog displays which ports are currently disabled due to the parameters being exceeded. ◦ After a waiting period, the Auto-Disable function enables the port again automatically. For this you go to the **Diagnostics > Ports > Auto-Disable** dialog and specify a waiting period for the relevant port in the Reset timer [s] column. • **unmarked** The Auto-Disable function on the port is inactive.

VLAN ID

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

Table

For information on how to customize the appearance of the table, see Working with tables, page 25.

The following table presents the table settings:

Setting	Description
VLAN ID	Displays the VLAN ID to which the table row relates.
Active	Activates/deactivates the DHCP Snooping function in this VLAN. The DHCP Snooping function forwards valid DHCP client messages to the trusted ports in VLANs without the Routing function. Possible values: • **marked** The DHCP Snooping function is active in this VLAN. • **unmarked** (default setting) The DHCP Snooping function is inactive in this VLAN. The device forwards DHCP packets according to the switching settings without monitoring the packets. The binding database remains unchanged. **NOTE:** To enable DHCP Snooping for a port, enable the DHCP Snooping function globally in the **Network Security > DHCP Snooping > Global** dialog. Verify that you assigned the port to a VLAN in which DHCP Snooping is enabled.

DHCP Snooping Statistics

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

The device logs the following:

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

Table

For information on how to customize the appearance of the table, see Working with tables, page 25.

The following table presents the table settings:

Setting	Description
Buttons	Reset: Resets the values in the table.
Port	Displays the port number.
MAC verify failures	Displays the number of discrepancies between the MAC address of the DHCP client in the ‘chaddr’ field of the DHCP data packet and the source address in the Ethernet packet.
Invalid client messages	Displays the number of incoming DHCP client messages received on the port for which the device expects the client on another port according to the DHCP Snooping binding database.
Invalid server messages	Displays the number of DHCP server messages the device received on the untrusted port.

DHCP Snooping Bindings

DHCP Snooping uses DHCP messages to set up and update the binding database.

- Static bindings

  The device allows you to 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 **Network Security > DHCP Snooping > Bindings** specify the settings for static and dynamic bindings.

- Set up new static bindings and set them to active/inactive.
- Display, activate/deactivate or delete static bindings that have been set up.

Table

For information on how to customize the appearance of the table, see Working with tables, page 25.

The following table presents the table settings:

Setting	Description
Buttons	The following list presents the icon descriptions: • Add: Opens the Create window to add a table row. In the MAC address field, you specify the MAC address which you bind to an IP address and a VLAN ID. Possible values: Valid Unicast MAC address. Specify the value with a colon separator, for example **00:11:22:33:44:55**. • Remove: Removes the selected table row. The prerequisite is that in the Active column the checkbox is unmarked. Also, the device removes the dynamic bindings of this port set up with the IP Source Guard function.
MAC address	Displays the MAC address that you bind to an IP address and a VLAN ID.
IP address	Specifies the IP address for the static DHCP Snooping binding. Possible values: Valid Unicast IPv4 address smaller than **224.x.x.x** and outside the range **127.0.0.0/8** (default setting: **0.0.0.0**)
VLAN ID	Specifies the VLAN ID to which the table row relates. Possible values: **<VLAN IDs of the set-up VLANs>**
Port	Specifies the port for the static DHCP Snooping binding. Possible values: Available ports.
Remaining binding time	Displays the remaining time for the dynamic DHCP Snooping binding.
Active	Activates/deactivates the specified static DHCP Snooping binding. Possible values: • **marked** The static DHCP Snooping binding is active. The prerequisite is that in the **Time > Basic Settings** dialog the date and time are set correctly in the device. Otherwise, the bindings may get lost after rebooting the device. • **unmarked** (default setting) The static DHCP Snooping binding is inactive.

IP Source Guard

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

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

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

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

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

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

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

NOTE:

For the device to verify the IP address and the MAC address of the source of the data packets received on the port, enable the Verify MAC function.

For the device to verify 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 **Network Security > IP Source Guard** contains the following dialogs:

- IP Source Guard Port, page 172
- IP Source Guard Bindings, page 173

IP Source Guard Port

This dialog **Network Security > IP Source Guard > Port** display and set up the following device properties for each port:

- Include/exclude source MAC addresses for the filtering.
- Activate/deactivate the IP Source Guard function.

Table

For information on how to customize the appearance of the table, see Working with tables, page 25.

The following table presents table settings:

Setting	Description
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.

IP Source Guard Bindings

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

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

Table

For information on how to customize the appearance of the table, see Working with tables, page 25.

The following table presents the table settings:

Setting	Description
Buttons	The following list presents the icon descriptions: • Add: Opens the Create window to add a table row. ◦ In the MAC address field, you specify the MAC address for the static binding. ◦ In the IP address field, you specify the IP address for the static binding. ◦ In the VLAN ID field, you specify the VLAN ID. ◦ From the Port drop-down list, you select the port number. • Remove: Removes the selected table row. The prerequisite is that in the Active column the checkbox is unmarked.
MAC address	Displays the MAC address of the binding.
IP address	Displays the IP address of the binding.
VLAN ID	Displays the VLAN ID of the binding.
Port	Displays the number of the port of the binding.
Hardware status	Displays the hardware status of the binding. The device applies the binding to the hardware only if the settings are correct. Before the device applies the static IPSG binding to the hardware, it checks the following prerequisites: • The Active checkbox is marked. • The IP Source Guard function on the port is active, in the **Network Security > IP Source Guard > Port** dialog the Active checkbox is marked. Possible values: • **marked** The binding is active, the device applies the binding to the hardware. • **unmarked** The binding is inactive.
Active	Activates/deactivates the specified static IPSG binding between the specified MAC address and the specified IP address, for the specified VLAN on the specified port. Possible values: • **marked** The static IPSG binding is active. • **unmarked** (default setting) The static IPSG binding is inactive. **NOTE:** To make the static binding effective, activate the IP Source Guard function on the corresponding port. In the **Network Security > IP Source Guard > Port** dialog, mark the Active checkbox.

Dynamic ARP Inspection

Dynamic ARP Inspection is a function that supports the network security. This function analyzes ARP packets, logs them, and discards invalid and hostile ARP packets.

The Dynamic ARP Inspection function helps prevent a range of man-in-the-middle attacks. With this kind of attack, a hostile station listens in on the data stream from other subscribers by encroaching on the ARP cache of its unsuspecting neighbors. The hostile station sends ARP requests and ARP responses and enters the IP address of another subscriber for its own MAC address in the IP-to-MAC address relationship (binding).

Using the following measures, the Dynamic ARP Inspection function helps ensure that the device only forwards valid ARP requests and ARP responses.

- Listening in on ARP requests and ARP responses on untrusted ports.
- Verifying that the determined packets have a valid IP to MAC address relationship (binding) before the device updates the local ARP cache and before the device forwards the packets to the related destination address.
- Discarding invalid ARP packets.

The device allows you to specify up to 100 active ARP ACLs (access lists). You can activate up to 20 rules for each ARP ACL.

This menu **Network Security > Dynamic ARP Inspection** contains the following dialogs:

- Dynamic ARP Inspection Global, page 175
- Dynamic ARP Inspection Configuration, page 177
- Dynamic ARP Inspection ARP Rules, page 179
- Dynamic ARP Inspection Statistics, page 180

Dynamic ARP Inspection Global

Network Security > Dynamic ARP Inspection > Global

Configuration

The following table presents configuration settings:

Setting	Description
Verify source MAC	Activates/deactivates the source MAC address verification. The device executes the verification in both ARP requests and ARP responses. Possible values: • **marked** The source MAC address verification is active. The device verifies 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 verification in ARP responses. Possible values: • **marked** The destination MAC address verification is active. The device verifies 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 verification of the destination MAC address of the incoming ARP packets is inactive.

Setting	Description
Verify IP address	Activates/deactivates the IP address verification. In ARP requests, the device verifies the source IP address. In ARP responses, the device verifies 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 verifies 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.

Dynamic ARP Inspection Configuration

The dialog **Network Security > Dynamic ARP Inspection > Configuration** contains the following tabs:

- Port, page 177
- VLAN ID, page 178

Port

Table

For information on how to customize the appearance of the table, see Working with tables, page 25.

The following table presents the table settings:

Setting	Description
Port	Displays the port number.
Trust	Activates/deactivates the monitoring of ARP packets on untrusted ports. Possible values: • **marked** Monitoring is active. The device monitors ARP packets on untrusted ports. The device immediately forwards ARP packets on trusted ports. • **unmarked** (default setting) Monitoring is inactive.
Rate limit	Specifies the maximum number of ARP packets per interval on this port. If the rate of incoming ARP packets is currently exceeding the specified limit in a burst interval, then the device discards the additional incoming ARP packets. You specify the burst interval in the Burst interval column. Optionally, the device also deactivates the port if you activate the auto-disable function. You enable/disable the Auto-Disable function in the Auto-disable column. Possible values: • **-1** (default setting) Deactivates the limitation of the number of ARP packets per burst interval on this port. • **0..300**packets per interval Limits the maximum number of ARP packets per burst interval on this port.
Burst interval	Specifies the length of the burst interval in seconds on this port. The burst interval is relevant for the rate limiting function. You specify the maximum number of ARP packets per burst interval in the Rate limit column. Possible values: **1..15** (default setting: **1**).
Auto-disable	Activates/deactivates the Auto-Disable function for the parameters that the Dynamic ARP Inspection function is monitoring on the port. Possible values: • **marked** (default setting) The Auto-Disable function is active on the port. The prerequisite is that in the **Network Security > Dynamic ARP Inspection > Global** dialog, in the Configuration frame the Auto-disable checkbox is marked. ◦ If the port receives more ARP packets than specified in the Rate limit field in the time specified in the Burst interval column, then the device disables the port. The ***Link status*** LED for the port flashes 3 × per period. ◦ The **Diagnostics > Ports > Auto-Disable** dialog displays which ports are currently disabled due to the parameters being exceeded. ◦ After a waiting period, the Auto-Disable function enables the port again automatically. For this you go to the **Diagnostics > Ports > Auto-Disable** dialog and specify a waiting period for the relevant port in the Reset timer [s] column. • **unmarked** The Auto-Disable function on the port is inactive.

VLAN ID

Table

For information on how to customize the appearance of the table, see Working with tables, page 25.

The following table presents the table settings:

Setting	Description
VLAN ID	Displays the VLAN ID to which the table row relates.
Log	Activates/deactivates the logging of invalid ARP packets that the device determines in this VLAN. If the device detects an error when checking the IP, source MAC or destination MAC address, or when checking the IP-to-MAC address relationship (binding), then the device identifies an ARP packet as invalid. Possible values: • **marked** The logging of invalid packets is active. The device registers invalid ARP packets. • **unmarked** (default setting) The logging of invalid packets is inactive.
Binding check	Activates/deactivates the checking of incoming ARP packets that the device receives on untrusted ports and on VLANs for which the Dynamic ARP Inspection function is active. For these ARP packets the device checks the ARP ACL and the DHCP Snooping relationship (bindings). Possible values: • **marked** (default setting) The binding check of ARP packets is active. • **unmarked** The binding check of ARP packets is inactive.
Strict ACL check	Activates/deactivates the strict checking of incoming ARP packets based on the ARP ACL rules specified. Possible values: • **marked** The strict checking is active. The device checks the incoming ARP packets based on the ARP ACL rule specified in the ACL column. • **unmarked** (default setting) The strict checking is inactive. The device checks the incoming ARP packets based on the ARP ACL rule specified in the ACL column and subsequently on the entries in the DHCP Snooping database.
ACL	Specifies the ARP ACL that the device uses. Possible values: • **<rule name>** You add and edit the rules in the **Network Security > Dynamic ARP Inspection > ARP Rules** dialog.
Active	Activates/deactivates the Dynamic ARP Inspection function in this VLAN. Possible values: • **marked** The Dynamic ARP Inspection function is active in this VLAN. • **unmarked** (default setting) The Dynamic ARP Inspection function is inactive in this VLAN.

Dynamic ARP Inspection ARP Rules

This dialog **Network Security > Dynamic ARP Inspection > ARP Rules** allows you to specify rules for checking and filtering ARP packets.

Table

For information on how to customize the appearance of the table, see Working with tables, page 25.

The following table presents the table settings:

Setting	Description
Buttons	The following list presents the icon descriptions: • Add: Opens the Create window to add a table row. ◦ From the Name drop-down list, you select the name of the ARP rule or specify a new name. Enter the name in the search box. – To use an existing name, select the desired item from the search results. – To add a name, click the Create link below the search box. ◦ In the Source IP address field, you specify the source IP address of the ARP rule. ◦ In the Source MAC address field, you specify the source MAC address of the ARP rule. • Remove: Removes the selected table row.
Name	Displays the name of the ARP rule.
Source IP address	Specifies the source address of the IP data packets to which the device applies the rule. Possible values: • Valid IPv4 address The device applies the rule to IP data packets with the specified source address.
Source MAC address	Specifies the source address of the MAC data packets to which the device applies the rule. Possible values: • Valid MAC address The device applies the rule to MAC data packets with the specified source address.
Active	Activates/deactivates the ARP rule. Possible values: • **marked** (default setting) The rule is active. • **unmarked** The rule is inactive.

Dynamic ARP Inspection Statistics

This window **Network Security > Dynamic ARP Inspection > Statistics** displays the number of discarded and forwarded ARP packets in an overview.

Table

For information on how to customize the appearance of the table, see Working with tables, page 25.

The following table presents the table settings:

Setting	Description
Buttons	Reset: Resets the values in the table.
VLAN ID	Displays the VLAN ID to which the table row relates.
Packets forwarded	Displays the number of ARP packets that the device forwards after checking them using the Dynamic ARP Inspection function.
Packets dropped	Displays the number of ARP packets that the device discards after checking them using the Dynamic ARP Inspection function.
DHCP drops	Displays the number of ARP packets that the device discards after checking the DHCP Snooping relationship (binding).
DHCP permits	Displays the number of ARP packets that the device forwards after checking the DHCP Snooping relationship (binding).
ACL drops	Displays the number of ARP packets that the device discards after checking them using the ARP ACL rules.
ACL permits	Displays the number of ARP packets that the device forwards after checking them using the ARP ACL rules.
Bad source MAC	Displays the number of ARP packets that the device discards after the Dynamic ARP Inspection function detected an error in the source MAC address.
Bad destination MAC	Displays the number of ARP packets that the device discards after the Dynamic ARP Inspection function detected an error in the destination MAC address.
Invalid IP address	Displays the number of ARP packets that the device discards after the Dynamic ARP Inspection function detected an error in the IP address.

ACL

In this menu **Network Security > ACL**, you specify the settings for the Access Control Lists (ACL). Access Control Lists contain rules which the device applies successively to the data stream on its ports or VLANs.

If a data packet matches the criteria of one or more rules, then the device applies the action specified in the first applicable rule to the data stream. The device ignores the rules that follow the first applicable rule. Possible actions include:

- **permit**: The device forwards the data packet to a port or to a VLAN.

  When necessary, the device forwards a copy of the data packets to a further port.
- **deny**: The device drops the data packet.

In the default setting, the device forwards every data packet. As soon as you assign an Access Control List to a port or VLAN, then this behavior changes. The device enters at the end of an Access Control List an implicit *Deny-All* rule. Consequently, the device discards data packets that do not match the criteria of any rules. If you want a different behavior, then add a *Permit-All* rule at the end of your Access Control Lists.

Proceed as follows to set up Access Control Lists and rules:

- Make a time profile if necessary. See the **Time > Time Profile** dialog. The device applies Access Control Lists with a time profile at specified times instead of permanently.
- Make a rule and specify the rule settings. See the **Network Security > ACL > IPv4 Rule** dialog, or the **Network Security > ACL > MAC Rule** dialog.
- Assign the Access Control List to the ports and VLANs of the device. See the **Network Security > ACL > Assignment** dialog.

The menu contains the following dialogs:

- ACL IPv4 Rule, page 182
- ACL MAC Rule, page 189
- ACL Assignment, page 193

ACL IPv4 Rule

In this dialog **Network Security > ACL > IPv4 Rule**, you specify the rules that the device applies to the IP data packets.

An Access Control List (group) contains one or more rules. The device applies the rules of an Access Control List successively, beginning with the rule with the numerically lowest value in the Index column.

The device allows you to filter according to the following criteria:

- Source or destination IP address of a data packet
- Type of the transmitting protocol
- Source or destination port of a data packet
- Classification according to DSCP
- Classification according to ToS

Table

For information on how to customize the appearance of the table, see Working with tables, page 25.

The following table presents the table settings:

Setting	Description
Buttons	The following list presents the icon descriptions: • Add: Opens the Create window to add a table row. ◦ From the Group name drop-down list, you select the Access Control List name to which the rule belongs or add a new name. Enter the name in the search box. – To use an existing name, select the desired item from the search results. – To add a name, click the Create link below the search box. ◦ In the Index field, you specify the number of the rule within the Access Control List. If the Access Control List contains multiple rules, then the device processes the rule with the lowest index value first. • Remove: Removes the selected table row.
Group name	Displays the name of the Access Control List. The Access Control List contains the rules.
Index	Displays the number of the rule within the Access Control List. You specify the index number when you add a table row. If the Access Control List contains multiple rules, then the device processes the rule with the numerically lowest value first.
Match every packet	Specifies to which IP data packets the device applies the rule. Possible values: • **marked** (default setting) The device applies the rule to every IP data packet. • **unmarked** The device applies the rule to IP data packets depending on the value in the following fields: ◦ Source IP address, Destination IP address, Protocol ◦ DSCP, TOS priority, TOS mask ◦ ICMP type, ICMP code ◦ IGMP type ◦ Established ◦ Packet fragmented ◦ TCP flag
Source IP address	Specifies the source address of the IP data packets to which the device applies the rule. Possible values: • **?.?.?.?** (default setting) The device applies the rule to IP data packets with any source address. • Valid IPv4 address The device applies the rule to IP data packets with the specified source address. You use the **?** character as a wild card. Example **192.?.?.32**: The device applies the rule to IP data packets whose source address begins with **192.** and ends with **.32**. • Valid IPv4 address/bit mask The device applies the rule to IP data packets with the specified source address. The inverse bit mask 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**.

Setting	Description
Destination IP address	Specifies the destination address of the IP data packets to which the device applies the rule. Possible values: • **?.?.?.?** (default setting) The device applies the rule to IP data packets with any destination address. • Valid IPv4 address The device applies the rule to data packets with the specified destination address. You use the **?** character as a wild card. Example **192.?.?.32**: The device applies the rule to IP data packets whose source address begins with **192.** and ends with **.32**. • Valid IPv4 address/bit mask The device applies the rule to data packets with the specified destination address. The inverse bit mask specify the address range with bit-level accuracy. Example **192.168.1.0/0.0.0.127**: The device applies the rule to IP data packets with a destination address in the range from **192.168.1.0** to **….127**.
Protocol	Specifies the IP protocol or Layer 4 protocol type of the data packets to which the device applies the rule. The device applies the rule only to data packets that contain the specified value in the *Protocol* field. Possible values: • **any** (default setting) The device applies the rule to every IP data packet without evaluating the protocol type. • **icmp** Internet Control Message Protocol (RFC 792) • **igmp** Internet Group Management Protocol • **ip-in-ip** IP in IP tunneling (RFC 2003) • **tcp** Transmission Control Protocol (RFC 793) • **udp** User Datagram Protocol (RFC 768) • **ip** Internet Protocol
Source TCP/UDP port	Specifies the source port of the IP data packets to which the device applies the rule. The prerequisite is that in the Protocol column the value **TCP** or **UDP** is specified. Possible values: • **any** (default setting) The device applies the rule to every IP data packet without evaluating the source port. • **1..65535 (2^{16}-1)** The device applies the rule only to IP data packets containing the specified source port. The device supports up to 8 port ranges. You can assign a specified port range to multiple rules. To specify a port range, you can use one of the following operators: ◦ **<** Range below the specified port number ◦ **>** Range above the specified port number ◦ **!=** Entire port range except the specified port Each **!=** operator used takes up 2 available port ranges. To have a maximum number of port ranges available, you can combine neighboring ranges (for example **>1023** and **<1024**). In this case, the device uses only one port range.

Setting	Description
Destination TCP/ UDP port	Specifies the destination port of the IP data packets to which the device applies the rule. The prerequisite is that in the Protocol column the value **TCP** or **UDP** is specified. Possible values: • **any** (default setting) The device applies the rule to every IP data packet without evaluating the destination port. • **1..65535 (2^{16}-1)** The device applies the rule only to IP data packets containing the specified destination port. The device supports up to 8 port ranges. You can assign a specified port range to multiple rules. To specify a port range, you can use one of the following operators: ◦ **<** Range below the specified port number ◦ **>** Range above the specified port number ◦ **!=** Entire port range except the specified port Each **!=** operator used takes up 2 available port ranges. To have a maximum number of port ranges available, you can combine neighboring ranges (for example **>1023** and **<1024**). In this case, the device uses only one port range.
DSCP	Specifies the Differentiated Service Code Point (DSCP value) in the header of the IP data packets to which the device applies the rule. Possible values: • **–** (default setting) The device applies the rule to every IP data packet without evaluating the DSCP value. • **0..63** The device applies the rule only to IP data packets containing the specified DSCP value.
TOS priority	Specifies the *IP Precedence (ToS)* value in the header of the IP data packets to which the device applies the rule. Possible values: • **any** (default setting) The device applies the rule to every IP data packet without evaluating the *ToS* value. • **0..7** The device applies the rule only to IP data packets containing the specified *ToS* value.
TOS mask	Specifies the bit mask for the *ToS* value in the header of the IP data packets to which the device applies the rule. The prerequisite is that in the TOS priority column a *ToS* value is specified. Possible values: • **any** (default setting) The device applies the rule to IP data packets and evaluates the *ToS* value completely. • **1..1f** The device applies the rule to IP data packets and evaluates the bits of the *ToS* value specified in the bit mask.
ICMP type	Specifies the ICMP type in the TCP header of the IP data packets to which the device applies the rule. Possible values: • **-1** (default setting) ICMP type matching is inactive. • **0..255** The device applies the rule to every IP data packet and evaluates the specified ICMP type.

Setting	Description
ICMP code	Specifies the ICMP code in the TCP header of the IP data packets to which the device applies the rule. The prerequisite is that in the ICMP type field an ICMP value is specified. Possible values: • **-1** (default setting) ICMP code matching is inactive. • **0..255** The device applies the rule to every IP data packet and evaluates the specified ICMP code.
IGMP type	Specifies the IGMP type in the TCP header of the IP data packets to which the device applies the rule. Possible values: • **0** (default setting) IGMP type matching is inactive. • **1..255** The device applies the rule to every IP data packet and evaluates the specified IGMP type.
Established	Activates/deactivates applying the ACL rule to TCP data packets which have either the RST bit, or the ACK bit set in the TCP header. Possible values: • **marked** The device applies the rule to every IP data packet in which the RST bit, or the ACK bit is set in the TCP header. • **unmarked** (default setting) Matching is inactive.
Packet fragmented	Activates/deactivates applying the ACL rule to the packet fragments. To filter the complete data packet including its fragments, add 2 ACL rules. • Create an ACL rule for the initial data packet to filter on both at the protocol level and at the TCP/UDP ports. • Create a second ACL rule for the fragments to filter only at the protocol level. Possible values: • **marked** The device applies the ACL rule to the fragments. Use this setting in the second ACL rule for the fragments. • **unmarked** (default setting) The device does not apply the ACL rule to the fragments.

Setting	Description
TCP flag	Specifies the TCP flag and mask value. The device allows you to enter multiple values, by separating the values with a comma. Specify the flags as either **+** or **-**. Possible values: • **-** (default setting) TCP flag matching is inactive. • **-** When you use this value in combination with the following flags, the device evaluates packets in which the flag is not set. • **+** When you use this value in combination with the following flags, the device evaluates packets in which the flag is set. • **fin** Indicates that the sending device has finished its transmission. • **syn** Indicates that the **Synchronize sequence** numbers are significant. Only the first packet sent from each end device has this flag set. • **rst** Indicates a reset of the TCP connection. • **psh** Indicates the push function, in which a device asks to push the buffered data to the receiving application. • **ack** Indicates that the **Acknowledgment** field is significant. Every packet, after the initial syn packet sent by the client, has this flag set. • **urg** Indicates that the **Urgent pointer** field is significant.
Action	Specifies how the device processes received IP data packets when the device applies the rule. Possible values: • **permit** (default setting) The device forwards the IP data packets. • **deny** The device drops the IP data packets.
Redirection port	Specifies the port to which the device forwards the IP data packets. The prerequisite is that in the Action column the value **permit** is specified. The device does not provide the option of mirroring IP data packets across VLAN boundaries. Possible values: • **–** (default setting) The Redirection port function is inactive. • **<Port number>** The device forwards the IP data packets to the specified port.
Mirror port	Specifies the port to which the device forwards a copy of the IP data packets. The prerequisite is that in the Action column the value **permit** is specified. The device does not provide the option of mirroring IP data packets across VLAN boundaries. Possible values: • **–** (default setting) The Mirror port function is inactive. • **<Port number>** The device forwards a copy of the IP data packets to the specified port.

Setting	Description
Assigned queue ID	Specifies the priority queue to which the device assigns the IP data packets. Possible values: • **-** (default setting) • **0..7**
Log	Activates/deactivates the logging in the log file. See the **Diagnostics > Report > System Log** dialog. Possible values: • **marked** Logging is active. The prerequisite is that in the **Network Security > ACL > Assignment** dialog the Access Control List is assigned to a VLAN or port. The device registers in the log file, in an interval of 30 s, how many times it applied the deny rule to IP data packets. • **unmarked** (default setting) Logging is inactive. The device allows you to activate this function for up to 128 deny rules.
Time profile	Specifies if the device applies the rule permanently or time-controlled. Possible values: • **<empty>** (default setting) The device applies the rule permanently. • **[Time Profile]** The device applies the rule only at the times specified in the selected time profile. You edit the time profiles in the **Time > Time Profile** dialog. The implied *Deny-All* rule of the ACLs is permanently valid independently of the time control.
Rate limit	Specifies the limit for the data transfer rate for the port specified in the Redirection port column. The limit applies to the summary of the data sent and received. This function limits the data stream on the port or in the VLAN: Possible values: • **0** (default setting) No limitation of the data transfer rate. • **8..4294967295 (2^{32}-1)** If the data transfer rate on the port exceeds the value specified, then the device discards superfluous IP data packets. The prerequisite is that in the Burst size column a value >**0** is specified. You specify the measurement unit of the limit in the Unit column.
Unit	Specifies the measurement unit for the data transfer rate specified in the Rate limit column. Possible values: • **kbps** kBytes per second
Burst size	Specifies the limit in KByte for the data volume during temporary bursts. Possible values: • **0** (default setting) No limitation of the data volume. • **1..128** If during temporary bursts on the port the data volume exceeds the value specified, then the device discards superfluous MAC data packets. The prerequisite is that in the Rate limit column a value >**0** is specified. Recommendation: • If the bandwidth is defined: Burst size = bandwidth × allowed duration of a burst / 8 • If the bandwidth is undefined: Burst size = 10 × MTU (*Maximum Transmission Unit*) of the port

ACL MAC Rule

In this dialog **Network Security > ACL > MAC Rule**, specify the rules that the device applies to the MAC data packets.

An Access Control List (group) contains one or more rules. The device applies the rules of an Access Control List successively, beginning with the rule with the numerically lowest value in the Index column.

The device allows you to filter according to the following criteria:

- Source or destination MAC address of a data packet
- Type of the transmitting protocol
- Membership of a specific VLAN
- Service class of a data packet

Table

For information on how to customize the appearance of the table, see Working with tables, page 25.

The following table presents the table settings:

Setting	Description
Buttons	The following list presents the icon descriptions: • Add: Opens the Create window to add a table row. ◦ From the Group name drop-down list, you select the Access Control List name to which the rule belongs or add a new name. Enter the name in the search box. – To use an existing name, select the desired item from the search results. – To add a name, click the Create link below the search box. ◦ In the Index field, you specify the number of the rule within the Access Control List. If the Access Control List contains multiple rules, then the device processes the rule with the lowest index value first. • Remove: Removes the selected table row.
Group name	Displays the name of the Access Control List. The Access Control List contains the rules.
Index	Displays the number of the rule within the Access Control List. You specify the index number when you add a table row. If the Access Control List contains multiple rules, then the device processes the rule with the numerically lowest value first.
Match every packet	Specifies to which MAC data packets the device applies the rule. Possible values: • **marked** (default setting) The device applies the rule to every MAC data packet. • **unmarked** The device applies the rule to MAC data packets depending on the value in the following fields: ◦ Source MAC address ◦ Destination MAC address ◦ Ethertype ◦ Ethertype custom value ◦ VLAN ID ◦ COS
Source MAC address	Specifies the source address of the MAC data packets to which the device applies the rule. Possible values: • **??:??:??:??:??:??** (default setting) The device applies the rule to MAC data packets with any source address. • Valid MAC address The device applies the rule to MAC data packets with the specified source address. You use the **?** character as a wild card. Example **00:11:??:??:??:??**: The device applies the rule to MAC data packets whose source address begins with **00:11**. • Valid MAC address/bit mask The device applies the rule to MAC data packets with the specified source address. The bit mask 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**.

Setting	Description
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 specify the address range with bit-level accuracy. Example **00:11:22:33:44:54/FF:FF:FF:FF:FF:FC**: The device applies the rule to MAC data packets with a destination address in the range from **00:11:22:33:44:54** to **…:57**.
Ethertype	Specifies the *Ethertype* keyword of the MAC data packets to which the device applies the rule. Possible values: • **custom** (default setting) The device applies the value specified in the Ethertype custom value column. • **appletalk** • **arp** • **ibmsna** • **ipv4** • **ipv6** • **ipxold** • **mplsmcast** • **mplsucast** • **netbios** • **novell** • **rarp** • **pppoe**
Ethertype custom value	Specifies the *Ethertype* value of the MAC data packets to which the device applies the rule. The prerequisite is that in the Ethertype column the value **custom** is specified. Possible values: • **0** (default setting) The device applies the rule to every MAC data packet without evaluating the *Ethertype* value. • **600..ffff** The device applies the rule only to MAC data packets that contain the *Ethertype* value specified here.
VLAN ID	Specifies the VLAN ID of the MAC data packets to which the device applies the rule. Possible values: • **0** (default setting) The device applies the rule to every MAC data packet without evaluating the VLAN ID. • **1..4042**
COS	Specifies the Class of Service (COS) value of the MAC data packets to which the device applies the rule. Possible values: • **0..7** • **any** (default setting) The device applies the rule to every MAC data packet without evaluating the Class of Service value.
Action	Specifies how the device processes received MAC data packets when the device applies the rule. Possible values: • **permit** (default setting) The device forwards the MAC data packets. • **deny** The device discards the MAC data packets.

Setting	Description
Redirection port	Specifies the port to which the device forwards the MAC data packets. The prerequisite is that in the Action column the value **permit** is specified. The device does not provide the option of mirroring IP data packets across VLAN boundaries. Possible values: • **–** (default setting) The Redirection port function is inactive. • **<Port number>** The device forwards the MAC data packets to the specified port.
Mirror port	Specifies the port to which the device forwards a copy of the MAC data packets. The prerequisite is that in the Action column the value **permit** is specified. The device does not provide the option of mirroring IP data packets across VLAN boundaries. Possible values: • **–** (default setting) The Mirror port function is disabled. • **<Port number>** The device forwards a copy of the MAC data packets to the specified port.
Assigned queue ID	Specifies the ID of the priority queue to which the device forwards the MAC data packets. Possible values: • **-** (default setting) • **0..7**
Log	Activates/deactivates the logging in the log file. See the **Diagnostics > Report > System Log** dialog. Possible values: • **marked** Logging is active. The prerequisite is that in the **Network Security > ACL > Assignment** dialog the Access Control List is assigned to a VLAN or port. The device registers in the log file, in an interval of 30 s, how many times it applied the deny rule to MAC data packets. • **unmarked** (default setting) Logging is inactive. The device allows you to activate this function for up to 128 deny rules.
Time profile	Specifies if the device applies the rule permanently or time-controlled. Possible values: • **<empty>** (default setting) The device applies the rule permanently. • **[Time Profile]** The device applies the rule only at the times specified in the selected time profile. You edit the time profiles in the **Time > Time Profile** dialog. The implied *Deny-All* rule of the ACLs is permanently valid independently of the time control.
Rate limit	Specifies the limit for the data transfer rate for the port specified in the Redirection port column. The limit applies to the summary of the data sent and received. This function limits the data stream on the port or in the VLAN: Possible values: • **0** (default setting) No limitation of the data transfer rate. • **8..4294967295 (2^{32}-1)** If the data transfer rate on the port exceeds the value specified, then the device discards superfluous MAC data packets. The prerequisite is that in the Burst size column a value >**0** is specified. You specify the measurement unit of the limit in the Unit column.

Setting	Description
Unit	Specifies the measurement unit for the data transfer rate specified in the Rate limit column. Possible values: • **kbps** kBytes per second
Burst size	Specifies the limit in KByte for the data volume during temporary bursts. Possible values: • **0** (default setting) No limitation of the data volume. • **1..128** If during temporary bursts on the port the data volume exceeds the value specified, then the device discards superfluous MAC data packets. The prerequisite is that in the Rate limit column a value >**0** is specified. Recommendation: • If the bandwidth is defined: Burst size = bandwidth × allowed duration of a burst / 8 • If the bandwidth is undefined: Burst size = 10 × MTU (*Maximum Transmission Unit*) of the port

ACL Assignment

This dialog **Network Security > ACL > Assignment** allows you to 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 greater the priority. In this process, the device applies the rules with a high priority before the rules with a low priority.

The device allows you to specify a maximum of 50 ACLs, which can each contain a certain number of rules. The number of rules that you can actually assign to the ports and VLANs might be smaller than the number of rules specified in the device. An example in the “Configuration” user manual illustrates the factors that affect the possible number that you can actually assign.

The assignment of Access Control Lists to ports and VLANs results in the following different types of ACLs:

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

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

NOTE: Before you enable the function, verify that at least one active table row in the table allows you to access. Otherwise, the connection to the device terminates if you change the settings. Access to the device management is only possible using the Command Line Interface through the serial connection.

Table

For information on how to customize the appearance of the table, see Working with tables, page 25.

The following table presents the table settings:

Setting	Description
Buttons	The following list presents the icon descriptions: • Add: Opens the Create window to assign a rule to a port or a VLAN. ◦ From the Port/VLAN drop-down list, you select the port or the VLAN to which the device applies the rule. ◦ In the Priority field, you specify the sequence in which the device applies the rules to the data stream. ◦ From the Direction drop-down list, you select if the device applies the rule to received or sent data packets. ◦ From the Group name drop-down list, you select the rule that the device assigns to the port or VLAN. • Remove: Removes the selected table row.
Group name	Displays the name of the Access Control List. The Access Control List contains the rules.
Type	Displays if the Access Control List contains MAC rules or IPv4 rules. Possible values: • **mac** The Access Control List contains MAC rules. • **ip** The Access Control List contains IPv4 rules. You edit Access Control Lists with IPv4 rules in the **Network Security > ACL > IPv4 Rule** dialog. You edit Access Control Lists with MAC rules in the **Network Security > ACL > MAC Rule** dialog.
Port	Displays the port to which the Access Control List is assigned. The field remains empty when the Access Control List is assigned to a VLAN.
VLAN ID	Displays the VLAN to which the Access Control List is assigned. The field remains empty when the Access Control List is assigned to a port.
Direction	Displays that the device applies the Access Control List to received data packets. The device can apply the Access Control Lists only to received data packets.
Priority	Displays the priority of the Access Control List. Using the priority, you specify the sequence in which the device applies the Access Control Lists to the data stream. The device applies the rules in ascending order which starts with priority **1**. If an Access Control List is assigned to a port and to a VLAN with the same priority, then the device applies the rules to the port first. Possible values: • **1..4294967295 (2^{32}-1)**
Active	Displays if the Access Control List on the port or in the VLAN is active. Possible values: • **marked** (default setting) The Access Control List is active. • **unmarked** The Access Control List is inactive.

Switching

The menu contains the following dialogs:

- Switching Global, page 195
- Rate Limiter, page 196
- Filter for MAC Addresses, page 198
- IGMP Snooping, page 200
- Time-Sensitive Networking, page 212
- MRP-IEEE, page 218
- GARP, page 225
- QoS/Priority, page 227
- VLAN, page 234
- L2-Redundancy, page 244

Switching Global

This dialog **Switching > Global** allows you to specify the following settings:

- Change the Aging time of the MAC address table (forwarding database) entries
- Enable the flow control in the device

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

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

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

The connected devices then stop sending data packets for the duration of the signaling. On an uplink port, this can possibly cause undesired sending interruptions in the greater-level network segment (“wandering backpressure”). The flow control mechanism thus lowers the network to the bandwidth that the slowest device in the network can process.

Configuration

The following table presents the configuration settings:

Setting	Description
MAC address	Displays the MAC address of the device.
Aging time [s]	Specifies the aging time in seconds. Possible values: • **10..500000** (default setting: **30**) The device monitors the age of the learned unicast MAC addresses. The device deletes address entries that exceed a particular age (aging time) from its MAC address table (forwarding database). You find the MAC address table (forwarding database) in the **Switching > Filter for MAC Addresses** dialog.
Flow control	Activates/deactivates the flow control in the device. Possible values: • **marked** The flow control is active in the device. Additionally activate the flow control on the required ports. See the **Basic Settings > Port** dialog, Configuration tab, checkbox in the Flow control column. • **unmarked** (default setting) The flow control is inactive in the device. If you are using a redundancy function, then you deactivate the flow control on the participating ports. If the flow control and the redundancy function are active at the same time, it is possible that the redundancy function operates differently than intended.

Rate Limiter

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

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

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

The dialog **Switching > Limiter** contains the following tabs:

- Ingress, page 196
- Egress, page 198

Ingress

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

Table

For information on how to customize the appearance of the table, see Working with tables, page 25.

The following table presents the table settings:

Setting	Description
Port	Displays the port number.
Unit	Specifies the unit for the threshold value: Possible values: • **percent** (default setting) Specifies the threshold value as a percentage of the data rate of the port. • **pps** Specifies the threshold value in data packets per second.
Broadcast mode	Activates/deactivates the rate limiter function for received broadcast data packets. Possible values: • **marked** • **unmarked** (default setting) If the threshold value is exceeded, then the device discards the excess broadcast data packets on this port.
Broadcast threshold	Specifies the threshold value for received broadcasts on this port. Possible values: • **0..14880000** (default setting: **0**) The value **0** deactivates the rate limiter function on this port. ◦ If you select the value **percent** in the Unit column, then enter a percentage value from **1** to **100**. ◦ If you select the value **pps** in the Unit column, then enter an absolute value for the data rate.
Known multicast mode	Activates/deactivates the rate limiter function for received known multicast data packets. Possible values: • **marked** • **unmarked** (default setting) If the threshold value is exceeded, then the device discards the excess multicast data packets on this port.
Known multicast threshold	Specifies the threshold value for received multicasts on this port. Possible values: • **0..14880000** (default setting: **0**) The value **0** deactivates the rate limiter function on this port. ◦ If you select the value **percent** in the Unit column, then enter a percentage value from **0** to **100**. ◦ If you select the value **pps** in the Unit column, then enter an absolute value for the data rate.
Unknown frame mode	Activates/deactivates the rate limiter function for received unicast and multicast data packets with an undefined 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 undefined destination address on this port. Possible values: • **0..14880000** (default setting: **0**) The value **0** deactivates the rate limiter function on this port. ◦ If you select the value **percent** in the Unit column, then enter a percentage value from **0** to **100**. ◦ If you select the value **pps** in the Unit column, then enter an absolute value for the data rate.

Egress

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

Table

For information on how to customize the appearance of the table, see Working with tables, page 25.

The following table presents the table settings:

Setting	Description
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.

Filter for MAC Addresses

This dialog **Switching > Filter for MAC Addresses** allows you to display and edit address filters for the MAC address table (forwarding database). Address filters specify the way the data packets are forwarded in the device based on the destination MAC address.

Each table row represents one filter. The device automatically sets up the filters. The device allows you to set up additional filters manually.

The device forwards the data packets as follows:

- When the table contains the destination address of a data packet, the device forwards the data packet from the receiving port to the port specified in the table row.
- When there is no table row for the destination address, the device forwards the data packet from the receiving port to every other port.

Table

To delete the learned MAC addresses from the MAC address table (forwarding database), click in the **Basic Settings > Restart** dialog the Clear FDB button.

For information on how to customize the appearance of the table, see Working with tables, page 25.

The following table presents the table settings:

Setting	Description
Buttons	The following list presents the icon descriptions: •  Add: Opens the Create window to add a table row. ◦ In the MAC address field, you specify the destination MAC address. ◦ In the VLAN ID field, you specify the VLAN ID. ◦ In the list field, you select the ports. – If the destination MAC address is a unicast address, select exactly one port. – If the destination MAC address is a multicast or broadcast address, select one or more ports. – Do not select a port to add a *Discard* filter. The device discards data packets with the destination MAC address specified in the table row. •  Remove: Removes the selected table row. •  Clear FDB: Deletes the MAC addresses from the forwarding table that have the value **Learned** in the Status column.
Address	Displays the destination MAC address to which the table row relates.
VLAN ID	Displays the ID of the VLAN to which the table row relates. The device learns the MAC addresses for every VLAN separately (independent VLAN learning).

Setting	Description
Status	Displays how the device has set up the address filter. Possible values: • **Learned** Address filter set up automatically by the device based on received data packets. • **Mgmt** MAC address of the device. The address filter is protected against changes. • **Other** Static address added by the following function: ◦ 802.1X ◦ Port Security • **Permanent** Address filter set up manually. The address filter stays set up permanently. • **GMRP** Multicast address filter automatically set up by GMRP. • **IGMP** Address filter automatically set up by IGMP Snooping. • **MRP-MMRP** Multicast address filter automatically set up by MMRP.
<Port number>	Displays how the corresponding port transmits data packets which it directs to the adjacent destination address. Possible values: • **–** The port does not transmit any data packets to the destination address. • **Learned** The port transmits data packets to the destination address. The device has automatically set up the filter based on received data packets. • **IGMP learned** The port transmits data packets to the destination address. The device has automatically set up the filter based on IGMP. • **Unicast static** The port transmits data packets to the destination address. A user has set up the filter. • **Multicast static** The port transmits data packets to the destination address. A user has set up the filter.

IGMP Snooping

The Internet Group Management Protocol (IGMP) is a protocol for dynamically managing Multicast groups. The protocol describes the distribution of Multicast data packets between routers and end devices on Layer 3.

The device lets you use the IGMP Snooping function to also use the IGMP mechanisms on Layer 2:

- Without IGMP Snooping, the device forwards the Multicast data packets to every port.
- With the activated IGMP Snooping function, the device forwards the Multicast data packets only on ports to which Multicast receivers are connected. This reduces the network load. The device evaluates the IGMP data packets transmitted on Layer 3 and uses the information on Layer 2.

Activate the IGMP Snooping function not until the following conditions are fulfilled:

- There is a Multicast router in the network that generates IGMP queries (periodic queries).
- The devices participating in IGMP Snooping forward the IGMP queries.

The device links the IGMP reports with the entries in its MAC address table (forwarding database). When a multicast receiver joins a multicast group, the device adds a table row for this port in the **Switching > Filter for MAC Addresses** dialog. When the multicast receiver leaves the multicast group, the device removes the table row.

This menu **Switching > IGMP Snooping** contains the following dialogs:

- IGMP Snooping Global, page 201
- IGMP Snooping Configuration, page 202
- IGMP Snooping Enhancements, page 206
- IGMP Snooping Querier, page 209
- IGMP Snooping Multicasts, page 211

IGMP Snooping Global

This dialog **Switching > IGMP Snooping > Global** allows you to enable the IGMP Snooping function in the device and set the function up for each port and each VLAN.

Operation

The following table presents the operation settings:

Setting	Description
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

The following table presents the information settings:

Setting	Description
Buttons	Reset IGMP snooping counters: Deletes the IGMP Snooping entries and resets the counter in the Information frame to **0**.
Processed multicast controls	Displays the number of Multicast control data packets processed. This statistic encompasses the following packet types: • IGMP Reports • IGMP Queries version V1 • IGMP Queries version V2 • IGMP Queries version V3 • IGMP Queries with an incorrect version • PIM or DVMRP packets The device uses the Multicast control data packets to set up the MAC address table (forwarding database) for transmitting the Multicast data packets. Possible values: • **0..2147483647 (2^{31}-1)** You use the Clear IGMP snooping data button in the **Basic Settings > Restart** dialog or the command `clear igmp-snooping` using the Command Line Interface to reset the IGMP Snooping entries, including the counter for the processed multicast control data packets.

IGMP Snooping Configuration

This dialog **Switching > IGMP Snooping > Configuration** allows you to enable the IGMP Snooping function in the device and set the function up for each port and each VLAN.

The dialog contains the following tabs:

- VLAN ID, page 202
- Port, page 204

VLAN ID

In this tab you set up the IGMP Snooping function for every VLAN.

Table

For information on how to customize the appearance of the table, see Working with tables, page 25.

The following table presents the table settings:

Setting	Description
VLAN ID	Displays the ID of the VLAN to which the table row relates.
Active	Activates/deactivates the IGMP Snooping function for this VLAN. The prerequisite is that the IGMP Snooping function is globally enabled. Possible values: • **marked** IGMP Snooping is activated for this VLAN. The VLAN has joined the Multicast data stream. • **unmarked** (default setting) IGMP Snooping is deactivated for this VLAN. The VLAN has left the Multicast data stream.
Group membership interval	Specifies the time in seconds for which a VLAN from a dynamic Multicast group remains entered in the MAC address table (forwarding database) when the device does not receive any more report data packets from the VLAN. Specify a value larger than the value in the Max. response time column. Possible values: • **2..3600** (default setting: **260**)
Max. response time	Specifies the time in seconds in which the members of a Multicast group respond to a query data packet. For their response, the members specify a random time within the response time. You thus help prevent the multicast group members from responding to the query at the same time. Specify a value smaller than the value in the Group membership interval column. Possible values: • **1..25** (default setting: **10**)
Fast leave admin mode	Activates/deactivates the Fast Leave function for this VLAN. Possible values: • **marked** When the Fast Leave function is active and the device receives an IGMP Leave message from a multicast group, the device immediately removes the entry from its MAC address table (forwarding database). • **unmarked** (default setting) When the Fast Leave function is inactive, the device first sends MAC-based queries to the members of the multicast group and removes an entry when a VLAN does not send any more report messages.

Setting	Description
MRP expiration time	Multicast Router Present Expiration Time. Specifies the time in seconds for which the device waits for a query on this port that belongs to a VLAN. When the port does not receive a query data packet, the device removes the port from the list of ports with connected multicast routers. You have the option of configuring this parameter only if the port belongs to an existing VLAN. Possible values: • **0** unlimited timeout - no expiration time • **1..3600** (default setting: **260**)
Unknown multicasts	Specifies how the device forwards data packets with unknown Multicast addresses. The prerequisite is that in the **Switching > IGMP Snooping > Multicasts** dialog, Configuration frame, Unknown multicasts option list, the **flood** radio button is selected. Possible values: • **discard** The device discards data packets with an undefined MAC Multicast address. • **flood** The device forwards data packets with an undefined MAC Multicast address to every port. • **query ports** The device forwards data packets with an undefined MAC Multicast address to the query ports. You can assign this item to a maximum of 16 VLANs in this dialog.

Port

In this tab you set up the IGMP Snooping function for every port.

Table

For information on how to customize the appearance of the table, see Working with tables, page 25.

The following table presents the table settings:

Setting	Description
Port	Displays the port number.
Active	Activates/deactivates the IGMP Snooping function on the port. The prerequisite is that the IGMP Snooping function is globally enabled. Possible values: • **marked** (default setting) IGMP Snooping is active on this port. The device includes the port in the multicast data stream. • **unmarked** IGMP Snooping is inactive on this port. The port left the multicast data stream.
Group membership interval	Specifies the time in seconds for which a port, from a dynamic multicast group, remains entered in the MAC address table (forwarding database) when the device does not receive any more report data packets from the port. Possible values: • **2..3600** (default setting: **260**) Specify the value larger than the value in the Max. response time column.
Max. response time	Specifies the time in seconds in which the members of a Multicast group respond to a query data packet. For their response, the members specify a random time within the response time. You thus help prevent the multicast group members from responding to the query at the same time. Possible values: • **1..25** (default setting: **10**) Specify a value lower than the value in the Group membership interval column.
MRP expiration time	Specifies the Multicast Router Present Expiration Time. The MRP expiration time is the time in seconds for which the device waits for a query packet on this port. When the port does not receive a query data packet, the device removes the port from the list of ports with connected multicast routers. Possible values: • **0** unlimited timeout - no expiration time • **1..3600** (default setting: **260**)
Fast leave admin mode	Activates/deactivates the Fast Leave function on the port. Possible values: • **marked** When the Fast Leave function is active and the device receives an IGMP Leave message from a multicast group, the device immediately removes the entry from its MAC address table (forwarding database). • **unmarked** (default setting) When the Fast Leave function is inactive, the device first sends MAC-based queries to the members of the multicast group and removes an entry when a port does not send any more report messages.
Static query port	Activates/deactivates the Static query port mode. Possible values: • **marked** The Static query port mode is active. The port is a static query port in the set-up VLANs. If you use the RCP function and the device operates as slave, then do not activate the Static query port mode for the ports on the secondary ring/network. • **unmarked** (default setting) The Static query port mode is inactive. The port is not a static query port. The device transmits IGMP report messages to the port only if it receives IGMP queries.
VLAN IDs	Displays the ID of the VLANs to which the table row relates.

IGMP Snooping Enhancements

This dialog **Switching > IGMP Snooping > Snooping Enhancements** allows you to select a port for a VLAN and to set up the port.

Table

For information on how to customize the appearance of the table, see Working with tables, page 25.

The following table presents the table settings:

Setting	Description
Buttons	 Wizard: Opens the Wizard window that helps you select and set up the ports. See Wizard: IGMP snooping enhancements, page 209.
VLAN ID	Displays the ID of the VLAN to which the table row relates.

Setting	Description
<Port number>	Displays for every VLAN set up in the device if the relevant port is a query port. Additionally, the field displays if the device transmits every Multicast stream in the VLAN to this port. Possible values: • **–** The port is not a query port in this VLAN. • **L** = Learned The device detected the port as a query port because the port received IGMP queries in this VLAN. The port is not a statically set up query port. • **A** = Automatic The device detected the port as a query port. The prerequisite is that you set up the port as **Learn by LLDP**. • **S** = Static (manual setting) A user specified the port as a static query port. The device transmits IGMP reports only to ports on which it previously received IGMP queries – and to statically set-up query ports. To assign this value, perform the following steps: ◦ Open the Wizard window. ◦ On the Configuration page, mark the **Static** checkbox. • **P** = Learn by LLDP (manual setting) A user specified the port as **Learn by LLDP**. With the Link Layer Discovery Protocol (LLDP), the device detects 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. ◦ On the Configuration page, mark the **Learn by LLDP** checkbox. • **F** = Forward All (manual setting) A user specified the port so that the device forwards every received Multicast stream in the VLAN to this port. Use this setting for diagnostic purposes, for example. To assign this value, perform the following steps: ◦ Open the Wizard window. ◦ On the Configuration page, mark the **Forward all** checkbox.
Display categories	Enhances the clarity of the display. The table emphasizes the cells which contain the specified value. This helps to analyze and sort the table according to your needs. Possible values: • **Learned (L)** The table displays cells which contain the value **L** and possibly further values. Cells which contain other values than **L** only, the table displays with the “**-**“ symbol. • **Static (S)** The table displays cells which contain the value **S** and possibly further values. Cells which contain other values than **S** only, the table displays with the “**-**“ symbol. • **Automatic (A)** The table displays cells which contain the value **A** and possibly further values. Cells which contain other values than **A** only, the table displays with the “**-**“ symbol. • **Learned by LLDP (P)** The table displays cells which contain the value **P** and possibly further values. Cells which contain other values than **P** only, the table displays with the “**-**“ symbol. • **Forward all (F)** The table displays cells which contain the value **F** and possibly further values. Cells which contain other values than **F** only, the table displays with the “**-**“ symbol.

Wizard: IGMP Snooping Enhancements

The Wizard window helps you select and set up the ports.

The Wizard window guides you through the following steps:

- Selection VLAN/Port, page 209
- Configuration, page 209

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

Selection VLAN/Port

The following table presents the selection VLAN/Port settings:

Setting	Description
VLAN ID	Select the VLAN ID.
Port	Select the ports.

Configuration

The following table presents the configuration settings:

Setting	Description
VLAN ID	Displays the selected VLAN ID.
Port	Displays the number of the selected ports.
Static	Specifies the port as a static query port in the set-up VLANs. The device transmits IGMP report messages to the ports at which it receives IGMP queries. This allows you to also transmit IGMP report messages to other selected ports or connected Schneider Electric devices (**Automatic**).
Learn by LLDP	Specifies the port as **Learn by LLDP**. Allows the device to 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 sends on this port every data packet with a Multicast address in the destination address field.

IGMP Snooping Querier

The device forwards a Multicast stream only to those ports to which a Multicast receiver is connected.

To detect which ports Multicast receivers are connected to, the device sends query data packets on the ports at a given interval. When a Multicast receiver is connected, it joins the Multicast stream by responding to the device with a report data packet.

This dialog **Switching > IGMP Snooping > Querier** allows you to set up the Snooping Querier settings globally and for the set-up VLANs.

Operation

The following table presents the operation setting:

Setting	Description
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.

The following table presents the configuratio settings:

Setting	Description
Protocol version	Specifies the IGMP version of the *General Query* data packets. Possible values: • **1** IGMP v1 • **2** (default setting) IGMP v2 • **3** IGMP v3
Query interval [s]	Specifies the time in seconds after which the device itself generates *General Query* data packets when it has received query data packets from the Multicast router. Possible values: • **1..1800** (default setting: **60**)
Expiry interval [s]	Specifies the time in seconds after which an active querier switches from the passive state back to the active state if it has not received any query packets for longer than specified here. Possible values: • **60..300** (default setting: **125**)

Table

In the table you specify the Snooping Querier settings for the set-up VLANs.

For information on how to customize the appearance of the table, see Working with tables, page 25.

The following table presents the table settings:

Setting	Description
VLAN ID	Displays the ID of the VLAN to which the table row relates.
Active	Activates/deactivates the IGMP Snooping Querier function for this VLAN. Possible values: • **marked** The IGMP Snooping Querier function is active for this VLAN. • **unmarked** (default setting) The IGMP Snooping Querier function is inactive for this VLAN.
Current state	Displays if the Snooping Querier is active for this VLAN. Possible values: • **marked** The Snooping Querier is active for this VLAN. • **unmarked** The Snooping Querier is inactive for this VLAN.
IP address	Specifies the IP address that the device adds as the source address in generated *General Query* data packets. You use the address of the multicast router. Possible values: • Valid IPv4 address (default setting: **0.0.0.0**)
Protocol version	Displays the Internet Group Management Protocol (IGMP) version of the *General Query* data packets. Possible values: • **1** IGMP v1 • **2** (default setting) IGMP v2 • **3** IGMP v3
Max. response time	Displays the time in seconds in which the members of a Multicast group respond to a query data packet. For their response, the members specify a random time within the response time. This helps prevent every Multicast group member to respond to the query at the same time.
Last querier address	Displays the IP address of the Multicast router from which the last received IGMP query was sent out..
Last querier version	Displays the IGMP version that the Multicast router used when sending out the last IGMP query received in this VLAN.

IGMP Snooping Multicasts

This dialog **Switching > IGMP Snooping > Multicasts** allows you to specify how it forwards data packets with **unknown Multicast** addresses: Either the device discards these data packets, floods them to every port, or forwards them only to the ports that previously received query packets.

The device also forwards the data packets with known Multicast addresses to the query ports.

Configuration

The following table presents the configuration setting:

Setting	Description
Unknown multicasts	Specifies how the device forwards data packets with unknown Multicast addresses. Possible values: • **Discard** The device discards data packets with an undefined MAC Multicast address. • **Send to all ports** (default setting) The device forwards data packets with an undefined MAC Multicast address to every port. You can overwrite this setting per VLAN. See the Unknown multicasts column in the **Switching > IGMP Snooping > Configuration** dialog, VLAN ID tab.

Table

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

For information on how to customize the appearance of the table, see Working with tables, page 25.

The following table presents the table settings:

Setting	Description
VLAN ID	Displays the ID of the VLAN to which the table row relates.
Known multicasts	Specifies how the device forwards data packets with known Multicast addresses. Possible values: • **send to query and registered ports** The device forwards data packets with a known MAC/IP Multicast address to the query ports and to the registered ports. • **send to registered ports** (default setting) The device forwards data packets with a known MAC/IP Multicast address to registered ports.

Time-Sensitive Networking

This menu **Switching > TSN > Configuration** contains the following dialogs:

- TSN Configuration, page 212
- TSN Gate Control List, page 215

TSN Configuration

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

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

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

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

Operation

The following table presents operation setting:

Setting	Description
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 greater 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

The following table presents the base time setting:

Setting	Description
DateTime[ns]	Specifies the time at which the cycle starts related to the Universal Time Coordinated (UTC). The device converts the value into the PTP time scale directly without considering the leap seconds. Possible values: • **<Day of the week, date>** (depending on the language and region settings of your computer) • **hh:mm:ss AM/PM** Hour:Minute:Second • **0..999999999 (10⁹-1)** Specifies the offset of nanoseconds. **NOTE:** When you specify the base time in the future, the cycle starts as many seconds earlier than specified in the UTC offset [s] field. See the **Time > PTP > Boundary Clock > Global** dialog.

Configuration

The following table presents the configuration setting:

Setting	Description
Cycle time [ns]	Specifies the duration of a cycle in nanoseconds. Possible values: • **50000..10000000 (10^7)** (default setting: **1000000**) 50 µs .. 10 ms

Table

For information on how to customize the appearance of the table, see Working with tables, page 25.

On devices with 16 or more ports, the TSN function is available on the following ports:

- ***1/1***..***1/8*** on a device with 16 ports
- ***1/1***..***1/12*** on a device with 20 or 24 ports

The following table presents the table settings:

Setting	Description
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. Verify 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. ◦ Verify the setting in the Operation frame. ◦ Verify 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.

TSN Gate Control List

The menu **Switching > TSN > Gate Control List** contains the following dialogs:

- TSN Configured Gate Control List, page 216
- TSN Current Gate Control List, page 217

TSN Configured Gate Control List

In this dialog **Switching > TSN > Gate Control List > Configured**, you specify the time slots of the cycle for the TSN-capable ports. Adding a table row you specify the opened gates and the duration of the time slot.

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

The dialog contains the following tabs:

- One tab for every TSN-capable port.

  The number of TSN-capable ports depends on the device.

<Port number>

Configuration

The following table presents the configuration settings:

Setting	Description
Status	Displays the template assigned to the Gate Control List. Possible values: • **-** No template. No entries are assigned to the Gate Control List. • **default 2 time slots** Template with 3 entries: ◦ First entry is the *traffic class* **7**. ◦ Second entry is the *traffic class* **6** to **0**. ◦ Third entry is a guard band. • **default 3 time slots** Template with 5 entries: ◦ First entry is the *traffic class* **7**. ◦ Second entry is a guard band. ◦ Third entry is the *traffic class* **6**. ◦ Fourth entry is the *traffic class* **5** to **0**. ◦ Fifth entry is a guard band. • **<any other template name>** The template was assigned using the Command Line Interface.
Template	Opens the Template window to assign a different template to the Gate Control List. When you select a different template and click the Ok button, the device replaces the entries in the table. From the drop-down list, you select one of the following templates: • **default 2 time slots** • **default 3 time slots** The device allows you to assign additional templates using the Command Line Interface.

Table

For information on how to customize the appearance of the table, see Working with tables, page 25.

The following table presents the table settings:

Setting	Description
Buttons	Delete: Deletes the selected table row.
Index	Displays the index number of the entry in the Gate Control List, which specifies the chronological order of the timeslots.
Gate states	Specifies the opened gates in case the TSN function on the port is active. • The data packets whose *traffic class* is assigned to a selected gate are selected for transmission – Gate state *OPEN*. • The data packets whose *traffic class* is assigned to a not selected gate are not selected for transmission – Gate state *CLOSED*. Possible values: • **-** (default setting) No gate selected. The device does not open any gate on the port during the time slot is processed. From the drop-down list, unselect every gate. • **0..7** The device opens the selected gates on the port during the time slot is processed. From the drop-down list, select one or more items. You assign the VLAN priorities to a *traffic class* in the **Switching > QoS/Priority > 802.1D/p Mapping** dialog.
Interval [ns]	Specifies the duration of the time slot in nanoseconds. Possible values: • **1000..10000000 (10^7)** 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 ◦ The sum of the time slots must be 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.

TSN Current Gate Control List

In this dialog **Switching > TSN > Gate Control List > Current**, you monitor the settings of the cycle for the TSN-capable ports. Every table row represents a specified time slot.

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

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

The dialog contains the following tabs:

- One tab for every TSN-capable port.

  The number of TSN-capable ports depends on the device.

<Port number>

Table

For information on how to customize the appearance of the table, see Working with tables, page 25.

The following table presents the table settings:

Setting	Description
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.

MRP-IEEE

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

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

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

The menu **Switching > MRP-IEEE** contains the following dialogs:

- MRP-IEEE Configuration, page 218
- MRP-IEEE Multiple MAC Registration Protocol, page 219
- MRP-IEEE Multiple VLAN Registration Protocol, page 222

MRP-IEEE Configuration

This dialog **Switching > MRP-IEEE > Configuration** allows you to set the various MRP-IEEE timers. By maintaining a relationship between the various timer values, the protocol operates efficiently and with less likelihood of unnecessary attribute withdrawals and re-registrations. The default timer values effectively maintain these relationships.

When you reconfigure the timers, maintain the following relationships:

- To allow for re-registration after a *Leave* or *LeaveAll* event, even if there is a lost message, specify the *Leave* timer value **≥ (2x JoinTime) + 60**.
- To minimize the volume of *Rejoin* data packets the device generates following a *LeaveAll* event, specify the value for the *LeaveAll* timer larger than the *Leave* timer value.

Table

For information on how to customize the appearance of the table, see Working with tables, page 25.

The following table presents the table settings:

Setting	Description
Port	Displays the port number.
Join time [1/100s]	Specifies the *Join* timer which controls the interval between transmit opportunities applied to the Applicant state machine. Possible values: • **10..100** (default setting: **20**)
Leave time [1/100s]	Specifies the *Leave* timer which controls the period that the Registrar state machine waits in the *Leave (LV)* state before transitioning to the *Empty (MT)* state. Possible values: • **20..600** (default setting: **60**)
Leave all time [1/100s]	Specifies the *LeaveAll* timer which controls the frequency with which the *LeaveAll* state machine generates *LeaveAll* PDUs. Possible values: • **200..6000** (default setting: **1000**)

MRP-IEEE Multiple MAC Registration Protocol

The Multiple MAC Registration Protocol (MMRP) allows end devices and MAC switches to 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 allows you to 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 **Switching > MRP-IEEE > MMRP** contains the following tabs:

- Configuration, page 219
- Service requirement, page 221
- Statistics, page 221

Configuration

In this tab you select active MMRP port participants and set the device to transmit periodic events. The dialog also allows you to 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

The following table presents the operation setting:

Setting	Description
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

The following table presents the configuration setting:

Setting	Description
Periodic state machine	Enables/disables the global periodic state machine in the device. Possible values: • **On** With MMRP Operation enabled globally, the device transmits MMRP messages in one-second intervals, on MMRP participating ports. • **Off** (default setting) Disables the periodic state machine in the device.

Table

For information on how to customize the appearance of the table, see Working with tables, page 25.

The following table presents the table settings:

Setting	Description
Port	Displays the port number.
Active	Activates/deactivates the port MMRP participation. Possible values: • **marked** (default setting) With MMRP enabled globally and on this port, the device sends and receives MMRP messages on this port. • **unmarked** Disables the port MMRP participation.
Restricted group registration	Activates/deactivates the restriction of dynamic MAC address registration using MMRP on the port. Possible values: • **marked** If enabled and a static filter entry for the MAC address exists on the VLAN concerned, then the device registers the MAC address attributes dynamically. • **unmarked** (default setting) Activates/deactivates the restriction of dynamic MAC address registration using MMRP on the port.

Service requirement

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

A port is setup only as **ForwardAll** or **Forbidden**.

Table

For information on how to customize the appearance of the table, see Working with tables, page 25.

The following table presents the table settings:

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

Statistics

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

Information

The following table presents information settings:

Setting	Description
Buttons	Reset statistics: Resets the port statistics counters and the values in the Last received MAC address column.
Transmitted MMRP PDU	Displays the number of MMRPDUs transmitted in the device.
Received MMRP PDU	Displays the number of MMRPDUs received in the device.
Received bad header PDU	Displays the number of MMRPDUs received with a bad header in the device.
Received bad format PDU	Displays the number of MMRPDUs with a bad data field that were not transmitted in the device.
Transmission failed	Displays the number of MMRPDUs not transmitted in the device.

Table

For information on how to customize the appearance of the table, see Working with tables, page 25.

The following table presents table settings:

Setting	Description
Port	Displays the port number.
Transmitted MMRP PDU	Displays the number of MMRPDUs transmitted on the port.
Received MMRP PDU	Displays the number of MMRPDUs received on the port.
Received bad header PDU	Displays the number of MMRPDUs with a bad header that were received on the port.
Received bad format PDU	Displays the number of MMRPDUs with a bad data field that were not transmitted on the port.
Transmission failed	Displays the number of MMRPDUs not transmitted on the port.
Last received MAC address	Displays the MAC address from which the port last received MMRPDUs.

MRP-IEEE Multiple VLAN Registration Protocol

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

The dialog **Switching > MRP-IEEE > MVRP** contains the following tabs:

- Configuration, page 223
- Statistics, page 224

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

The following table presents the operation setting:

Setting	Description
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

The following table presents the configuration setting:

Setting	Description
Periodic state machine	Enables/disables the periodic state machine in the device. Possible values: • **On** The periodic state machine is enabled. With MVRP Operation enabled globally, the device transmits MVRP periodic events every 1 s, on MVRP participating ports. • **Off** (default setting) The periodic state machine is disabled. Disables the periodic state machine in the device.

Table

For information on how to customize the appearance of the table, see Working with tables, page 25.

The following table presents the table settings:

Setting	Description
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 allows you to add a dynamic VLAN for this entry. • **unmarked** (default setting) Disables the Restricted VLAN registration function on this port.

Statistics

Devices on a LAN exchange Multiple VLAN Registration Protocol Data Units (MVRPDUs) to maintain statuses of VLANs on active ports. This tab allows you to monitor the MVRP data packets.

Information

The following table presents the information settings:

Setting	Description
Buttons	Reset statistics: Resets the port statistics counters and the values in the Last received MAC address column.
Transmitted MVRP PDU	Displays the number of MVRPDUs transmitted in the device.
Received MVRP PDU	Displays the number of MVRPDUs received in the device.
Received bad header PDU	Displays the number of MVRPDUs received with a bad header in the device.
Received bad format PDU	Displays the number of MVRPDUs with a bad data field that the device blocked.
Transmission failed	Displays the number of detected failures while adding a message into the MVRP queue.
Message queue failures	Displays the number of MVRPDUs that the device blocked.

Table

For information on how to customize the appearance of the table, see Working with tables, page 25.

The following table presents the table settings:

Setting	Description
Port	Displays the port number.
Transmitted MVRP PDU	Displays the number of MVRPDUs transmitted on the port.
Received MVRP PDU	Displays the number of MVRPDUs received on the port.
Received bad header PDU	Displays the number of MVRPDUs with a bad header that the device received on the port.
Received bad format PDU	Displays the number of MVRPDUs with a bad data field that the device blocked on the port.
Transmission failed	Displays the number of MVRPDUs that the device blocked on the port.
Registrations failed	Displays the number of unsuccessful registration attempts on the port.
Last received MAC address	Displays the MAC address from which the port last received MVRPDUs.

GARP

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

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

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

The menu **Switchting > GARP** contains the following dialogs:

- GMRP, page 225
- GVRP, page 227

GMRP

Switching > GARP > GMPR

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 allwos the devices to distribute the information across the network devices that support extended filtering services.

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

Operation

The following table presents the operation setting:

Setting	Description
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

The following table presents the multicasts setting:

Setting	Description
Unknown multicasts	Enables/disables the unknown multicast data to be either flooded or discarded. Possible values: • **discard** The device discards unknown multicast data. • **flood** (default setting) The device forwards unknown multicast data to every port.

Table

For information on how to customize the appearance of the table, see Working with tables, page 25.

The following table presents table settings:

Setting	Description
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.

GVRP

Switching > GARP > GVRP

The GARP VLAN Registration Protocol or Generic VLAN Registration Protocol (GVRP) is a protocol that facilitates control of Virtual Local Area Networks (VLANs) within a larger network. GVRP is a Layer 2 network protocol, used to automatically set up devices in a VLAN network.

GVRP is a GARP application that provides IEEE 802.1Q-compliant VLAN pruning, and setting up dynamic VLAN on 802.1Q trunk ports. With GVRP, the device exchanges VLAN configuration information with other GVRP devices. Thus, the device reduces the unnecessary broadcast and undefined unicast traffic. Exchanging VLAN configuration information also allows you to dynamically add and manage VLANs connected through the 802.1Q trunk ports.

Operation

The following table presents the operation setting:

Setting	Description
Operation	Enables/disables the GVRP function globally in the device. The device participates in GVRP message exchanges. If the function is disabled, then the device ignores GVRP messages. Possible values: • **On** The GVRP function is enabled. • **Off** (default setting) The GVRP function is disabled.

Table

For information on how to customize the appearance of the table, see Working with tables, page 25.

The following table presents the table settings:

Setting	Description
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.

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 greater 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.

This menu **Switching > QoS/Priority** contains the following dialogs:

- QoS/Priority Global, page 228
- QoS/Priority Port Configuration, page 229
- 802.1D/p Mapping, page 229
- IP DSCP Mapping, page 231
- Queue Management, page 232

QoS/Priority Global

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

Configuration

The following table presents the configuration settings:

Setting	Description
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).

QoS/Priority Port Configuration

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

Table

For information on how to customize the appearance of the table, see Working with tables, page 25.

The following table presents the table settings:

Setting	Description
Port	Displays the port number.
Port priority	Specifies what VLAN priority information the device writes into a data packet if the data packet contains no priority information. After this, the device forwards the data packet depending on the value specified in the Trust mode column. Possible values: • **0..7** (default setting: **0**)
Trust mode	Specifies how the device handles a received data packet if the data packet contains QoS/priority information. Possible values: • **untrusted** The device forwards the data packet according to the priority specified in the Port priority column. The device ignores the priority information contained in the data packet. In the **Switching > QoS/Priority > 802.1D/p Mapping** dialog, you assign a *traffic class* to every VLAN priority. • **trustDot1p** (default setting) The device forwards the data packet according to the priority information in the VLAN tag. In the **Switching > QoS/Priority > 802.1D/p Mapping** dialog, you assign a *traffic class* to every VLAN priority. • **trustIpDscp** ◦ If the data packet is an IP packet, then: The device forwards the data packet according to the IP DSCP value contained in the data packet. In the **Switching > QoS/Priority > IP DSCP Mapping** dialog you assign a *traffic class* to every IP DSCP value. ◦ If the data packet is not an IP packet, then: The device forwards the data packet according to the priority specified in the Port priority column. In the **Switching > QoS/Priority > 802.1D/p Mapping** dialog, you assign a *traffic class* to every VLAN priority.
Untrusted traffic class	Displays the *traffic class* assigned to the VLAN priority information specified in the Port priority column. In the **Switching > QoS/Priority > 802.1D/p Mapping** dialog, you assign a *traffic class* to every VLAN priority. Possible values: • **0..7**

802.1D/p Mapping

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

In this dialog **Switching > QoS/Priority > 802.1D/p Mapping**, you assign a *traffic class* to every VLAN priority. You assign the *traffic classes* to the priority queues of the ports.

Table

For information on how to customize the appearance of the table, see Working with tables, page 25.

The following table presents the table settings:

Setting	Description
VLAN priority	Displays the VLAN priority.
Traffic class	Specifies the *traffic class* assigned to the VLAN priority. Possible values: • **0..7** **0** assigned to the priority queue with the lowest priority. **7** assigned to the priority queue with the highest priority. **NOTE:** Among other things redundancy mechanisms use the highest *traffic class*. Therefore, select another *traffic class* for application data.

Default Assignment of the VLAN Priority to *Traffic Classes*

The following table presents the default mapping between VLAN priorities and traffic classes according to IEEE 802.1D:

VLAN Priority	*Traffic class*	Content description according to IEEE 802.1D
0	2	**Best Effort** Normal data without prioritizing
1	0	**Background** Non-time-sensitive data and background services
2	1	**Standard** Normal data
3	3	**Excellent Effort** Crucial data
4	4	**Controlled Load** Time-sensitive data with a high priority
5	5	**Video** Video transmission with delays and jitter <100 ms
6	6	**Voice** Voice transmission with delays and jitter <10 ms
7	7	**Network Control** Data for network management and redundancy mechanisms

IP DSCP Mapping

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

In this dialog **Switching > QoS/Priority > IP DSCP Mapping**, you assign a *traffic class* to every DSCP value. You assign the *traffic classes* to the priority queues of the ports.

Table

For information on how to customize the appearance of the table, see Working with tables, page 25.

The following table presents the table settings:

Setting	Description
DSCP value	Displays the DSCP value.
Traffic class	Specifies the *traffic class* which is assigned to the DSCP value. Possible values: • **0..7** **0** assigned to the priority queue with the lowest priority. **7** assigned to the priority queue with the highest priority.

Default Assignment of the DSCP Values to *Traffic Classes*

The following table lists the default DSCP values, their names, and the associated traffic classes:

DSCP Value	DSCP Name	*Traffic class*
0	Best Effort /CS0	2
1-7		2
8	CS1	0
9,11,13,15		0
10,12,14	AF11,AF12,AF13	0
16	CS2	1
17,19,21,23		1
18,20,22	AF21,AF22,AF23	1
24	CS3	3
25,27,29,31		3
26,28,30	AF31,AF32,AF33	3
32	CS4	4
33,35,37,39		4
34,36,38	AF41,AF42,AF43	4
40	CS5	5
41,42,43,44,45,47		5
46	EF	5
48	CS6	6
49-55		6
56	CS7	7
57-63		7

Queue Management

This dialog **Switching > QoS/Priority > Queue Management** allows you to enable and disable the Strict priority function for the *traffic classes*. When you disable the Strict priority function, the device processes the priority queues of the ports with *Weighted Fair Queuing*.

You also have the option of assigning a minimum bandwidths to every *traffic classes* which the device uses to process the priority queues with *Weighted Fair Queuing*.

Table

For information on how to customize the appearance of the table, see Working with tables, page 25.

The following table presents the table settings:

Setting	Description
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 greater 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 greater 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 allows you to limit the rate of a strict high-priority queue. Limiting a strict high-priority queue allows the device also to process low-priority queues. To use queue shaping, you set the maximum bandwidth for a particular queue.

VLAN

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

- High flexibility
  - With VLAN you distribute the data packets to logical networks in the existing infrastructure. Without VLAN, it would be necessary to have additional devices and complicated cabling.
  - With VLAN you specify network segments independently of the location of the individual end devices.
- Improved throughput
  - In VLANs data packets can be transferred by priority.

    When the priority is high, the device transfers the data of a VLAN preferentially, for example for time-sensitive applications such as VoIP phone calls.
  - When the data packets and Broadcasts are distributed in small network segments instead of in the entire network, the network load is considerably reduced.
- Increased security

  The distribution of the data packets among individual logical networks makes unwanted accessing more difficult and strengthens the system against attacks such as MAC Flooding or MAC Spoofing.

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

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

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

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

- Private VLAN
- Voice VLAN
- Port-based VLAN

The menu **Switching > VLAN** contains the following dialogs:

- VLAN Global, page 234
- VLAN Configuration, page 235
- VLAN Port, page 237
- VLAN Voice, page 238
- Private VLAN, page 241

VLAN Global

This dialog **Switching > VLAN > Global** allows you to view general VLAN parameters for the device.

Configuration

The following table presents the configuration settings:

Setting	Description
Buttons	Reset VLAN settings: Resets the VLAN settings of the device to the default setting.
Max. VLAN ID	Highest ID assignable to a VLAN. See the **Switching > VLAN > Configuration** dialog.
VLANs (max.)	Displays the maximum number of VLANs possible. See the **Switching > VLAN > Configuration** dialog.
VLANs	Number of VLANs currently set up in the device. See the **Switching > VLAN > Configuration** dialog. The VLAN 1 is permanently set up in the device.

VLAN Configuration

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

You distinguish between the following VLANs:

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

  For the following functions the device sets up dynamic VLANs:

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

Table

For information on how to customize the appearance of the table, see Working with tables, page 25.

The following table presents the table settings:

Setting	Description
Buttons	The following list presents the icon descriptions: •  Add: Opens the Create window to add a table row. In the VLAN ID field, you specify the VLAN ID. •  Remove: Removes the selected table row.
VLAN ID	ID of the VLAN. The device supports up to 128 VLANs simultaneously set up. Possible values: • **1..4042**
Status	Displays how the VLAN is set up. Possible values: • **other** VLAN **1** or VLAN set up using the 802.1X function. See the **Network Security > 802.1X** dialog. • **permanent** VLAN set up by the user. or VLAN set up using the MRP function. See the **Switching > L2-Redundancy > MRP** dialog. If you save the settings in the non-volatile memory, then the VLANs with this setting remain set up after a restart. • **dynamicMvrp** VLAN set up using the MVRP function. See the **Switching > MRP-IEEE > MVRP** dialog. VLANs with this setting are write-protected. The device removes a VLAN from the table as soon as the last port leaves the VLAN.
Name	Specifies the name of the VLAN. Possible values: • Alphanumeric ASCII character string with 0..32 characters

Setting	Description
RSPAN VLAN	Specifies the VLAN as the RSPAN VLAN. Possible values: • **marked** The device uses the VLAN exclusively to send the RSPAN data packets in the direction of the *Destination port* of the *Destination switch*. See the **Diagnostics > Ports > RSPAN** dialog. Do not use the VLAN for any other purposes. The device disables source MAC address learning in the VLAN. • **unmarked** (default setting) The device does not use the VLAN to send RSPAN data packets.
<Port number>	Specifies if the respective port transmits data packets of the VLAN and if the data packets contain a VLAN tag. Possible values: • **-** (default setting) The port is not a member of the VLAN and does not transmit data packets of the VLAN. • **T** = Tagged The port is a member of the VLAN and transmits the data packets with a VLAN tag. You use this setting for uplink ports, for example. • **LT** = Tagged Learned The port is a member of the VLAN and transmits the data packets with a VLAN tag. The device has automatically set up the entry based on the GVRP or MVRP function. • **F** = Forbidden The port is not a member of the VLAN and does not transmit data packets of this VLAN. Additionally, the device helps prevent the port from becoming a VLAN member through the MVRP function. • **U** = Untagged (default setting for VLAN 1) The port is a member of the VLAN and transmits the data packets without a VLAN tag. Use this setting if the connected device does not evaluate any VLAN tags, for example on end ports. • **LU** = Untagged Learned The port is a member of the VLAN and transmits the data packets without a VLAN tag. The device has automatically set up the entry based on the GVRP or MVRP function.

VLAN Port

In this dialog **Switching > VLAN > Port**, 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 allows you to assign a VLAN to the ports and thus specify the port VLAN ID.

Additionally, you also specify for each port how the device forwards data packets and one of the following situations occurs:

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

Table

For information on how to customize the appearance of the table, see Working with tables, page 25.

The following table presents the table settings:

Setting	Description
Port	Displays the port number.
Port-VLAN ID	Specifies the VLAN ID which the device assigns to data packets received without a VLAN tag. Prerequisites: • The port does not belong to a private VLAN. • In the Acceptable packet types column, the value **admitAll** is specified. Possible values: • **1..4042** (default setting: **1**) A VLAN you set up. If you use the MRP function and you did not assign a VLAN to the ring ports, then 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. The prerequisite is that the port does not operate in a private VLAN. Possible values: • **marked** The ingress filtering is active. The device compares the VLAN ID in the data packet with the VLANs of which the port is a member. See the **Switching > VLAN > Configuration** dialog. If the VLAN ID in the data packet matches one of these VLANs, then the device forwards the data packet. Otherwise, the device discards the data packet. • **unmarked** (default setting) The ingress filtering is inactive. The device forwards received data packets without comparing the VLAN ID. Thus, the device also forwards data packets in VLANs in which the port is not a member.

VLAN Voice

Switching > VLAN > Voice

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

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

Another benefit of the Voice VLAN feature is that the VoIP phone obtains VLAN ID or priority information from the device using LLDP-MED. As a result, the VoIP

phone sends voice data packets with VLAN tag, priority tag or untagged. This depends on the specified Voice VLAN Interface mode. You activate Voice VLAN on the port which is connecting to the VoIP phone.

Operation

The following table presents the operation setting:

Setting	Description
Operation	Enables/disables the Voice function of the device globally. Possible values: • **On** • **Off** (default setting)

Table

For information on how to customize the appearance of the table, see Working with tables, page 25.

The following table presents the table settings:

Setting	Description
Port	Displays the port number.
Voice VLAN mode	Specifies if the port transmits or discards received data packets without voice VLAN tagging or with voice VLAN priority information. Possible values: • **disabled** (default setting) Deactivates the Voice function for this table row. • **none** Allows the IP telephone to use its own configuration for sending untagged voice data packets. • **vlan/dot1p-priority** The port filters data packets of the voice VLAN using the vlan and dot1p priority tags. • **untagged** The port filters data packets without a voice VLAN tag. • **vlan** The port filters data packets of the voice VLAN using the vlan tag. • **dot1p-priority** The port filters data packets of the voice VLAN using the dot1p priority tags. If you select this value, then additionally specify a proper value in the Priority column.
Data priority mode	Specifies the trust mode for the data packets on the particular port. The device uses this mode for data packets on the voice VLAN, when it detects a VoIP telephone and a PC using the same cable for transmitting data. Possible values: • **marked** (default setting) If voice data packets are present on the interface, then the data packets have the normal priority. • **unmarked** If voice data packets are present and the value **dot1p-priority** is specified in the Voice VLAN mode column, then the data packets have the priority **0**. If the interface only transmits data, then the data has the normal priority.
Status	Displays the status of the Voice VLAN on the port. Possible values: • **marked** The Voice VLAN is enabled. • **unmarked** The Voice VLAN is disabled.
VLAN ID	Specifies the VLAN ID to which the table row relates. To forward data packets to this VLAN using this filter, select in the Voice VLAN mode column the value **vlan**. Possible values: • **1..4042** (default setting: **0**)
Priority	Specifies the Voice VLAN Priority of the port. Prerequisites: • The port does not belong to a private VLAN. • In the Voice VLAN mode column, the value **dot1p-priority** is specified. Possible values: • **0..7** • **none** Deactivates the Voice VLAN Priority of the port.

Setting	Description
DSCP	Specifies the IP DSCP value. Possible values: • **0 (be/cs0)..63** (default setting: **0 (be/cs0)**) Some values in the list also have a DSCP keyword, for example **0 (be/cs0)**, **10 (af11)** and **46 (ef)**. These values are compatible with the *IP Precedence* model. In the **Switching > QoS/Priority > IP DSCP Mapping** dialog you assign a *traffic class* to every IP DSCP value.
Bypass authentication	Activates the Voice VLAN Authentication mode. If you deactivate the function and set the value in the Voice VLAN mode column to **dot1p-priority**, then voice devices require an authentication. Possible values: • **marked** (default setting) If you activated the function in the **Network Security > 802.1X > Global** dialog, then set the Port control parameter for this port to the **multiClient** value before activating this function. You find the Port control parameter in the **Network Security > 802.1X > Global** dialog. • **unmarked**

Private VLAN

In this dialog **Switching > VLAN > Private VLAN**, you set up private VLANs.

A private VLAN separates a regular VLAN into 2 or more smaller domains. This helps to provide privacy but allows the connected end devices to communicate with the same destination. Each private VLAN has one *primary* VLAN and one or more *secondary* VLANs (*isolated* or *community*).

In a private VLAN, the device controls the data stream between specific ports. The device forwards untagged data packets only. The device allows you to isolate the ports within the private VLAN and restrict them from communicating with each other.

The dialog contains the following tabs:

- VLAN type, page 241
- VLAN association, page 242
- Port association, page 242

VLAN Type

In this tab you specify for the VLANs set up in the device which role they perform in the private VLAN. See the **Switching > VLAN > Configuration** dialog.

Table

For information on how to customize the appearance of the table, see Working with tables, page 25.

The following table presents the table settings:

Setting	Description
VLAN ID	Displays the VLAN ID.
VLAN type	Specifies the role of the port in the private VLAN. Possible values: • **primary** The *primary* VLAN is the unique identifier of the entire private VLAN including its *secondary* VLANs. The ports participating in a private VLAN are automatically members of the *primary* VLAN. • **isolated** The ports you want to be isolated from other ports are members of the *isolated* (*secondary*) VLAN. The ports can communicate with the *promiscuous* port but cannot communicate with each other. In the VLAN association tab, you can associate only one *isolated* VLAN to a *primary* VLAN. • **community** The ports associated with the *community* (*secondary*) VLAN can communicate with the *promiscuous* port as well as with each other. In the VLAN association tab, you can associate multiple *community* VLANs to a *primary* VLAN. • **unconfigured** (default setting) The VLAN is not part of a private VLAN. If you want the VLAN not to be part of the private VLAN, select this item.

VLAN Association

In this tab you specify the subdomains by associating *community* or *isolated* VLANs with a *primary* VLAN. The device allows you to set up a maximum of 20 subdomains.

Table

For information on how to customize the appearance of the table, see Working with tables, page 25.

The following table presents the table settings:

Setting	Description
Primary	Displays the VLANs for which you have specified the role **primary** in the VLAN type tab.
Secondary	Specifies the *community* or *isolated* VLANs you associate with the *primary* VLAN. Possible values: • **<VLAN IDs>** The device lets you associate: ◦ One *isolated* VLAN or ◦ One or more *community* VLANs To remove a VLAN from the association, delete the corresponding ID from the field.

Port Association

In this tab you specify which physical ports are members of a private VLAN and the role of the ports in the private VLAN.

Table

For information on how to customize the appearance of the table, see Working with tables, page 25.

The following table presents the table settings:

Setting	Description
Port	Displays the number of the physical port.
Switchport mode	Specifies the role of the port in the private VLAN. Possible values: • **host** The port performs as a *host* port in the private VLAN. • **promiscuous** The port performs as a *promiscuous* port in the private VLAN. • **general** (default setting) The port does not belong to a private VLAN. If you want the port not to be part of a private VLAN, select this item. If a port operates in a private VLAN, then changing the following settings for this port has no effect: • Port-VLAN ID column, see the **Switching > VLAN > Port** dialog • Acceptable packet types column, see the **Switching > VLAN > Port** dialog • Ingress filtering column, see the **Switching > VLAN > Port** dialog • Priority column, see the **Switching > VLAN > Voice** dialog
Host primary	Specifies the *primary* VLAN to be associated when the port performs as a *host* port in the private VLAN. The drop-down list contains the IDs of the *primary* VLANs specified in the VLAN type tab. Possible values: • **<VLAN IDs>** Select an item from the drop-down list.
Host secondary	Specifies the *secondary* VLAN to be associated when the port performs as a *host* port in the private VLAN. The drop-down list contains the IDs of the *isolated* and *community* VLANs specified in the VLAN type tab. Possible values: • **<VLAN IDs>** Select an item from the drop-down list.
Promiscuous primary	Specifies the *primary* VLAN to be associated when the port performs as a *promiscuous* port in the private VLAN. The drop-down list contains the IDs of the *primary* VLANs specified in the VLAN type tab. Possible values: • **<VLAN IDs>** Select an item from the drop-down list.
Promiscuous secondary	Specifies the *secondary* VLAN to be associated when the port performs as a *promiscuous* port in the private VLAN. The drop-down list contains the IDs of the *isolated* and *community* VLANs specified in the VLAN type tab. Possible values: • **<VLAN IDs>** The device allows you to associate: ◦ One *isolated* VLAN or ◦ One or more *community* VLANs To remove a VLAN from the association, delete the corresponding ID from the field.

L2-Redundancy

This menu **Switching > L2–Redundancy** contains the following dialogs:

- MRP, page 244
- HIPER Ring, page 247
- Spanning Tree, page 249
- Link Aggregation, page 269
- Link Backup, page 276
- FuseNet, page 278

MRP

Switching > L2–Redundancy > MRP

Loops during the configuration phase may lead to unintended equipment operation.

⚠WARNING

UNINTENDED EQUIPMENT OPERATION

- Set up each device of the MRP configuration individually.
- Complete the configuration of the other devices of the ring configuration before you connect the redundant lines.

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

The Media Redundancy Protocol (MRP) is a protocol that allows you to 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 Media Redundancy Protocol (MRP) according to IEC 62439.

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

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

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

When you work with oversized Ethernet packets (the value in the MTU column for the port is >**1518**, see the **Basic Settings > Port** dialog), the switching time of the MRP Ring reconfiguration depends on the following parameters:

- Bandwidth of the ring line
- Size of the Ethernet packets
- Number of devices in the ring

Set the recovery time sufficiently large to help avoid delays in the MRP packages due to latencies in the devices. You can find the formula for calculating the switching time in IEC 62439-2, section 9.5.

Operation

The following table presents the operation settings:

Setting	Description
Buttons	Delete ring configuration: Disables the redundancy function and resets the settings in the dialog to the default setting.
Operation	Enables/disables the MRP function. After you set up the parameters for the MRP Ring, enable the function here. Possible values: • **On** The MRP function is enabled. After you set up the devices in the MRP Ring, the redundancy is active. • **Off** (default setting) The MRP function is disabled.

Ring Port 1/Ring Port 2

The following table presents the ring port 1/Ring port 2 settings:

Setting	Description
Port	Specifies the port that operates as a ring port. Possible values: • **<Port number>**
Operation	Displays the operating status of the ring port. Possible values: • **forwarding** The port is enabled, connection exists. • **blocked** The port is blocked, connection exists. • **disabled** The port is disabled. • **not-connected** No connection exists.
Fixed backup	Activates/deactivates the *Backup port* function for the Ring port 2. **NOTE:** The switch over to the *Primary port* can exceed the maximum ring recovery time. Possible values: • **marked** The Ring port 2 backup function is active. When the ring is closed, the *Ring Manager* device reverts back to the primary ring port. • **unmarked** (default setting) The Ring port 2 backup function is inactive. When the ring is closed, the *Ring Manager* device continues to send data on the secondary ring port.

Configuration

The following table presents configuration settings:

Setting	Description
Ring manager	Enables/disables the Ring manager function. If there is one device at each end of the line, then you activate this function. Possible values: • **On** The Ring manager function is enabled. The device operates in the *Ring Manager* mode. **⚠WARNING** **UNINTENDED EQUIPMENT OPERATION** Do not enable the **Ring manager** function on a device on which the **RCP** function is enabled. **Failure to follow these instructions can result in death, serious injury, or equipment damage.** • **Off** (default setting) The Ring manager function is disabled. The device operates exclusively in the *Ring Client* mode.
Domain name	Specifies the name of the MRP domain that the device belongs to. Possible values: • Alphanumeric ASCII character string with 0..255 characters You can specify any name. By entering a descriptive name, you can simplify the administration of MRP domains.
Ring recovery	Specifies the maximum recovery time in milliseconds for reconfiguration of the ring. This setting is effective only if the device operates in the *Ring Manager* mode. Possible values: • **500ms** • **200ms** (default setting) Shorter switching times make greater demands on the response time of every individual device in the ring. Use values lower than **500ms** if the other devices in the ring also support this shorter recovery time. When you are working with oversized Ethernet packets, the number of devices in the ring is limited. The switching time depends on several parameters. See the preceding description.
VLAN ID	Specifies the VLAN ID which you assign to the ring ports. Possible values: • **0** (default setting) No VLAN assigned. In the **Switching > VLAN > Configuration** dialog, assign for VLAN **1** the value **U** to the ring ports. • **1..4042** VLAN assigned. If you assign a non-existing VLAN to the ring ports, then the device automatically sets up this VLAN. In the **Switching > VLAN > Configuration** dialog, the device adds a table row for the VLAN and assigns the value **T** to the ring ports.

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

Information

The following table presents the information settings:

Setting	Description
Information	Displays the status of the ring. Possible values: • **Redundancy available. Ring is closed.** Normal operation. The components in the ring operate as intended. • **Configuration error: Error on ring port link.** The device has detected a link error on a ring port. Verify that the correct port is selected in the Ring port 1 and Ring port 2 frames. • **Redundancy not available. Ring is open. Check the Ring clients.** The device has not detected a configuration error, but no redundancy is available. • **Redundancy not available. At least one ring port is disabled.** At least one of the ring ports is disabled. Verify that both ring ports are enabled. See the **Basic Settings > Port** dialog. • **Configuration error: Packets from another ring manager received.** Another device exists in the ring that operates in the *Ring Manager* mode. Enable the Ring manager function only on one device in the ring. • Configuration error: Ring link is connected to wrong port. A line in the ring is connected with a different port instead of with a ring port. The device only receives test data packets on one of the ring ports.
Last time the ring was open	Displays the date and time at which the device last detected an open ring. The field displays a valid value if the device operates in the *Ring Manager* mode.
Number of times the ring was open	Displays the number of times the device has detected an open ring. The field displays a valid value if the device operates in the *Ring Manager* mode.

HIPER Ring

Switching > L2–Redundancy > HIPER Ring

Loops during the configuration phase may lead to unintended equipment operation.

⚠WARNING

UNINTENDED EQUIPMENT OPERATION

- Set up each device of the HIPER Ring configuration individually.
- Complete the configuration of the other devices of the ring configuration before you connect the redundant lines.

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. The device operates exclusively in the *Ring Client* mode. This function allows you to extend an existing HIPER Ring or to replace a device already participating as a *Ring Client* in a HIPER Ring.

A HIPER Ring contains a *Ring Manager (RM)* device which controls the ring. The *Ring Manager* device sends watchdog packets into the ring on both the primary and secondary ports. When the *Ring Manager* device receives the watchdog packets on both ports, the *Primary port* remains in the **forwarding** state and the secondary port remains in the **discarding** state.

The device operates exclusively in the *Ring Client* mode. This means that the device detects watchdog packets on its ring ports and sends a *Link Down* or *Link Up* packet to the *Ring Manager* device when the link status changes.

The device only supports Fast Ethernet and Gigabit Ethernet ports as ring ports. Furthermore, the device only supports HIPER Ring in VLAN **1**.

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

NOTE:

Set up the devices of the HIPER Ring individually. Before you connect the redundant link, complete the setup of every device of the HIPER Ring. You thus help avoid loops during the configuration phase.

Operation

The following table presents the operation setting:

Setting	Description
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

The following table presents the ring port 1/ring port 2 settings:

Setting	Description
Port	Specifies the port number of the primary/secondary ring port. Possible values: • **-** (default setting) No primary/secondary ring port selected. • **<Port number>** Number of the ring port
State	Displays the state of the primary/secondary ring port. Possible values: • **not-available** The HIPER Ring client is disabled. or No primary or secondary ring port selected. • **active** The ring port is enabled and logically up. • **inactive** No link available on the ring port. As soon as the link on a ring port is interrupted, the device sends a *Link Down* packet to the *Ring Manager* device on the other ring port.

Information

The following table presents information setting:

Setting	Description
Mode	Displays that the device operates in the *Ring Client* mode.

Spanning Tree

Loops during the configuration phase may lead to unintended equipment operation.

⚠WARNING

UNINTENDED EQUIPMENT OPERATION

- Set up each device of the Spanning Tree configuration individually.
- Complete the configuration of the other devices of the Spanning Tree configuration before you connect the redundant lines.

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 to help avoid loops. If a network component becomes inoperable on the path, then the device calculates the new topology and reactivates these paths.

The Rapid Spanning Tree Protocol (RSTP) enables fast switching to a newly calculated topology without interrupting existing connections. RSTP gets average reconfiguration times of less than a second. When you use RSTP in a ring with 10 to 20 devices, you can get reconfiguration times in the order of milliseconds.

The device supports the Multiple Spanning Tree Protocol (MSTP) standardized in IEEE 802.1, which is a further development of the Spanning Tree Protocol (STP).

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

This menu **Switching > L2-Redundancy > Spanning Tree** contains the following dialogs:

- Spanning Tree Global, page 250
- Spanning Tree MSTP, page 256
- Spanning Tree Port, page 261

Spanning Tree Global

In this dialog **Switching > L2-Redundancy > Spanning Tree > Global**, you enable/disable the Spanning Tree function and specify the bridge settings.

Operation

The following table presents the operation setting:

Setting	Description
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

The following table presents the variant setting:

Setting	Description
Variant	Specifies the protocol used for the Spanning Tree function: Possible values: • **rstp** (default setting) The protocol **RSTP** is active. With RSTP (IEEE 802.1Q-2005), the Spanning Tree function operates for the underlying physical layer. • **mstp** The protocol **MSTP** is active. To help avoid longer recovery times, specify the maximum value **40** in the Tx holds field.

Traps

The following table presents the traps setting:

Setting	Description
Send trap	Activates/deactivates the sending of SNMP traps for the following events: • Another bridge takes over the *Root bridge* role. • The topology changes. A port changes its Port state from forwarding into discarding or from discarding into forwarding. Possible values: • **marked** (default setting) The sending of SNMP traps is active. • **unmarked** The sending of SNMP traps is inactive.

Bridge Configuration

The following table presents the bridge configuration settings:

Setting	Description
Bridge ID	Displays the *Bridge Identifier* of the device. The device with the numerically lowest *Bridge Identifier* value takes over the role of the *Root bridge* in the network. Possible values: • **<Bridge priority> / <MAC address>** Value in the Priority field / MAC address of the device
Priority	Specifies the *Bridge priority* of the device. Possible values: • **0..61440** in steps of 4096 (default setting: **32768 (2^{15})**) To make this device the *Root bridge*, assign the numerically lowest value for the priority in the network to the device.
Hello time [s]	Specifies the time in seconds between the sending of two configuration messages (Hello data packets). Possible values: • **1..2** (default setting: **2**) If the device takes over the role of the *Root bridge*, then the other devices in the network use the value specified here. Otherwise, the device uses the value that the *Root bridge* specifies. See the Root information frame. Due to the interaction with the Tx holds parameter, do not change the default setting.
Forward delay [s]	Specifies the delay time for the status change in seconds. Possible values: • **4..30** (default setting: **15**) If the device takes over the role of the *Root bridge*, then the other devices in the network use the value specified here. Otherwise, the device uses the value that the *Root bridge* specifies. See the Root information frame. In the Rapid Spanning Tree Protocol (RSTP), the bridges negotiate a status change without a specified delay. The Spanning Tree function uses the parameter to delay the status change between the statuses **disabled**, **discarding**, **learning**, **forwarding**. The parameters Forward delay [s] and Max age have the following relationship: Forward delay [s] ≥ (Max age/2) + 1 If you enter values in the fields that contradict this relationship, then the device replaces these values with the last valid values or with the default value.
Max age	Specifies the maximum permitted branch length, namely the number of devices to the *Root bridge*. Possible values: • **6..40** (default setting: **20**) If the device takes over the role of the *Root bridge*, then the other devices in the network use the value specified here. Otherwise, the device uses the value that the *Root bridge* specifies. See the Root information frame. The Spanning Tree function uses the parameter to specify the validity of STP-BPDUs in seconds.

Setting	Description
Tx holds	Limits the maximum transmission rate for sending BPDUs. Possible values: • **1..40** (default setting: **10**) To help avoid longer recovery times when using the **MSTP** protocol, set the maximum value to **40**. When the device sends a BPDU, the device increments a counter on this port. When the counter reaches the value specified here, the port stops sending BPDUs. On the one hand, this reduces the load generated by RSTP, and on the other when the device does not receive BPDUs, a communication interruption can be caused. The device decrements the counter by **1** every second. In the following second, the device sends a maximum of **1** new BPDU.
BPDU guard	Activates/deactivates the BPDU guard function in the device. With this function, the device helps protect the network from incorrect configurations, attacks with STP-BPDUs, and unwanted topology changes. Possible values: • **marked** The BPDU guard is active. ◦ The device applies the function to manually specified *Edge ports*. For these ports, in the **Switching > L2-Redundancy > Spanning Tree > Port** dialog, CIST tab the checkbox in the Admin edge port column is marked. ◦ If an *Edge port* receives an STP-BPDU, then the device disables the port. For this port, in the **Basic Settings > Port** dialog, Configuration tab the checkbox in the Port on column is unmarked. • **unmarked** (default setting) The BPDU guard is inactive. To reset the status of the port to the value **forwarding**, you proceed as follows: • If the port is still receiving BPDUs: ◦ In the **Switching > L2-Redundancy > Spanning Tree > Port** dialog, CIST tab unmark the checkbox in the Admin edge port column. or ◦ In the **Switching > L2-Redundancy > Spanning Tree > Global** dialog, unmark the BPDU guard checkbox. • To re-enable the port again you use the Auto-Disable function. As an alternative, proceed as follows: ◦ Open the **Basic Settings > Port** dialog, Configuration tab. ◦ Mark the checkbox in the Port on column.

Setting	Description
BPDU filter (all admin edge ports)	Activates/deactivates the STP-BPDU filter on every manually specified *Edge port*. For these ports, in the **Switching > L2-Redundancy > Spanning Tree > Port** dialog, CIST tab the checkbox in the Admin edge port column is marked. Possible values: • **marked** The BPDU filter is active on every *Edge port*. The function does not use these ports in Spanning Tree operations. ◦ The device does not send STP-BPDUs on these ports. ◦ The device drops any STP-BPDUs received on these ports. • **unmarked** (default setting) The global BPDU filter is inactive. You have the option to explicitly activate the BPDU filter for single ports. See the Port BPDU filter column in the **Switching > L2-Redundancy > Spanning Tree > Port** dialog.
Auto-disable	Activates/deactivates the Auto-Disable function for the parameters that BPDU guard is monitoring on the port. Possible values: • **marked** The Auto-Disable function for the BPDU guard is active. ◦ When the port receives an STP-BPDU, the device disables an *Edge port*. The Link status LED for the port flashes 3 × per period. ◦ The **Diagnostics > Ports > Auto-Disable** dialog displays which ports are currently disabled due to the parameters being exceeded. ◦ After a waiting period, the Auto-Disable function enables the port again automatically. For this you go to the **Diagnostics > Ports > Auto-Disable** dialog and specify a waiting period for the relevant port in the Reset timer [s] column. • **unmarked** (default setting) The Auto-Disable function for the BPDU guard is inactive.

Root Information

The following table presents the the root information settings:

Setting	Description
Root ID	Displays the *Bridge Identifier* of the *Root bridge*. Possible values: • **<Bridge priority> / <MAC address>**
Priority	Displays the *Bridge priority* of the *Root bridge*. Possible values: • **0..61440** in steps of 4096
Hello time [s]	Displays the time in seconds that the *Root bridge* specifies between the sending of two configuration messages (Hello data packets). Possible values: • **1..2** The device uses this specified value. See the Bridge configuration frame.
Forward delay [s]	Displays the delay time in seconds set up by the *Root bridge* for status changes. Possible values: • **4..30** The device uses this specified value. See the Bridge configuration frame. In the Rapid Spanning Tree Protocol (RSTP), the bridges negotiate a status change without a specified delay. The Spanning Tree function uses the parameter to delay the status change between the statuses **disabled**, **discarding**, **learning**, **forwarding**.
Max age	Specifies the maximum permitted branch length that the *Root bridge* sets up, namely the number of devices to the *Root bridge*. Possible values: • **6..40** (default setting: **20**) The Spanning Tree function uses the parameter to specify the validity of STP-BPDUs in seconds.

Topology Information

The following table presents the topology information settings:

Setting	Description
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 path leads to the *Root bridge*. If the device takes over the role of the *Root bridge*, then the field displays the value **no Port**.
Root path cost	Displays the path cost for the path that leads from the *Root port* of the device to the *Root bridge* of the layer 2 network. Possible values: • **0** The device takes over the role of the *Root bridge*. • **1..200000000 (2×10^8)**
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>**

Spanning Tree MSTP

In this dialog **Switching > L2-Redundancy > Spanning Tree > MSTP**, you manage the settings of the global and local MST instances.

In contrast to the local MST instances, the global MST instance is set up permanently in the device. The global MST instance contains the VLANs that are not explicitly allocated to a local MST instance.

The device supports up to 4 local MST instances. To add a local MST instance, click the  button.

While STP has a single Spanning Tree spanning the network, MSTP allows you to set up one Spanning Tree per VLAN or group of VLANs. Thus it is possible to specify several smaller Spanning Trees covering one network.

How to help avoid longer convergence times:

- Only use devices in the network that support RSTP or MSTP.
- Adjust the following parameters to the topology and number of bridges:
  - Maximum allowed number of devices to the *Root bridge*

    Switching > L2-Redundancy > Spanning Tree > Global dialog, Max age field
  - Maximum allowed number of bridges within the MST region in a branch to the *Root bridge*

    Switching > L2-Redundancy > Spanning Tree > MSTP dialog, Global CIST parameter frame, Hops (max.) field

For bridges in an MST region, specify identical values for the following parameters:

- Name of the MST region
- Revision level of the MST region
- Allocation of the VLANs to the MST instances
  - Include ports connecting the bridges of an MST region as members in the VLANs set up on the bridges. The ports are to transmit the data packets with a VLAN tag. You thus help avoid potential connection interruptions within the MST region when the topology is changed.
  - Include ports connecting an MST region with other MST regions or with the CST region (boundary ports) as members in the VLANs set up in both regions. The ports are to transmit the data packets with a VLAN tag. You thus help avoid potential connection interruptions when topology changes affecting the boundary ports are made.

MST Region Identifier

The following table presents the MST region identifier settings:

Setting	Description
Name	Specifies the name of the MST region to which the device belongs. Possible values: • Alphanumeric ASCII character string with 1..32 characters
Revision level	Specifies the version number of the MST region to which the device belongs. Possible values: • **0..65535 (2^{16}-1)** (default setting: **1**)
Checksum	Displays the MD5 checksum of the MST configuration.

Global CIST Parameter

The following table presents the global CIST parameter settings:

Setting	Description
Hops (max.)	Specifies the maximum number of bridges within the MST region in a branch to the *Root bridge*. Possible values: • **6..40** (default setting: **20**)
Attached VLANs	Displays the IDs of the VLANs that are assigned only to the global MST instance and to no other local MST instance. Possible values: • **ID of the statically configured VLANs** (default setting: **1**)
Bridge ID	Displays the *Bridge Identifier* of the device. Possible values: • **<Bridge priority> / <MAC address>** The value is made up as follows: ◦ Value in the Priority field. See the **Switching > L2-Redundancy > Spanning Tree > Global** dialog, Bridge configuration frame. ◦ MAC address of the device.
Root ID	Displays the *Bridge Identifier* of the CIST *Root bridge* of the whole Layer 2 network. Possible values: • **<Bridge priority> / <MAC address>** The device with the numerically lowest *Bridge Identifier* value takes over the role of the CIST *Root bridge* in the network. The following devices are able to take over the role of the *Root bridge*: • Bridges not belonging to any MST region • Bridges belonging to the global instance of an MST region In the whole Layer 2 network, the bridges use the time settings of the CIST *Root bridge*, for example Hello time [s].
Regional root ID	Displays the *Bridge Identifier* of the *Root bridge* that belongs to the global instance of the MST region to which this device belongs. Possible values: • **<Bridge priority> / <MAC address>** The values in the Regional root ID and Root ID fields are identical when the regional *Root bridge* has the numerically lowest *Bridge Identifier* value in the whole Layer 2 network.
Root port	Displays the port of the device from which the path leads to the CIST *Root bridge* of the whole Layer 2 network. Possible values: • **no Port** The device currently has the role of the *Root bridge*. • **<Port number>** The path to the CIST *Root bridge* of the whole Layer 2 network leads over this port.

Setting	Description
Root path cost	Displays the path cost for the path that leads from the regional *Root bridge* of the MST region to the CIST *Root bridge* of the whole Layer 2 network. Possible values: • **0** The regional *Root bridge* simultaneously has the role of the CIST *Root bridge*. • **1..200000000 (2×10^8)** For the devices within an MST region, the Root path cost values are identical. If you do not use the MSTP function, then the Root path cost values are identical to the root path costs of STP or RSTP. In this case, every device considers itself as an own region.
Internal root path cost	Displays the internal path cost for the path that leads from the *Root port* of the device to the regional *Root bridge* of the MST region. Possible values: • **0** The local bridge simultaneously has the role of the regional *Root bridge*. • **1..200000000 (2×10^8)**

Table

For information on how to customize the appearance of the table, see Working with tables, page 25.

The following table presents the table settings:

Setting	Description
Buttons	The following list presents the icon descriptions: •  Add: Adds a table row. The device supports up to local 16 instances. •  Remove: Removes the selected table row. •  Configure VLANs: Opens the Configure VLANs window to allocate VLANs to the local MST instance which is selected in the table.
MSTI	Displays the instance number of the local MST instance.
Attached VLANs	Displays the IDs of the VLANs that are allocated to this local MST instance.
Priority	Specifies the *Bridge priority* of the local MST instance. Possible values: • **0..61440** in steps of 4096 (default setting: **32768 (2^{15})**) Assign the numerically lowest value for the priority in this local MST instance to the device to make this device the *Root bridge*.
Bridge ID	Displays the *Bridge Identifier*. The device with the numerically lowest *Bridge Identifier* value takes over the role of the regional MSTI *Root bridge* in the instance. Possible values: • **<Bridge priority + Number of the instance> / <MAC address>** Sum of the value in the Priority and MSTI fields / MAC address of the device.
Time since topology change	Displays the time that has elapsed since the last topology change within this instance.
Topology changes	Displays how many times the device has put a port into the **forwarding** status using the Spanning Tree function since the Spanning Tree instance was started.
Topology change	Displays if the device has detected a topology change within the instance. Possible values: • **marked** The device has detected a topology change. • **unmarked** The device has not detected a topology change.
Root ID	Displays the *Bridge Identifier* of the *Root bridge* in this instance. Possible values: • **<Bridge ID> / <MAC address>**
Root path cost	Displays the path cost for the path that leads from the *Root port* of the device to the *Root bridge* of the instance. Possible values: • **0** The bridge is simultaneously the *Root bridge* of the instance. • **1..200000000 (2×10^8)**
Root port	Displays the port of the device from which the path leads to the *Root bridge* of the instance. Possible values: • **no Port** The device currently has the role of the *Root bridge*. • **<Port number>** The path to the *Root bridge* of the instance leads over this port.

Spanning Tree Port

In this dialog **Switching > L2-Redundancy > Spanning Tree > Port**, 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, page 261
- Guards, page 265
- MSTI <MSTI>, page 267

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 values. The abbreviation CIST stands for *Common and Internal Spanning Tree*.

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

Table

For information on how to customize the appearance of the table, see Working with tables, page 25.

The following table presents the table settings:

Setting	Description
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 role of the port in the CIST. Possible values: • **root** Port with the cheapest path to the *Root bridge*. • **alternate** Port with the alternative path to the *Root bridge* (currently blocking). • **designated** Port for the side of the tree averted from the *Root bridge* (currently blocking). • **backup** Port receives STP-BPDUs from its own device. • **master** Port with the cheapest path to the CIST. The port is the CIST *Root port* of the regional CIST *Root bridge*. The port is unique in an MST region. • **disabled** The port is inactive. See the **Basic Settings > Port** dialog, Configuration tab.
Port path cost	Specifies the path costs of the port. Possible values: • **0..200000000 (2×10^8)** (default setting: **0**) When the value is **0**, the device automatically calculates the path costs depending on the data rate of the port.
Port priority	Specifies the priority of the port. Possible values: • **0..240** in steps of 16 (default setting: **128**) This value represents the first 4 bits of the port ID.

Setting	Description
Received bridge ID	Displays the *Bridge Identifier* of the device from which this port last received an STP-BPDU. Possible values: • For ports with the **designated** role, the device displays the information for the STP-BPDU last received by the port. This helps to diagnose the detected STP problems in the network. • For the **alternate**, **backup**, **master**, and **root** port roles, in the stationary condition (static topology) this information is identical to the information of the **designated** port role. • If a port has no connection or if it did not receive any STP-BDPUs yet, then the device displays the values that the port can send with the **designated** role.
Received port ID	Displays the port ID of the device from which this port last received an STP-BPDU. Possible values: • For ports with the **designated** role, the device displays the information for the STP-BPDU last received by the port. This helps to diagnose the detected STP problems in the network. • For the **alternate**, **backup**, **master**, and **root** port roles, in the stationary condition (static topology) this information is identical to the information of the **designated** port role. • If a port has no connection or if it did not receive any STP-BDPUs yet, then the device displays the values that the port can send with the **designated** role.
Received path cost	Displays the path cost that the greater-level bridge has from its *Root port* in the local MST instance to the *Root bridge*. Possible values: • For ports with the **designated** role, the device displays the information for the STP-BPDU last received by the port. This helps to diagnose the detected STP problems in the network. • For the **alternate**, **backup**, **master**, and **root** port roles, in the stationary condition (static topology) this information is identical to the information of the **designated** port role. • If a port has no connection or if it did not receive any STP-BDPUs yet, then the device displays the values that the port can send with the **designated** role.
Admin edge port	Activates/deactivates the Admin edge port mode. If the port is connected to an end device, then use the Admin edge port mode. This setting allows the *Edge port* to change faster to the forwarding state after linkup and thus a faster accessibility of the end device. Possible values: • **marked** The Admin edge port mode is active. The port is connected to an end device. ◦ After the connection is set up, the port changes to the **forwarding** state without changing to the **learning** state beforehand. ◦ If the port receives an STP-BPDU and the BPDU guard function is active, then the device deactivates the port. See the **Switching > L2-Redundancy > Spanning Tree > Global** dialog. • **unmarked** (default setting) The Admin edge port mode is inactive. The port is connected to another STP bridge. After the connection is set up, the port changes to the **learning** status before changing to the **forwarding** state, if applicable.

Setting	Description
Auto edge port	Activates/deactivates the automatic detection of whether you connect an end device to the port. The prerequisite is that the checkbox in the Admin edge port column is unmarked. Possible values: • **marked** (default setting) The automatic detection is active. After the installation of the connection and after 1.5 × Hello time [s], the device sets the port to the **forwarding** status (default setting 1.5 × 2 s) if the port did not receive any STP-BPDUs during this time. • **unmarked** The automatic detection is inactive. After the installation of the connection, and after Max age the device sets the port to the **forwarding** status. (default setting: 20 s)
Oper edge port	Displays if an end device or an STP bridge is connected to the port. Possible values: • **marked** An end device is connected to the port. The port does not receive any STP-BPDUs. • **unmarked** An STP bridge is connected to the port. The port receives STP-BPDUs.
Oper PointToPoint	Displays if the port is connected to an STP device through a direct full-duplex link. Possible values: • **marked** The port is connected directly to an STP device through a full-duplex link. The direct, decentralized communication between 2 bridges provides short reconfiguration times. • **unmarked** The port is connected in another way, for example through a half-duplex link or through a hub.
Port BPDU filter	Activates/deactivates the filtering of STP-BPDUs on the port explicitly. The prerequisite is that the port is a manually specified *Edge port*. For these ports, the checkbox in the Admin edge port column is marked. Possible values: • **marked** The BPDU filter is active on the port. The function excludes the port from Spanning Tree operations. ◦ The device does not send STP-BPDUs on the port. ◦ The device drops any STP-BPDUs received on the port. • **unmarked** (default setting) The BPDU filter is inactive on the port. You have the option to globally activate the BPDU filter for every *Edge port*. See the **Switching > L2-Redundancy > Spanning Tree > Global** dialog, Bridge configuration frame. If the BPDU filter (all admin edge ports) checkbox is marked, then the BPDU filter is still active on the port.

Setting	Description
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 also. Possible values: • **marked** The BPDU flood mode is active. • **unmarked** (default setting) The BPDU flood mode is inactive.

Guards

This tab lets you specify the settings for various protection functions on the ports.

Table

For information on how to customize the appearance of the table, see Working with tables, page 25.

The following table presents the table settings:

Setting	Description
Port	Displays the port number.
Root guard	Activates/deactivates the monitoring of STP-BPDUs on the port. The prerequisite is that the Loop guard function is inactive. With this setting the device helps you protect the network from incorrect configurations or attacks with STP-BPDUs that try to change the topology. This setting is relevant only for ports with the STP role **designated**. Possible values: • **marked** The monitoring of STP-BPDUs is active. ◦ If the port receives an STP-BPDU with better path information to the *Root bridge*, then the device discards the STP-BPDU and sets the status of the port to the value **discarding** instead of **root**. ◦ If there are no STP-BPDUs with better path information to the *Root bridge*, then the device resets the status of the port after 2 × Hello time [s]. • **unmarked** (default setting) The monitoring of STP-BPDUs is inactive.
TCN guard	Activates/deactivates the monitoring of *Topology Change* notifications on the port. With this setting the device helps you protect the network from attacks with STP-BPDUs that try to change the topology. Possible values: • **marked** The monitoring of *Topology Change* notifications is active. ◦ The port ignores the *Topology Change* flag in received STP-BPDUs. ◦ If the received BPDU contains other information that causes a topology change, then the device processes the BPDU even if the TCN guard function is active. Example: The device receives better path information for the *Root bridge*. • **unmarked** (default setting) The monitoring of *Topology Change* notifications is inactive. If the device receives STP-BPDUs with a *Topology Change* flag, then the device deletes the MAC address table (forwarding database) of the port and forwards the *Topology Change* notifications.
Loop guard	Activates/deactivates the monitoring of loops on the port. The prerequisite is that the Root guard function is inactive. With this setting the device helps prevent loops if the port does not receive any more STP-BPDUs. Use this setting only for ports with the STP role **alternate**, **backup** or **root**. Possible values: • **marked** The monitoring of loops is active. This helps prevent loops for example, if you disable the Spanning Tree function on the remote device or if the connection is interrupted only in the receiving direction. ◦ If the port does not receive any STP-BPDUs for a while, then the device sets the status of the port to the value **discarding** and marks the checkbox in the Loop state column. ◦ If the port receives STP-BPDUs again, then the device sets the status of the port to a value according to Port role and unmarks the checkbox in the Loop state column. • **unmarked** (default setting) The monitoring of loops is inactive. If the port does not receive any STP-BPDUs for a while, then the device sets the status of the port to the value **forwarding**.

Setting	Description
Loop state	Displays if the loop state of the port is inconsistent. Possible values: • **marked** The loop state of the port is inconsistent: ◦ The port is not receiving any STP-BPDUs and the Loop guard function is enabled. ◦ The device sets the state of the port to the value **discarding**. The device thus helps prevent any potential loops. • **unmarked** The loop state of the port is consistent. The port receives STP-BPDUs.
Trans. into loop	Displays how many times the loop state of the port became inconsistent (marked checkbox in the Loop state column).
Trans. out of loop	Displays how many times the loop state of the port became consistent (unmarked checkbox in the Loop state column).
BPDU guard effect	Displays if the port received an STP-BPDU as an *Edge port*. Prerequisite: • The port is a manually specified *Edge port*. In the **Switching > L2-Redundancy > Spanning Tree > Port** dialog, the checkbox for this port in the Admin edge port column is marked. • In the **Switching > L2-Redundancy > Spanning Tree > Global** dialog, the BPDU guard function is active. Possible values: • **marked** The port is an *Edge port* and received an STP-BPDU. The device deactivates the port. For this port, in the **Basic Settings > Port** dialog, Configuration tab the checkbox in the Port on column is unmarked. • **unmarked** The port is an *Edge port* and has not received any STP-BPDUs, or the port is not an *Edge port*. To reset the status of the port to the value **forwarding**, you proceed as follows: • If the port is still receiving BPDUs: ◦ In the CIST tab, unmark the checkbox in the Admin edge port column. or ◦ In the **Switching > L2-Redundancy > Spanning Tree > Global** dialog, unmark the BPDU guard checkbox. • To activate the port, proceed as follows: ◦ Open the **Basic Settings > Port** dialog, Configuration tab. ◦ Mark the checkbox in the Port on column.

MSTI <MSTI>

This tab allows you to specify the settings on the ports for path costs and priority in the local MST instance, and to view values.

Table

For information on how to customize the appearance of the table, see Working with tables, page 25.

The following table presents the table settings:

Setting	Description
Port	Displays the port number.
Port state	Displays the transmission status of the port. Possible values: • **discarding** The port is blocked and forwards only STP-BPDUs. • **learning** The port is blocked, but it learns the MAC addresses of received data packets. • **forwarding** The port forwards data packets. • **disabled** The port is inactive. See the **Basic Settings** > **Port** dialog, Configuration tab. • **manualFwd** The Spanning Tree function is disabled on the port. The port forwards STP-BPDUs. • **notParticipate** The port is not participating in STP.
Port role	Specifies the role of the port in the local instance. Possible values: • **root** Port with the cheapest path to the *Root bridge*. • **alternate** Port with the alternative path to the *Root bridge* (currently interrupted). • **designated** Port for the side of the tree averted from the *Root bridge*. • **backup** Port which receives STP-BPDUs from its own device. • **master** Port with the cheapest path to the CIST. The port is the CIST *Root port* of the CIST Regional Root. The port is unique in an MST region. • **disabled** The port is inactive. See the **Basic Settings** > **Port** dialog, Configuration tab.
Port path cost	Specifies the path costs of the port in the local instance. Possible values: • **0..200000000 (2×10^8)** (default setting: **0**) When the value is **0**, the device automatically calculates the path costs depending on the data rate of the port.
Port priority	Specifies the priority of the port in the local instance. Possible values: • **0..240** in steps of 16 (default setting: **128**)
Received bridge ID	Displays the *Bridge Identifier* of the device from which this port last received an STP-BPDU in the local instance.

Setting	Description
Received port ID	Displays the port ID of the device from which this port last received an STP-BPDU. Possible values: • For ports with the **designated** role, the device displays the information for the STP-BPDU last received by the port. This helps to diagnose the detected STP problems in the network. • For the **alternate**, **backup**, **master**, and **root** port roles, in the stationary condition (static topology) this information is identical to the information of the **designated** port role. • If a port has no connection or if it did not receive any STP-BDPUs yet, then the device displays the values that the port can send with the **designated** role.
Received path cost	Displays the path cost that the greater-level bridge has from its *Root port* to the *Root bridge*. Possible values: • For ports with the **designated** role, the device displays the information for the STP-BPDU last received by the port. This helps to diagnose the detected STP problems in the network. • For the **alternate**, **backup**, **master**, and **root** port roles, in the stationary condition (static topology) this information is identical to the information of the **designated** port role. • If a port has no connection or if it did not receive any STP-BDPUs yet, then the device displays the values that the port can send with the **designated** role.

Link Aggregation

Loops during the configuration phase may lead to unintended equipment operation.

⚠WARNING

UNINTENDED EQUIPMENT OPERATION

- Set up each device of the Link Aggregation configuration individually.
- Complete the configuration of the other devices of the Link Aggregation configuration before you connect the redundant lines.

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

The Link Aggregation function **Switching > L2-Redundancy > Link Aggregation** allows you to 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 greater availability and a greater transmission bandwidth.

The criteria for distributing the load to the parallel links are based on the Hashing option function.

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

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

The device allows you to set a maximum of 2 Link Aggregation groups.

Configuration

The following table presents the configuration setting:

Setting	Description
Hashing option	Specifies which information the device uses to distribute the packets to the physical ports of the LAG interface. The device sends packets containing the same distribution-relevant information over the same physical port to keep the packet order. This setting overwrites the value specified in the Hashing option column for the port. Possible values: • **sourceMacVlan** The device uses the **Source MAC address**, **VLAN ID**, **EtherType** fields of the packet, and the physical ingress port. • **destMacVlan** The device uses the **Destination MAC address**, **VLAN ID**, **EtherType** fields of the packet, and the physical ingress port. • **sourceDestMacVlan** (default setting) The device uses the **Source MAC address**, **Destination MAC address**, **VLAN ID**, **EtherType** fields of the packet, and the physical ingress port. • **sourceIPsourcePort** The device uses the **Source IP address** and **Source TCP/UDP port** fields of the packet. • **destIPdestPort** The device uses the **Destination IP address** and **Destination TCP/UDP port** fields of the packet. • **sourceDestIPPort** The device uses the **Source IP address**, **Destination IP address**, **Source TCP/UDP port**, and **Destination TCP/UDP port** fields of the packet.

Table

For information on how to customize the appearance of the table, see Working with tables, page 25.

Buttons

The following table presents the icon descriptions:

Icon	Description
Add	Opens the Create window to add a table row for a LAG interface or to assign a physical port to a LAG interface. • From the Trunk port drop-down list, you select the LAG interface number. • From the Port drop-down list, you select the number of a physical port to assign to the LAG interface. After you set up a LAG interface, the device adds the LAG interface to the table in the **Basic Settings > Port** dialog, Statisticstab.
Remove	Removes the selected table row.

Trunk Port

Displays the LAG interface number.

The following table presents the trunk port settings:

Setting	Description
Name	Specifies the name of the LAG interface. Possible values: • Alphanumeric ASCII character string with 1..15 characters
Link/Status	Displays the operating state of the LAG interface and the physical ports. Possible values: • **up** (**lag/…** row) The LAG interface is operational. The prerequisites are: ◦ The Static link aggregation function is active on this LAG interface. or ◦ LACP is active on the physical ports assigned to the LAG interface, see the LACP active column. and The key specified for the LAG interface in the LACP admin key column matches the keys specified for the physical ports in the LACP port actor admin key column. and The number of operational physical ports assigned to the LAG interface is greater than or equal to the value specified in the Active ports (min.) column. • **up** The physical port is operational. • **down** (**lag/…** row) The LAG interface is inoperable. • **down** The physical port is disabled. or No cable connected or no active link.
Active	Activates/deactivates the LAG interface. Possible values: • **marked** (default setting) The LAG interface is active. Consider that the following protocols do not work properly on the physical ports when you activate the LAG interface: ◦ PTP ◦ 802.1AS • **unmarked** The LAG interface is inactive.
STP active	Activates/deactivates the Spanning Tree function on this LAG interface. The prerequisite is that in the **Switching > L2-Redundancy > Spanning Tree > Global** dialog the Spanning Tree function is enabled. You can also activate/deactivate the Spanning Tree function on the LAG interfaces in the **Switching > L2-Redundancy > Spanning Tree > Port** dialog. Possible values: • **marked** (default setting) The Spanning Tree function is active on this LAG interface. • **unmarked** The Spanning Tree function is inactive on this LAG interface.

Setting	Description
Static link aggregation	Activates/deactivates the Static link aggregation function on the LAG interface. The device aggregates the assigned physical ports to the LAG interface, even if the remote site does not support LACP. Possible values: • **marked** The Static link aggregation function is active on this LAG interface. The device aggregates an assigned physical port to the LAG interface as soon as the physical port gets a link. The device does not send LACPDUs and discards received LACPDUs. • **unmarked** (default setting) The Static link aggregation function is inactive on this LAG interface. If the connection was successfully negotiated using LACP, then the device aggregates an assigned physical port to the LAG interface.
Hashing option	Specifies which information the device uses to distribute the packets to the individual physical ports of the LAG interface. This setting has priority over the value selected in the Configuration frame, Hashing option drop-down list. For further information on the values, see the description of the Hashing option drop-down list in the Configuration frame.
MTU	Specifies the maximum allowed size of Ethernet packets on the LAG interface in bytes. Any present VLAN tag is not taken into account. This setting allows you to 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)
Track name	Displays the name of the tracking object made up of the values displayed in the Type and Track ID columns.
Active ports (min.)	Specifies the minimum number of physical ports to be active for the LAG interface to stay active. If the number of active physical ports is lower than the specified value, then the device deactivates the LAG interface. If a redundancy function like Spanning Tree or MRP over LAG is active in the device, then you use this function to force the device to switch automatically to the redundant line. Possible values: • **1..x** (default setting: **1**) The maximum value depends on the number of physical ports assigned to the LAG interface.
Type	Displays if the LAG interface is based on the Static link aggregation function or on LACP. Possible values: • **static** The LAG interface is based on the Static link aggregation function. • **dynamic** The LAG interface is based on LACP.

Setting	Description
Send trap (Link up/ down)	Activates/deactivates the sending of SNMP traps when the device detects a change in the link up/down status for this interface. Possible values: • **marked** (default setting) The sending of SNMP traps is active. The prerequisite is that in the **Diagnostics > Status Configuration > Alarms (Traps)** dialog the Alarms (Traps) function is enabled and at least one trap destination is specified. When the device detects a link up/down status change, the device sends an SNMP trap. • **unmarked** The sending of SNMP traps is inactive.
LACP admin key	Specifies the LAG interface key. The device uses this key to identify the ports that can be aggregated to the LAG interface. Possible values: • **0..65535 (2^{16}-1)** You specify the corresponding value for the physical ports in the LACP port actor admin key column.

Port

Displays the physical port number assigned to the LAG interface.

The following table presents the port settings:

Setting	Description
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 (2^{16}-1)** If this value matches the value of the LAG interface specified in the LACP admin key column, then the device only aggregates this physical port to the LAG interface.
LACP actor admin state	Specifies the actor state values that the LAG interface transmits in the LACPDUs. This allows you to control the LACPDU parameters. The device allows you to mix the values. From the drop-down list, select one or more items. Possible values: • **ACT** (**LACP_Activity** state) When selected, the link transmits the LACPDUs cyclically, otherwise when requested. • **STO** (**LACP_Timeout** state) When selected, the link transmits the LACPDUs cyclically using the short timeout, otherwise using the long timeout. • **AGG** (**Aggregation** state) When selected, the device interprets the link as a candidate for aggregation, otherwise as an individual link. For further information on the values, see IEEE 802.1AX-2014.

Setting	Description
LACP actor oper state	Displays the actor state values that the LAG interface transmits in the LACPDUs. Possible values: • **ACT** (**LACP_Activity** state) When visible, the link transmits the LACPDUs cyclically, otherwise when requested. • **STO** (**LACP_Timeout** state) When visible, the link transmits the LACPDUs cyclically using the short timeout, otherwise using the long timeout. • **AGG** (**Aggregation** state) When visible, the device interprets the link as a candidate for aggregation, otherwise as an individual link. • **SYN** (**Synchronization** state) When visible, the device interprets the link as **IN_SYNC**, otherwise as **OUT_OF_SYNC**. • **COL** (**Collecting** state) When visible, collection of incoming frames is enabled on this link, otherwise disabled. • **DST** (**Distributing** state) When visible, distribution of outgoing frames is enabled on this link, otherwise disabled. • **DFT** (**Defaulted** state) When visible, the link uses defaulted operational information, administratively specified for the Partner. Otherwise the link uses the operational information received from a LACPDU. • **EXP** (**Expired** state) When visible, the link receiver is in the **EXPIRED** state.
LACP partner oper SysID	Displays the MAC address of the remote device connected to this physical port. The LAG interface has received this information in a LACPDU from the partner.
LACP partner oper port	Displays the port number of the remote device connected to this physical port. The LAG interface has received this information in a LACPDU from the partner.
LACP partner oper port state	Displays the partner state values that the LAG interface receives in the LACPDUs. Possible values: • **ACT** • **STO** • **AGG** • **SYN** • **COL** • **DST** • **DFT** • **EXP** For further information on the values, see the description of the LACP actor oper state column and IEEE 802.1AX-2014.

Link Backup

Loops during the configuration phase may lead to unintended equipment operation.

⚠WARNING

UNINTENDED EQUIPMENT OPERATION

- Set up each device of the Link Backup configuration individually.
- Complete the configuration of the other devices of the Link Backup configuration before you connect the redundant lines.

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

With Link Backup, you set up pairs of redundant links. Each pair has a *Primary port* and a *Backup port*. The *Primary port* forwards the data packets until the device detects an error. If the device detects an error on the *Primary port*, then the Link Backup function transfers the data packets over to the *Backup port*.

The dialog **Switching > L2-Redundancy > Link Backup** also allows you to set a **Fail Back** option. When you activate the **Fail Back** function and the *Primary port* returns to normal operation, the device first blocks the data packets on the *Backup port* and then forwards the data packets to the *Primary port*. This process helps protect the device from causing loops in the network.

Operation

The following table presents the operation setting:

Setting	Description
Operation	Enables/disables the Link Backup function globally in the device. Possible values: • **On** Enables the Link Backup function. • **Off** (default setting) Disables the Link Backup function.

Table

For information on how to customize the appearance of the table, see Working with tables, page 25.

The following table presents the table settings:

Setting	Description
Buttons	The following list presents the icon descriptions: •  Add: Adds a table row. •  Remove: Removes the selected table row.
Primary port	Displays the *Primary port* of the interface pair. When you enable the Link Backup function, this port is responsible for forwarding the data packets. Possible values: • Physical ports
Backup port	Displays the *Backup port* to which the device forwards the data packets if the device detects an error on the *Primary port*. Possible values: • Physical ports except for the port you set as the *Primary port*.
Description	Specifies the Link Backup pair. Enter a name to identify the Backup pair. Possible values: • Alphanumeric ASCII character string with 0..255 characters
Primary port status	Displays the status of the *Primary port* for this Link Backup pair. Possible values: • **forwarding** The link is up, no shutdown, and forwarding data packets. • **blocking** The link is up, no shutdown, and blocking data packets. • **down** The cable is unplugged, the port is powered off, the port link is interrupted, or a function in the device has disabled the port. • **unknown** The Link Backup feature is globally disabled, or the port pair is inactive. Therefore, the device ignores the port pair settings.
Backup port status	Displays the status of the *Backup port* for this Link Backup pair. Possible values: • **forwarding** The link is up, no shutdown, and forwarding data packets. • **blocking** The link is up, no shutdown, and blocking data packets. • **down** The cable is unplugged, the port is powered off, the port link is interrupted, or a function in the device has disabled the port. • **unknown** The Link Backup feature is globally disabled, or the port pair is inactive. Therefore, the device ignores the port pair settings.
Fail back	Activates/deactivates the automatic **Fail back**. Possible values: • **marked** (default setting) The automatic **Fail back** is active. After the delay timer expires, the *Backup port* changes to **blocking** and the *Primary port* changes to **forwarding**. • **unmarked** The automatic **Fail back** is inactive. The *Backup port* continues forwarding data packets even after the *Primary port* re-establishes a link or you manually change the admin status of the *Primary port* from **shutdown** to **no shutdown**.

Setting	Description
Fail back delay [s]	Specifies the delay time in seconds that the device waits after the *Primary port* re-establishes a link. Furthermore, this timer also applies when you manually set the admin status of the *Primary port* from **shutdown** to **no shutdown**. After the delay timer expires, the *Backup port* changes to **blocking** and the *Primary port* changes to **forwarding**. Possible values: • **0..3600** (default setting: **30**) When set to **0**, immediately after the *Primary port* re-establishes a link, the *Backup port* changes to **blocking** and the *Primary port* changes to **forwarding**. Furthermore, immediately after you manually set the admin status of from **shutdown** to **no shutdown**, the *Backup port* changes to **blocking** and the *Primary port* changes to **forwarding**.
Active	Activates/deactivates the Link Back up pair configuration. Possible values: • **marked** The Link Backup pair is active. The device senses the link and administration status and forwards the data packets according to the pair configuration. • **unmarked** (default setting) The Link Backup pair is inactive. The ports forward the data packets according to standard switching.

Create

The following table presents the create settings:

Setting	Description
Primary port	Specifies the *Primary port* of the backup interface pair. During normal operation this port is responsible for forwarding the data packets. Possible values: • Physical ports
Backup port	Specifies the *Backup port* to which the device transfers the data packets to if the device detects an error on the *Primary port*. Possible values: • Physical ports except for the port you set as the *Primary port*.

FuseNet

The FuseNet protocols allows you to couple rings that are operating with one of the following redundancy protocols:

- MRP
- HIPER Ring
- RSTP

NOTE: If you use the Ring/Network Coupling function to couple networks, then verify that the networks only contain Schneider Electric devices.

Use the following table to select the FuseNet coupling protocol to be used in the network:

Main Ring	Connected Network		
	MRP	**HIPER Ring**	**RSTP**
MRP	Sub Ring[1)]	RCP Ring/Network Coupling	RCP Ring/Network Coupling
HIPER Ring	Sub Ring	Ring/Network Coupling	RCP Ring/Network Coupling
RSTP	RCP	RCP	–

–: No suitable coupling protocol.

(1): With the MRP function set up on different VLANs.

This menu **Switching > L2-Redundancy > FuseNet** contains the following dialogs:

- Sub Ring, page 279
- Ring/Network Coupling, page 283
- Redundant Coupling Protocol, page 289

Sub Ring

Loops during the configuration phase may lead to unintended equipment operation.

⚠WARNING

UNINTENDED EQUIPMENT OPERATION

- Set up each device of the Sub Ring configuration individually.
- Complete the configuration of the other devices of the ring configuration before you connect the redundant lines.

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

This dialog **Switching > L2-Redundancy > FuseNet > Sub Ring** allows you to set up the device to operate in the *Sub Ring Manager* mode.

The Sub Ring function allows you to easily couple network segments to existing redundancy rings. The *Sub Ring Manager* device couples a Sub Ring to an existing ring (base ring).

You can integrate any devices that support MRP as participants in the Sub Ring. These devices do not require support for the Sub Ring function.

When setting up Sub Rings, remember the following rules:

- The device supports Link Aggregation in the Sub Ring
- No spanning tree on Sub Ring ports
- Same MRP domain on devices within a Sub Ring
- Different VLANs for base ring and Sub Ring

Specify the VLAN settings as follows:

- VLAN **X** for base ring
  - on the ring ports of the devices participating in the base ring
  - on the base ring ports of the *Sub Ring Manager* device
- VLAN **Y** for Sub Ring
  - on the ring ports of the devices participating in the Sub Ring
  - on the Sub Ring ports of the *Sub Ring Manager* device

  NOTE: To help avoid loops, only close the redundant line when the settings are specified in every device participating in the ring.

Operation

The following table presents the operation setting:

Setting	Description
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

The following table presents the information setting:

Setting	Description
Table entries (max.)	Displays the maximum number of Sub Rings supported by the device.

Table

For information on how to customize the appearance of the table, see Working with tables, page 25.

The following table presents the table settings:

Setting	Description
Buttons	The following list presents the icon descriptions: •  Add: Opens the Create window to add a table row. In the Sub Ring ID field, you specify the number that uniquely identifies the Sub Ring. Possible values: ◦ **1..40000** You can replace the value prefilled by the device with any value in the range. The device allows you to set a maximum of 8 Sub Ring instances. •  Remove: Removes the selected table row.
Sub Ring ID	Displays the number that uniquely identifies the Sub Ring.
Name	Specifies the optional name of the Sub Ring. Possible values: • Alphanumeric ASCII character string with 0..255 characters
Active	Activates/deactivates the Sub Ring. Activate the Sub Ring when the configuration of every device participating in the Sub Ring is complete. Close the Sub Ring only after activating the Sub Ring function. Possible values: • **marked** The Sub Ring is active. • **unmarked** (default setting) The Sub Ring is inactive.
Status	Displays the operational state of the Sub Ring configuration. Possible values: • **noError** The device detects an acceptable Sub Ring configuration. • **ringPortLinkError** ◦ The ring port has no link. ◦ One of the Sub Ring lines is connected to one more port of the device. But the Sub Ring line is not connected to one of the ring ports of the device. • **multipleSRM** The *Sub Ring Manager* device receives data packets from more than one *Sub Ring Manager* devices in the Sub Ring. • **noPartnerManager** The *Sub Ring Manager* device receives its own data packets. • **concurrentVLAN** The Media Redundancy Protocol (MRP) in the base ring uses the VLAN of the *Sub Ring Manager* domain. • **concurrentPort** One more redundancy protocol uses the ring port of the *Sub Ring Manager* domain. • **concurrentRedundancy** The *Sub Ring Manager* domain is inactive because of one more active redundancy protocol. • **trunkMember** The ring port of the *Sub Ring Manager* domain is member of a Link Aggregation connection. • **sharedVLAN** The *Sub Ring Manager* domain is inactive because shared VLAN is active and the main ring also uses the Media Redundancy Protocol (MRP).

Setting	Description
Redundancy	Displays if the redundancy is available. When a component of the Sub Ring becomes inoperable, the redundant line takes over its function. Possible values: • **redGuaranteed** The redundancy is available. • **redNotGuaranteed** The redundancy is unavailable.
Port	Specifies the port that connects the device to the Sub Ring. Possible values: • **<Port number>**
Administrative mode	Specifies the mode of the *Sub Ring Manager* device. There are 2 *Sub-Ring Manager* devices that connect the Sub Ring to the base ring. As long as the Sub Ring is physically closed, one *Sub Ring Manager* device blocks its Sub Ring port. Possible values: • **manager** (default setting) The Sub Ring port forwards data packets. When this value is set on both devices that couple the Sub Ring to the base ring, the device with the greater MAC address functions as the **redundantManager**. • **redundantManager** The Sub Ring port is blocked while the Sub Ring is physically closed. If the Sub Ring is interrupted, then the Sub Ring port transmits the data packets. When this value is set on both devices that couple the Sub Ring to the base ring, the device with the greater MAC address functions as the **redundantManager**. • **singleManager** Use this value when the Sub Ring is coupled to the base ring through one single device. The prerequisite is that there are 2 instances of the Sub Ring in the table. Assign this value to both instances. The Sub Ring port of the instance with the greater port number is blocked while the Sub Ring is physically closed.
Operational mode	Displays the mode of the *Sub Ring Manager* device. Possible values: • **manager** The Sub Ring port forwards data packets. • **redundantManager** The Sub Ring port is blocked while the Sub Ring is physically closed. If the Sub Ring is interrupted, then the Sub Ring port transmits the data packets. • **singleManager** The Sub Ring is coupled to the base ring through one single device. This device blocks its Sub Ring port with the greater port number while the Sub Ring is physically closed. • **disabled** The Sub Ring is inactive.

Setting	Description
Port status	Displays the connection status on the Sub Ring port. Possible values: • **forwarding** The port is passing frames according to the forwarding behavior of IEEE 802.1D. • **disabled** The port is dropping every frame. • **blocked** The port is dropping every frame with the exception of the following cases: ◦ The port passes frames used by the selected ring protocol specified to pass blocked ports. ◦ The port passes frames from other protocols specified to pass blocked ports. • **not-connected** The port link is interrupted.
Sub Ring status	Displays the operational state of the Sub Ring in the *Sub Ring Manager* domain. Possible values: • **undefined** Undefined state • **open** The Sub Ring is opened. • **closed** The Sub Ring is closed.
VLAN	Specifies the VLAN to which this Sub Ring is assigned. If no VLAN exists with the specified VLAN ID, then the device sets up the VLAN. Possible values: • Available set-up VLANs (default setting: **0**) If you do not want to use a separate VLAN for this Sub Ring, then you keep the value as **0**.
Partner MAC	Displays the MAC address of the *Sub Ring Manager* device at the other end of the Sub Ring.
MRP domain	Specifies the MRP domain of the *Sub Ring Manager* device. Assign the same MRP domain name to every member of a Sub Ring. If you only use Schneider Electric devices, then you use the default value for the MRP domain; otherwise adjust this value if necessary. With multiple Sub Rings, the function allows you to use the same MRP domain name for the Sub Rings. Possible values: • Permitted MRP domain names (default setting: **255.255.255.255.255.255.255.255.255.255.255.255.255.255.2-55**)
Protocol	Specifies the protocol. Possible values: • **iec-62439-mrp**

Ring/Network Coupling

Loops during the configuration phase may lead to unintended equipment operation.

⚠WARNING

UNINTENDED EQUIPMENT OPERATION

- Set up each device of the Ring/Network Coupling configuration individually.
- Complete the configuration of the other devices of the ring configuration before you connect the redundant lines.

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 set up a HIPER Ring, MRP Ring, or Fast HIPER Ring before setting up the Ring/Network Coupling function.

In the **Switching > L2-Redundancy > FuseNet > Ring/Network Coupling** dialog, you can perform the following tasks:

- Display an overview of the existing Ring/Network Coupling.
- Set up a Ring/Network Coupling instance.
- Enable/disable the Ring/Network Coupling instance.
- Delete the Ring/Network Coupling instance.

When configuring the coupling ports, specify the following settings in the **Basic Settings > Port** dialog:

Port type	Bit rate	Port on	Autoneg	Manual configuration
TX	100 Mbit/s	**marked**	**unmarked**	**100M FDX**
TX	1 Gbit/s	**marked**	**marked**	–
Optical	100 Mbit/s	**marked**	**unmarked**	**100M FDX**
Optical	1 Gbit/s	**marked**	**marked**	–
Optical	2.5 Gbit/s	**marked**	–	**2.5G FDX**

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

If you set up VLANs, then note the VLAN configuration of the coupling and partner coupling ports. Specify the following settings for the coupling and partner coupling ports:

- **Switching > VLAN > Port** dialog
  - Value in the Port-VLAN ID column = **1**
  - Checkbox in the Ingress filtering column = unmarked
- **Switching > VLAN > Configuration** dialog
  - VLAN membership = **T**

Independently of the VLAN settings, the device sends the ring coupling frames with VLAN ID **1** and priority **7**. Verify that the device sends VLAN 1 frames tagged in the local ring and in the connected network. Tagging the VLAN frames maintains the priority of the ring coupling frames.

The Ring/Network Coupling function operates with test packets. The devices send their test packets with a VLAN tag, including VLAN ID **1** and the highest VLAN priority **7**. If the unblocked port is a member in VLAN **1** and transmits the data packets without a VLAN tag, then the device also sends test packets.

Operation

The following table presents the operation settings:

Setting	Description
Buttons	Reset: Disables the redundancy function and resets the parameters in the dialog to the default setting.
Operation	Enables/disables the Ring/Network Coupling function. Possible values: • **On** The Ring/Network Coupling function is enabled. • **Off** (default setting) The Ring/Network Coupling function is disabled.

Information

The following table presents the information settings:

Setting	Description
Redundancy	Displays if the redundancy is available. When a component of the ring becomes inoperable, the redundant line takes over its function. Possible values: • **redGuaranteed** The redundancy is available. • **redNotGuaranteed** The redundancy is unavailable.
Configuration failure	You have set up the function incorrectly, or there is no ring port connection. Possible values: • **noError** • **slaveCouplingLinkError** The coupling line is not connected to the coupling port of the slave device. Instead, the coupling line is connected to another port of the slave device. • **slaveControlLinkError** The control port of the slave device has no data link. • **masterControlLinkError** The control line is not connected to the control port of the master device. Instead, the control line is connected to another port of the master device. • **twoSlaves** The control line connects two slave devices. • **localPartnerLinkError** The partner coupling line is not connected to the partner coupling port of the slave device. Instead, the partner coupling line is connected to another port of the slave device in **one-switch coupling** mode. • **localInvalidCouplingPort** In **one-switch coupling** mode, the coupling line is not connected on the same device as the partner line. Instead, the coupling line is connected to another device. • **couplingPortNotAvailable** The coupling port is not available because the module to which the port refers is not available or the port does not exist on this module. • **controlPortNotAvailable** The control port is not available because the module to which the port refers is not available or the port does not exist on this module. • **partnerPortNotAvailable** The partner coupling port is not available because the module to which the port refers is not available or the port does not exist on this module.

Mode

The following table presents the mode setting:

Setting	Description
Type	Specifies the method used to couple the networks together. Possible values: • **one-switch coupling** (default setting) Specify the port settings in the Coupling port and Partner coupling port frames. • **two-switch coupling, master** Specify the port settings in the Coupling port frame. • **two-switch coupling with control line, master** Specify the port settings in the Coupling port and Control port frames. • **two-switch coupling, slave** Specify the port settings in the Coupling port frame. • **two-switch coupling with control line, slave** Specify the port settings in the Coupling port and Control port frames.

Coupling Port

The following table presents the coupling port settings:

Setting	Description
Port	Specifies the port to which you connect the redundant link. Possible values: • **-** No port selected. • **<Port number>** If you also have set up ring ports, then specify the coupling and ring ports on different ports. To help prevent continuous loops, the device disables the coupling port in the following cases: • disabling the function • changing the configuration while the connections are operating on the ports When the device has deactivated the coupling port, the Port on checkbox is unmarked in the **Basic Settings > Port** dialog, Configuration tab.
State	Displays the status of the selected port. Possible values: • **active** The port is active. • **standby** The port is in stand-by mode. • **not-connected** The port is not connected. • **not-applicable** The port is incompatible with the set-up control mode.

Partner Coupling Port

The following table presents the partner couping port settings:

Setting	Description
Port	Specifies the port on which you connect the partner port. The field is visible when you select the **one-switch coupling** radio button in the Mode frame. Possible values: • **-** (default setting) No port selected. • **<Port number>** If you also have set up ring ports, then specify the coupling and ring ports on different ports.
Interface index	Displays the index number of the port that the partner device uses for the connection. The field is visible when you select a two-switch coupling method in the Mode frame.
State	Displays the status of the selected port. Possible values: • **active** The port is active. • **standby** The port is in stand-by mode. • **not-connected** The port is not connected. • **not-applicable** The port is incompatible with the set-up control mode.
IP address	Displays the IP address of the partner device, when the devices are connected. The prerequisite is that you enable the partner device in the network. The field is visible when you select a two-switch coupling method in the Mode frame.

Control Port

The following table presents the control port settings:

Setting	Description
Port	Displays the port on which you connect the control line. Possible values: • **-** (default setting) No port selected. • **<Port number>**
State	Displays the status of the selected port. Possible values: • **active** The port is active. • **standby** The port is in stand-by mode. • **not-connected** The port is not connected. • **not-applicable** The port is incompatible with the set-up control mode.

Configuration

The following table presents the configuration settings:

Setting	Description
Redundancy mode	Specifies if the device responds to a detected failure in the remote ring or network. Possible values: • **redundant ring/network coupling** Either the main line or the redundant line is active. Both lines are not active simultaneously. If the device detects that the link is interrupted between the devices in the remote ring or network, then the standby device keeps the redundant port in the standby mode. • **extended redundancy** (default setting) If the device detects a potential connection interruption between the devices in the remote ring or network, then the standby device forwards data on the redundant port. In this case, the main line and the redundant line are active simultaneously. This setting allows you to maintain continuity in the remote network. **NOTE:** During the reconfiguration period, package duplications can occur. Therefore, if your application is able to detect package duplications, then you can select this setting.
Coupling mode	Specifies the mode of coupling a specific type of network. Possible values: • **ring coupling** (default setting) The device couples redundant rings. The device allows you to couple rings that use the following redundancy protocols: ◦ HIPER Ring ◦ Fast HIPER Ring ◦ MRP Ring • **network coupling** The device couples network segments. The function allows you to couple mesh and bus networks together.

Redundant Coupling Protocol

Loops during the configuration phase may lead to unintended equipment operation.

⚠WARNING

UNINTENDED EQUIPMENT OPERATION

- Set up each device of the Redundant Coupling Protocol (RCP) configuration individually.
- Complete the configuration of the other devices of the ring configuration before you connect the redundant lines.

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 greater-level network is more of a challenge.

When you want to use a standard protocol such as MRP for the ring redundancy and RSTP to couple the rings together, the RCP function **Switching > L2-Redundancy > FuseNet > RCP** provide options for you.

Do not use the following redundancy protocols on the ports of the RCP primary ring and the RCP secondary rings:

- Sub Ring
- Ring/Network Coupling

Operation

The following table presents the operation setting:

Setting	Description
Operation	Enables/disables the RCP function. Possible values: • **On** The RCP function is enabled. **⚠WARNING** **UNINTENDED EQUIPMENT OPERATION** Do not enable the **RCP** function on a device on which the **Ring manager** function is enabled. **Failure to follow these instructions can result in death, serious injury, or equipment damage.** • **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.

The following table presents the primary ring/network secondary ring/network:

Setting	Description
Inner port	Specifies the inner port number in the primary ring/secondary ring. The port is directly connected to the partner bridge. Possible values: • **-** (default setting) No port selected. • **<Port number>**
Outer port	Specifies the outer port number in the primary ring/secondary ring. Possible values: • **-** (default setting) No port selected. • **<Port number>**
Primary Ring protocol/Secondary Ring protocol	Displays the protocol that is active on the redundant coupling port in the devices in the primary/secondary ring. If the RCP function is disabled, then the device displays the **NONE** value for both primary and secondary ring protocols. If you disable the active protocol on either primary or secondary ring, the device will display the **NONE** value for that respective ring protocol.

Coupler Configuration

The following table presents the coupler configuration settings:

Setting	Description
Role	Specifies the role of the local device. Possible values: • **master** The device operates as master. • **slave** The device operates as slave. • **auto** (default setting) The device automatically selects its role as master or slave.
Current role	Displays the **current role** of the local device. The value can be different from the set-up role: • If you set up both partner bridges as **auto**, then the partner bridge that is currently coupling the instances takes the **master** role. The other partner bridge takes the **slave** role. • If both partner bridges are set up as **master** or both as **slave**, then the partner bridge with the smaller Basis MAC address takes the **master** role. The other partner bridge takes the **slave** role. • If the protocol is started and the partner bridge cannot be found for a bridge in the set-up role **master**, **slave** or **auto**, then the bridge sets its own role to **listening**. • If the device detects a potential configuration problem, for example, the inner ring ports are connected crosswise, then the device sets its role to **error**.
Timeout [ms]	Specifies the maximum time, in milliseconds, during which the slave device waits for test packets from the master device on the outer ports before the slave device takes over the coupling. This only applies in the state in which both inner ports of the slave device have lost the connection to the master device. Specify the timeout longer than the longest assumable interruption time for the redundancy protocol of the faster instance. Otherwise, loops can occur. Possible values: • **5..60000** in steps of 5 (default setting: **250**) If you enter a value which is not a multiple of 5, then the device rounds up the value to the nearest multiple of 5.
Partner MAC address	Displays the basic MAC address of the partner device.
Partner 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.

Diagnostics

The menu contains the following dialogs:

- Status Configuration, page 292
- System, page 313
- Email Notification, page 320
- Syslog, page 327
- Ports, page 331
- LLDP, page 352
- Loop Protection, page 358
- SFlow, page 361
- Report, page 364

Status Configuration

This menu **Diagnostics > Status Configuration** contains the following dialogs:

- Device Status, page 292
- Security Status, page 296
- Signal Contact, page 302
- MAC Notification, page 307
- Alarms (Traps), page 308

Device Status

The device status **Diagnostics > Status Configuration > Device Status** provides an overview of the overall condition of the device. Many process visualization systems record the device status for a device to present its condition in graphic form.

The device displays its 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, page 293
- Port, page 295
- Status, page 295

Global

Device Status

The following table presents the device status setting:

Setting	Description
Device status	Displays the status of the device. The device determines the status from the individual monitored parameters. Possible values: • **ok** • **error** The device displays this value to indicate a detected error in one of the monitored parameters.

Traps

The following table presents the traps setting:

Setting	Description
Send trap	Activates/deactivates the sending of SNMP traps when the device detects a change in a monitored function. Possible values: • **marked** (default setting) The sending of SNMP traps is active. The prerequisite is that in the **Diagnostics > Status Configuration > Alarms (Traps)** dialog the Alarms (Traps) function is enabled and at least one trap destination is specified. If the device detects a change in the monitored functions, then the device sends an SNMP trap. • **unmarked** The sending of SNMP traps is inactive.

Table

For information on how to customize the appearance of the table, see Working with tables, page 25.

The following table presents the table settings:

Setting	Description
Connection errors	Activates/deactivates the monitoring of the link status of the port/interface. Possible values: • **marked** Monitoring is active. If the link interrupts on a monitored port/interface, then in the Device status frame, the value changes to **error**. In the Port tab, you have the option of selecting the ports/interfaces to be monitored individually. • **unmarked** (default setting) Monitoring is inactive.
Temperature	Activates/deactivates the monitoring of the temperature in the device. Possible values: • **marked** (default setting) Monitoring is active. If the temperature exceeds the specified upper threshold value or falls below the specified lower threshold value, then in the Device status frame, the value changes to **error**. • **unmarked** Monitoring is inactive. You specify the temperature threshold values in the **Basic Settings > System** dialog, Upper temp. limit [°C] field and Lower temp. limit [°C] field.
External memory removed	Activates/deactivates the monitoring of the active external memory (**ENVM**). Possible values: • **marked** Monitoring is active. If you remove the active external memory (**ENVM**) from the device, then in the Device status frame, the value changes to **error**. • **unmarked** (default setting) Monitoring is inactive.
External memory not in sync with NVM	Activates/deactivates the monitoring of the configuration profile in the device and in the external memory (**ENVM**). Possible values: • **marked** Monitoring is active. In the Device status frame, the value changes to **error** in the following situations: ◦ The configuration profile only exists in the device. ◦ The configuration profile in the device differs from the configuration profile in the external memory (**ENVM**). • **unmarked** (default setting) Monitoring is inactive.

Setting	Description
Ring redundancy	Activates/deactivates the monitoring of the ring redundancy. Possible values: • **marked** Monitoring is active. In the Device status frame, the value changes to **error** in the following situations: ◦ The device operates as a Redundancy Manager. The redundancy function of the device uses the alternative connection. There is no longer a redundancy reserve. ◦ The device, as a ring participant, has detected an error in its ring redundancy settings. • **unmarked** (default setting) Monitoring is inactive.
Power supply	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 error, then in the Device status frame, the value changes to **error**. • **unmarked** Monitoring is inactive.

Port

Table

For information on how to customize the appearance of the table, see Working with tables, page 25.

The following table presents the table settings:

Setting	Description
Port	Displays the port number.
Propagate connection error	Activates/deactivates the monitoring of the link on the port/interface. Possible values: • **marked** Monitoring is active. If the link on the selected port/interface is interrupted, then in the Device status frame, the value changes to **error**. • **unmarked** (default setting) Monitoring is inactive. This setting takes effect when you mark the Connection errors checkbox in the Global tab.

Status

Table

For information on how to customize the appearance of the table, see Working with tables, page 25.

The following table presents the table settings:

Setting	Description
Timestamp	Displays the date and time of the event.
Cause	Displays the event which caused the SNMP trap.

Security Status

This dialog **Diagnostics > Status Configuration > Security Status** gives you an overview of the **Security Status** settings in the device.

The device displays its status as **error** or **ok** in the **Security Status** frame. The device determines this status from the individual monitoring results.

The device displays detected error in the Status tab and also in the **Basic Settings > System** dialog, Security status frame.

The dialog contains the following tabs:

- Global, page 296
- Port, page 301
- Status, page 302

Global

Security status

The following table presents the security status setting:

Setting	Description
Security status	Displays the status of the security-relevant settings in the device. The device determines the status from the individual monitored parameters. Possible values: • **ok** • **error** The device displays this value to indicate a detected error in one of the monitored parameters.

Traps

The following table presents the traps setting:

Setting	Description
Send trap	Activates/deactivates the sending of SNMP traps when the device detects a change in a monitored function. Possible values: • **marked** The sending of SNMP traps is active. The prerequisite is that in the **Diagnostics > Status Configuration > Alarms (Traps)** dialog the Alarms (Traps) function is enabled and at least one trap destination is specified. If the device detects a change in the monitored functions, then the device sends an SNMP trap. • **unmarked** (default setting) The sending of SNMP traps is inactive.

Table

For information on how to customize the appearance of the table, see Working with tables, page 25.

The following table presents the table settings:

Setting	Description
Password default settings unchanged	Activates/deactivates the monitoring of the password for the locally set up user account **admin**. Possible values: • **marked** (default setting) Monitoring is active. If the password is set to the default setting for the **admin** user account, then in the Security status frame, the value changes to **error**. • **unmarked** Monitoring is inactive. You set the password in the **Device Security > User Management** dialog.
Min. password length shorter than 8	Activates/deactivates the monitoring of the Min. password length policy. Possible values: • **marked** (default setting) Monitoring is active. If the value for the Min. password length policy is less than **8**, then in the Security status frame, the value changes to **error**. • **unmarked** Monitoring is inactive. You specify the Min. password length policy in the **Device Security > User Management** dialog in the Configuration frame.
Password policy settings deactivated	Activates/deactivates the monitoring of the Password policies settings. Possible values: • **marked** (default setting) Monitoring is active. If the value for at least one of the following policies is less than **1**, then in the Security status frame, the value changes to **error**. ◦ Upper-case characters (min.) ◦ Lower-case characters (min.) ◦ Digits (min.) ◦ Special characters (min.) • **unmarked** Monitoring is inactive. You specify the policy settings in the **Device Security > User Management** dialog in the Password policy frame.
User account password policy check deactivated	Activates/deactivates the monitoring of the Policy check function. Possible values: • **marked** Monitoring is active. If the Policy check function is inactive for at least one user account, then in the Security status frame, the value changes to **error**. • **unmarked** (default setting) Monitoring is inactive. You activate the Policy check function in the **Device Security > User Management** dialog.
Telnet server active	Activates/deactivates the monitoring of the Telnet server. Possible values: • **marked** (default setting) Monitoring is active. If you enable the Telnet server, then in the Security status frame, the value changes to **error**. • **unmarked** Monitoring is inactive. You enable/disable the Telnet server in the **Device Security > Management Access > Server** dialog, Telnet tab.

Setting	Description
HTTP server active	Activates/deactivates the monitoring of the HTTP server. Possible values: • **marked** (default setting) Monitoring is active. If you enable the HTTP server, then in the Security status frame, the value changes to **error**. • **unmarked** Monitoring is inactive. You enable/disable the HTTP server in the **Device Security > Management Access > Server** dialog, HTTP tab.
SNMP unencrypted	Activates/deactivates the monitoring of the SNMP server. Possible values: • **marked** (default setting) Monitoring is active. If at least one of the following conditions applies, then in the Security status frame, the value changes to **error**: ◦ The SNMPv1 function is enabled. ◦ The SNMPv2 function is enabled. ◦ The encryption for SNMPv3 is disabled. You enable the encryption in the **Device Security > User Management** dialog, in the SNMP encryption type column. • **unmarked** Monitoring is inactive. You specify the settings for the SNMP agent in the **Device Security > Management Access > Server** dialog, SNMP tab.
Access to System Monitor 1 through the serial interface possible	Activates/deactivates monitoring the option of starting the System Monitor 1. When active, you can start the System Monitor 1 through the serial connection during system startup. Possible values: • **marked** Monitoring is active. If you activate the option of starting the System Monitor 1, then in the Security status frame, the value changes to **error**. • **unmarked** (default setting) Monitoring is inactive. If you activate the option of starting the System Monitor 1, the value in the Security status frame remains unchanged. You activate/deactivate the option of starting the System Monitor 1 in the **Diagnostics > System > Selftest** dialog.
Saving the configuration profile on the external memory possible	Activates/deactivates the monitoring of the configuration profile in the external memory (**ENVM**). Possible values: • **marked** Monitoring is active. If you activate the saving of the configuration profile in the external memory (**ENVM**), then in the Security status frame, the value changes to **error**. • **unmarked** (default setting) Monitoring is inactive. You activate/deactivate the saving of the configuration profile in the external memory (**ENVM**) in the **Basic Settings > External Memory** dialog.
Link interrupted on enabled device ports	Activates/deactivates the monitoring of the link on the active ports. Possible values: • **marked** Monitoring is active. If the link interrupts on an active port, then in the Security status frame, the value changes to **error**. In the Port tab, you have the option of selecting the ports to be monitored individually. • **unmarked** (default setting) Monitoring is inactive.

Setting	Description
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 > Global** dialog.
Load unencrypted config from external memory	Activates/deactivates the monitoring of loading unencrypted configuration profiles from the external memory (**ENVM**). Possible values: • **marked** (default setting) Monitoring is active. If the settings allow the device to load an unencrypted configuration profile from the external memory (**ENVM**), then in the Security status frame, the value changes to **error**. If the following preconditions are fulfilled, then the Security status frame in the **Basic Settings > System** dialog, displays an alarm. ◦ The configuration profile stored in the external memory (**ENVM**) is unencrypted. and ◦ The Config priority column in the **Basic Settings > External Memory** dialog has the value **first**. • **unmarked** Monitoring is inactive.
IEC 61850-MMS active	Activates/deactivates the monitoring of the IEC 61850-MMS function. Possible values: • **marked** (default setting) Monitoring is active. If you enable the IEC 61850-MMS function, then in the Security status frame, the value changes to **error**. • **unmarked** Monitoring is inactive. You enable/disable the IEC 61850-MMS function in the **Advanced > Industrial Protocols > IEC 61850-MMS** dialog, Operation frame.
Self-signed HTTPS certificate present	Activates/deactivates the monitoring of the digital certificate of the HTTPS server. Possible values: • **marked** (default setting) Monitoring is active. If the HTTPS server uses a self-generated digital certificate, then in the Security status frame, the value changes to **error**. • **unmarked** Monitoring is inactive.
Modbus TCP active	Activates/deactivates the monitoring of the Modbus TCP function. Possible values: • **marked** (default setting) Monitoring is active. If you enable the Modbus TCP function, then in the Security status frame, the value changes to **error**. • **unmarked** Monitoring is inactive. You enable/disable the Modbus TCP function in the **Advanced > Industrial Protocols > Modbus TCP** dialog, Operation frame.

Setting	Description
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.
Secure Boot is inactive	Activates/deactivates the monitoring of the Secure Boot function. Possible values: • **marked** (default setting) Monitoring is active. Until you activate the Secure Boot function, the value in the Security status frame continues to display **error**. Once activated, the value changes to **ok**. • **unmarked** Monitoring is inactive. You activate the Secure Boot function in the **Basic Settings > Software** dialog, Software update frame.
Support Mode is active	Activates/deactivates the monitoring of the Support Mode function. Possible values: • **marked** (default setting) Monitoring is active. If the value in the Security status frame changes to **error** due to this setting, contact the manufacturer. • **unmarked** Monitoring is inactive.

Port

Table

For information on how to customize the appearance of the table, see Working with tables, page 25.

The following table presents the table settings:

Setting	Description
Port	Displays the port number.
Link interrupted on enabled device ports	Activates/deactivates the monitoring of the link on the active ports. Possible values: • **marked** Monitoring is active. If the port is enabled (**Basic Settings > Port** dialog, Configuration tab, Port on checkbox is **marked**) and the link is down on the port, then in the Security status frame, the value changes to **error**. • **unmarked** (default setting) Monitoring is inactive. This setting takes effect when you mark the Link interrupted on enabled device ports checkbox in the **Diagnostics > Status Configuration > Security Status** dialog, Global tab.

Status

Table

For information on how to customize the appearance of the table, see Working with tables, page 25.

The following table presents the table settings:

Setting	Description
Timestamp	Displays the date and time of the event.
Cause	Displays the event which caused the SNMP trap.

Signal Contact

The signal contact is a potential-free relay contact. The device thus allows you to 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.

This menu **Diagnostics > Status Configuration > Signal Contact** contains the following dialogs:

- Signal Contact 1 / Signal Contact 2, page 302

Signal Contact 1 / Signal Contact 2

In this dialog **Diagnostics > Status Configuration > Signal Contact > Signal Contact 1**, 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, page 303
- Port, page 306
- Status, page 306

Global

Configuration

The following table presents the configuration settings:

Setting	Description
Mode	Specifies which events the signal contact indicates. Possible values: • **Manual setting** (default setting for Signal Contact 2, if present) You use this setting to manually open or close the signal contact, for example to turn on or off a remote device. See the Contact option list. • **Monitoring correct operation** (default setting) Using this setting the signal contact indicates the status of the parameters specified in the table below. • **Device status** Using this setting the signal contact indicates the status of the parameters monitored in the **Diagnostics > Status Configuration > Device Status** dialog. In addition, you can read the status in the Signal contact status frame. • **Security status** Using this setting the signal contact indicates the status of the parameters monitored in the **Diagnostics > Status Configuration > Security Status** dialog. In addition, you can read the status in the Signal contact status frame. • **Device/Security status** Using this setting the signal contact indicates the status of the parameters monitored in the **Diagnostics > Status Configuration > Device Status** and the **Diagnostics > Status Configuration > Security Status** dialog. In addition, you can read the status in the Signal contact status frame.
Contact	Toggles the signal contact manually. The prerequisite is that from the Mode drop-down list the **Manual setting** item is selected. Possible values: • **open** The signal contact is opened. • **close** The signal contact is closed.

Signal Contact Status

The following table presents the signal contact status settings:

Setting	Description
Signal contact status	Displays the 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

The following table presents the trap configuration setting:

Setting	Description
Send trap	Activates/deactivates the sending of SNMP traps when the device detects a change in a monitored function. Possible values: • **marked** The sending of SNMP traps is active. The prerequisite is that in the **Diagnostics > Status Configuration > Alarms (Traps)** dialog the Alarms (Traps) function is enabled and at least one trap destination is specified. If the device detects a change in the monitored functions, then the device sends an SNMP trap. • **unmarked** (default setting) The sending of SNMP traps is inactive.

Table

For information on how to customize the appearance of the table, see Working with tables, page 25.

The following table presents the table settings:

Setting	Description
Connection errors	Activates/deactivates the monitoring of the link status of the port/interface. Possible values: • **marked** Monitoring is active. If the link interrupts on a monitored port/interface, then the signal contact opens. In the Port tab, you have the option of selecting the ports/interfaces to be monitored individually. • **unmarked** (default setting) Monitoring is inactive.
Temperature	Activates/deactivates the monitoring of the temperature in the device. Possible values: • **marked** (default setting) Monitoring is active. If the temperature exceeds the specified upper threshold value or falls below the specified lower threshold value, then the signal contact opens. • **unmarked** Monitoring is inactive. You specify the temperature threshold values in the **Basic Settings > System** dialog, Upper temp. limit [°C] field and Lower temp. limit [°C] field.
External memory removed	Activates/deactivates the monitoring of the active external memory (**ENVM**). Possible values: • **marked** Monitoring is active. If you remove the active external memory (**ENVM**) from the device, then the signal contact opens. • **unmarked** (default setting) Monitoring is inactive.
External memory not in sync with NVM	Activates/deactivates the monitoring of the configuration profile in the device and in the external memory (**ENVM**). Possible values: • **marked** Monitoring is active. The signal contact opens in the following situations: ◦ The configuration profile only exists in the device. ◦ The configuration profile in the device differs from the configuration profile in the external memory (**ENVM**). • **unmarked** (default setting) Monitoring is inactive.
Ring redundancy	Activates/deactivates the monitoring of the ring redundancy. Possible values: • **marked** Monitoring is active. The signal contact opens in the following situations: ◦ The device operates as a Redundancy Manager. The redundancy function of the device uses the alternative connection. There is no longer a redundancy reserve. ◦ The device, as a ring participant, has detected an error in its ring redundancy settings. • **unmarked** (default setting) Monitoring is inactive.

Setting	Description
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 error, then the signal contact opens. • **unmarked** Monitoring is inactive.

Port

Table

For information on how to customize the appearance of the table, see Working with tables, page 25.

The following table presents the table settings:

Setting	Description
Port	Displays the port number.
Propagate connection error	Activates/deactivates the monitoring of the link on the port/interface. Possible values: • **marked** Monitoring is active. If the link interrupts on the selected port/interface, then the signal contact opens. • **unmarked** (default setting) Monitoring is inactive. This setting takes effect when you mark the Connection errors checkbox in the Global tab.

Status

Table

For information on how to customize the appearance of the table, see Working with tables, page 25.

The following table presents the table settings:

Setting	Description
Timestamp	Displays the date and time of the event.
Cause	Displays the event which caused the SNMP trap.

MAC Notification

Diagnostics > Status Configuration > MAC Notification

The device allows you to track changes in the network using the MAC address of the devices in the network. The device saves the combination of port and MAC address in its MAC address table (forwarding database). If the device (un)learns the MAC address of a (dis)connected device, then the device sends an SNMP trap.

This function is intended for ports to which you connect end devices and thus the MAC address changes infrequently.

Operation

The following table presents the operation setting:

Setting	Description
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

The following table presents the configuration setting:

Setting	Description
Interval [s]	Specifies the send interval in seconds. If the device (un)learns the MAC address of a (dis)connected device, then the device sends an SNMP trap after this time. Possible values: • **0..2147483647 (2^{31}-1)** (default setting: **1**) Before sending an SNMP trap, the device registers up to 20 MAC addresses. If the device detects a high number of changes, then the device sends the SNMP trap before the send interval expires.

Table

For information on how to customize the appearance of the table, see Working with tables, page 25.

The following table presents the table settings:

Setting	Description
Port	Displays the port number.
Active	Activates/deactivates the MAC Notification function on the port. Possible values: • **marked** The MAC Notification function is active on the port. The device sends an SNMP trap in case of one of the following events: ◦ The device learns the MAC address of a newly connected device. ◦ The device unlearns the MAC address of a disconnected device. The prerequisite is that in the **Diagnostics > Status Configuration > Alarms (Traps)** dialog the Alarms (Traps) function is enabled and at least one trap destination is specified. • **unmarked** (default setting) The MAC Notification function is inactive on the port.
Last MAC address	Displays the MAC address of the device last connected on or disconnected from the port. The device detects the MAC addresses of devices which are connected as follows: • directly connected to the port • connected to the port through other devices in the network
Last MAC status	Displays the status of the Last MAC address value on this port. Possible values: • **added** The device detected that another device was connected at the port. • **removed** The device detected that the connected device was removed from the port. • **other** The device did not detect a status.

Alarms (Traps)

The device allows you to send an SNMP trap in response to specific events.

You specify the events for which the device triggers an SNMP trap in the following dialogs:

- **Diagnostics > Status Configuration > Device Status**
- **Diagnostics > Status Configuration > Security Status**
- **Diagnostics > Status Configuration > MAC Notification**

This menu **Diagnostics > Status Configuration > Alarms (Traps)** contains the following dialogs:

- Trap V3 User Management, page 308
- Trap Destinations, page 311

Trap V3 User Management

In this dialog **Diagnostics > Status Configuration > Alarms (Traps) > Trap V3 User Management**, you specify the SNMPv3 trap users who can send SNMP traps to the trap destination(s). The device supports encrypted SNMPv3 traps and authentication for sending.

SNMPv3 trap users have permission to send SNMPv3 traps to the specified SNMPv3 trap hosts.

SNMPv3 trap users are intended for sending SNMPv3 traps to SNMPv3 trap hosts exclusively. SNMPv3 trap users are different from the user accounts set up in the device. Do not confuse them. See the **Device Security > User Management** dialog.

Table

For information on how to customize the appearance of the table, see Working with tables, page 25.

The following table presents the table settings:

Setting	Icon	Description
Buttons	 Add	Opens the Create window to add a table row. The device adds an SNMPv3 trap user with the parameters you specify in this window. • From the User to be cloned drop-down list, you select the user account, from which the device clones the authentication settings. You need to select one of the user accounts set up in the device. You set up device user accounts in the **Device Security > User Management** dialog. • In the Trap User name field, you specify the name for the SNMPv3 trap user. Possible values: ◦ Alphanumeric ASCII character string with 1..32 characters • From the Trap User Auth Protocol drop-down list, you select the protocol for sending SNMPv3 traps with authentication. Possible values: ◦ none The device sends unencrypted SNMPv3 traps without authentication. ◦ hmacmd5 The device sends SNMPv3 traps signed using the Message-Digest Algorithm 5 (HMACMD5). Available if this algorithm is already set for the user to be cloned. ◦ hmacsha The device sends SNMPv3 traps signed using the Secure Hash Algorithm (HMACSHA). Available if this algorithm is already set for the user to be cloned. • In the Trap User Auth Password field, you specify the password that the SNMPv3 trap user uses to authenticate before sending. Possible values: ◦ Alphanumeric ASCII character string with 8..64 characters The prerequisite is that from the Trap User Auth Protocol drop-down list, an item other than none is selected. • From the Trap User Priv Protocol drop-down list, you select the protocol that the device uses for this user to encrypt the SNMPv3 traps. Possible values: ◦ none (default setting) No encryption. ◦ des *Data Encryption Standard (DES)*. Available if this protocol is already set for the user to be cloned. ◦ aesCfb128 *Advanced Encryption Standard (AES128)*. Available if this protocol is already set for the user to be cloned. • In the Trap User Priv Password field, you specify the password that the SNMPv3 trap user uses to authenticate before sending. Possible values: ◦ Alphanumeric ASCII character string with 8..64 characters The prerequisite is that from the Trap User Auth Protocol drop-down list, an item other than none is selected. When you click the Ok button, the device adds the table row for the SNMPv3 trap user. If you have selected an item other than none in the Trap User Auth Protocol or Trap User Priv Protocol drop-down list, the Credentials window opens first. Then, you enter the required password(s). Even if you enter an incorrect password, the device still adds the SNMPv3 trap user. However, when the device sends SNMPv3 traps, the trap destination cannot decrypt them.
	 Remove	Removes the selected table row.
SNMPv3 Notification User		Displays the name of the SNMPv3 trap user.
Authentication		Displays the protocol for sending SNMPv3 traps with authentication in the context of the SNMPv3 trap user.
Auth Password		Displays ***** (asterisks) instead of the authentication password of the SNMPv3 trap user. To change the password, add another SNMPv3 trap user and then delete the existing one.
Privacy		Displays the protocol that the device uses for this user to encrypt the SNMPv3 traps.

Setting	Icon	Description
Priv Password		Displays ***** (asterisks) instead of the password that the SNMPv3 trap user uses to authenticate before sending. To change the password, add another SNMPv3 trap user and then delete the existing one.
User status		Displays the status of the SNMPv3 trap user. Possible values: • **marked** (default setting) The SNMPv3 trap user is active. • **unmarked** The SNMPv3 trap user is inactive.

Trap Destinations

In this dialog **Diagnostics > Status Configuration > Alarms (Traps) > Trap Destinations**, you specify the trap destinations to which the device sends SNMP traps.

For SNMPv3, the following conditions apply:

- The device sends SNMPv3 traps to the trap destination specified for the relevant SNMPv3 trap user.
- The device supports a maximum of 10 trap destinations for SNMPv3.

Operation

The following table presents the operation setting:

Setting	Description
Operation	Enables/disables sending SNMP traps. Possible values: • **On** (default setting) Sending SNMP traps is enabled. • **Off** Sending SNMP traps is disabled.

SNMPv1/v2 Trap Community

The following table presents the SNMPv1/v2 trap community setting:

Setting	Description
Name	Specifies the community string that the device sends in each SNMPv1/v2 trap for authentication to the trap destination. Possible values: • Alphanumeric ASCII character string with 0..64 characters **trap** (default setting)

Table

For information on how to customize the appearance of the table, see Working with tables, page 25.

The following table presents the table settings:

Setting	Icon	Description
Buttons	 Add	Opens the Create window to add a table row. Thus, you set up a trap destination on the device. • In the Name field, you specify a name for the trap destination. Possible values: ◦ Alphanumeric ASCII character string with 1..32 characters • From the Type drop-down list, you select the SNMP version which the device uses to send SNMP traps to the trap destination. Possible values: ◦ **V1** SNMP version 1 Do not use this setting if you transmit data over untrusted networks. ◦ **V3** SNMP version 3 • In the Address field, you specify the IP address and the port of the trap destination. Possible values: ◦ **<IPv4 address>:<port>** If you do not specify a port, then the device automatically adds port **162** to the trap destination. • From the SNMPv3 Trap user drop-down list, you select the SNMPv3 trap user in whose context the device sends SNMPv3 traps to the trap destination. The prerequisite is that you select the **V3** item from the Type drop-down list. You select one of the users that you have set up in the **Diagnostics > Status Configuration > Alarms (Traps) > Trap V3 User Management** dialog. • From the Security level drop-down list, you select whether the device sends the SNMPv3 traps encrypted and whether authentication is required before sending. The prerequisite is that you select the **V3** item from the Type drop-down list. Possible values: ◦ **noAuthNoPriv** The device sends unencrypted SNMPv3 traps without authentication. Do not use this setting if you transmit data over untrusted networks. ◦ **authNoPriv** The device sends unencrypted SNMPv3 traps. The user needs to authenticate before sending SNMPv3 traps. ◦ **authPriv** The device sends encrypted SNMPv3 traps. The user needs to authenticate before sending SNMPv3 traps.
	 Re-move	Removes the selected table row.
Name		Displays the name you specified for the trap destination (trap host).
SNMP Protocol		Displays the SNMP version which the device uses to send SNMP traps to the trap destination.
Address		Specifies the IP address and the port of the trap destination (trap host). Possible values: • **<IPv4 address>:<port>** If you do not specify a port, then the device automatically adds port **162** to the trap destination.
SNMPv3 Trap user		Specifies the SNMPv3 trap user that the device uses to send SNMPv3 traps to the trap destination. You select one of the SNMPv3 trap users that you have set up in the **Diagnostics > Status Configuration > Alarms (Traps) > Trap V3 User Management** dialog.

Setting	Icon	Description
Security level		Specifies whether the device sends the SNMPv3 traps encrypted and whether authentication is required before sending. Possible values: • **noAuthNoPriv** The device sends unencrypted SNMPv3 traps without authentication. Do not use this setting if you transmit data over untrusted networks. • **authNoPriv** The device sends unencrypted SNMPv3 traps. The user needs to authenticate before sending SNMPv3 traps. • **authPriv** The device sends encrypted SNMPv3 traps. The user needs to authenticate before sending SNMPv3 traps.
Type		Displays the notification type.
Active		Activates/deactivates the sending of SNMP traps to the trap destination. Possible values: • **marked** (default setting) The sending of SNMP traps to this trap destination is active. • **unmarked** The sending of SNMP traps to this trap destination is inactive.

System

This menu **Diagnostics > System** contains the following dialogs:

- System Information, page 313
- Hardware State, page 313
- IP Address Conflict Detection, page 314
- ARP, page 317
- Selftest, page 318

System Information

This dialog **Diagnostics > System > System Information** displays the 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.

The following table presents the system information setting:

Setting	Description
Buttons	Save system information: Saves the HTML page on your PC using the web browser dialog.

Hardware State

This dialog **Diagnostics > System > Hardware State** provides information about the distribution and state of the flash memory of the device.

Information

The following table presents the information setting:

Setting	Description
Operating hours	Displays the total operating time of the device since it was delivered. Possible values: • **..d ..h ..m ..s** Day(s) Hour(s) Minute(s) Second(s)

Table

For information on how to customize the appearance of the table, see Working with tables, page 25.

The following table presents the table settings:

Setting	Description
Flash region	Displays the name of the parameter, for example for the relevant memory area.
Description	Displays a description for the parameter.
Flash sectors	Displays how many sectors are assigned to the memory area.
Sector erase operations	Displays how many times the device has overwritten the sectors of the memory area.

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 **Diagnostics > System > IP Address Conflict Detection**, 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

The following table presents the operation setting:

Setting	Description
Operation	Enables/disables the IP Address Conflict Detection function. Possible values: • **On** (default setting) The IP Address Conflict Detection function is enabled. The device verifies that its IP address is unique in the network. • **Off** The IP Address Conflict Detection function is disabled.

Information

The following table presents the information setting:

Setting	Description
Conflict detected	Displays if an address conflict currently exists. Possible values: • **marked** The device detects an address conflict. • **unmarked** The device does not detect an address conflict.

Configuration

The following table presents the configuration settings:

Setting	Description
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 verification. ◦ When the device resolves the address conflict, the device management returns to the network again. • **passive** Passive address conflict detection. The device analyzes the data stream in the network. If another device in the network is using the same IP address, then the device initially “defends” its IP address. The device stops sending if the other device keeps sending with the same IP address. ◦ As a “defence” the device sends gratuitous ARP data packets. The device repeats this procedure for the number of times specified in the Address protections field. ◦ If the other device continues sending with the same IP address, then after the period specified in the Release delay [s] field, the device periodically checks if the address conflict still exists. ◦ When the device resolves the address conflict, the device management returns to the network again.
Send periodic ARP probes	Activates/deactivates the periodic address conflict detection. Possible values: • **marked** (default setting) The periodic address conflict detection is active. ◦ The device periodically sends an ARP probe data packet every 90 to 150 seconds and waits for the time specified in the Detection delay [ms] field for a response. ◦ If the device detects an address conflict, then the device applies the passive detection mode function. If the Send trap function is active, then the device sends an SNMP trap. • **unmarked** The periodic address conflict detection is inactive.
Detection delay [ms]	Specifies the period in milliseconds for which the device waits for a response after sending a ARP data packets. Possible values: • **20..500** (default setting: **200**)
Release delay [s]	Specifies the period in seconds after which the device checks again if the address conflict still exists. Possible values: • **3..3600** (default setting: **15**)
Address protections	Specifies how many times the device sends gratuitous ARP data packets in the passive detection mode to “defend” its IP address. Possible values: • **0..100** (default setting: **1**)

Setting	Description
Protection interval [ms]	Specifies the period in milliseconds after which the device sends gratuitous ARP data packets again in the passive detection mode to “defend” its IP address. Possible values: • **20..10000** (default setting: **10000**)
Send trap	Activates/deactivates the sending of SNMP traps when the device detects an address conflict. Possible values: • **marked** (default setting) The sending of SNMP traps is active. The prerequisite is that in the **Diagnostics > Status Configuration > Alarms (Traps)** dialog the Alarms (Traps) function is enabled and at least one trap destination is specified. If the device detects an address conflict, then the device sends an SNMP trap. • **unmarked** The sending of SNMP traps is inactive.

Table

For information on how to customize the appearance of the table, see Working with tables, page 25.

The following table presents the table settings:

Setting	Description
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.

ARP

This dialog **Diagnostics > System > ARP** displays the MAC and IP addresses of the neighboring devices connected to the device management.

The device can display both IPv4 and IPv6 addresses. For IPv6, the device obtains the addresses of the neighboring devices with the use of the Neighbor Discovery Protocol (NDP).

Table

For information on how to customize the appearance of the table, see Working with tables, page 25.

The following table presents the table settings:

Setting	Description
Buttons	Clear ARP table: Deletes the dynamically set up addresses from the ARP table.
Port	Displays the port number.
IP address	Displays the IPv4 address or the IPv6 address of a neighboring device.
MAC address	Displays the MAC address of a neighboring device.
Last updated	Displays the time in seconds since the 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.

Selftest

This dialog allows you to do the following:

- Activate/deactivate the RAM self-test the device performs during system startup.
- Activate/deactivate the option of starting the System Monitor 1 during system startup.
- Specify how the device behaves in the case of a detected error.

Configuration

If the device does not detect any readable configuration profile when restarting, then the following settings **block your access to the device permanently**.

- SysMon1 is available checkbox is **unmarked**.
- Load default configuration 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.

The following table presents the configuration settings:

Setting	Description
RAM test	Activates/deactivates the RAM memory verification the device performs during the system startup. Possible values: • **marked** (default setting) The RAM memory verification is activated. During the system startup, the device checks the RAM memory. • **unmarked** The RAM memory verification is deactivated. This shortens the boot time for the device.
SysMon1 is available	Activates/deactivates the option of starting the System Monitor 1 during system startup. Possible values: • **marked** (default setting) During system startup, the boot menu will display the System Monitor 1 item. To actually start the System Monitor 1, set the device to the Recovery Mode. • **unmarked** During system startup, the boot menu will not display the System Monitor 1 item. No one can start the System Monitor 1. The System Monitor 1 provides functions for recovering the operating settings of the device.
Load default config on error	Activates/deactivates the loading of the default settings if the device does not detect any readable configuration profile when restarting. Possible values: • **marked** (default setting) The device loads the default settings. • **unmarked** The device interrupts the restart and stops. Access to the device management is only possible using the Command Line Interface through the serial connection. To regain access to the device through the network, start the System Monitor 1 and reset the settings. After the system startup, the device uses the default settings.

Table

In this table you specify how the device behaves in the case of a detected error.

For information on how to customize the appearance of the table, see Working with tables, page 25.

The following table presents the table settings:

Setting	Description
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 detected error in the consistency verification. • **hardware** The device detects hardware errors, for example in the chip set.
Action	Specifies how the device behaves if the adjacent event occurs. Possible values: • **logOnly** The device registers the detected error in the log file. See the **Diagnostics > Report > System Log** dialog. • **sendTrap** The device sends an SNMP trap. The prerequisite is that in the **Diagnostics > Status Configuration > Alarms (Traps)** dialog the Alarms (Traps) function is enabled and at least one trap destination is specified. • **reboot** (default setting) The device triggers a restart.

Email Notification

The device allows you to 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.

This menu **Diagnostics > Email Notification** contains the following dialogs:

- Email Notification Global, page 320
- Email Notification Recipients, page 324
- Email Notification Mail Server, page 325

Email Notification Global

In this dialog **Diagnostics > Email Notification > Global**, you specify the sender settings. Also, you specify for which event severities the device sends the emails immediately and for which periodically.

Operation

The following table presents the operation setting:

Setting	Description
Operation	Enables/disables the sending of emails: Possible values: • **On** The sending of emails is enabled. • **Off** (default setting) The sending of emails is disabled.

Information

The following table presents the information settings:

Setting	Description
Buttons	Clear email notification statistics: Resets the counters in the Information frame to **0**.
Sent messages	Displays how many times the device has successfully sent an email to the mail server.
Undeliverable messages	Displays how many times the device has unsuccessfully tried to send an email to the mail server.
Time of the last messages sent	Displays the date and time at which the device has last sent an email to the mail server.

Certificates/CRLs

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

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

The following table presents the certificates/CRLs settings:

Setting	Description
Buttons	Clear all Certificates/CRLs: Deletes the digital certificates and CRLs transferred onto the device from the non-volatile memory (**NVM**).
URL	Specifies the path and file name of the digital certificate or CRL. The device accepts digital certificates and CRLs with the following properties: • X.509 format • .PEM file name extension • Base64-coded and enclosed by the lines -----BEGIN CERTIFICATE----- … -----END CERTIFICATE----- or -----BEGIN CRL----- … -----END CRL----- The device gives you the following options for transferring the file onto the device: • Import from the PC When the file is located on your PC or on a network drive, drag and drop it onto the area. As an alternative, click in the area to select the file. • Import from an FTP server Do not use this method if you transmit data over untrusted networks. When the file is on an FTP server, specify the URL for the file in the following form: ftp://<user>:<password>@<IP address>[:port]/<path>/<file name> • Import from a TFTP server Do not use this method if you transmit data over untrusted networks. When the file is on a TFTP server, specify the URL for the file in the following form: tftp://<IP address>/<path>/<file name> • Import from an SCP or SFTP server When the file is on an SCP or SFTP server, specify the URL for the file in the following form: ◦ scp:// or sftp://<IP address>/<path>/<file name> Click the Start button to open the Credentials window. In this window, you enter the User name and Password to log into the server. ◦ scp:// or sftp://<user>:<password>@<IP address>/<path>/<file name> Remember to set up the SCP or SFTP server as an SSH known host before the device accesses the server for the first time. See the **Device Security > SSH Known Hosts** dialog.
Start	Transfers the file specified in the URL field onto the device. In this dialog, you can transfer a maximum of 20 digital certificates and additionally a maximum of 20 CRLs onto the device. For the changes to take effect after transferring a digital certificate or a CRL into the device, disable and re-enable the Email Notification function. See the Operation frame.

Sender

The following table presents the sender setting:

Setting	Description
Email address	Specifies the email address of the device. The device sends the emails using this email address as the sender. Possible values: • Alphanumeric ASCII character string with 0..255 characters

Notification Urgent

Here you specify the settings for emails which the device sends immediately.

The following table presents the notification urgent settings:

Setting	Description
Severity	Specifies the minimum severity of events for which the device immediately sends an email. If an event of this severity occurs, or of a more urgent severity, then the device sends an email to the recipients. Possible values: • **emergency** • **alert** (default setting) • **critical** • **error** • **warning** • **notice** • **informational** • **debug**
Subject	Specifies the subject of the email. Possible values: • Alphanumeric ASCII character string with 0..255 characters

Notification Non-Urgent

Here you specify the settings for emails which the device sends periodically.

The following table presents the notification non-urgent settings:

Setting	Description
Severity	Specifies the minimum severity of events for which the device periodically sends an email. If an event of this severity occurs, or of a more urgent severity, then the device registers the event in the buffer. The device sends the buffer content periodically or when the buffer overflows. If an event of a less urgent severity occurs, then the device does not register the event in the buffer. Possible values: • **emergency** • **alert** • **critical** • **error** • **warning** (default setting) • **notice** • **informational** • **debug**
Subject	Specifies the subject of the email. Possible values: • Alphanumeric ASCII character string with 0..255 characters
Sending interval [min]	Specifies the send interval in minutes. If the device has registered at least one event, then the device sends an email with the log file after the time expires. Possible values: • **30..1440** (default setting: **30**)
Send	Sends an email immediately with the buffer content and clears the buffer.

Meaning of the Event Severities

The following table lists the event severity levels and their corresponding meanings:

Severity	Meaning
emergency	Device not ready for operation
alert	Immediate user intervention required
critical	Critical status
error	Error status
warning	Warning
notice	Significant, normal status
informational	Information message
debug	Debug message

Email Notification Recipients

In this dialog **Diagnostics > Email Notification > Recipients**, you specify the recipients to which the device sends the emails. The device allows you to specify up to 10 recipients.

Table

For information on how to customize the appearance of the table, see Working with tables, page 25.

The following table presents the table settings:

Setting	Description
Buttons	The following list presents the icon descriptions: • Add: Adds a table row. • Remove: Removes the selected table row.
Index	Displays the index number to which the table row relates. The device automatically assigns the value when you add a table row.
Notification type	Specifies whether the device sends the emails to this recipient immediately or periodically. Possible values: • **urgent** (default setting) The device sends the emails to this recipient immediately. • **non-urgent** The device sends the emails to this recipient periodically.
Email address	Specifies the email address of the recipient. Possible values: • Valid email address with up to 255 characters
Active	Activates/deactivates the informing of the recipient. Possible values: • **marked** The informing of the recipient is active. • **unmarked** (default setting) The informing of the recipient is inactive.

Email Notification Mail Server

In this dialog **Diagnostics > Email Notification > Mail Server**, you specify the settings for the mail servers. The device supports encrypted and unencrypted connections to the mail server.

Table

For information on how to customize the appearance of the table, see Working with tables, page 25.

The following table presents the table settings:

Setting	Description
Buttons	The following list presents the icon descriptions: • Add: Adds a table row. • Remove: Removes the selected table row. • Connection test: Opens the Connection test window to send a test email. If the mail server settings are correct, then the selected recipients receive a test email. ◦ From the Recipient drop-down list, you select to which recipients the device sends the test email. Possible values: – urgent The device sends the test email to the recipients to which the device sends emails immediately. – non-urgent The device sends the test email to the recipients to which the device sends emails periodically. ◦ In the Message text field, you specify the text of the test email.
Index	Displays the index number to which the table row relates. The device automatically assigns the value when you add a table row.
Description	Specifies the name of the server. Possible values: • Alphanumeric ASCII character string with 0..255 characters
IP address	Specifies the IP address or the DNS name of the server. Possible values: • Valid IPv4 address (default setting: **0.0.0.0**) • Valid IPv6 address • DNS name in the format **<domain>.<tld>** or **<host>.<domain>.<tld>** The prerequisite is that you also enable the Client function in the **Advanced > DNS > Client > Global** dialog. To establish an encrypted connection using a digital certificate, verify that the `Common Name` or `Subject Alternative Name` information in the digital certificate that you have transferred onto the device matches the value you specify here. Otherwise, the device will not be able to verify the identity of the server.
Destination TCP port	Specifies the TCP port of the server. Possible values: • **1..65535 (2^{16}-1)** (default setting: **25**) Exception: Port **2222** is reserved for internal functions. Frequently used TCP-Ports: • SMTP **25** • Message Submission **587**
Encryption	Specifies the protocol which encrypts the connection between the device and the mail server. Possible values: • **none** (default setting) The device establishes an 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

Setting	Description
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.

Syslog

The device allows you to report selected events, independent of the severity of the event, to different syslog servers.

In this dialog **Diagnostics > Syslog**, you specify the settings for this function and manage up to 8 syslog servers.

Operation

The following table presents the operation setting:

Setting	Description
Operation	Enables/disables the sending of events to the syslog servers. Possible values: • **On** The sending of events is enabled. The device sends the events specified in the table to the specified syslog servers. • **Off** (default setting) The sending of events is disabled.

Certificates/CRLs

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

A Certificate Revocation List (CRL) contains a list of digital certificates revoked by the Certification Authority (CA) before their scheduled expiration date. When establishing a secure connection to the server, the device stops setting up the connection if the CRL includes the public certificate of the server. The device logs

the event in the System Log. For security reasons, use only CRLs signed by a Certification Authority (CA).

The following table presents the certificates/CRLs

Setting	Description
Buttons	Clear all Certificates/CRLs: Deletes the digital certificates and CRLs transferred onto the device from the non-volatile memory (**NVM**).
URL	Specifies the path and file name of the digital certificate or CRL. The device accepts digital certificates and CRLs with the following properties: • X.509 format • .PEM file name extension • Base64-coded and enclosed by the lines -----BEGIN CERTIFICATE----- … -----END CERTIFICATE----- or -----BEGIN CRL----- … -----END CRL----- The device gives you the following options for transferring the file onto the device: • Import from the PC When the file is located on your PC or on a network drive, drag and drop it onto the area. As an alternative, click in the area to select the file. • Import from an FTP server Do not use this method if you transmit data over untrusted networks. When the file is on an FTP server, specify the URL for the file in the following form: ftp://<user>:<password>@<IP address>[:port]/<path>/<file name> • Import from a TFTP server Do not use this method if you transmit data over untrusted networks. When the file is on a TFTP server, specify the URL for the file in the following form: tftp://<IP address>/<path>/<file name> • Import from an SCP or SFTP server When the file is on an SCP or SFTP server, specify the URL for the file in the following form: ◦ scp:// or sftp://<IP address>/<path>/<file name> Click the Start button to open the Credentials window. In this window, you enter the User name and Password to log into the server. ◦ scp:// or sftp://<user>:<password>@<IP address>/<path>/<file name> Remember to set up the SCP or SFTP server as an SSH known host before the device accesses the server for the first time. See the **Device Security > SSH Known Hosts** dialog.
Start	Transfers the file specified in the URL field onto the device. In this dialog, you can transfer a maximum of 32 digital certificates and additionally a maximum of 32 CRLs onto the device. For the changes to take effect after transferring a digital certificate or a CRL into the device, disable and re-enable the Syslog function. See the Operation frame.

Table

For information on how to customize the appearance of the table, see Working with tables, page 25.

The following table presents the table settings:

Setting	Description
Buttons	The following list presents the icon descriptions: • Add: Adds a table row. • Remove: Removes the selected table row.
Index	Displays the index number to which the table row relates. The device automatically assigns the value when you add a table row. When you delete a table row, this leaves a gap in the numbering. When you add a table row, the device fills the first gap. Possible values: • **1..8**
IP address	Specifies the IP address of the syslog server. Possible values: • Valid IPv4 address (default setting: **0.0.0.0**) • Valid IPv6 address • DNS name in the format **<domain>.<tld>** or **<host>.<domain>.<tld>** The prerequisite is that you also enable the Client function in the **Advanced > DNS > Client > Global** dialog. To establish an encrypted connection using a digital certificate, verify that the `Common Name` or `Subject Alternative Name` information in the digital certificate that you have transferred onto the device matches the value you specify here. Otherwise, the device will not be able to verify the identity of the server.
Destination UDP port	Specifies the TCP or UDP port on which the syslog server expects the log entries. Possible values: • **1..65535 (2^{16}-1)** (default setting: **514**)
Transport type	Specifies the transport type the device uses to send the events to the syslog server. Possible values: • **udp** (default setting) The device sends the events over the UDP port specified in the Destination UDP port column. • **tls** The device sends the events over TLS on the TCP port specified in the Destination UDP port column.
Min. severity	Specifies the minimum severity of the events. The device sends a log entry for events with this severity and with more urgent severities to the syslog server. Possible values: • **emergency** • **alert** • **critical** • **error** • **warning** (default setting) • **notice** • **informational** • **debug**

Setting	Description
Type	Specifies the type of the log entry transmitted by the device. Possible values: • **systemlog** (default setting) • **audittrail**
Active	Activates/deactivates the transmission of events to the syslog server. Possible values: • **marked** The device sends events to the syslog server. • **unmarked** (default setting) The transmission of events to the syslog server is deactivated.

Ports

The menu **Diagnostics > Ports** contains the following dialogs:

- SFP, page 331
- TP cable diagnosis, page 332
- Port Monitor, page 333
- Auto-Disable, page 343
- Port Mirroring, page 346
- RSPAN, page 349

SFP

This dialog **Diagnostics > Ports > SFP** allows you to look at the SFP transceivers currently connected to the device and their properties.

Table

The table displays valid values if the device is equipped with SFP transceivers.

For information on how to customize the appearance of the table, see Working with tables, page 25.

The following table presents the table settings:

Setting	Description
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.

TP Cable Diagnosis

This feature **Diagnostics > Ports > TP cable diagnosis** tests the cable attached to an interface for short or open circuit. The table displays the cable status and estimated length. The device also displays the individual cable pairs connected to the port. When the device detects a short circuit or a broken cable, it also displays the estimated distance to where it detected the problem.

To receive dependable results, use the TP cable diagnosis function for twisted-pair cables with a minimum length of 10 meters.

NOTE: This test temporarily interrupts the data stream on the port.

Information

The following table presents the information settings:

Setting	Description
Port	Displays the port number.
Start cable diagnosis...	Opens the Select port window. From the Port drop-down list you select the port to be tested. Use for copper-based ports only. To initiate the cable test on the selected port, click the Ok button.
Status	Status of the Virtual Cable Tester. Possible values: • **active** Cable testing is in progress. To start the test, click the Start cable diagnosis... button. This action opens the Select port window. • **success** The device successfully performed a test. • **failure** The device detected that the test was interrupted. • **uninitialized** The device has not performed any test yet.

Table

For information on how to customize the appearance of the table, see Working with tables, page 25.

The following table presents the table settings:

Setting	Description
Cable pair	Displays the cable pair to which this table row relates. The device uses the first PHY index supported to display the values.
Result	Displays the results of the cable test. Possible values: • **normal** The cable is functioning properly. • **open** There is a break in the cable causing an interruption. • **short** Wires in the cable are touching together causing a short circuit. • **unknown** The device displays this value for untested cable pairs. The device displays different values than expected in the following cases: • If no cable is connected to the port, then the device displays the value **unknown** instead of **open**. • If the port is inactive, then the device displays the value **short**.
Min. length	Displays the minimum estimated length of the cable in meters. If the cable length is undefined 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 undefined 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 undefined or in the Information frame the Status field displays the value **active**, **failure** or **uninitialized**, then the device displays the value **0**.

Port Monitor

The Port Monitor function monitors the adherence to the specified parameters on the ports. If the Port Monitor function detects that the parameters are being exceeded, then the device performs an action.

To apply the Port Monitor function, perform the following steps:

- Global tab
  - Enable the Port Monitor function in the Operation frame.
  - Activate for each port those parameters that you want the Port Monitor function to monitor.
- Link flap, CRC/Fragments and Overload detection tabs
  - Specify the threshold values for the parameters for each port.
- Link speed/Duplex mode detection tab
  - Activate the allowed combinations of speed and duplex mode for each port.
- Global tab
  - Specify for each port an action that the device carries out if the Port Monitor function detects that the parameters have been exceeded.
- Auto-disable tab
  - Mark the Auto-disable checkbox for the monitored parameters if you have specified the **auto-disable** action at least once.

The dialog **Diagnostics > Ports > Port Monitor** contains the following tabs:

- Global, page 334
- Auto-disable, page 337
- Link flap, page 338
- CRC/Fragments, page 339
- Overload detection, page 339
- Link speed/Duplex mode detection, page 340

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

The following table presents the operation setting:

Setting	Description
Operation	Enables/disables the Port Monitor function globally. Possible values: • **On** The Port Monitor function is enabled. • **Off** (default setting) The Port Monitor function is disabled.

Table

For information on how to customize the appearance of the table, see Working with tables, page 25.

The following table presents the table settings:

Setting	Description
Buttons	 Reset: Opens the **Which statistic should be deleted?** window. The window displays the ports that you can enable again and reset the related counters to **0**. Click and select a table row to enable the corresponding port again.This affects the counters in the following dialogs: • **Diagnostics > Ports > Port Monitor** dialog ◦ Link flap tab ◦ CRC/Fragments tab ◦ Overload detection tab • **Diagnostics > Ports > Auto-Disable** dialog
Port	Displays the port number.
Link flap on	Activates/deactivates the monitoring of link flaps on the port. Possible values: • **marked** Monitoring is active. ◦ The Port Monitor function monitors link flaps on the port. ◦ If the device detects too many link flaps, then the device executes the action specified in the Action column. ◦ On the Link flap tab, specify the parameters to be monitored. • **unmarked** (default setting) Monitoring is inactive.
CRC/Fragments on	Activates/deactivates the monitoring of CRC/fragment errors detected on the port. Possible values: • **marked** Monitoring is active. ◦ The Port Monitor function monitors CRC/fragment errors detected on the port. ◦ If the device detects too many CRC/fragment errors, then the device executes the action specified in the Action column. ◦ On the CRC/Fragments tab, specify the parameters to be monitored. • **unmarked** (default setting) Monitoring is inactive.
Duplex mismatch detection active	Activates/deactivates the monitoring of duplex mismatches on the port. Possible values: • **marked** Monitoring is active. ◦ The Port Monitor function monitors duplex mismatches on the port. ◦ If the device detects a duplex mismatch, then the device executes the action specified in the Action column. • **unmarked** (default setting) Monitoring is inactive.
Overload detection on	Activates/deactivates the overload detection on the port. Possible values: • **marked** Monitoring is active. ◦ The Port Monitor function monitors the data load on the port. ◦ If the device detects a data overload on the port, then the device executes the action specified in the Action column. ◦ On the Overload detection tab, specify the parameters to be monitored. • **unmarked** (default setting) Monitoring is inactive.

Setting	Description
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.

Setting	Description
Action	Specifies the action that the device carries out if the Port Monitor function detects that the parameters have been exceeded. Possible values: • **disable port** The device disables the port and sends an SNMP trap. The Link status LED for the port flashes 3 × per period. ◦ To re-enable the port, select the table row of the port, click the  button. ◦ If the parameters are no longer being exceeded, then the Auto-Disable function enables the relevant port again after the specified waiting period. The prerequisite is that on the Auto-disable tab the checkbox for the monitored parameter is marked. • **send trap** The device sends an SNMP trap. The prerequisite is that in the **Diagnostics > Status Configuration > Alarms (Traps)** dialog the Alarms (Traps) function is enabled and at least one trap destination is specified. • **auto-disable** (default setting) The device disables the port and sends an SNMP trap. The Link status LED for the port flashes 3 × per period. The prerequisite is that on the Auto-disable tab the checkbox for the monitored parameter is marked. ◦ The **Diagnostics > Ports > Auto-Disable** dialog displays which ports are currently disabled due to the parameters being exceeded. ◦ After a waiting period, the Auto-Disable function enables the port again automatically. For this you go to the **Diagnostics > Ports > Auto-Disable** dialog and specify a waiting period for the relevant port in the Reset timer [s] column.
Port status	Displays the operating state of the port. Possible values: • **up** The port is enabled. • **down** The port is disabled. • **notPresent** Physical port unavailable.

Auto-Disable

In this tab you activate the Auto-Disable function for the parameters monitored by the Port Monitor function.

Table

For information on how to customize the appearance of the table, see Working with tables, page 25.

The following table presents the table settings:

Setting	Description
Reason	Displays the parameters monitored by the Port Monitor function. Mark the adjacent checkbox so that the Port Monitor function carries out the **auto-disable** action if it detects that the monitored parameters have been exceeded.
Auto-disable	Activates/deactivates the Auto-Disable function for the adjacent parameters. Possible values: • **marked** The Auto-Disable function for the adjacent parameters is active. If the adjacent parameters are exceeded and the value **auto-disable** is specified in the Action column, then the device carries out the Auto-Disable function. • **unmarked** (default setting) The Auto-Disable function for the adjacent parameters is inactive.

Link Flap

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

- The number of link changes.
- The period during which the Port Monitor function monitors a parameter to detect discrepancies.

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

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

Table

For information on how to customize the appearance of the table, see Working with tables, page 25.

The following table presents the table settings:

Setting	Description
Port	Displays the port number.
Sampling interval [s]	Specifies in seconds, the period during which the Port Monitor function monitors a parameter to detect discrepancies. Possible values: • **1..180** (default setting: **10**)
Link flaps	Specifies the number of link changes. If the Port Monitor function detects this number of link changes in the monitored period, then the device performs the specified action. Possible values: • **1..100** (default setting: **5**)
Last sampling interval	Displays the number of errors that the device has detected during the period that has elapsed.
Total	Displays the total number of errors that the device has detected since the port was enabled.

CRC/Fragments

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

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

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

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

Table

For information on how to customize the appearance of the table, see Working with tables, page 25.

The following table presents the table settings:

Setting	Description
Port	Displays the port number.
Sampling interval [s]	Specifies in seconds, the period during which the Port Monitor function monitors a parameter to detect discrepancies. Possible values: • **5..180** (default setting: **10**)
CRC/Fragments count [ppm]	Specifies the detected fragment error rate (in parts per million). If the Port Monitor function detects this fragment error rate in the monitored period, then the device performs the specified action. Possible values: • **1..1000000 (10^6)** (default setting: **1000**)
Last active interval [ppm]	Displays the fragment error rate that the device has detected during the period that has elapsed.
Total [ppm]	Displays the fragment error rate that the device has detected since the port was enabled.

Overload Detection

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

- The load threshold values.
- The period during which the Port Monitor function monitors a parameter to detect discrepancies.

You also see the number of data packets that the device has detected up to now.

The Port Monitor function monitors those ports for which the checkbox in the Overload detection on column is marked on the Global tab.

The Port Monitor function does not monitor a port if the port operates in any of the following roles:

- Member of a Link Aggregation group

Table

For information on how to customize the appearance of the table, see Working with tables, page 25.

The following table presents the table settings:

Setting	Description
Port	Displays the port number.
Type	Specifies the type of data packets that the device takes into account when monitoring the load on the port. Possible values: • **all** The Port Monitor function monitors Broadcast, Multicast and Unicast packets. • **bc** (default setting) The Port Monitor function monitors only Broadcast packets. • **bc-mc** The Port Monitor function monitors only Broadcast and Multicast packets.
Unit	Specifies the unit for the data rate. Possible values: • **pps** (default setting) packets per second • **kbps** kbit per second The prerequisite is that in the Type column the value **all** is specified.
Lower threshold	Specifies the lower threshold value for the data rate. The Auto-Disable function enables the port again only when the load on the port is lower than the value specified here. Possible values: • **0..10000000 (10^7)** (default setting: **0**)
Upper threshold	Specifies the upper threshold value for the data rate. If the Port Monitor function detects this load in the monitored period, then the device performs the specified action. Possible values: • **0..10000000 (10^7)** (default setting: **0**))
Interval [s]	Specifies in seconds, the period that the Port Monitor function observes a parameter to detect that a parameter is being exceeded. Possible values: • **1..20** (default setting: **1**)
Packets	Displays the number of Broadcast, Multicast and Unicast packets that the device has detected during the period that has elapsed.
Broadcast packets	Displays the number of Broadcast packets that the device has detected during the period that has elapsed.
Multicast packets	Displays the number of Multicast packets that the device has detected during the period that has elapsed.
kbit/s	Displays the data rate in Kbits per second that the device has detected during the period that has elapsed.

Link speed/Duplex Mode Detection

In this tab you activate the allowed combinations of speed and duplex mode for each port.

The Port Monitor function monitors those ports for which the checkbox in the Link speed/Duplex mode detection on column is marked on the Global tab.

The Port Monitor function monitors only enabled physical ports.

Table

For information on how to customize the appearance of the table, see Working with tables, page 25.

The following table presents the table settings:

Setting	Description
Port	Displays the port number.
10M HDX	Activates/deactivates the port monitor to accept a half-duplex and 10 Mbit/s data rate combination on the port. Possible values: • **marked** The port monitor takes into consideration the speed and duplex combination. • **unmarked** If the port monitor detects the speed and duplex combination on the port, then the device executes the action specified in the Global tab.
10M FDX	Activates/deactivates the port monitor to accept a full-duplex and 10 Mbit/s data rate combination on the port. Possible values: • **marked** The port monitor takes into consideration the speed and duplex combination. • **unmarked** If the port monitor detects the speed and duplex combination on the port, then the device executes the action specified in the Global tab.
100M HDX	Activates/deactivates the port monitor to accept a half-duplex and 100 Mbit/s data rate combination on the port. Possible values: • **marked** The port monitor takes into consideration the speed and duplex combination. • **unmarked** If the port monitor detects the speed and duplex combination on the port, then the device executes the action specified in the Global tab.
100M FDX	Activates/deactivates the port monitor to accept a full-duplex and 100 Mbit/s data rate combination on the port. Possible values: • **marked** The port monitor takes into consideration the speed and duplex combination. • **unmarked** If the port monitor detects the speed and duplex combination on the port, then the device executes the action specified in the Global tab.
1G FDX	Activates/deactivates the port monitor to accept a full-duplex and 1 Gbit/s data rate combination on the port. Possible values: • **marked** The port monitor takes into consideration the speed and duplex combination. • **unmarked** If the port monitor detects the speed and duplex combination on the port, then the device executes the action specified in the Global tab.
2.5G FDX	Activates/deactivates the port monitor to accept a full-duplex and 2.5 Gbit/s data rate combination on the port. Possible values: • **marked** The port monitor takes into consideration the speed and duplex combination. • **unmarked** If the port monitor detects the speed and duplex combination on the port, then the device executes the action specified in the Global tab.

Auto-Disable

The Auto-Disable function allows you to 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 **Diagnostics > Ports > Auto-Disable** contains the following tabs:

- Port, page 343
- Status, page 345

Port

This tab displays which ports are currently disabled due to the parameters being exceeded. If the parameters are no longer being exceeded and you specify a waiting period in the Reset timer [s] column, then the Auto-Disable function automatically enables the relevant port again.

Table

For information on how to customize the appearance of the table, see Working with tables, page 25.

The following table presents the table settings:

Setting	Description
Buttons	Reset: Opens the **Which statistic should be deleted?** window. The window displays the ports that you can enable again and reset the related counters to **0**. Click and select a table row to enable the corresponding port again. This affects the counters in the following dialogs: • **Diagnostics > Ports > Auto-Disable** dialog • **Diagnostics > Ports > Port Monitor** dialog ◦ Link flap tab ◦ CRC/Fragments tab ◦ Overload detection tab
Port	Displays the port number.
Reset timer [s]	Specifies the waiting period in seconds, after which the Auto-Disable function enables the port again. Possible values: • **0** (default setting) The timer is inactive. The port remains disabled. • **30..4294967295 (2^{32}-1)** If the parameters are no longer being exceeded, then the Auto-Disable function enables the port again after the waiting period specified here.
Error time	Displays when the device disabled the port due to the parameters being exceeded.
Remaining time [s]	Displays the remaining time in seconds, until the Auto-Disable function enables the port again.
Component	Displays the software component in the device that disabled the port. Possible values: • **PORT_MON** Port Monitor See the **Diagnostics > Ports > Port Monitor** dialog. • **PORT_ML** Port Security See the **Network Security > Port Security** dialog. • **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.

Setting	Description
Reason	Displays the monitored parameter that led to the port being disabled. Possible values: • **none** No monitored parameter. The port is enabled. • **Link flap** Too many link changes. See the **Diagnostics > Ports > Port Monitor** dialog, Link flap tab. • **CRC error** Too many CRC/fragment errors are detected. See the **Diagnostics > Ports > Port Monitor** dialog, CRC/Fragments tab. • **Duplex mismatch** Duplex mismatch detected. See the **Diagnostics > Ports > Port Monitor** dialog, Global tab. • **DHCP snooping** Too many DHCP packages from untrusted sources. See the **Network Security > DHCP Snooping > Configuration** dialog, Port tab. • **ARP rate** Too many ARP packages from untrusted sources. See the **Network Security > Dynamic ARP Inspection > Configuration** dialog, Port tab. • **BPDU rate** STP-BPDUs received. See the **Switching > L2-Redundancy > Spanning Tree > Global** dialog. • **MAC-based port security** Too many data packets from undesired senders. See the **Network Security > Port Security** dialog. • **Overload detection** Overload. See the **Diagnostics > Ports > Port Monitor** dialog, Overload detection tab. • **Speed duplex** Impermissible combination of speed and duplex mode detected. See the **Diagnostics > Ports > Port Monitor** dialog, Link speed/Duplex mode detection tab. • **Loop protection** A layer 2 network loop detected on the port. See the **Diagnostics > Loop Protection** dialog, Loop detected column.
Active	Displays if the port is currently disabled due to the parameters being exceeded. Possible values: • **marked** The port is currently disabled. • **unmarked** The port is enabled.

Status

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

Table

For information on how to customize the appearance of the table, see Working with tables, page 25.

The following table presents the table settings:

Setting	Description
Reason	Displays the parameters that the device monitors. Mark the adjacent checkbox so that the Auto-Disable function disables and, when applicable, enables the port again if the monitored parameters are exceeded.
Category	Displays which function the adjacent parameter belongs to. Possible values: • **port monitor** The parameter belongs to the functions in the **Diagnostics > Ports > Port Monitor** dialog. • **network security** The parameter belongs to the functions in the **Network Security** dialog. • **l2 redundancy** The parameter belongs to the functions in the **Switching > L2-Redundancy** dialog or to the Loop Protection function, see the **Diagnostics > Loop Protection** dialog.
Auto-disable	Displays if the Auto-Disable function is active/inactive for the adjacent parameter. Possible values: • **marked** The Auto-Disable function for the adjacent parameters is active. The Auto-Disable function disables and, when applicable, enables the relevant port again if the monitored parameters are exceeded. • **unmarked** (default setting) The Auto-Disable function for the adjacent parameters is inactive.

Port Mirroring

The Port Mirroring function **Diagnostics > Ports > Port Mirroring** allows you to 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

The following table presents the operation settings:

Setting	Description
Buttons	Reset config: Resets the settings in the dialog to the default settings and restores the previously applied settings.
Operation	Enables/disables the Port Mirroring function. Possible values: • **On** The Port Mirroring function is enabled. The device copies the data packets from the selected source ports to the destination port. • **Off** (default setting) The Port Mirroring function is disabled.

Destination Port

The following table presents the destination port settings:

Setting	Description
Primary port	Specifies the destination port. Suitable ports are those ports that are not used for the following purposes: • Source port • Uplink port on which a Layer 2 redundancy protocol is active Possible values: • **-** (default setting) No destination port selected. • **<Port number>** Number of the destination port. The device copies the data packets from the source ports to this port. On the destination port, the device adds a VLAN tag to the data packets that the source port sends. The destination port sends the unmodified data packets that the source port receives. **NOTE:** The destination port needs sufficient bandwidth to absorb the data stream. If the copied data stream exceeds the bandwidth of the destination port, then the device discards superfluous data packets on the destination port.
Secondary port	Specifies a second destination port. The prerequisite is that you have specified a primary port. Possible values: • **-** (default setting) No destination port selected. • **<Port number>** Number of the destination port. The device copies the data packets from the source ports to this port. The port sends the same data as the port specified above. Exception: ◦ No RSPAN data
Allow management	Activates/deactivates the access to the device management using the destination port. Possible values: • **marked** The access to the device management using the destination port is active. The device allows users to have access to the device management using the destination port without interrupting the active Port Mirroring session. ◦ The device duplicates multicasts, broadcasts and undefined unicasts on the destination port. ◦ The VLAN settings on the destination port remain unchanged. The prerequisite for access to the device management using the destination port is that the destination port is not a member of the VLAN of the device management. • **unmarked** (default setting) The access to the device management using the destination port is inactive. The device prohibits the access to the device management using the destination port.

Table

For information on how to customize the appearance of the table, see Working with tables, page 25.

The following table presents the table settings:

Setting	Description
Source port	Displays the port number.
Enabled	Activates/deactivates the copying of the data packets from this source port to the destination port. Possible values: • **marked** The copying of the data packets is active. The port is specified as a source port. • **unmarked** (default setting) The copying of the data packets is inactive. • (Grayed-out display) It is not possible to copy the data packets for this port. Possible causes: ◦ The port is already specified as a destination port. ◦ The port is a logical port, not a physical port. **NOTE:** The device allows you to activate every physical port as source port except for the destination port.
Type	Specifies which data packets the device copies to the destination port. On the destination port, the device adds a VLAN tag to the data packets that the source port sends. The destination port sends the unmodified data packets that the source port receives. Possible values: • **none** (default setting) No data packets. • **tx** Data packets that the source port sends. Verify that the PTP function is disabled on this port. For further possible prerequisites see the description below. • **rx** Data packets that the source port receives. Verify that no SFlow sampler is active on this port. • **txrx** Data packets that the source port sends. Verify that the PTP function is disabled on this port. For further possible prerequisites see the description below. **NOTE:** With the **txrx** setting the device copies each transmitted data packet. The destination ports needs at least a bandwidth that corresponds to the sum of the send and receive channel of the source ports. For example, for similar ports the destination port is at 100 % capacity when the send and receive channel of a source port are at 50 % capacity respectively. The prerequisite to use the settings **tx** and **txrx** is that the source port and the destination ports belong to the same port group. • The following ports belong to port group 1: ◦ ***1/1***..***1/8*** on a device with 16 ports ◦ ***1/1***..***1/12*** on a device with 20 or 24 ports • The following ports belong to port group 2: ◦ ***1/9***..***1/16*** on a device with 16 ports ◦ ***1/13***..***1/20*** on a device with 20 ports ◦ ***1/13***..***1/24*** on a device with 24 ports Example of settings **tx** or **txrx** on a device with 16 ports: • Source port: ***1/9*** • Primary port: ***1/10*** • Secondary port: ***1/16***

RSPAN

In this dialog **Diagnostics > Ports > RSPAN**, you specify the settings for the RSPAN function. The RSPAN function is an extension of the local mirroring function and uses multiple devices in specific roles to forward mirrored data packets to a single *Destination switch*. For that, RSPAN uses an RSPAN VLAN reserved specifically for this purpose.

Using the RSPAN function, a *Source switch* mirrors data packets that it receives or sends on the ports you have selected and sends them on the RSPAN VLAN to a device in another role. An optional *Intermediate switch* transfers the mirrored data packets in the direction of the *Destination switch*. The *Destination switch* makes the data packets accessible on a local port for monitoring and analysis.

Before you set up the RSPAN function, decide on the role that the device will operate in:

- *Source switch*

  The device forwards the data packets received or sent on the selected *Source ports* to the RSPAN VLAN.

- *Destination switch*

  The device receives the data packets from the *Source switches* or *Intermediate switches* on the RSPAN VLAN and makes the packets accessible for monitoring and analysis.

- *Intermediate switch*

  If you use one or more *Intermediate switches* on the path between the *Source switch* and *Destination switch*, then the Port Mirroring function is not required for this role.

  You only set up the RSPAN VLAN and make the *Destination port* that is connected to the *Destination switch* or to another *Intermediate switch* a member of this VLAN. See the **Switching > VLAN > Configuration** dialog.

Operation

The following table presents the operation settings:

Setting	Description
Buttons	Reset config: Resets the settings in the dialog to the default settings.
Operation	Enables/disables the RSPAN function. Possible values: • **On** The RSPAN function is enabled. The device operates in the *Source switch* or *Destination switch* role, depending on the settings in the Role frame. • **Off** (default setting) The RSPAN function is disabled. The device does not take part in the RSPAN function, or it operates in the *Intermediate switch* role, for which no settings are necessary in this dialog.

Role

In the Role frame, you specify whether the device operates in the *Source switch* or *Destination switch* role. Depending on your selection, further settings are possible in this dialog either in the Source switch, page 350 tab or the Destination switch, page 351 tab.

The following table presents the role setting:

Setting	Description
Role	Specifies the role that the device will operate in. Possible values: • **Source switch** (default setting) The device will operate in the *Source switch* role. • **Destination switch** The device will operate in the *Destination switch* role.

Source Switch

For this role, you specify the *Source ports*. The device will forward the data packets received or sent on the *Source ports* to the *Reflector port*. The device sends the mirrored data packets with the RSPAN VLAN tag.

Reflector Port

The following table presents the reflector port setting:

Setting	Description
Reflector port	Specifies the port to which the device internally sends the mirrored data packets. The *Reflector port* then forwards the mirrored data packets to the RSPAN VLAN. Preparatory steps: • Specify an existing VLAN ID in the RSPAN frame. Possible values: • **-** (default setting) No port selected. • **<Port number>**

RSPAN

The following table presents the RSPAN setting:

Setting	Description
RSPAN Destination VLAN ID	The device tags the mirrored data packets with this VLAN ID and then forwards them to the *Reflector port*. The VLAN 1 is the default VLAN for the device management and cannot be used as the RSPAN VLAN. Prerequisites: • In the **Switching > VLAN > Configuration** dialog, the VLAN is already set up. • In the **Switching > VLAN > Configuration** dialog, the RSPAN VLAN column, the checkbox is marked for the particular VLAN. Possible values: • **0** (default setting) The RSPAN VLAN is inactive as it is not connected to any monitoring session. • **2..4042** Verify that the same VLAN is set up on the *Intermediate switches* and on the *Destination switch*.

Table

The following table presents the table settings:

Setting	Description
Source port	Displays the port number.
Active	Activates/deactivates the mirroring of data packets that the port receives and sends. Possible values: • **marked** The device mirrors the data packets that the port receives and sends. The device can mirror up to 8 ports simultaneously. • **unmarked** (default setting) The device does not mirror the data packets that the port receives and sends. Use this setting for the *Reflector port* and the *Destination port*.
Type	Specifies which data packets the device mirrors on this port. Possible values: • **none** (default setting) The device does not mirror the data packets that the port receives and sends. • **tx** The device mirrors the data packets that the port sends. • **rx** The device mirrors the data packets that the port receives. • **txrx** The device mirrors the data packets that the port receives and sends.

Destination Switch

In the *Destination switch* role, the device serves as the destination for mirrored data packets originating from other devices.

RSPAN

The following table presents the RSPAN setting:

Setting	Description
RSPAN Source VLAN ID	The device forwards each data packet received in this VLAN to the specified *Destination port*. The VLAN 1 is used to access the device management and cannot be used as the RSPAN VLAN. Prerequisites: • In the **Switching** > **VLAN** > **Configuration** dialog, the VLAN is already set up. • In the **Switching** > **VLAN** > **Configuration** dialog, the RSPAN VLAN column, the checkbox is marked for the particular VLAN. Possible values: • **0** (default setting) The RSPAN VLAN is inactive as it is not connected to any monitoring session. • **2..4042** Verify that the same VLAN is set up on the *Intermediate switches* and on the *Destination switch*.

Destination Port

The following table presents the destination port setting:

Setting	Description
Destination port	The device forwards the RSPAN data packets that it receives from the *Source switches* or *Intermediate switches* to this port. Possible values: • **-** (default setting) No port selected. • **<Port number>** This port needs sufficient bandwidth to accommodate the data stream. If the mirrored data stream exceeds the bandwidth of this port, then the device discards superfluous data packets on the port. The prerequisite is that the port is not used for any of the following purposes: ◦ Mirroring source port ◦ Layer 2 redundancy protocols

LLDP

The device allows you to gather information about neighboring devices. For this, the device uses the Link Layer Discovery Protocol (LLDP). This information allows a network management station to map the structure of the network.

This menu **Diagnostics > LLDP** allows you to set up the topology discovery and to display the information received in tabular form.

The menu contains the following dialogs:

- LLDP Configuration, page 352
- LLDP Topology Discovery, page 355

LLDP Configuration

This dialog **Diagnostics > LLDP > Configuration** allows you to set up the topology discovery for every port.

Operation

The following table presents the operation setting:

Setting	Description
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

The following table presents the configuration settings:

Setting	Description
Transmit interval [s]	Specifies the interval in seconds at which the device sends LLDP data packets. Possible values: • **5..32768 (2^{15})** (default setting: **30**)
Transmit interval multiplier	Specifies the factor for determining the time-to-live value for the LLDP data packets. Possible values: • **2..10** (default setting: **4**) The time-to-live value coded in the LLDP header results from multiplying this value with the value in the Transmit interval [s] field.
Reinit delay [s]	Specifies the delay in seconds for the reinitialization of a port. Possible values: • **1..10** (default setting: **2**) If in the Operation column the value **Off** is specified, then the device tries to reinitialize the port after the time specified here has elapsed.
Transmit delay [s]	Specifies the delay in seconds for transmitting successive LLDP data packets after the device settings change. Possible values: • **1..8192** (default setting: **2**) The recommended value is between a minimum of **1** and a maximum of a quarter of the value in the Transmit interval [s] field.
Notification interval [s]	Specifies the interval in seconds for transmitting LLDP notifications. Possible values: • **5..3600** (default setting: **5**) After transmitting a notification trap, the device waits for a minimum of the time specified here before transmitting the next notification trap.

Table

For information on how to customize the appearance of the table, see Working with tables, page 25.

The following table presents the table settings:

Setting	Description
Port	Displays the port number.
Operation	Specifies if the port transmits LLDP data packets. Possible values: • **transmit** The port sends LLDP data packets but does not save any information about neighboring devices. • **receive** The port receives LLDP data packets but does not send any information to neighboring devices. • **receive and transmit** (default setting) The port transmits LLDP data packets and saves information about neighboring devices. • **disabled** The port does not send LLDP data packets and does not save information about neighboring devices.
Notification	Activates/deactivates the LLDP notifications on the port. Possible values: • **marked** LLDP notifications are active on the port. • **unmarked** (default setting) LLDP notifications are inactive on the port.
Transmit port description	Activates/deactivates the transmitting of a TLV (Type Length Value) with the port description. Possible values: • **marked** (default setting) The transmitting of the TLV is active. The device sends the TLV with the port description. • **unmarked** The transmitting of the TLV is inactive. The device does not send a TLV with the port description.
Transmit system name	Activates/deactivates the transmitting of a TLV (Type Length Value) with the device name. Possible values: • **marked** (default setting) The transmitting of the TLV is active. The device sends the TLV with the device name. • **unmarked** The transmitting of the TLV is inactive. The device does not send a TLV with the device name.
Transmit system description	Activates/deactivates the transmitting of the TLV (Type Length Value) with the system description. Possible values: • **marked** (default setting) The transmitting of the TLV is active. The device sends the TLV with the system description. • **unmarked** The transmitting of the TLV is inactive. The device does not send a TLV with the system description.
Transmit system capabilities	Activates/deactivates the transmitting of the TLV (Type Length Value) with the system capabilities. Possible values: • **marked** (default setting) The transmitting of the TLV is active. The device sends the TLV with the system capabilities. • **unmarked** The transmitting of the TLV is inactive. The device does not send a TLV with the system capabilities.

Setting	Description
Neighbors (max.)	Limits the number of neighboring devices to be recorded for this port. Possible values: • **1..50** (default setting: **10**)
FDB mode	Specifies which function the device uses to record neighboring devices on this port. Possible values: • **lldpOnly** The device uses only LLDP data packets to record neighboring devices on this port. • **macOnly** The device uses learned MAC addresses to record neighboring devices on this port. The device uses the MAC address only if there is no other entry in the MAC address table (forwarding database) for this port. • **both** The device uses LLDP data packets and learned MAC addresses to record neighboring devices on this port. • **autoDetect** (default setting) If the device receives LLDP data packets at this port, then the device operates the same as with the **lldpOnly** setting. Otherwise, the device operates the same as with the **macOnly** setting.

LLDP Topology Discovery

Devices in networks send notifications in the form of packets which are also defined as "LLDPDU" (LLDP data units). The data that is sent and received through LLDPDUs is useful for many reasons. Thus the device detects which devices in the network are neighbors and through which ports they are connected.

The dialog **Diagnostics > LLDP > Topology Discovery** allows you to display the network and to detect the connected devices along with their specific features.

The dialog contains the following tabs:

- LLDP, page 355
- LLDP-MED, page 356

LLDP

This tab displays the collected LLDP information for the neighboring devices. This information allows a network management station to map the structure of the network.

When devices both with and without an active topology discovery function are connected to a port, the topology table hides the devices without active topology discovery.

When only devices without active topology discovery are connected to a port, the table contains one line for this port to represent every device. This line contains the number of connected devices.

The MAC address table (forwarding database) contains MAC addresses of devices that the topology table hides for the sake of clarity.

When you use one port to connect several devices, for example through a hub, the table shows one line for each connected device.

Table

For information on how to customize the appearance of the table, see Working with tables, page 25.

The following table presents the table settings:

Setting	Description
Port	Displays the port number.
Neighbor identifier	Displays the chassis ID of the neighboring device. This can be the basis MAC address of the neighboring device, for example.
FDB	Displays if the connected device has active LLDP support. Possible values: • **marked** The connected device does not have active LLDP support. The device uses information from its MAC address table (forwarding database) • **unmarked** The connected device has active LLDP support.
Neighbor address	Displays the IPv4 address or hostname with which the access to the neighboring device management is possible.
Neighbor IPv6 address	Displays the IPv6 address with which the access to the neighboring device management is possible.
Neighbor port description	Displays a description for the port of the neighboring device.
Neighbor system name	Displays the device name of the neighboring device.
Neighbor system description	Displays a description for the neighboring device.
Port ID	Displays the ID of the port through which the neighboring device is connected to the device.
Autonegotiation supported	Displays if the port of the neighboring device supports auto-negotiation.
Autonegotiation	Displays if auto-negotiation is active on the port of the neighboring device.
PoE supported	Displays if the port of the neighboring device supports Power over Ethernet (PoE).
PoE enabled	Displays if Power over Ethernet (PoE) is active on the port of the neighboring device.

LLDP-MED

LLDP for Media Endpoint Devices (LLDP-MED) is an extension to LLDP that operates between endpoint devices and network devices. It specifically provides support for VoIP applications. In this support rule, it provides an additional set of common advertisement, Type Length Value (TLV), messages. The device uses the TLVs for capabilities discovery such as network policy, Power over Ethernet, inventory management and location information.

Table

For information on how to customize the appearance of the table, see Working with tables, page 25.

The following table presents the table settings:

Setting	Description
Port	Displays the port number.
Device class	Displays the device class of the remotely connected device. Possible values: • **notDefined** The device has capabilities not covered by any of the LLDP-MED classes. • **endpointClass1** The device has **endpointClass1** capabilities. • **endpointClass2** The device has **endpointClass2** capabilities. • **endpointClass3** The device has **endpointClass3** capabilities. • **networkConnectivity** The device has network connectivity device capabilities.
VLAN ID	Displays the extension of the VLAN Identifier for the remote system connected to this port, as defined in IEEE 802.3. • **0** Priority tagged packets Only the 802.1D priority is significant and the device uses the default VLAN ID of the ingress port. • **1..4042** Valid Port VLAN ID
Priority	Displays the value of the *802.1D Priority* which is associated with the remote system connected to the port.
DSCP	Displays the value of the *Differentiated Service Code Point (DSCP)* which is associated with the remote system connected to the port.
Unknown bit status	Displays the *Unknown Bit Status* of incoming data packets. Possible values: • **true** The network policy for the specified application type is undefined. In this case, the device ignores the Layer 2 priority and value of the DSCP field. • **false** Indicates a specified network policy.
Tagged bit status	Displays the tagged bit status. Possible values: • **true** The application uses a tagged VLAN. • **false** For the specific application the device uses untagged VLAN operation. In this case, the device ignores both the VLAN ID and the Layer 2 priority fields. The DSCP value on Layer 3, however, is relevant.
Hardware revision	Displays the vendor-specific hardware revision string as advertised by the remote endpoint.
Firmware revision	Displays the vendor-specific firmware revision string as advertised by the remote endpoint.
Software revision	Displays the vendor-specific software revision string as advertised by the remote endpoint.
Serial number	Displays the vendor-specific serial number as advertised by the remote endpoint.
Manufacturer name	Displays the vendor-specific manufacturer name as advertised by the remote endpoint.

Setting	Description
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.

Loop Protection

The Loop Protection function **Diagnostics > Loop Protection** 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

The following table presents the operation setting:

Setting	Description
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 allows you to monitor Ethernet loops with the signal contact. See the **Diagnostics > Status Configuration > Signal Contact > Signal Contact 1** dialog, checkbox for the Ethernet loops parameter. • **Off** (default setting) The Loop Protection function is disabled. The device neither sends *loop detection* packets nor evaluates received *loop detection* packets.

Configuration

The following table presents the configuration setting:

Setting	Description
Auto-disable	Activates/deactivates the Auto-Disable function for Loop Protection. Possible values: • **marked** The Auto-Disable function for Loop Protection is active. The prerequisite for disabling the port is that in the Action column the value auto-disable or all is specified. The device allows you to specify the waiting period in seconds after which the Auto-Disable function enables the port again. To do this, in the **Diagnostics > Ports > Auto-Disable** dialog, specify the waiting period in the Reset timer [s] column. • **unmarked** (default setting) The Auto-Disable function for Loop Protection is inactive.

Global

The following table presents the global settings:

Setting	Description
Transmit interval	Specifies the interval in seconds at which the device sends *loop detection* packets if the Loop Protection function is active on the port. Possible values: • **1..10** (default setting: **5**)
Receive threshold	Specifies the threshold value for the number of consecutive *loop detection* packets received. If the number reaches or exceeds this threshold value, then the device will perform the action specified in the Action column. Possible values: • **1..50** (default setting: **1**)

Table

For information on how to customize the appearance of the table, see Working with tables, page 25.

The following table presents the table settings:

Setting	Description
Buttons	 Clear port statistics: Resets the values in the following columns: • Loops • Sent frames • Received frames
Port	Displays the port number.
Active	Activates/deactivates the Loop Protection function on the port. Possible values: • **marked** The Loop Protection function is active on the port. Activate the function only on ports which are not part of a redundant network path. This helps avoid an accidental shutdown of redundant network paths. If the device receives a *loop detection* packet on this port, sent from another port on the same device, then the device performs the action specified in the Action column. • **unmarked** (default setting) The Loop Protection function is inactive on the port. The port neither sends *loop detection* packets nor evaluates received *loop detection* packets.
Mode	Specifies the behavior of the Loop Protection function on the port. Possible values: • **active** The device sends *loop detection* packets and evaluates received *loop detection* packets. • **passive** (default setting) The device evaluates received *loop detection* packets.
Action	Specifies the action the device performs when it detects a layer 2 network loop on this port. Possible values: • **trap** The device sends a trap. • **auto-disable** (default setting) The device disables the port using the Auto-Disable function. The prerequisite for disabling the port is that in the Configuration frame the Auto-disable checkbox is marked. • **all** The device sends a trap. Then the device disables the port using the Auto-Disable function. The prerequisite for disabling the port is that in the Configuration frame the Auto-disable checkbox is marked.
VLAN ID	Specifies the VLAN in which the device sends the *loop detection* packets. Possible values: • **0** (default setting) The device sends the *loop detection* packets without a VLAN tag. • **1..4042** The device sends the *loop detection* packets in the specified VLAN. The prerequisite is that in the **Switching > VLAN > Port** dialog the VLAN is already set up and that the port is a member of the VLAN.
Loop detected	Displays if the device has detected a layer 2 network loop on the port. Possible values: • **yes** The device has detected a layer 2 network loop on the port. After the loop has ended and the port is enabled again, the device resets the value to **no**. • **no** The device has not detected a layer 2 network loop on the port.
Loops	Displays the number of loops the device has detected on the port since the last port statistics reset or since the last system startup.

Setting	Description
Last loop time	Displays the time at which the device detected the last loop on the port. The prerequisite for the correct evaluation of the value is that in the **Time > Basic Settings** dialog the system time of the device is synchronized with the appropriate reference time.
Sent frames	Displays the number of *loop detection* packets sent on the port since the last port statistics reset or since the last system startup.
Received frames	Displays the number of sent and received back *loop detection* packets on the port since the last port statistics reset or since the last system startup.
Discarded frames	Displays the number of discarded *loop detection* packets on the port. Examples of reasons for discarded packets: • The device detects packets with an incorrect format. • The device detects packets with expired timestamps (packets received more than 5 seconds after sending). • The device received a data packet with an unexpected VLAN information. • The device detects received packets on a port that is disabled.

SFlow

sFlow is a standard protocol for monitoring networks. The device contains the sFlow feature which gives you visibility into network activity, allowing for effective management and control of network resources.

The sFlow monitoring system consists of an sFlow agent and a central sFlow collector. The agent uses the following forms of sampling:

- statistical packet-based sampling of packet flows
- time-based sampling of counters

The device combines both types of samples into datagrams. sFlow uses the datagrams to forward the sampled data packet statistics to an sFlow collector for analysis.

To perform packet flow sampling, you set up an instance with a sampling rate. You then set up the instance with a polling interval for counter sampling.

The menu **Diagnostics > SFlow** contains the following dialogs:

- SFlow Configuration, page 361
- SFlow Receiver, page 363

SFlow Configuration

This dialog **Diagnostics > SFlow > Configuration** displays device parameters and allows you to set up sFlow instances.

The dialog contains the following tabs:

- Global, page 362
- Sampler, page 362
- Poller, page 362

Global

Information

The following table presents the information settings:

Setting	Description
Version	Displays the MIB version, the organization responsible for agent implementation, and the device software revision.
IP address	Displays the IP address associated with the agent providing SNMP connectivity.

Sampler

Table

For information on how to customize the appearance of the table, see Working with tables, page 25.

The following table presents the table settings:

Setting	Description
Port	Displays the physical source of data for the sampler. If you use this port also as a source port for the Port Mirroring function, the device cannot simultaneously copy received data packets (**rx**, **txrx**) using the Port Mirroring function.
Receiver	Specifies the receiver index associated with the sampler. Possible values: • **-** (default setting) • **(1)..(8)** The value refers to the corresponding Index settings specified in the **Diagnostics > SFlow > Receiver** dialog.
Sampling rate	Specifies the static sampling rate for the sampling of the packets from this source. Possible values: • **0** (default setting) Deactivates the sampling. • **256..65536** When you click the  button after changing the value, the device changes the value to the closest value that the device hardware supports. When the ports receive data, the device increments to the set value and then samples the data.
Max. header size [byte]	Specifies the maximum header size in bytes copied from a sampled packet. Possible values: • **20..256** (default setting: **128**)

Poller

Table

For information on how to customize the appearance of the table, see Working with tables, page 25.

The following table presents the table settings:

Setting	Description
Port	Displays the physical source of data for the poller counter.
Receiver	Specifies the receiver index associated with the query counter. Possible values: • **-** (default setting) • **(1)..(8)** The value refers to the corresponding Index settings specified in the **Diagnostics > SFlow > Receiver** dialog.
Interval [s]	Specifies the maximum number of seconds between successive samples of the counters which are associated with this data source. Possible values: • **0..86400** (default setting: **0**) A sampling interval with the value **0** deactivates the sampling of the counters.

SFlow Receiver

Diagnostics > SFlow > Receiver

To help avoid a condition where 2 persons or organizations attempt to assume control of the same sampler, the person or organization sets both the Name and Timeout [s] parameters in the same *SNMP Set request*.

When releasing a sampler, the controlling person or organization deletes the value in the Name column or sets the value in the Timeout [s] field to **0**. The device then resets the other parameters in this row to their default values.

Table

For information on how to customize the appearance of the table, see Working with tables, page 25.

The following table presents the table settings:

Setting	Description
Index	Displays the index number to which the table row relates.
Name	Specifies the name of the person or company which controls the receiver. Edit this field before making changes to other sampler parameters. Possible values: • Alphanumeric ASCII character string with 0..127 characters An empty field indicates that the settings in this table row are currently unused.
Timeout [s]	Specifies the time, in seconds, remaining before the sampler is released and stops sampling. Possible values: • **-1** No timeout. The device does not release the sampler and does not stop sampling. • **0** (default setting) The timeout has expired. The sampler is released and the sampling has stopped. The device resets the other parameters in this row to their default values. • **1..2147483647 (2^{31}-1)**
Datagram size [byte]	Specifies the maximum number of data bytes that are sent in one sample datagram. Possible values: • **200..3996** (default setting: **1400**)
IP address	Specifies the IP address of the sFlow collector. Possible values: • Valid IPv4 address (default setting: **0.0.0.0**)
Destination UDP port	Specifies the number of the UDP port for sFlow datagrams. Possible values: • **1..65535 (2^{16}-1)** (default setting: **6343**) Exception: Port **2222** is reserved for internal functions.
Datagram version	Displays the version of sFlow datagrams requested.

Report

The menu **Diagnostics > Report** contains the following dialogs:

- Report Global, page 364
- Persistent Logging, page 368
- System Log, page 370
- Audit Trail, page 370

Report Global

The device allows you to 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 **Diagnostics > Report > Global**, you specify the required settings. By assigning the severity you specify which events the device registers.

The dialog allows you to save a ZIP archive with detailed device information for support purposes on your PC.

Console Logging

The following table presents the console logging settings:

Setting	Description
Buttons	Download support information: Generates a ZIP archive which the web browser lets you download from the device. The ZIP archive contains files with detailed device information for support purposes. For further information, see Support Information: Files in ZIP archive, page 367.
Operation	Enables/disables the Console logging function. Possible values: • **On** The Console logging function is enabled. The device logs the events on the console. • **Off** (default setting) The Console logging function is disabled.
Severity	Specifies the minimum severity for the events. The device logs events with this severity and with more urgent severities. For further information, see Meaning of the event severities, page 368. The device outputs the messages on the serial interface. Possible values: • **emergency** • **alert** • **critical** • **error** • **warning** (default setting) • **notice** • **informational** • **debug**

SNMP Logging

When you enable the logging of SNMP requests, the device sends these as events with the preset severity **notice** to the list of syslog servers. The preset minimum severity for a syslog server entry is **critical**.

To send SNMP requests to a syslog server, you have a number of options to change the default settings. Select the ones that meet your requirements best.

- Set the severity for which the device generates SNMP requests as events to **warning** or **error**. Change the minimum severity for a syslog entry for one or more syslog servers to the same value.

  You also have the option of adding a separate syslog server entry for this.
- Set only the severity for SNMP requests to **critical** or greater. The device then sends SNMP requests as events with the severity **critical** or greater 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.

The following table presents the SNMP logging settings:

Setting	Description
Log SNMP get request	Enables/disables the logging for the reception of *SNMP Get requests*. Possible values: • **On** The logging is enabled. The device logs each received *SNMP Get request* as an event in the syslog. From the Severity get request drop-down list, you select the severity for this event. • **Off** (default setting) The logging is disabled.
Log SNMP set request	Enables/disables the logging for the reception of *SNMP Set requests*. Possible values: • **On** The logging is enabled. The device logs each received *SNMP Set request* as an event in the syslog. From the Severity set request drop-down list, you select the severity for this event. • **Off** (default setting) The logging is disabled.
Severity get request	Specifies the severity of the event that the device logs for received *SNMP Get requests*. For further information, see Meaning of the event severities, page 368. Possible values: • **emergency** • **alert** • **critical** • **error** • **warning** • **notice** (default setting) • **informational** • **debug**
Severity set request	Specifies the severity of the event that the device logs for received *SNMP Set requests*. For further information, see Meaning of the event severities, page 368. Possible values: • **emergency** • **alert** • **critical** • **error** • **warning** • **notice** (default setting) • **informational** • **debug**

Buffered Logging

The device buffers logged events in 2 separate storage areas so that the log entries for urgent events are kept.

This dialog alows you to specify the minimum severity for events that the device buffers in the storage area with a greater priority.

The following table presents the buffured logging settings:

Setting	Description
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 greater priority. For further information, see Meaning of the event severities, page 368. Possible values: • **emergency** • **alert** • **critical** • **error** • **warning** (default setting) • **notice** • **informational** • **debug**

CLI Logging

The following table presents the CLI logging setting:

Setting	Description
Operation	Enables/disables the CLI logging function. Possible values: • **On** The CLI logging function is enabled. The device logs every command received using the Command Line Interface. • **Off** (default setting) The CLI logging function is disabled.

Support Information: Files in ZIP archive

The following table lists the files contained in the support ZIP archive, their formats, and their purpose:

File name	For-mat	Comments
audittrail.html	HTML	Contains the chronological recording of the system events and saved user changes in the *Audit Trail* protocol.
config.xml	XML	Contains the settings of the device saved in the "Selected" configuration profile. The file name is the same as the name of the "Selected" configuration profile.
defaultconfig.xml	XML	Contains the default settings of the device.
runningconfig.xml	XML	Contains the operating settings of the device.
script	TEXT	Contains the output of the command `show running-config script`.
supportinfo.html	HTML	Contains device internal service information.
systeminfo.html	HTML	Contains information about the settings and operating parameters.
systemlog.html	HTML	Contains the logged events in the Log file. See the **Diagnostics > Report > System Log** dialog.

Meaning of the Event Severities

The following table explains the different event severity levels and their corresponding meanings:

Severity	Meaning
emergency	Device not ready for operation
alert	Immediate user intervention required
critical	Critical status
error	Error status
warning	Warning
notice	Significant, normal status
informational	Information message
debug	Debug message

Persistent Logging

The device allows you to save log entries permanently in a file in the external memory (**ENVM**). Therefore, even after the device is restarted you have access to the log entries.

In this dialog **Diagnostics > Report > Persistent Logging**, you limit the size of the log file and specify the minimum severity for the events to be saved. When the log file reaches the specified size, the device archives this file and saves the following log entries in a newly generated file.

In the table the device displays you the log files held in the external memory (**ENVM**). As soon as the specified maximum number of files has been attained, the device deletes the oldest file and renames the remaining files. This helps ensure that there is enough memory space in the external memory (**ENVM**).

NOTE: Verify that an external memory (**ENVM**) is connected. To verify if an external memory (**ENVM**) is connected, see the Status column in the **Basic Settings > External Memory** dialog. Monitor the external memory connection using the Device Status function, see the External memory removed parameter in the **Diagnostics > Status Configuration > Device Status** dialog.

Operation

The following table presents the operation setting:

Setting	Description
Operation	Enables/disables the Persistent Logging function. Only activate this function if the external memory (**ENVM**) is available in the device. Possible values: • **On** (default setting) The Persistent Logging function is enabled. The device saves the log entries in a file in the external memory (**ENVM**). • **Off** The Persistent Logging function is disabled.

Configuration

The following table presents the configuration settings:

Setting	Description
Max. file size [kbyte]	Specifies the maximum size of the log file in KBytes. When the log file reaches the specified size, the device archives this file and saves the following log entries in a newly generated file. Possible values: • **0..4096** (default setting: **1024**) The value **0** deactivates saving of log entries in the log file.
Files (max.)	Specifies the number of log files that the device keeps in the external memory (**ENVM**). As soon as the specified maximum number of files has been attained, the device deletes the oldest file and renames the remaining files. Possible values: • **0..25** (default setting: **4**) The value **0** deactivates saving of log entries in the log file.
Severity	Specifies the minimum severity of the events. The device saves the log entry for events with this severity and with more urgent severities in the log file in the external memory (**ENVM**). Possible values: • **emergency** • **alert** • **critical** • **error** • **warning** (default setting) • **notice** • **informational** • **debug**
Log file target	Specifies the external memory device for logging. Possible values: • **usb** External USB memory (EAM)

Table

For information on how to customize the appearance of the table, see Working with tables, page 25.

The following table presents the table settings:

Setting	Description
Buttons	 Clear persistent log file: Deletes the log files from the external memory (**ENVM**).
Index	Displays the index number to which the table row relates. Possible values: • **1..25** The device automatically assigns this number.
File name	Displays the file name of the log file in the external memory (**ENVM**). Possible values: • **messages** • **messages.X**
File size [byte]	Displays the size of the log file in the external memory (**ENVM**) in bytes.

System Log

This dialog **Diagnostics > Report > System Log** displays the System Log file. The device logs device-internal events in the System Log file. The device keeps the logged events even after a restart.

To search the System Log file, use the search function of your web browser.

The dialog allows you to download a copy of the System Log file onto your computer. The device provides the file to be downloaded in HTML format.

The following table presents the button descriptions:

Button	Description
 Save log file	Downloads a copy of the System Log file onto your computer, based on the web browser settings.
 Clear log file	Clears the System Log file on the device.

Audit Trail

This dialog **Diagnostics > Report > Audit Trail** displays the Audit Trail. The dialog allows you to save the log file as an HTML file on your PC.

To search the log file for search terms, use the search function of your web browser.

The device logs system events and writing user actions to the device. This allows you to keep track of WHO changes WHAT in the device and WHEN. The prerequisite is that the access role **auditor** or **administrator** is assigned to your user account.

The device logs the following user actions, among others:

- A user logging into the device management with the Command Line Interface (local or remote)
- A user logging off manually
- Automatic logging off of a user in the Command Line Interface after a specified period of inactivity
- Device restart
- Locking of a user account due to too many consecutive unsuccessful login attempts
- Locking of the access to the device management due to unsuccessful login attempts
- Commands executed in the Command Line Interface, apart from `show` commands
- Changes to configuration variables
- Changes to the system time
- File transfer operations, including device software updates
- Configuration changes using Ethernet Switch Configurator
- Device software updates and automatic configuration of the device through the external memory (**ENVM**)
- Opening and closing of SNMP through an HTTPS tunnel

The device does not log passwords. The logged entries are write-protected and remain saved in the device after a restart.

During system startup, access to the System Monitor 1 is possible using the default settings of the device. If an attacker gains physical access to the device, then he is able to reset the device settings to its default values using the System

Monitor 1. After this, the device and log file are accessible using the standard password.

⚠WARNING

UNINTENDED EQUIPMENT OPERATION

- Take appropriate measures to restrict physical access to the device.
- If necessary, deactivate access to the System Monitor 1 using the **SysMon1** checkbox in **Diagnostics > System > Selftest**.

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

The following table presents the button description:

Setting	Description
Buttons	 Save audit trail file: Saves the HTML page on your PC using the web browser dialog.

Advanced

The **Advanced** menu contains the following dialogs:

- DHCP, page 372
- DNS, page 383
- Industrial Protocols, page 388
- Tracking, page 398
- Digital IO Module, page 403
- Command Line Interface, page 406

DHCP

The **DHCP** menu (**Advanced > DHCP**) contains the following dialogs:

- DHCP Server, page 372
- DHCP L2 Relay, page 380

DHCP Server

The Dynamic Host Configuration Protocol (DHCP) lets a server assign the IP settings to the devices on the network (clients). The DHCP server stores and assigns the available IP addresses and further settings, if specified.

The DHCP server in the device listens for requests on UDP port 67 and responds to the client devices on UDP port 68. When the device receives a DHCP request, it validates the IP address to be assigned before leasing the IP address and other IP settings to the requesting client device.

This menu (**Advanced > DHCP > DHCP Server**) contains the following dialogs:

- DHCP Server Global, page 372
- DHCP Server Pool, page 373
- DHCP Server Lease Table, page 378

DHCP Server Global

This dialog (**Advanced > DHCP > DHCP Server > Global**) allows to activate the DHCP Server function either globally or per port according to your requirements.

Operation

The following table presents the **Operation** area of the **DHCP Server Global** dialog:

Setting	Description
Operation	Enables/disables the DHCP Server function of the device globally. Possible values: • **On** • **Off** (default setting)

Configuration

The following table presents the **Configuration** area of the **DHCP Server Global** dialog:

Setting	Description
IP probe	Activates/deactivates the probing for unique IP addresses. Before assigning an IP address, the device sends an *ICMP echo request* packet to check whether this IP address is already in use on the network. Possible values: • **marked** (default setting) The **IP probe** function is active. • **unmarked** The **IP probe** function is inactive.

Table

The following table presents the **Table** area of the **DHCP Server Global** dialog:

Setting	Description
Port	Displays the number of the physical port on which the device listens for DHCP requests and reponds to the client devices.
DHCP server active	Activates/deactivates the **DHCP Server** function on this port. The prerequisite is that you enable the function globally. Possible values: • **marked** (default setting) The **DHCP Server** function is active. • **unmarked** The **DHCP Server** function is inactive.

NOTE: For information on how to customize the appearance of the table, see Working with Tables, page 25.

DHCP Server Pool

In this dialog (**Advanced > DHCP > DHCP Server > Pool**), you can specify the settings for assigning a certain IP address to client devices from which the device receives a DHCP request.

The device assigns an IP address from a specific pool (address range) depending on which physical port the requesting client device is connected to or in which VLAN it is a member. The MAC address of the requesting client device is a further criterion for the pool from which the device assigns an IP address.

If specified, the device processes further information to assign an IP address from a certain pool to the client device. This can be, for example, the following information in the DHCP request:

- *Circuit ID*
- *Class ID*
- *Client ID*
- *Remote ID*

The device provides a maximum of 128 pools. Up to 1000 client devices can receive their IP settings from the device.

The device manages the IP settings in two types of pools.

- Static pools

  To assign the same IP address to a specific device each time, the device manages the relevant IP settings in a pool whose address range is exactly one IP address.

  Static pools are useful, for example, to assign a fixed IP address to a server, NAS, or printer.

- Dynamic pools

  To assign IP addresses from a certain address range, the device manages the relevant IP settings in a pool whose address range includes multiple IP addresses.

  Dynamic pools are useful, for example, to assign a certain IP address to client devices that belong to a certain VLAN.

In addition to the IP settings, the device can assign further parameters (DHCP options) to the client devices. Assigning such parameters is an smart way to automatically set up client devices as they obtain their IP settings. The device lets you specify such parameters for each pool.

The device lets you specify the boot parameters for PXE-compliant clients to boot a bootloader image downloaded from a TFTP server. Possible applications include booting an installation environment, a rescue system, or a live system over the network.

To activate the PXE boot extension for a specific pool, you add the following values to the pool settings:

- *Vendor Identifier*
- *Client System Architecture*
- URL to a bootloader image file on a TFTP server

The device expects the information for *Vendor Identifier* and *Client System Architecture* in summarized form as the *Class Identifier* in the DHCP option 60 field. When a PXE-compliant client device broadcasts a *DHCP Discover* message with a matching *Class Identifier* in the DHCP option 60 field, the device responds with the settings specified in the relevant pool.

NOTE: The device does not check the integrity, authenticity and availability of the TFTP servers and the bootloader image files involved. Use the PXE boot extension only if you trust the transfer network.

Table

The following table presents the **Table** area of the **DHCP Server Pool** dialog:

Setting	Description
Buttons	**Add** Adds a table row.
	Remove Removes the selected table row.
Index	Displays the index number to which the table row relates. The device automatically assigns the value when you add a table row.
Active	Activates/deactivates the DHCP server function on this port. Possible values: • **marked** The DHCP server function is active. • **unmarked** (default setting) The DHCP server function is inactive.
IP range start	Specifies the fixed IP address for a static pool or the start IP address of an address range. Possible values: • Valid IPv4 address (default setting: **0.0.0.0**)
IP range end	Specifies the end IP address of an address range. For a static pool, keep the default setting or add the same value as specified in the **IP range start** column. Possible values: • Valid IPv4 address (default setting: **0.0.0.0**)
Port	Specifies the number of the physical port on which the requesting client device is connected. Possible values: • **All** (default setting) The device assigns an IP address to the requesting client device regardless of the port on which the local device receives the DHCP request. • **<Port number>** The device assigns an IP address to the requesting client device only if the local device receives the DHCP request on the specified port. The prerequisite is that the item **-** is selected from the drop-down list in the VLAN ID column.
VLAN ID	Specifies the VLAN to which the table row relates. The prerequisite is that the item **All** is selected from the drop-down list in the Port column. Possible values: • **-** (default setting) • **1..4042** The value **1** represents the VLAN in which device management is accessible in the default setting.
MAC address	Specifies the MAC address of the requesting client device. Possible values: • **–** (default setting) For the IP address assignment, the server ignores this variable. • Valid Unicast MAC address Specify the value with a colon separator, for example **00:11:22:33:44:55**.

Setting	Description
DHCP relay	Specifies the IP address of the DHCP relay through which the clients transmit their requests to the DHCP server. When the device receives a DHCP request through a different DHCP relay, it ignores this DHCP request. Possible values: • **–** (default setting) No DHCP relay specified. • Valid IPv4 address IP address of the DHCP relay.
Client ID	Specifies the customized identifier for the client instead of the MAC address. Possible values: • **–** (default setting) The device ignores the parameter during assignment of an IP address from the pool. • Sequence of hexadecimal character pairs with 1..254 pairs separated by a space. Example: **41 42 43 44 4F** **NOTE:** If you have high security requirements and do not want to trust the clients implicitly, consider using the *remote ID* or the *circuit ID* instead of the *client ID*. The *remote ID* and the *circuit ID* are inserted by a DHCP relay and are therefore harder to spoof.
Remote ID	Specifies the *remote ID*. The DHCP relay inserts the *remote ID* into the DCHP request. Possible values: • **–** (default setting) The device ignores the parameter during assignment of an IP address from the pool. • Sequence of hexadecimal character pairs with 1..254 pairs separated by a space. Example: **41 42 43 44 4F**
Circuit ID	Specifies the *circuit ID*. The DHCP relay inserts the *circuit ID* into the DCHP request. Possible values: • **–** (default setting) The device ignores the parameter during assignment of an IP address from the pool. • Sequence of hexadecimal character pairs with 1..254 pairs separated by a space. Example: **41 42 43 44 4F**
Vendor ID	Specifies the *Vendor Identifier*. If specified, the device activates the PXE boot extension for the relevant pool. Only use this setting if you transmit the bootloader image file over trusted networks. When a PXE-compliant client device broadcasts a *DHCP Discover* message with a matching *Class Identifier* in the DHCP option 60 field, the device responds with the settings specified in the relevant pool. A matching *Class Identifier* contains the following information: • The string specified here. • The value selected in the Client Architecture column. Possible values: • **–** (default setting) The PXE boot extension is inactive for the relevant pool. The device ignores the *Class Identifier* in the DHCP option 60 field of received *DHCP Discover* messages. • Alphanumeric ASCII character string with 1..9 characters

Setting	Description
Client Architecture	Specifies the *Client System Architecture*. If specified, the device activates the PXE boot extension for the relevant pool. Only use this setting if you transmit the bootloader image file over trusted networks. When a PXE-compliant client device broadcasts a *DHCP Discover* message with a matching *Class Identifier* in the DHCP option 60 field, the device responds with the settings specified in the relevant pool. A matching *Class Identifier* contains the following information: • The string specified in the **Vendor ID** column. • The value selected here. Possible values: • **intel-x86pc** (default setting) Intel x86 architecture, the common architecture for most desktop PCs and servers • **nec-pc98** NEC's PC-98 series, a PC series based on the x86 architecture • **efi-itanium** Intel Itanium 64-bit processor architecture with EFI (Extensible Firmware Interface) • **dec-alpha** DEC Alpha processor architecture • **arc-x86** Advanced RISC Computing, a variant of the x86 architecture used in specific systems • **intel-lean-client** Intel architecture designed for thin clients • **efi-ia32** Intel Architecture 32-bit with EFI, typically used on older Intel processors (32-bit version of x86) • **efi-bc** Boot Continuity platform using EFI • **efi-xscale** Intel Xscale, a microprocessor series based on ARM architecture, used in embedded systems • **efi-x86-64** x86-64 architecture, also known as AMD64 or Intel 64, with EFI
Schneider Electric device	Activates/deactivates the Schneider Electric multicasts. If the device in this IP address range serves only Schneider Electric client devices, then activate this function. Possible values: • **marked** In this IP address range, the device serves only Schneider Electric client devices. The Schneider Electric multicasts are activated. • **unmarked** (default setting) In this IP address range, the device serves client devices of different manufacturers. The Schneider Electric multicasts are deactivated.
Configuration URL	Specifies the URL to a file containing additional settings for the client device to get up and running. If you have specified a value in the **Vendor ID** column and selected a value in the **Client Architecture** column, the URL refers to a bootloader image file on a TFTP server. A PXE-compliant client boots using the file provided in the URL. Possible values: • Alphanumeric ASCII character string with 0..70 characters When you leave this field blank, the device leaves this option field blank in the *DHCP Offer* message. Example: tftp://192.168.1.10/path/file.name

Setting	Description
Lease time [s]	Specifies the limited period in seconds for which the device leases each IP address. The client device is responsible for renewing the IP address before the period expires. If the client device does not renew its IP address in time, then the IP address returns to the address pool. Possible values: • **60..220752000 (2555 d)** (default setting: **86400**) • **4294967295 (2^{32}-1)** Use this value for assignments unlimited in time, and for assignments using BOOTP.
Default gateway	Specifies the IP address of the *default gateway*. A value of **0.0.0.0** disables the attachment of the option field in the DHCP message. Possible values: • Valid IPv4 address (default setting: **0.0.0.0**)
Netmask	Specifies the mask of the network to which the client belongs. A value of **0.0.0.0** disables the attachment of the option field in the DHCP message. Possible values: • Valid IPv4 netmask (default setting: **255.255.255.0**)
WINS server	Specifies the IP address of the Windows Internet Name Server which converts NetBIOS names. A value of **0.0.0.0** disables the attachment of the option field in the DHCP message. Possible values: • Valid IPv4 address (default setting: **0.0.0.0**)
NTP server	Specifies the IP address of an external NTP server. A value of **0.0.0.0** disables the attachment of the option field in the DHCP message. Possible values: • Valid IPv4 address (default setting: **0.0.0.0**)
DNS server	Specifies the IP address of the DNS server. A value of **0.0.0.0** disables the attachment of the option field in the DHCP message. Possible values: • Valid IPv4 address (default setting: **0.0.0.0**)
Hostname	Specifies the hostname. When you leave this field blank, the device leaves this option field blank in the DHCP message. Possible values: • Alphanumeric ASCII character string with 0..64 characters

NOTE: For information on how to customize the appearance of the table, see Working with Tables, page 25.

DHCP Server Lease Table

This dialog (**Advanced > DHCP > DHCP Server > Lease Table**) displays the presently assigned IP addresses for each port.

Table

The following table presents the **Table** area of the **DHCP Server Lease Table** dialog:

Setting	Description
Port	Displays the number of the port through which the device to which the IP address is assigned is connected.
IP address	Displays the IP address to which the table row relates.
Status	Displays the lease phase. According to the standard for DHCP operations, there are 4 phases when assigning an IP address: Discovery, Offer, Request, and Acknowledgement. Possible values: • **BOOTP** A DHCP client is attempting to discover a DHCP server for IP address allocation. • **offering** The DHCP server is validating that the IP address is suitable for the client. • **requesting** The DHCP client is acquiring the offered IP address. • **bound** The DHCP server is leasing the IP address to a client. • **renewing** The DHCP client is requesting an extension to the lease. • **rebinding** The DHCP server is assigning the IP address to the client after a successful renewal. • **declined** The DHCP server denied the request for the IP address. • **released** The IP address is available for other clients.
Remaining lifetime	Displays how long the assigned IP address is still valid.
Leased MAC address	Displays the MAC address of the device to which the IP address is assigned.
Gateway	Displays the Gateway IP address of the device to which the IP address is assigned.
Client ID	Displays the *client ID* of the device to which the IP address is assigned.
Remote ID	Displays the *remote ID* of the device to which the IP address is assigned.
Circuit ID	Displays the *circuit ID* of the device to which the IP address is assigned.

NOTE: For information on how to customize the appearance of the table, see Working with Tables, page 25.

DHCP L2 Relay

On the front panel of the device you find the following hazard message:

⚠WARNING

UNINTENDED EQUIPMENT 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 **DHCP L2 Relay** menu (**Advanced > DHCP L2 Relay**) contains the following dialogs:

- DHCP L2 Relay Configuration, page 380
- DHCP L2 Relay Statistics, page 383

DHCP L2 Relay Configuration

This dialog (**Advanced > DHCP L2 Relay > Configuration**) allows to 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, page 381
- VLAN ID, page 382

Operation

The following table presents the **Operation** area of the **DHCP L2 Relay Configuration** dialog:

Setting	Description
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

The following table presents the **Table** area of the **Interface** tab:

Setting	Description
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.

NOTE: For information on how to customize the appearance of the table, see Working with Tables, page 25.

VLAN ID

Table

The following table presents the **Table** area of the **VLAN ID** tab:

Setting	Description
VLAN ID	VLAN to which the table row relates.
Active	Activates/deactivates the **DHCP L2 Relay** function in this VLAN. The prerequisite is that you enable the function globally. Possible values: • **marked** The **DHCP L2 Relay** function is active. • **unmarked** (default setting) The **DHCP L2 Relay** function is inactive.
Circuit ID	Activates or deactivates the addition of the *Circuit ID* to the *Option 82* information. Possible values: • **marked** (default setting) Enables *Circuit ID* and *Remote ID* to be sent together. • **unmarked** The device sends only the *Remote ID*.
Remote ID type	Specifies the components of the *Remote ID* for this VLAN. The **Remote ID** field displays the string the device uses as *Remote ID*. Possible values: • **ip** Specifies the IP address of the device as *Remote ID*. • **mac** (default setting) Specifies the MAC address of the device as *Remote ID*. • **client-id** Specifies the system name of the device as *Remote ID*. • **other** When you select this item, enter any character string in the Remote ID column.
Remote ID	Displays the *Remote ID* that the device uses for this VLAN. If the item **other** is selected from the **Remote ID type** drop-down list, then enter any character string. Possible values: • Alphanumeric ASCII character string with 1..32 characters The device enters ASCII code values into the packet. If the item **client-id** or **other** is selected from the **Remote ID type** drop-down list, then the device processes the ASCII code of the characters. For example, when you enter the string **abc**, the device enters the value **616263** into the packet. If the device does not accept the string you entered, then perform the following steps: • Click the  button to undo the unsaved changes in the current dialog. • From the **Remote ID type** drop-down list, select the item **other**. • Click the  button without modifying the string. • Enter the arbitrary string.

NOTE: For information on how to customize the appearance of the table, see Working with Tables, page 25.

DHCP L2 Relay Statistics

The device monitors the data stream on the ports and displays the results in tabular form (**Advanced > DHCP L2 Relay > Statistics**).

This table is divided into various categories to aid you in data stream analysis.

The DHCPv6 relay options are not displayed in the statistics table.

Table

The following table presents the **Table** area of the **DHCP L2 Relay Statistics** dialog:

Setting	Description
Buttons	**Reset** Resets the counter for the statistics to **0**.
Port	Displays the port number.
Untrusted server messages with Option 82	Displays the number of DHCP server messages received with *Option 82* information on the untrusted interface.
Untrusted client messages with Option 82	Displays the number of DHCP client messages received with *Option 82* information on the untrusted interface.
Trusted server messages without Option 82	Displays the number of DHCP server messages received without *Option 82* information on the trusted interface.
Trusted client messages without Option 82	Displays the number of DHCP client messages received without *Option 82* information on the trusted interface.

NOTE: For information on how to customize the appearance of the table, see Working with Tables, page 25.

DNS

The **DNS** menu (**Advanced > DNS**) contains the following dialog:

- DNS Client, page 383

DNS Client

DNS (Domain Name System) is a service in the network that translates hostnames into IP addresses. This name resolution allows to contact other devices using their hostnames instead of their IP addresses.

Using the **Client** function the device sends requests for resolving hostnames in IP addresses to a DNS server.

This menu (**Advanced > DNS > Client**) contains the following dialogs:

- DNS Client Global, page 384
- DNS Client Current, page 384
- DNS Client Static, page 385
- DNS Client Static Hosts, page 386

DNS Client Global

In this dialog (**Advanced > DNS > Client > Global**), you can enable the **Client** function and the **Cache** function.

Operation

The following table presents the **Operation** area of the **DNS Client Global** dialog:

Setting	Description
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

The following table presents the **Cache** area of the **DNS Client Global** dialog:

Setting	Description
Buttons	**Flush cache** Deletes every entry from the DNS cache.
Cache	Enables/disables the Cache function. Possible values: • **On** (default setting) The **Cache** function is enabled. The device caches up to 128 DNS server responses (hostname and corresponding IP address). When the cache contains a matching entry, the hostname of a new request the device resolves itself. This makes sending a new query to the DNS server unnecessary. • **Off** The **Cache** function is disabled.

DNS Client Current

This dialog (**Advanced > DNS > Client > Current**) displays to which DNS servers the device sends requests for resolving hostnames in IP addresses.

Table

The following table presents the **Table** area of the **DNS Client Current** dialog:

Setting	Description
Index	Displays the sequential number of the DNS server.
Address	Displays the IP address of the DNS server. The device forwards requests for resolving hostnames in IP addresses to the DNS server with this IP address.

NOTE: For information on how to customize the appearance of the table, see Working with Tables, page 25.

DNS Client Static

In this dialog (**Advanced > DNS > Client > Static**), you can specify the DNS servers to which the device forwards requests for resolving hostnames in IP addresses.

The device allows to specify up to 4 IP addresses or to transfer the IP addresses from a DHCP server.

Configuration

The following table presents the **Configuration** area of the **DNS Client Static** dialog:

Setting	Description
Source	Specifies the source from which the device obtains the IP address of DNS servers to which the device addresses requests. Possible values: • **user** The device uses the IP addresses specified in the table. • **mgmt-dhcp** (default setting) The device uses the IP addresses which the DHCP server delivers to the device.
Domain name	Specifies the domain name according to RFC 1034 which the device adds to hostnames without a domain suffix. Possible values: • Alphanumeric ASCII character string with 0..255 characters
Request timeout [s]	Specifies the time interval in seconds for sending again a request to the server. Possible values: • **0** Deactivates the function. The device does not send a request to the server again. • **1..3600** (default setting: **3**)
Request retransmits	Specifies, how many times the device retransmits a request. The prerequisite is that in the **Request timeout [s]** field a value >**0** is specified. Possible values: • **0..100** (default setting: **2**)

Table

The following table presents the **Table** area of the **DNS Client Static** dialog:

Setting	Description
Buttons	**Add** Opens the **Create** window to add a table row. • In the Index field, you specify the index number. Possible values: ◦ **1..4** The device lets you specify up to 4 external DNS servers. • In the **IP address** field, you specify the IP address of the DNS server. Possible values: ◦ Valid IPv4 address ◦ Valid IPv6 address
	Remove Removes the selected table row.
Index	Displays the sequential number of the DNS server. You specify the index number when you add a table row.
IP address	Specifies the IP address of the DNS server. Possible values: • Valid IPv4 address • Valid IPv6 address
Active	Activates/deactivates the table row. Prerequisites: • In the **Advanced > DNS > Client > Global** dialog the *DNS client* function is enabled. • In the Configuration frame, the item **user** is selected from the Source drop-down list. Possible values: • **marked** (default setting) The table row is active. The device sends requests to the DNS server specified in the first active table row. When the device does not receive a response from this server, it sends the requests to the DNS server specified in the next active table row. The relevant timeout is specified in the Configuration frame, Request timeout [s] field. • **unmarked** The table row is inactive. The device does not send requests to this DNS server.

NOTE: For information on how to customize the appearance of the table, see Working with Tables, page 25.

DNS Client Static Hosts

This dialog (**Advanced > DNS > Client > Static Hosts**) allows to specify up to 64 hostnames to 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 the corresponding entry, it forwards the request.

Table

The following table presents the **Table** area of the **DNS Client Static Hosts** dialog:

Setting	Description
Buttons	**Add** Opens the **Create** window to add a table row: • In the **Index** field, specify the index number. Possible values: ◦ **1..64** The device lets you specify up to 64 static hosts. • In the **Name** field, you specify the hostname of the related device. Possible values: ◦ Alphanumeric ASCII character string with 1..255 characters • In the **IP address** field, you specify the IP address of the related device. Possible values: ◦ Valid IPv4 address ◦ Valid IPv6 address
	Remove Removes the selected table row.
Index	Displays the index number to which the table row relates. You specify the index number when you add a table row.
Name	Specifies the hostname. Possible values: • Alphanumeric ASCII character string with 1..255 characters
IP address	Specifies the IP address under which the host is reachable. Possible values: • Valid IPv4 address • Valid IPv6 address
Active	Activates/deactivates the table row. Possible values: • **marked** (default setting) The table row is active. When the device receives a request for this hostname, it provides the requesting client device with the associated IP address. • **unmarked** The table row is inactive. When the device receives a DNS request for this hostname, it forwards the request to a DNS server specified in the **Advanced > DNS > Client > Static** dialog.

NOTE: For information on how to customize the appearance of the table, see Working with Tables, page 25.

Industrial Protocols

The **Industrial Protocols** menu (**Advanced > Industrial Protocols**) contains the following dialogs:

- IEC 61850-MMS, page 388
- Modbus TCP, page 390
- EtherNet/IP, page 392
- OPC UA Server, page 393
- Service Discovery, page 396

IEC 61850-MMS

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

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

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

This dialog (**Advanced > Industrial Protocols > IEC 61850-MMS**) allows to 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

The following table presents the **Operation** area of the **IEC 61850-MMS** dialog:

Setting	Description
Operation	Enables/disables the **IEC 61850-MMS** server. Possible values: • **On** The IEC 61850-MMS server is enabled. • **Off** (default setting) The **IEC 61850-MMS** server is disabled. The IEC61850 MIBs stay accessible.

Information

The following table presents the **Information** area of the **IEC 61850-MMS** dialog:

Setting	Description
Status	Displays the current **IEC 61850-MMS** server status. Possible values: • **unavailable** • **starting** • **running** • **stopping** • **halted** • **error**
Active sessions	Displays the number of active MMS server connections.

Configuration

The following table presents the **Configuration** area of the **IEC 61850-MMS** dialog:

Setting	Description
Buttons	**Download ICD file** Copies the ICD file to your PC.
	Download CID file Copies the CID file to your PC.
Write access	Activates/deactivates the write access to the MMS server. Possible values: • **marked** The write access to the MMS server is activated. This setting lets you change the device settings using the IEC 61850 MMS protocol. • **unmarked** (default setting) The write access to the MMS server is deactivated. The MMS server is accessible as read-only.
Technical key	Specifies the Intelligent Electronic Device (IED) name, also known as Technical Key. The IED name is eligible independently of the system name. Possible values: • Alphanumeric ASCII character string with 0..32 characters The device accepts the following characters: ◦ **_** ◦ **0..9** ◦ **a..z** ◦ **A..Z** (default setting: **KEY**) To get the MMS server to use the IED name, click the button and restart the MMS server. The connection to connected clients is then interrupted.
TCP port	Specifies TCP port for MMS server access. Possible values: • **1..65535 (2^{16}-1)** (default setting: **102**) Exception: Port **2222** is reserved for internal functions. **NOTE:** The server restarts automatically after you change the port. In the process, the device terminates open connections to the server.
Sessions (max.)	Specifies the maximum number of MMS server connections. Possible values: • **1..15** (default setting: **5**)

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 (**Advanced > Industrial Protocols > Modbus TCP**) allows to specify the parameters of the protocol. To monitor and control the parameters of the device, you need an application with a Human-Machine Interface and the memory

mapping table. Refer to the tables located in the “Configuration” user manual for the supported objects and memory mapping.

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

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

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

Operation

The following table presents the **Operation** area of the **Modbus TCP** dialog:

Setting	Description
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

The following table presents the **Configuration** area of the **Modbus TCP** dialog:

Setting	Description
Write access	Activates/deactivates the write access to the **Modbus TCP** parameters. **NOTE:** Activating the **Modbus TCP** write-access can cause a security risk, because the protocol does not authenticate user access. Possible values: • **marked** (default setting) The **Modbus TCP** server read/write access is active. This lets you change the device settings using the **Modbus TCP** function. • **unmarked** The Modbus TCP server read-only access is active.
TCP port	Specifies the TCP port number that the **Modbus TCP** server uses for communication. Possible values: • **<TCP Port number>** (default setting: **502**) Specifying **0** is not allowed.
Sessions (max.)	Specifies the maximum number of concurrent sessions that the **Modbus TCP** server maintains. Possible values: • **1..5** (default setting: **5**)

EtherNet/IP

This dialog (**Advanced > Industrial Protocols > EtherNet/IP**) allows to specify the EtherNet/IP settings. The following options are available:

- Enable/disable the **EtherNet/IP** function in the device.
- Specify a VLAN which forwards the **EtherNet/IP** packets exclusively.
- Activate/deactivate the read/write capability of the **EtherNet/IP** function.
- Download the Electronic Data Sheet (EDS) file from the device.

Operation

The following table presents the **Operation** area of the **EtherNet/IP** dialog:

Setting	Description
Operation	Enables/disables the **EtherNet/IP** function in the device. Possible values: • **On** The **EtherNet/IP** function is enabled. • **Off** (default setting) The **EtherNet/IP** function is disabled.

Configuration

The following table presents the **Operation** area of the **EtherNet/IP** dialog:

Setting	Description
Buttons	**Download EDS file** Copies the following information in a zip file onto your PC: • Electronic Data Sheet (EDS) with device related information • Device icon
Write access	Activates/deactivates the read/write capability of the EtherNet/IP function. Possible values: • **marked** The **EtherNet/IP** function accepts set/get requests. • **unmarked** (default setting) The **EtherNet/IP** function accepts only get requests.

VLAN Configuration

The following table presents the **VLAN Configuration** area of the **EtherNet/IP** dialog:

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

OPC UA Server

The protocol *OPC UA* is a standardized protocol for industrial communication defined in the standard IEC 62541. The OPC UA Server function monitors the *OPC UA* information model data for the industrial automation equipments such as Programmable Logic Controllers (PLC), sensors and meters.

To monitor the *OPC UA* information model data of the connected end devices, use an *OPC UA* client application.

In this dialog (**Advanced > Industrial Protocols > OPC UA Server**), you can enable the OPC UA Server function and specify the required settings. You can also specify the number of sessions allowed to be open at the same time. The dialog allows to manage the *OPC UA* user accounts required to access the device using an *OPC UA* client application. Every *OPC UA* user requires an active *OPC UA* user account to gain access to the *OPC UA* server of the device.

Operation

The following table presents the **Operation** area of the **OPC UA Server** dialog:

Setting	Description
Operation	Enables/disables the **OPC UA Server** function in the device. Possible values: • **On** The **OPC UA Server** function is enabled. • **Off** (default setting) The **OPC UA Server** function is disabled.

Configuration

The following table presents the **Configuration** area of the **OPC UA Server** dialog:

Setting	Description
Listening port	Specifies the TCP port number that the **OPC UA Server** server uses for communication. Possible values: • **1..65535 (2^{16}-1)** (default setting: **4840**) Exception: Port **2222** is reserved for internal functions.
Sessions (max.)	Specifies the maximum number of *OPC UA* connections to the device that can be set up simultaneously. Each accessing *OPC UA* client application establishes a separate *OPC UA* connection to the device. Possible values: • **1..5** (default setting: **5**)
Security policy	Specifies the authentication and encryption protocol that the device applies for the *OPC UA* user. Possible values: • **none** (default setting) The *OPC UA* user does not need to authenticate oneself. • **basic128Rsa15** The *OPC UA* user authenticates using the *Basic128Rsa15* protocol. • **basic256** The *OPC UA* user authenticates using the *Basic256* protocol. • **basic256Sha256** The *OPC UA* user authenticates using the *Basic256Sha256* protocol.

Table

The following table presents the **Operation** area of the **OPC UA Server** dialog:

Setting	Description
Buttons	**Add** Opens the **Create** window to add a table row. The device allows to specify up to 4 *OPC UA* user accounts. • In the **User name** field, you specify the name of the *OPC UA* user account. Possible values: Alphanumeric ASCII character string with 1..32 characters The device accepts the following characters: ◦ **a..z** ◦ **A..Z** ◦ **0..9** ◦ **<space>** ◦ **-_**
	Remove Removes the selected table row.
User name	Displays the name of the *OPC UA* user having access to the device using an *OPC UA* client application.
Password	Specifies the password that the user applies to access the device using an *OPC UA* client application. Displays ***** (asterisks) instead of the password with which the user logs in. To change the password, click the relevant field. Possible values: • Alphanumeric ASCII character string with 6..64 characters The device accepts the following characters: ◦ **a..z** ◦ **A..Z** ◦ **0..9** ◦ **!#$%&'()*+,-./:;<=>?@[\]^_`{}~**
Access role	Specifies the role that regulates the access of the *OPC UA* user using an *OPC UA* client application. Possible values: • **readOnly** (default setting) The *OPC UA* user account has read-only access to the device. The *OPC UA* user can view the *OPC UA* information model data of the connected end devices.
Active	Activates/deactivates the *OPC UA* user account in the device. Possible values: • **marked** The *OPC UA* user account is active. The device accepts the login of an *OPC UA* user with this user name. • **unmarked** (default setting) The *OPC UA* user account is inactive. The device rejects the login of an *OPC UA* user with this user name.

NOTE: For information on how to customize the appearance of the table, see Working with Tables, page 25.

Service Discovery

Service Discovery is part of a series of technologies summarized by the term Zero-configuration networking (zeroconf). Service Discovery uses multicast DNS (mDNS) and DNS service discovery (DNS-SD) to advertise the services offered by the device to other devices in the network that request the service. The device currently supports the **ITxPT Module Inventory** service. Additional services may follow in future releases.

Devices that support Service Discovery can automatically discover the available services on the network without having information about which devices are available. In public transportation, for example, such devices can be ticketing systems, passenger information systems, or vehicle tracking systems.

Devices that subscribe to the services will detect a new device as soon as you connect it to the network, and read its service data. For example, when you install a ticketing system in the network of a public transportation vehicle, the ticketing system needs to communicate with the existing passenger information system to deliver real-time updates on ticket sales and availability.

In this dialog (**Advanced > Industrial Protocols > Service Discovery**), you can select and set up the services that the device will advertise.

The dialog contains the following tab:

- ITxPT Module Inventory, page 396

ITxPT Module Inventory

The **ITxPT Module Inventory** service is part of the Information Technology for Public Transport (ITxPT) specification.

The intended use of the **ITxPT Module Inventory** service is module inventory in networks of vehicles. The **ITxPT Module Inventory** service allows devices subscribing to the service automatically to inventory the modules installed in the on-board IP network of vehicles. Modules in the sense of ITxPT might be other Schneider Electric devices or devices from the on-board network of the vehicle. For example, the on-board passenger information system. The service allows to collect information about the modules and monitor their status.

The device provides the information through *SRV records* and *TXT records*:

- The *SRV record* contains the location.
- The device provides the *TXT record* through mDNS.

  The *TXT record* contains information about the service.

The device transmits the *TXT record* once in the following cases:

- After an mDNS query containing the address _itxpt_socket._tcp.local.

  The device transmits the *TXT record* in response to multicast or unicast requests in the network for services offered by the device.
- Without a request
  - As soon as the **Service Discovery** function and the **ITxPT Module Inventory** service are enabled. See the **Operation** frame.
  - If the **Service Discovery** function and the **ITxPT Module Inventory** service are enabled, and the device detects changes regarding the global status or the port status of other devices in the network. Other devices might be other Schneider Electric devices or devices from the on-board network of the vehicle. For example, the on-board passenger information system.

Operation

The following table presents the **Operation** area of the **ITxPT Module Inventory** tab:

Setting	Description
Operation	Enables/disables the **Service Discovery** function. Simultaneously, the device activates/deactivates the **ITxPT Module Inventory** service to monitor the link status or the PoE status of the device. Possible values: • **On** The **Service Discovery** function is enabled. The **ITxPT Module Inventory** service is active. The device performs the following actions: ◦ On ports for which the checkbox in the **Link** column is marked: Monitoring the link status. Writing the link status into the *xstatus* attribute of the *TXT record*. ◦ On ports for which the checkbox in the **PoE** column is marked: Monitoring the PoE status. Writing the PoE status into the *xstatus* attribute of the *TXT record*. ◦ The device sends the *TXT record* one time to the devices subscribing to this service. The device sends the *TXT record* without a request in the following cases: ◦ When you enable the **Service Discovery** function. or ◦ When the device detects a change regarding the global status or the port status of other devices in the network. Other devices might be other Schneider Electric devices or devices from the on-board network of the vehicle. For example, the on-board passenger information system. • **Off** (default setting) The **Service Discovery** function and the**ITxPT Module Inventory** service are disabled.

Table

The following table presents the **Table** area of the **ITxPT Module Inventory** tab:

Setting	Description
Port	Displays the port number.
Link	Activates/deactivates the **ITxPT Module Inventory** service to monitor the link status of this port. Possible values: • **marked** The device performs the following actions: ◦ Monitoring the link status of this port. ◦ Writing the link status into the *xstatus* attribute of the *TXT record*. ◦ Transmitting the *TXT record* once, without a request being required. Other devices subscribing to this service data can analyze the data contained in the *TXT record*. Other devices might be other Schneider Electric devices or devices from the on-board network of the vehicle. For example, the on-board passenger information system. • **unmarked** (default setting) The device does not monitor the link status of this port.
PoE	Activates/deactivates the **ITxPT Module Inventory** service to monitor the PoE status of this port. Possible values: • **marked** The device performs the following actions: ◦ Monitoring the PoE status of this port. ◦ Writing the PoE status into the *xstatus* attribute of the *TXT record*. ◦ Transmitting the *TXT record* once, without a request being required. Other devices subscribing to this service data can analyze the data contained in the *TXT record*. Other devices might be other Schneider Electric devices or devices from the on-board network of the vehicle. For example, the on-board passenger information system. • **unmarked** (default setting) The device does not monitor the PoE status of this port.

NOTE: For information on how to customize the appearance of the table, see Working with Tables, page 25.

Tracking

The tracking function (**Advanced > Tracking**) allows to monitor tracking objects. Examples of monitored tracking objects are the link status of an interface or the reachability of a remote router or end device.

The device forwards status changes of the tracking objects to the registered applications, for example to the routing table or to a VRRP instance. The applications then react to the status changes:

- In the routing table, the device activates/deactivates the route linked to the tracking object.
- The VRRP instance linked to the tracking object reduces the priority of the virtual router so that a backup router takes over the role of the master.
- When the status of the tracking object changes, the device enables/disables the interface linked to the tracking object. The device displays the corresponding application in the **Advanced > Tracking > Applications** dialog.

If you set up the tracking objects in the **Advanced > Tracking > Configuration** dialog, then you can link applications with the tracking objects:

- Static routes with a tracking object in the **Routing > Routing Table** dialog, **Track name** column.
- Virtual routers with a tracking object in the **Routing > L3-Redundancy > VRRP > Tracking** dialog. Click the  button to open the **Create** window and select the tracking object from the Track name drop-down list.
- The interface status with a tracking object in the **Basic Settings > Port** dialog, **Track name** column.

The menu contains the following dialogs:

- Tracking Configuration, page 399
- Tracking Applications, page 402

Tracking Configuration

This dialog (**Advanced > Tracking > Configuration**) allows to set up the tracking objects.

Table

The following table presents the **Table** area of the **Tracking Configuration** dialog:

Setting	Description
Buttons	**Add** Opens the **Create** window to add a table row: • From the **Type** drop-down list, select the type of the tracking object. Possible values: ◦ **interface** The device monitors the link status of its physical ports or of its link aggregation, LRE or VLAN router interface. ◦ **logical** The device monitors tracking objects logically linked to each other and thus enables complex monitoring tasks. • In the **Track ID** field, specify the identification number of the tracking object. Possible values: ◦ **1..256**
	Remove Removes the selected table row.
Type	Specifies the type of the tracking object. Possible values: • **interface** The device monitors the link status of its physical ports or of its link aggregation, LRE or VLAN router interface. • **logical** The device monitors tracking objects logically linked to each other and thus enables complex monitoring tasks.
Track ID	Specifies the identification number of the tracking object. Possible values: • **1..256** This range is available to every type (**interface**, **ping** and **logical**).
Track name	Displays the name of the tracking object made up of the values displayed in the **Type** and **Track ID** columns.
Active	Activates/deactivates the monitoring of the tracking object. Possible values: • **marked** Monitoring is active. The device monitors the tracking object. • **unmarked** (default setting) Monitoring is inactive.
Description	Specifies the description. Here you describe what the device uses the tracking object for. Possible values: • Alphanumeric ASCII character string with 0..255 characters

Setting	Description
Status	Displays the monitoring result of the tracking object. Possible values: • **up** The monitoring result is positive: ◦ The link status is active. or ◦ The remote router or end device is reachable. or ◦ The result of the logical link is *TRUE*. • **down** The monitoring result is negative: ◦ The link status is inactive. or ◦ The remote router or end device is not reachable. or ◦ The result of the logical link is *FALSE*. • **notReady** The monitoring of the tracking object is inactive. You activate the monitoring in the Active column.
Changes	Displays the number of status changes since the tracking object has been activated.
Last changed	Displays the time of the last status change.
Send trap	Activates/deactivates the sending of an SNMP trap when someone activates or deactivates the tracking object. Possible values: • **marked** If someone activates or deactivates the tracking object in the Active column, then the device sends an SNMP trap. • **unmarked** (default setting) The device does not send an SNMP trap.
Port	Specifies the interface to be monitored for tracking objects of the **interface** type. Possible values: • **<Interface number>** Number of the physical ports or of the link aggregation, LRE or VLAN router interface. • **no Port** No tracking object of the **interface** type.
Link up delay [s]	Specifies the period in seconds after which the device evaluates the monitoring result as positive. If the link has been active on the interface for longer than the period specified here, then the Status column displays the value **up**. Possible values: • **0..255** • **–** No tracking object of the **logical** type.
Link down delay [s]	Specifies the period in seconds after which the device evaluates the monitoring result as negative. If the link has been inactive on the interface for longer than the period specified here, then the Status column displays the value **down**. Possible values: • **0..255** • **–** No tracking object of the **interface** type. If the link to every aggregated port is interrupted, then Link aggregation, LRE and VLAN router interfaces have a negative monitoring result. If the link to every physical port and link-aggregation interface which is a member of the VLAN is interrupted, then a VLAN router interface has a negative monitoring result.

Setting	Description
Logical operand A	Specifies the first operand of the logical link for tracking objects of the **logical** type. Possible values: • Tracking objects set up • **–** No tracking object of the **logical** type.
Logical operand B	Specifies the second operand of the logical link for tracking objects of the **logical** type. Possible values: • Tracking objects set up • **–** No tracking object of the **logical** type.
Operator	Links the tracking objects specified in the **Logical operand A** and **Logical operand B** fields. Possible values: • **and** Logical AND link • **or** Logical OR link • **–** No tracking object of the **logical** type.

NOTE: For information on how to customize the appearance of the table, see Working with Tables, page 25.

Tracking Applications

This dialog (**Advanced > Tracking > Applications**) informs which applications are linked with the tracking objects.

The following applications can be linked with tracking objects:

- Static routes with a tracking object in the **Routing > Routing Table** dialog, the **Track name** column.
- Virtual routers with a tracking object in the **Routing > L3-Redundancy > VRRP > Tracking** dialog. Click the  button to open the **Create** window and select the tracking object from the **Track name** drop-down list.
- The interface status with a tracking object in the **Basic Settings > Port** dialog, the **Track name** column.

Table

The following table presents the **Table** area of the **Tracking Application** dialog:

Setting	Description
Type	Displays the type of the tracking object.
Track ID	Displays the identification number of the tracking object.
Application	Displays the name of the application that is linked with the tracking object. Possible values: • Tracking objects of the **logical** type • Static routes • Virtual router of a VRRP instance • Interface status
Track name	Displays the name of the tracking object made up of the values displayed in the Type and Track ID columns.

NOTE: For information on how to customize the appearance of the table, see Working with Tables, page 25.

Digital IO Module

The digital inputs allow to capture and forward signals from digital sensors.

The **Digital IO Module** dialog (**Advanced > Digital IO Module**) contains the **IO input**, page 403 tab.

IO input Tab

The **IO input** tab allows to:

- Activate/deactivate the querying of the digital inputs globally
- Specify 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

The following table presents the **Operation** area of the **IO Input** tab:

Setting	Description
Operation	Enables/disables the cyclical queries from the digital inputs (IO Input). Possible values: • **On** Lets you query the input values. • **Off** (default setting)

Configuration

The following table presents the **Configuration** area of the **IO Input** tab:

Setting	Description
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

The following table presents the **Table** area of the **IO Input** tab:

Setting	Description
Input ID	Displays the slot number of the module (x) and number of the digital input (i) that applies to this table row. Notation: **x.i** Possible values: • x = **0..7** The value **0** equals the main unit (MU). • i = **1..4**
Value	Displays 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. • **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. Possible values: • **marked** The sending of SNMP traps is active. The prerequisite is that in the **Diagnostics > Status Configuration > Alarms (Traps)** dialog the Alarms (Traps) function is enabled and at least one trap destination is specified. 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 the device detects changes on the digital inputs, the device sends an SNMP trap. • **unmarked** (default setting) The sending of SNMP traps is inactive.

NOTE: For information on how to customize the appearance of the table, see Working with Tables, page 25.

Command Line Interface

This dialog (**Advanced > CLI**) allows to access the device using the Command Line Interface .

Prerequisites:

- In the **Device Security > Management Access > Server** dialog, SSH tab the SSH server is enabled.
- On your workstation, install a SSH-capable client application which registers a handler for URLs starting with ssh:// in your operating system.

Button

The following table presents the **Open SSH connection** button:

Button	Description
Open SSH connection	Opens the SSH-capable client application. When you click the button, the web application passes the URL of the device starting with ssh:// and the user name of the currently logged in user. If the web browser finds an SSH-capable client application, then the SSH-capable client establishes a connection to the device management using the SSH protocol.

Index

+ 23
802.1D/p mapping 229
802.1X 103, 143

A

Access control 143
Access control lists 181
Access restriction 127
ACL 181
address conflict detection 30
Address conflict detection 314
address, duplicate 35
Aging time 195
Alarm 308
alarm, ingress utilization 53
ARP 314
ARP inspection 174
ARP table 317
ARP table, clear 58
Audit trail 370
Authentication history 153
Authentication list 103
Auto disable ... 139–140, 166, 177–178, 253, 337–338, 343, 359
auto-shutdown power 57
autoneg, port configuration 50

B

backup config on remote server
  remote server, backup config 47
backup config when saving, external memory 49
banner 22
BOOTP 33
Boundary clock 74
Bridge 250
buttons 24

C

CA (Certification Authority) 108, 321, 327
cable crossing, manual 51
Cable diagnosis 332
certificate 28, 42
Certificate 108, 125–126, 300, 322, 328
Certificate Revocation List (CRL) 108, 322, 328
Certification Authority (CA) 108, 321, 327
class, detected 56
clear ARP table 58
clear email notification statistics 58
clear FDB 58
clear IGMP snooping data 58
clear log file 58
clear management access statistics 58
clear persistent log file 58
clear port statistics 58
CLI 130
clock settings 59
Command line interface 130
Community names 132
config priority, external memory 48
configuration encryption 45
configuration profile 40
Configuration profile
  save settings 24
  settings, save 24
configuration, IPv4 31
configuration, port 49
configuration, undo 46
configured power budget, PoE 55
ConneXium Network Manager 117
consumption, maximum 57
consumption, PoE 56
control elements 23
control interval 53
counter reset 57
credentials, backup config 47
CRL (Certificate Revocation List) 108, 322, 328
current settings, port configuration 50

D

data, system 28
daylight saving time 59
Daylight saving time 60
Default gateway 378
delivered current, PoE 55
delivered power, PoE 55
delivered, PoE 54
detected class, PoE 56
device software 38
device software, backup 38
device status 26
Device status 292
DHCP 33
DHCP L2 Relay 380
DHCP server 372
DHCP snooping 164
DHCP, IPv6 34
DHCPv6 L2 Relay 380
dialog area 23
digital certificate 28, 42
Digital certificate 108, 126, 300, 322, 328
Digital input 403
disable power, PoE 57
disable, IPv4/IPv6 33
display, update 25
DNS 383
DNS cache 384
DNS client 384
Domain name system 383
DoS 161
Download EDS for EtherNet/IP 392
DSCP 231
duplicate address detection 35
Dynamic ARP inspection 174

E

EAPOL 152
Egress rate limiter 196
elements 23
Email notification 320
email notification statistics, clear 58
enable, IPv4/IPv6 33
enable/disable PoE 54
encryption 40
encryption, configuration 45
ENVM 40, 43–44, 47, 369
Ethernet switch configurator 30
Ethernet Switch Configurator 300, 370

EtherNet/IP 301, 392
EtherNet/IP, Download EDS 392
EtherNet/IP, Read/write capability 392
EtherNet/IP, VLAN 392
Event severity 324, 368
external memory 29, 47
External memory 40, 43–44, 294, 299, 305, 369
external memory, backup config when saving 49
external memory, config priority 48
external memory, software auto update 48
external memory, SSH key 48
external memory, status 48
external memory, type 48
external memory, writable 48

F

factory reset 42
fast startup, PoE 56
FDB (MAC address table) 198
FDB, clear 58
Filter MAC addresses 198
filtering table rows 25
Fingerprint 121, 125
Flash memory 40, 313
Flow control 195
flow control, port configuration 51

G

GARP 225
gateway address 35
global power 54
GMRP 225
Guards 265
GVRP 227

H

Hardware state 313
HIPER Ring 248
Host key 122
HTML 313, 370
HTTP 122
HTTP server 299
HTTPS 123
humidity 28

I

IAS 103, 154
icon toolbar 22
IEC61850-MMS 300, 388
IEEE 802.1X 103
IGMP snooping 200
IGMP snooping data, clear 58
Ingress filtering 238
Ingress rate limiter 196
ingress utilization 52
ingress utilization, alarm 53
ingress utilization, control interval 53
ingress utilization, lower threshold 53
ingress utilization, upper threshold 53
Integrated authentication server 103, 154
IO input 403
IP access restriction 127
IP address conflict detection 314
IP DSCP mapping 231
IP parameter 35
IP parameter, valid IPv4 address 32
IP parameter, valid IPv4 netmask 32
IP source guard 171
IPv4 address, netmask 32
IPv4 address, valid 32
IPv4 rule 182
IPv4, configuration 31
IPv4, enable/disable 33
IPv6 33
IPv6 address 35
IPv6, DHCP 34
IPv6, enable/disable 33

L

L2 Relay (DHCP) 380
LDAP 103
LED status 29
Link aggregation 269
Link backup 276
Link status 294, 305
link-local 34
link/current settings, port configuration 50
LLDP 352
load/save 40
log file 57
Log file 58, 370
log file, clear 58
Login banner 131, 133
Loop protection 306
loopback 34
Loops 249
lower threshold 53

M

MAC address conflict detection 30
MAC address table (forwarding database) 198
MAC flood 138
MAC rule 189
MAC spoof 140
management access 30, 33
Management access 127
management access statistics, clear 58
management interface 34, 37
management VLAN 30
manual cable crossing, port configuration 51
Manufacturing message specification 388
maximum budget, PoE 54
maximum consumption, PoE 57
Media redundancy protocol 244
memory, external 47
menu pane 22
menu tree 23
MMRP 219
MMS 388
Modbus TCP 300, 390
modification mark 24
MRP 244
MRP-IEEE 218
MRP-IEEE configuration 218
MSTP 250
MTU, port configuration 51
multicast 34
MVRP 222

N

neighbor solicitation....35
NVM....24, 40, 42
NVM, external memory....46
NVM, running configuration....46

O

operation....46
operation, backup config....47
out-of-band management....37

P

Password....99, 298
Password length....98, 298
persistent log file, clear....58
Persistent logging....368
PoE Global....53
PoE port....53, 55
PoE port table....55
PoE, auto-shutdown power....57
PoE, configuration....54
PoE, configured power budget....55
PoE, consumption....56
PoE, delivered....54
PoE, delivered current....55
PoE, delivered power....55
PoE, detected class....56
PoE, disable power....57
PoE, enable/disable....54
PoE, fast startup....56
PoE, maximum budget....54
PoE, maximum consumption....57
PoE, module....55
PoE, power limit....56
PoE, priority....56
PoE, re-enable power....57
PoE, reserved....54
PoE, reserved power....55
PoE, send trap....54–55
PoE, status....56
PoE, threshold....55
PoE, threshold %....54
Port clients....151
port configuration....49
Port configuration....147, 229
port configuration, autoneg....50
port configuration, flow control....51
port configuration, link/current settings....50
port configuration, manual cable crossing....51
port configuration, manual configuration....50
port configuration, MTU....51
port configuration, power save....51
port configuration, power state....51
port configuration, send trap....51
port configuration, signal....51
port configuration, state....50
port configuration, track name....51
Port mirroring....346
Port monitor....343
Port priority....229
Port security....137
Port statistics....152
port statistics, clear....58
port status....29
Port VLAN....237
Port-based access control....143
power limit....56
power over Ethernet (poE)....53
power save, port configuration....51
power state, port configuration....51
Power supply....295, 306
power supply module....28
Pre-Login banner....133
Priority queue....228
priority, PoE....56
protocol, Ethernet switch configurator....30

Q

Queue management....232
Queues....228

R

RADIUS....103, 155
RADVD....34
RAM....42
RAM self-test....318
Rate limiter....196
RCP....289
re-enable power....57
Read/write capability for EtherNet/IP....392
reboot....57
Redundant coupling protocol....289
Relay (DHCP)....380
Request interval....67
reserved, PoE....54
reset the settings....42
Ring redundancy....295, 305
Ring structure....244
Ring/Network coupling....284
RNC....284
Root bridge....250
router advertisement....34
router solicitation....34
RSTP....249–250

S

Secure Boot....301
Secure Shell (SSH)....119
security status....27
Security status....296
selecting multiple table rows....25
Self-test....318
send trap, PoE....54–55
send trap, port configuration....51
Serial interface....299
set credentials, backup config....47
settings....40
settings, clock....59
Severity....324, 368
sFlow....361
SFP module....331
Signal contact....302
signal contact status....27
signal, port configuration....51
SNMP server....116, 299
SNMP traps..51, 54–55, 140, 251, 273, 293, 296, 304, 308, 317, 337, 401, 405
SNMPv1/v2....132
SNTP....65
SNTP client....66
SNTP server....69

software auto update, external memory....48
software update....38
software, backup....38
software, update....38
sorting table rows....25
Source guard....171
Spanning tree protocol....249
Ssecure Boot....39
SSH key, external memory....48
SSH server....119
standard buttons....24
startup, fast....56
status, device....26
status, external memory....48
status, LED....29
status, port....29
status, security....27
status, signal contact....27
Sub Ring....279
Support information....365
Support information (ZIP archive)....367
switch configurator....30
Syslog....327
system data....28
System information....313
System log....370
System Monitor 1....318
System time....59

T

table rows, filter....25
table rows, selecting multiple....25
table rows, sorting....25
tables....25
Telnet server....118, 298
temperature....28
Temperature....294, 305
threshold %, PoE....54
Threshold values network load....196
threshold, PoE....55
time configuration....59
Time profile....62
Time-Sensitive Networking....212
timeout....46
Topology discovery....355
track name, port configuration....51
Tracking....398
Transparent clock....82
Trap destination....311
trap, send....51, 55
traps....51, 54–55
Traps....140, 251, 273, 293, 296, 304, 308, 317, 337, 401, 405
Trust mode....229
TSN Configuration....212
TSN Gate Control List....216–217
Twisted-pair....332

U

undo configuration modifications....46
unsigned device software (allow upload)....39
update software, external memory....48
updating the display....25
upper threshold....53
uptime....28
Uptime....314
URL, backup config....47
USB port....37
User administration....98

V

Virtual local area network....234
VLAN....32, 34, 234, 360
VLAN configuration....235
VLAN for EtherNet/IP....392
VLAN ports....237
VLAN, management....30

W

watchdog....40, 46
Web server....122–123
working with tables....25
writable, external memory....48

Z

ZIP archive with support information....367

35 rue Joseph Monier
92500 Rueil Malmaison
France

www.se.com

QGH59084.03