

SIEMENS

SIMATIC NET

Industrial Ethernet Switches SCALANCE Layer 2 / Layer 3 Web Based Management (WBM) V1.1

Configuration Manual

SCALANCE XC-300
SCALANCE XR-300
SCALANCE XC-400
SCALANCE XR-500

07/2023


C79000-G8976-C661-02


<u>Introduction</u>	1
<u>Description</u>	2
<u>Security recommendations</u>	3
<u>Assignment of an IP address</u>	4
<u>Technical basics</u>	5
<u>Configuring with Web Based Management</u>	6
<u>Troubleshooting/FAQ</u>	7
<u>Appendix A "Syslog messages"</u>	A


Legal information

Warning notice system

This manual contains notices you have to observe in order to ensure your personal safety, as well as to prevent damage to property. The notices referring to your personal safety are highlighted in the manual by a safety alert symbol, notices referring only to property damage have no safety alert symbol. These notices shown below are graded according to the degree of danger.

 DANGER
indicates that death or severe personal injury will result if proper precautions are not taken.

 WARNING
indicates that death or severe personal injury may result if proper precautions are not taken.

 CAUTION
indicates that minor personal injury can result if proper precautions are not taken.

NOTICE
indicates that property damage can result if proper precautions are not taken.


If more than one degree of danger is present, the warning notice representing the highest degree of danger will be used. A notice warning of injury to persons with a safety alert symbol may also include a warning relating to property damage.

Qualified Personnel

The product/system described in this documentation may be operated only by **personnel qualified** for the specific task in accordance with the relevant documentation, in particular its warning notices and safety instructions. Qualified personnel are those who, based on their training and experience, are capable of identifying risks and avoiding potential hazards when working with these products/systems.

Proper use of Siemens products

Note the following:

 WARNING
Siemens products may only be used for the applications described in the catalog and in the relevant technical documentation. If products and components from other manufacturers are used, these must be recommended or approved by Siemens. Proper transport, storage, installation, assembly, commissioning, operation and maintenance are required to ensure that the products operate safely and without any problems. The permissible ambient conditions must be complied with. The information in the relevant documentation must be observed.

Trademarks

All names identified by ® are registered trademarks of Siemens AG. The remaining trademarks in this publication may be trademarks whose use by third parties for their own purposes could violate the rights of the owner.

Disclaimer of Liability

We have reviewed the contents of this publication to ensure consistency with the hardware and software described. Since variance cannot be precluded entirely, we cannot guarantee full consistency. However, the information in this publication is reviewed regularly and any necessary corrections are included in subsequent editions.

Table of contents

1	Introduction	11
1.1	Purpose of the Configuration Manual	11
1.2	Scope of the manual	11
1.3	Designations used.....	12
1.4	Predefined defaults	12
1.5	Supplementary documentation	13
1.6	Further documentation.....	13
1.7	New in this version	14
1.8	SIMATIC NET glossary.....	14
1.9	Security information	14
1.10	Firmware	15
1.11	Open source license conditions	15
1.12	Marken	15
2	Description	17
2.1	Product characteristics	17
2.2	System functions hardware equipment	18
2.3	Configuration limits	22
2.4	Requirements for installation and operation	26
2.5	Configuration License PLUG.....	26
3	Security recommendations	29
3.1	Security recommendations.....	29
3.2	Available services.....	32
4	Assignment of an IP address	35
4.1	Structure of an IP address.....	35
4.2	Initial assignment of an IP address	36
4.3	Address assignment with DHCP	37
5	Technical basics	39
5.1	PROFINET.....	39
5.2	EtherNet/IP	39
5.3	Redundancy mechanism	40
5.3.1	Spanning Tree.....	40
5.3.1.1	RSTP, MSTP, CIST	41

5.3.2	RSTP+	42
5.3.2.1	Properties and functions of RSTP+	42
5.3.2.2	Topology for RSTP+	43
5.3.2.3	Configuring RSTP+	46
5.3.2.4	Configuring Spanning Tree for RSTP+	47
5.3.2.5	Enable RSTP+	49
5.3.2.6	Configuring Ring Redundancy for RSTP+	50
5.3.2.7	Plug cables	50
5.3.3	HRP	51
5.3.4	MRP	52
5.3.4.1	MRP - Media Redundancy Protocol	52
5.3.4.2	Configuration in WBM	54
5.3.4.3	Configuration in STEP 7	54
5.3.5	MRP Interconnection	61
5.3.5.1	Topology and how it works	61
5.3.5.2	Devices for MRP Interconnection	62
5.3.5.3	Configuring an MRP Interconnection connection	64
5.3.5.4	Connecting the devices and basic configuration	65
5.3.5.5	Configuration of ring redundancy	66
5.3.5.6	Configuration of MRP Interconnection	68
5.3.6	Standby	73
5.4	VLAN	75
5.4.1	Basics	75
5.4.2	VLAN tagging	76
5.4.3	Private VLAN	77
5.4.4	VLAN tunnel	79
5.5	Mirroring	81
5.6	SNMP	82
5.7	Quality of Service	84
5.8	NAT/NAPT	84
6	Configuring with Web Based Management	87
6.1	Web Based Management	87
6.2	Login	88
6.3	The "Information" menu	92
6.3.1	Start page	92
6.3.2	Versions	98
6.3.3	I&M	99
6.3.4	ARP table	101
6.3.5	Log Table	101
6.3.6	Faults	103
6.3.7	Redundancy	104
6.3.7.1	Spanning Tree	104
6.3.7.2	VRRP Statistics	108
6.3.7.3	VRRPv3 Statistics	110
6.3.7.4	Ring Redundancy	111
6.3.7.5	Standby	113
6.3.7.6	MRP Interconnection	115
6.3.8	Ethernet Statistics	117

6.3.8.1	Interface Statistics.....	117
6.3.8.2	Packet Size.....	118
6.3.8.3	Packet Type.....	119
6.3.8.4	Packet Error	120
6.3.8.5	History.....	122
6.3.9	Unicast	123
6.3.10	Multicast	124
6.3.10.1	Multicast	124
6.3.10.2	IGMP Groups.....	126
6.3.11	LLDP	127
6.3.12	Fiber Monitoring Protocol.....	128
6.3.13	IPv4 Routing	129
6.3.13.1	Routing Table.....	129
6.3.13.2	OSPFv2 Interfaces	130
6.3.13.3	OSPFv2 Neighbors	132
6.3.13.4	OSPFv2 Virtual Neighbors	133
6.3.13.5	OSPFv2 LSDB	135
6.3.13.6	RIPv2 Statistics	136
6.3.13.7	NAT Translations	137
6.3.13.8	PIM interfaces.....	138
6.3.13.9	PIM Neighbors	139
6.3.13.10	PIM Routes.....	140
6.3.13.11	PIM RPs.....	141
6.3.13.12	PIM BSRs.....	142
6.3.13.13	MSDP Cache	143
6.3.14	DHCP Server	144
6.3.15	Diagnostics.....	145
6.3.16	SNMP	147
6.3.17	Security	147
6.3.17.1	Overview	147
6.3.17.2	Supported Function Rights	150
6.3.17.3	Roles	151
6.3.17.4	Groups	151
6.3.17.5	802.1X Port Status	152
6.3.17.6	MAC Authentication Address Table	154
6.3.18	System time.....	155
6.4	The "System" menu	156
6.4.1	Configuration.....	156
6.4.2	General	161
6.4.2.1	Device	161
6.4.2.2	Coordinates	162
6.4.3	Agent IP.....	163
6.4.4	DNS.....	163
6.4.4.1	DNS-Client.....	163
6.4.4.2	DNS domain	165
6.4.5	Restart.....	167
6.4.6	Load & Save	170
6.4.6.1	HTTP	173
6.4.6.2	TFTP	177
6.4.6.3	SFTP	181
6.4.6.4	Passwords.....	186
6.4.7	Events	188

6.4.7.1	Configuration.....	188
6.4.7.2	Severity Filters	192
6.4.8	SMTP Client	193
6.4.8.1	General	193
6.4.8.2	Recipient	195
6.4.9	DHCPv4	197
6.4.9.1	DHCP Client	197
6.4.9.2	DHCP Client Options	200
6.4.9.3	DHCP Server	201
6.4.9.4	Port-IP Address Mapping	205
6.4.9.5	Port Range.....	206
6.4.9.6	DHCP Options	207
6.4.9.7	Relay Agent Information	210
6.4.9.8	Static Leases	211
6.4.9.9	Host Options.....	213
6.4.9.10	DHCP snooping	214
6.4.10	SNMP	216
6.4.10.1	General	216
6.4.10.2	SNMPv3 Users.....	219
6.4.10.3	SNMPv3 User to Group mapping	221
6.4.10.4	SNMPv3 Access.....	222
6.4.10.5	SNMPv3 Views.....	224
6.4.10.6	Notifications	226
6.4.11	System Time	228
6.4.11.1	Manual Setting	228
6.4.11.2	DST Overview	230
6.4.11.3	DST Configuration.....	232
6.4.11.4	SNTP Client.....	235
6.4.11.5	NTP Client.....	238
6.4.11.6	SIMATIC Time Client.....	242
6.4.11.7	PTP Client	243
6.4.11.8	NTP Server.....	245
6.4.12	Automatic logout.....	246
6.4.13	Configuration of the SELECT/SET button	247
6.4.14	Syslog Client.....	248
6.4.15	Ports.....	250
6.4.15.1	Overview	250
6.4.15.2	Configuration.....	254
6.4.16	Fault Monitoring	259
6.4.16.1	Power Supply.....	259
6.4.16.2	Link Change.....	260
6.4.16.3	Redundancy.....	263
6.4.17	Diagnostics.....	263
6.4.18	PROFINET.....	265
6.4.19	EtherNet/IP	266
6.4.19.1	EtherNet/IP	266
6.4.19.2	DLR Status	268
6.4.20	PLUG	269
6.4.20.1	Configuration.....	269
6.4.21	Ping.....	273
6.4.22	DCP Discovery.....	274
6.4.23	Port Diagnostics.....	276

6.4.23.1	Cable Tester	276
6.4.23.2	SFP Diagnostics.....	277
6.4.24	Configuration Backup.....	279
6.5	The "Layer 2" menu	281
6.5.1	Configuration.....	281
6.5.2	QoS (Quality of Service)	285
6.5.2.1	CoS queue mapping.....	285
6.5.2.2	DSCP Mapping	287
6.5.2.3	QoS Trust.....	289
6.5.3	Rate Control.....	291
6.5.4	VLAN.....	293
6.5.4.1	General	293
6.5.4.2	Port Assignment	296
6.5.4.3	GVRP	298
6.5.4.4	Port Based VLAN	300
6.5.5	Private VLAN.....	302
6.5.5.1	General	302
6.5.5.2	IP Interface Mapping.....	304
6.5.6	Provider Bridge	306
6.5.6.1	Tunnel ports	306
6.5.7	Mirroring	308
6.5.7.1	General	308
6.5.7.2	Targets	311
6.5.7.3	Port	312
6.5.7.4	VLAN.....	313
6.5.7.5	MAC Flow	314
6.5.7.6	IP Flow	315
6.5.8	Dynamic MAC Aging	317
6.5.9	Ring Redundancy	318
6.5.9.1	Ring.....	318
6.5.9.2	Standby	322
6.5.9.3	MRP Interconnection.....	325
6.5.10	Spanning tree	328
6.5.10.1	General	328
6.5.10.2	CIST General	330
6.5.10.3	CIST Port.....	332
6.5.10.4	MST General	337
6.5.10.5	MST Port.....	338
6.5.10.6	Enhanced Passive Listening Compatibility.....	340
6.5.11	Loop Detection	342
6.5.12	Link aggregation	345
6.5.12.1	General	345
6.5.12.2	LACP timeout.....	349
6.5.13	DCP Forwarding	350
6.5.14	LLDP	352
6.5.15	Fiber Monitoring Protocol.....	353
6.5.16	Unicast	355
6.5.16.1	Filtering.....	355
6.5.16.2	Locked Ports	357
6.5.16.3	Learning	359
6.5.16.4	Blocking	360
6.5.17	Multicast	362

6.5.17.1	Groups	362
6.5.17.2	IGMP	364
6.5.17.3	GMRP	367
6.5.17.4	Blocking	369
6.5.18	Broadcast.....	371
6.5.19	PTP	372
6.5.19.1	General	372
6.5.19.2	TC General.....	373
6.5.19.3	TC port	374
6.5.20	RMON.....	376
6.5.20.1	Statistics	376
6.5.20.2	History.....	377
6.6	The "Layer 3" menu	380
6.6.1	Layer 3 Configuration	380
6.6.1.1	General	380
6.6.1.2	ICMP.....	382
6.6.2	Subnets	382
6.6.2.1	Overview	382
6.6.2.2	Configuration.....	386
6.6.3	NAT	388
6.6.3.1	NAT	388
6.6.3.2	Static	390
6.6.3.3	Pool.....	392
6.6.3.4	NAPT	393
6.6.4	Static Routes.....	395
6.6.5	Route Maps.....	396
6.6.5.1	General	396
6.6.5.2	Interface & Value Match	398
6.6.5.3	Filtering the source	400
6.6.5.4	Destination Match	401
6.6.5.5	Next Hop Match	402
6.6.5.6	Set.....	402
6.6.6	DHCP Relay Agent	403
6.6.6.1	General	403
6.6.6.2	Option.....	405
6.6.7	VRRP	408
6.6.7.1	Router	408
6.6.7.2	Configuration.....	410
6.6.7.3	Addresses Overview	413
6.6.7.4	Address Configuration	413
6.6.7.5	Interface Tracking	414
6.6.7.6	Address Tracking	416
6.6.8	VRRPv3	417
6.6.8.1	Router	417
6.6.8.2	Configuration.....	420
6.6.8.3	Addresses Overview	422
6.6.8.4	Address Configuration	423
6.6.8.5	Interface Tracking	424
6.6.8.6	Address Tracking	425
6.6.9	OSPFv2.....	427
6.6.9.1	Configuration.....	427
6.6.9.2	Redistribution	429

6.6.9.3	Summary Address	432
6.6.9.4	Areas	433
6.6.9.5	Area Range	435
6.6.9.6	Interfaces	436
6.6.9.7	Interface Authentication	439
6.6.9.8	Virtual Links.....	440
6.6.9.9	Virtual Link Authentication.....	443
6.6.10	RIPv2	444
6.6.10.1	Configuration.....	444
6.6.10.2	Interfaces	446
6.6.11	IGMP	447
6.6.11.1	IGMP	447
6.6.11.2	Static Groups	450
6.6.11.3	Multicast Sources.....	451
6.6.12	PIM.....	452
6.6.12.1	PIM.....	452
6.6.12.2	Interface.....	453
6.6.12.3	RP Static	454
6.6.12.4	RP Candidate	455
6.6.13	MSDP.....	457
6.6.13.1	MSDP.....	457
6.6.13.2	Peer.....	458
6.7	The "Security" menu.....	460
6.7.1	User management	460
6.7.2	Users	463
6.7.2.1	Local Users	463
6.7.2.2	Roles	466
6.7.2.3	Groups	468
6.7.3	Passwords.....	470
6.7.3.1	Passwords.....	470
6.7.3.2	Options	472
6.7.4	AAA.....	473
6.7.4.1	General	473
6.7.4.2	RADIUS Client	474
6.7.4.3	802.1X Authenticator	478
6.7.5	MAC ACL.....	484
6.7.5.1	Rules Configuration.....	484
6.7.5.2	Ingress Rules.....	487
6.7.5.3	Egress Rules.....	489
6.7.6	IP ACL	490
6.7.6.1	Rules Configuration.....	490
6.7.6.2	Protocol Configuration	492
6.7.6.3	Ingress Rules.....	494
6.7.6.4	Egress Rules.....	496
6.7.7	Management ACL	498
6.7.8	Brute Force Prevention	501
7	Troubleshooting/FAQ	505
7.1	Downloading new firmware using TFTP without WBM and CLI.....	505
7.2	Message: SINEMA configuration not yet accepted	506
7.3	Exchange of configuration data with STEP 7 Basic/Professional using a file.....	506

A	Appendix A "Syslog messages"	509
	Index	525

Introduction

1.1 Purpose of the Configuration Manual

This Configuration Manual is intended to provide you with the information you require to install, commission and operate IE switches. It is aimed primarily at planning, commissioning and maintenance personnel and at security officers. It provides you with the information you require to configure the IE switches.

The operating instructions of the device describe how you install and connect up the device correctly.

1.2 Scope of the manual

This Configuration Manual covers the following products:

- Devices with layer 2 functions:
 - SCALANCE XC-300
 - SCALANCE XR-300
- Devices with layer 3 functions:
 - SCALANCE XC-400
 - SCALANCE XR-500

Below, the products are also called IE switch, device or network component.

There are two variants of some devices with different article numbers. The two variants differ only in their factory settings. All other properties are identical.

This Configuration Manual applies to the following software versions:

- SCALANCE XC-300 firmware as of version 1.1
- SCALANCE XR-300 firmware as of version 1.1
- SCALANCE XC-400 firmware as of version 1.1
- SCALANCE XR-500 firmware as of version 1.1

1.3 Designations used

Classification	Description	Terms used
Type of the switch	This manual covers the configuration of functions of two switch types: <ul style="list-style-type: none"> Layer 2 devices have switching functions Layer 3 devices have routing functions in addition 	Layer 2 devices: <ul style="list-style-type: none"> SCALANCE XC-300 SCALANCE XR-300 Layer 3 devices: <ul style="list-style-type: none"> SCALANCE XC-400 SCALANCE XR-500
Product group	If information applies to all devices and variants of a product group, the product group is named.	e.g. SCALANCE XC-300
Device	If information relates to a specific device, the device name is used.	e.g. SCALANCE XC332

1.4 Predefined defaults

Industrial Ethernet profile

- Ring Redundancy: Off
- Ring Redundancy Mode: Off
- Spanning Tree Protocol (MSTP): On
- Passive Listening: Off
- VLAN Awareness: On
- PROFINET Device Diagnostics: On
- IGMP Snooping: Off
- IGMP Querier: Off
- IPv4 Address conflict detection defense method: Never give up
- EtherNet/IP Device Diagnostics: Off
- QoS Trust Mode: Trust CoS-DSCP
- Security By Default:
 - HTTP: Off
 - Telnet: Off
 - SNMP v1/v2c: Read-only
 - DCP: Setup mode
 - DHCP Opt. 66/67: Setup mode

1.5 Supplementary documentation

Documentation on the Internet

You can find the current version of the document on the Internet:

- SCALANCE Layer 2 switches:
under (<https://support.industry.siemens.com/cs/de/en/ps/15273/man>)
- SCALANCE Layer 3 switches:
under (<https://support.industry.siemens.com/cs/us/en/ps/15312/man>)

Enter the name or article number of the product in the search filter.

Orientation in the documentation

Apart from the configuration manual you are currently reading, the products also have the following documentation:

- Configuration manual "SCALANCE XC-300/XR-300/XC-400/XR-500 Command Line Interface (CLI)"
This document contains the CLI commands that are supported by the IE switches.
- Operating instructions
These documents contain information on installing, connecting up and approvals for the products.
 - SCALANCE XC-300 (<https://support.industry.siemens.com/cs/de/en/ps/29061/man>)
 - SCALANCE XR-300 (<https://support.industry.siemens.com/cs/us/en/ps/15298/man>)
 - SCALANCE XC-400 (<https://support.industry.siemens.com/cs/ww/en/ps/29621/man>)
 - SCALANCE XR-500 (<https://support.industry.siemens.com/cs/de/de/ps/15317/man>)

1.6 Further documentation

In the system manuals "Industrial Ethernet / PROFINET Industrial Ethernet" and "Industrial Ethernet / PROFINET passive network components", you will find information on other SIMATIC NET products that you can operate along with the devices of this product line in an Industrial Ethernet network.

There, you will find among other things optical performance data of the communications partner that you require for the installation.

You will find the system manuals here:

- On the Internet pages of Siemens Industry Online Support under the following entry IDs:
 - 27069465 (<https://support.industry.siemens.com/cs/de/en/view/27069465>)
Industrial Ethernet / PROFINET Industrial Ethernet System Manual
 - 84922825 (<https://support.industry.siemens.com/cs/de/en/view/84922825>)
Industrial Ethernet / PROFINET - Passive network components System Manual

1.7 New in this version

Layer 3 routing functionalities and IPv4 routing protocols are released with V1.1. The functions are only available on the layer 3 devices. The following routing protocols are supported:

- VRRP (Page 408) / VRRPv3 (Page 417)
- OSPFv2 (Page 427)
- RIPv2 (Page 444)
- IGMP (Page 447)
- PIM (Page 452)
- MSDP (Page 457)

The following WBM pages will be extended to include new system functions or parameters:

- Information > Diagnostics: Temperature table (Page 145)
- System > Load&Save: Updating firmware to an older version (Page 170).
A downgrade from V1.1 to V1.0 is only possible with SCALANCE XC-300/XR-300 because only these devices have been approved for V1.0.
- System > DHCP snooping (Page 214)
- System > Diagnostics (Page 263)
- Layer 2 > Mirroring > Destinations: ERTM Remote IP address (Encapsulated Remote Traffic Mirroring) (Page 311)
- Layer 2 > Link Aggregation > General: Frame Distribution - Destination&Source Port IP MAC (Page 345)

1.8 SIMATIC NET glossary

The SIMATIC NET glossary describes terms that may be used in this document.

You will find the SIMATIC NET glossary in the Siemens Industry Online Support at the following address:

50305045 (<https://support.industry.siemens.com/cs/ww/en/view/50305045>)

1.9 Security information

Siemens provides products and solutions with industrial security functions that support the secure operation of plants, systems, machines and networks.

In order to protect plants, systems, machines and networks against cyber threats, it is necessary to implement – and continuously maintain – a holistic, state-of-the-art industrial security concept. Siemens' products and solutions constitute one element of such a concept.

Customers are responsible for preventing unauthorized access to their plants, systems, machines and networks. Such systems, machines and components should only be connected to an enterprise network or the internet if and to the extent such a connection is necessary and only when appropriate security measures (e.g. firewalls and/or network segmentation) are in place.

For additional information on industrial security measures that may be implemented, please visit

<https://www.siemens.com/industrialsecurity> (<https://www.siemens.com/industrialsecurity>).

Siemens' products and solutions undergo continuous development to make them more secure. Siemens strongly recommends that product updates are applied as soon as they are available and that the latest product versions are used. Use of product versions that are no longer supported, and failure to apply the latest updates may increase customer's exposure to cyber threats.

To stay informed about product updates, subscribe to the Siemens Industrial Security RSS Feed under

<https://www.siemens.com/cert> (<https://www.siemens.com/cert>).

1.10 Firmware

Note on firmware/software support

Check regularly for new firmware/software versions or security updates and apply them. After the release of a new version, previous versions are no longer supported and are not maintained.

Firmware

The firmware is signed and encrypted. This ensures that only firmware created by Siemens can be downloaded to the device.

The firmware is available on the Internet pages of the Siemens Industry Online Support: (<https://support.industry.siemens.com/cs/de/en/ps/15273/dl>)

1.11 Open source license conditions

Note

Open source software

Read the license conditions for open source software carefully before using the product.

The license terms and copyright information can be downloaded from the WBM as a zip file.

- WBM: System > Load & Save > HTTP / TFTP / SFTP > LicenseCondition

1.12 Marken

The following and possibly other names not identified by the registered trademark sign ® are registered trademarks of Siemens AG:

SCALANCE, SINEC, OLM

Description

2.1 Product characteristics

The IE switches have the following properties:

- The Ethernet interfaces support the following modes:
 - 10 Mbps and 100 Mbps both in full and half duplex
 - 1000 Mbps and 10 Gbps full duplex
 - Autonegotiation
 - Autocrossing
 - Autopolarity
- EtherNet/IP
EtherNet/IP (Ethernet/Industrial Protocol) is an open industry standard for industrial real-time Ethernet based on TCP/IP and UDP/IP.
- PROFINET
PROFINET (Process Field Network) is an open industry standard for industrial real-time Ethernet based on TCP/IP and IT standards. Via PROFINET distributed IO devices can be connected to a controller.
- Redundancy method Spanning Tree Protocol.
The redundancy mechanism Spanning Tree defines several connection paths between nodes in a network, only one of which is ever active. This suppresses loops and optimizes the paths.
- Virtual networks (VLAN)
To structure Industrial Ethernet networks with a fast growing number of nodes, a physical network can be divided into several virtual subnets.
- Load limitation when using multicast and broadcast protocols, for example video transmission
By learning the multicast sources and destinations (IGMP snooping, IGMP querier), IE switches can filter multicast data traffic and so reduce the load in the network. Multicast and broadcast data traffic can be limited.
- Time-of-day synchronization
Diagnostics messages such as log table entries, e-mails are given a time stamp. The local time is uniform throughout the network thanks to synchronization with a SICLOCK time transmitter or SNTP/NTP server and therefore makes the identification of diagnostics messages of several devices easier. In addition, time synchronization via the precision time protocol (PTP, IEEE 1588) is supported.
- Quality of Service for classification of the network traffic is according to CoS (Class of Service - IEEE 802.11Q) and DSCP (Differentiated Services Code Point - RFC 2474)
- Port mirroring
Mirroring allows the data traffic of a port to be mirrored at another port (monitor port). The data traffic can then be analyzed at this monitor port without any effects on the data traffic.

2.2 System functions hardware equipment

- Network access protection complying with the standard IEEE 802.1X
Ports can be configured for end devices that support authentication according to IEEE 802.1X. The authentication is made via a RADIUS server that must be reachable over the network.
- Log table
The log table logs events that occur during operation. The user can specify which events cause an entry in the table.
- Link aggregation (IEEE 802.1AX) for bundling ports
- H-Sync support
For additional information, see section "Ring (Page 318)"
- S2 devices (PROFINET configuration with simple system redundancy)
S2 devices can establish two connections to the automation system, one application relationship (AR) each to the two IO controllers. When a communication connection is interrupted, all data and diagnostics functions remain available via the second connection. For information on which IE switches can be used as S2 device, refer to the section "System functions and hardware equipment".
You only configure S2 devices via STEP 7 Basic or Professional.
For additional information, see also: PROFINET in SIMATIC PCS 7 (<https://support.industry.siemens.com/cs/ww/en/view/72887082>)
- CiR/H-CiR support (configuration in run)
Configuration in Run (CiR) is a function for making system and configuration changes during operation. This function is available to a different extent for both standard automation systems and H-systems (H-CiR).
For information on which IE switches support CiR, refer to the section "System functions and hardware equipment".
You only configure CiR via STEP 7 Basic or Professional.
For additional information, see also: PROFINET in SIMATIC PCS 7 (<https://support.industry.siemens.com/cs/ww/en/view/72887082>)

2.2 System functions hardware equipment

Availability of the system functions

The following table shows the availability of the system functions on the IE switches. Note that all functions are described in this configuration manual and in the online help. Depending on your IE switch, some functions are not available.

We reserve the right to make technical changes.

Menu item in the WBM	System functions	SCALANCE XC-300/XR-300	SCALANCE XC-400/XR-500
Information	ARP table	✓	✓
	Log table	✓	✓
	Redundancy	✓	✓
	Ethernet statistics	✓	✓
	Unicast MAC table	✓	✓
	Multicast MAC table	✓	✓
	LLDP neighbors	✓	✓
	FMP diagnostics	✓	✓
	IPv4 routing	✓	✓
	DHCP Server	✓	✓
	Diagnostics (Temperature)	✓	✓
	SNMPv3 Groups	✓	✓
	Security	✓	✓
	System Time	✓	✓
System	DNS client	✓	✓
	SMTP client	✓	✓
	DHCP client	✓	✓
	DHCP server	✓	✓
	SNMP	✓	✓
	Manual time setting	✓	✓
	DST	✓	✓
	SNTP Client	✓	✓
	NTP Client	✓	✓
	NTP server	✓	✓
	PTP Client	✓	✓
	SIMATIC Time Client	✓	✓
	Auto logout	✓	✓
	Syslog client	✓	✓
	Fault monitoring	✓	✓
	PROFINET	✓	✓
	EtherNet/IP	✓	✓
	Cable tester	✓	✓
SFP diagnostics	✓	✓	

Description

2.2 System functions hardware equipment

Menu item in the WBM	System functions	SCALANCE XC-300/XR-300	SCALANCE XC-400/XR-500
Layer 2	Sending priorities	✓	✓
	CoS map	✓	✓
	DSCP mapping	✓	✓
	QoS prioritization	✓	✓
	CoS port reassignment	✓	✓
	Load control	✓	✓
	GVRP	✓	✓
	Port-based VLAN	✓	✓
	Private VLAN	✓	✓
	Provider bridge	✓	✓
	Switch-Port VLAN Trunk	✓	✓
	Port-based mirroring	✓	✓
	VLAN-based mirroring	✓	✓
	MAC ACL-based mirroring	✓	✓
	IP ACL-based mirroring	✓	✓
	Dynamic MAC aging	✓	✓
	Ring redundancy	✓	✓
	H-Sync support	✓	✓
	S2 devices	✓	✓
	CiR/H-CiR support	✓	✓
	Ring with RSTP	✓	✓
	Standby (HRP)	✓	✓
	Observer (HRP)	✓	✓
	MRP multiple rings	✓	✓
	MRP Interconnection	✓	✓
	Spanning Tree	✓	✓
	RSTP	✓	✓
	RSTP+	✓	✓
	MSTP	✓	✓
	Enhanced Passive Listening Compatibility	✓	✓
	Loop detection	✓	✓
	Link Aggregation / LACP	✓	✓
	DCP forwarding	✓	✓
	LLDP	✓	✓
	Fiber monitoring	✓	✓
	Unicast filter	✓	✓
Locked ports	✓	✓	
Unicast learning	✓	✓	
Unicast blocking	✓	✓	
Multicast groups	✓	✓	
IGMP	✓	✓	

Menu item in the WBM	System functions	SCALANCE XC-300/XR-300	SCALANCE XC-400/XR-500
	GMRP	✓	✓
	Multicast blocking	✓	✓
	Broadcast blocking	✓	✓
	PTP	✓	✓
	RMON	✓	✓
	RMON history	✓	✓
Layer 3	DHCP relay agent	✓	✓
	NAT/NAPT	✓	✓
	Static routes	-	✓
	ICMP	-	✓
	Route maps	-	✓
	VRRP / VRRPv3	-	✓
	OSPFv2	-	✓
	RIPv2	-	✓
	IGMP	-	✓
	PIM	-	✓
	MSDP	-	✓
Security	Users	✓	✓
	Passwords	✓	✓
	RADIUS authentication	✓	✓
	MAC authentication	✓	✓
	Guest VLAN	✓	✓
	802.1X reauthentication	✓	✓
	Management ACL	✓	✓
	MAC ACL	✓	✓
	IP ACL	✓	✓
	Brute Force Prevention	✓	✓

Availability of hardware

The following table shows the hardware of the IE switches.

We reserve the right to make technical changes.

	SCALANCE XC-300/XR-300/XC-400/XR-500
CPU support	✓
SELECT/SET button	✓
Signaling contact	✓
Serial USB console interface	✓
Display modes	✓
Pluggable transceiver slots	✓

2.3 Configuration limits

Configuration limits of the device

The following table lists the configuration limits for Web Based Management and the Command Line Interface of the device.

Depending on your IE switch, some functions are not available.

Menu item in the WBM	Configurable function	Maximum number	
		SCALANCE XC-300/XR-300	SCALANCE XC-400/XR-500
System	Maximum frame size (ingress)	9194	9194
	Syslog server	3	3
	E-mail server	3	3
	DHCP pools	24	24
	IPv4 addresses managed by the DHCP server (dynamic + static)	576	576
	DHCP static assignments per DHCP pool	24	24
	SNMPv1 trap recipient	10	10
	SNMPv3 Users	48	48
	SNMPv3 Groups	41	41
	SNMPv3 Views (incl. 2 default views)	46	46
	Sntp server	2	2
	NTP server	4	4
	Agent/TIA interfaces ¹⁾	1	1
	Devices displayed via DCP Discovery	100	100
	Maximum storage space for configuration backups	150 kBytes	150 kBytes

Menu item in the WBM	Configurable function	Maximum number	
		SCALANCE XC-300/XR-300	SCALANCE XC-400/XR-500
Layer 2	QoS priority queues	8	8
	Virtual LANs (port-based, including VLAN 1)	257	257
	Private VLAN	32	32
	Primary PVLANS	32	32
	Secondary isolated PVLANS	32	32
	Secondary community PVLANS	256	256
	Mirroring sessions (port-based)	5	5
	Mirroring sessions (VLAN)	4	4
	Mirroring sessions (MAC ACL)	4	4
	Mirroring sessions (IP ACL)	4	4
	ERTM mirroring sessions	5	5
	VLANs whose data traffic can be mirrored to a monitor port	255	255
	RSPAN sessions	5	5
	Standby ports	1	1
	MRP rings	4	4
	Configured MRP Interconnection connections	64	64
	Enabled MRP Interconnection connections	2	2
	Maximum number of devices with enabled MRP Interconnection in a ring	10	10
	Multiple Spanning Tree instances	64	64
	Link aggregations or EtherChannels	8	8
	Ports in a link aggregation	8	8
	Static unicast addresses	256	256
	Static multicast addresses without activated GMRP	512	512
Static multicast addresses with activated GMRP	50	50	
Addresses learned using IGMP snooping	512	512	

Description

2.3 Configuration limits

Menu item in the WBM	Configurable function	Maximum number	
		SCALANCE XC-300/XR-300	SCALANCE XC-400/XR-500
Layer 3	VLAN IP interfaces	127	127
	DHCP Relay shared Agent interfaces	24	127
	DHCP Relay Agent server	4	4
	NAT interfaces	1	5
	Dynamic NAT configurations (pools)	100	100
	Static NAT configurations	100	100
	Entries in the hardware routing table	-	4096
	Static routes	-	100
	Possible routes to the same destination	-	16
	VRRP router interfaces (only VLAN interfaces)	-	52
	OSPF areas per device	-	5
	OSPFv2 area range entries per OSPF area (intra-area summary)	-	3
	OSPFv3 area range entries per OSPF area (intra-area summary)	-	10
	OSPF interfaces	-	40
	OSPF interfaces per OSPF area	-	8
	OSPF virtual links (within an autonomous system)	-	8
	OSPFv3 neighbors	-	300
	OSPFv3 neighbors per interface	-	8
	OSPFv3 routes	-	1500
	OSPFv2 interfaces authentication keys	-	200 (40 interfaces each with 5 keys)
	OSPFv2 virtual links authentication keys	-	40 (8 virtual links each with 5 keys)
PIM multicast routes per device (sparse mode) ²⁾	-	1000	
PIM components	-	1	
Rendezvous points	-	3	
Candidates for rendezvous points	-	3	
Static rendezvous points	-	3	

Menu item in the WBM	Configurable function	Maximum number	
		SCALANCE XC-300/XR-300	SCALANCE XC-400/XR-500
Security	Users	30 (incl. the "admin" user preset in the factory)	30 (incl. the "admin" user preset in the factory)
	Roles	29	29
	Groups	32	32
	IP addresses of RADIUS servers	6	6
	Simultaneous MAC authentications (authenticated and blocked) per device ³⁾	2000	2000
	Simultaneous MAC authentications (authenticated and blocked) per port (configurable) ³⁾	200	200
	Simultaneous MAC authentications of static MAC addresses per port in "Sticky" MAC authentication mode	5	5
	Management ACL rules (access rules for management)	100	10
	MAC ACL rules	128	128
	Maximum number of configured MAC ACL rules that can be assigned to a port:		
	• Incoming frames (ingress rules) per port	128	128
	• Outgoing frames (egress rules) for all ports	50	50
	IP ACL rules	128	128
	Maximum number of configured IP ACL rules that can be assigned to a port or IP interface:		
• Incoming packets (ingress rules) per port or IP interface	128	128	
• Outgoing packets (egress rules) for all ports or IP interfaces	50	50	
End devices in the Guest VLAN per port	100	100	

¹⁾ This is an IP interface.

²⁾ The maximum number of PIM multicast routes per device is made up as follows:

SSM streams + SM streams + bidirectional streams (from IGMP joins)

Depending on the structure of the PIM network (hierarchical structure), a larger number of streams can be supported with bidirectional multicast.

³⁾ The maximum number of statically configurable MAC unicast entries is not dependent on the number of MAC authentications. If the maximum number of MAC authentications per device is exceeded, all MAC authentications of the port at which the value was exceeded are reset.

If the maximum number of MAC authentications per port is exceeded, all the MAC authentications of the port are reset.

2.4 Requirements for installation and operation

Requirements for installation and operation of the IE switches

A PG/PC with a network connection must be available in order to configure the IE switches. If no DHCP server is available, a PG/PC on which SINEC PNI is installed is necessary for the initial assignment of an IP address to the IE switches. The other configuration settings require a client PC with a Web browser (HTTPS) or a terminal software (SSH client).

2.5 Configuration License PLUG

The Configuration and License PLUG (CLP) is a USB storage medium for backing up and exchanging data and licenses.

The CLP has a USB type C interface and can be used with the following devices that have a corresponding interface:

- Siemens products
- Personal computers (PCs), such as desktop PCs, tablet PCs, laptops, or smartphones

Devices with a CLP slot support the following operating modes:

- **Without CLP**
The device saves the configuration data in the internal memory. This mode is active when no CLP is inserted.
- **With CLP**
In the startup phase:
 - When an CLP **with no data** (default setting) is plugged into a device, the device automatically saves its configuration data on the CLP during the startup phase. After that, it behaves like a CLP with data.
 - If a CLP **with data** is plugged into a device, the device automatically adopts the configuration of the CLP during the startup phase.

During operation:

- During operation, changes to the configuration are saved on the CLP and in the internal memory.
- The configuration data of the device is stored in a secured memory area of the CLP. This secured memory area can only be accessed via the authentication of the Siemens device.
- The device checks whether a CLP is inserted at one second intervals. If the device detects that the CLP has been removed, it restarts automatically.

NOTICE
Operating risk - Danger of data loss
Only pull and plug the CLP when the device is de-energized.

- The device signals deviations from normal operation of the CLP (e.g. incompatible data, incorrect operation or malfunctions) via the existing diagnostics mechanisms (e.g. LEDs or user interfaces).

Description

2.5 Configuration License PLUG

Security recommendations

3.1 Security recommendations

Software (security functions)

- Keep the firmware up to date. Check regularly for security updates for the device. You can find information on this at the Industrial Security (<https://www.siemens.com/industrialsecurity>) website.
- Inform yourself regularly about security recommendations published by Siemens ProductCERT (<https://www.siemens.com/cert>).
- Only activate protocols that you require to use the device.
- Restrict access to the management of the device with rules in an access control list (ACL).
- The option of VLAN structuring provides protection against DoS attacks and unauthorized access. Check whether this is practical or useful in your environment.
- Use a central logging server to log changes and accesses. Operate your logging server within the protected network area and check the logging information regularly.

Authentication

Note

Accessibility risk - Risk of data loss

Do not lose the passwords for the device. Access to the device can only be restored by resetting the device to factory settings which completely removes all configuration data.

- Replace the default passwords for all user accounts, access modes and applications (if applicable) before you use the device.
- Define rules for the assignment of passwords.
- Use passwords with a high password strength. Avoid weak passwords, (e.g. password1, 123456789, abcdefgh) or recurring characters (e.g. abcabc).
This recommendation also applies to symmetrical passwords/keys configured on the device.
- Make sure that passwords are protected and only disclosed to authorized personnel.
- Do not use the same passwords for multiple user names and systems.
- Store the passwords in a safe location (not online) to have them available if they are lost.
- Regularly change your passwords to increase security.
- A password must be changed if it is known or suspected to be known by unauthorized persons.

3.1 Security recommendations

- When user authentication is performed via RADIUS, make sure that all communication takes place within the security environment or is protected by a secure channel.
- Watch out for link layer protocols that do not offer their own authentication between endpoints, such as ARP or IPv4. An attacker could use vulnerabilities in these protocols to attack hosts, switches and routers connected to your layer 2 network, for example, through manipulation (poisoning) of the ARP caches of systems in the subnet and subsequent interception of the data traffic. Appropriate security measures must be taken for non-secure layer 2 protocols to prevent unauthorized access to the network. Physical access to the local network can be secured or secure, higher layer protocols can be used, among other things.

Certificates and keys

- There is a preset SSL/TLS (RSA) certificate with 4096 bit key length in the device. Replace this certificate with a user-generated, high-quality certificate with key. Use a certificate signed by a reliable external or internal certification authority. You can install the certificate via the WBM ("System > Load and Save").
- Use certificates with a key length of 4096 bits.
- Use the certification authority including key revocation and management to sign the certificates.
- Make sure that user-defined private keys are protected and inaccessible to unauthorized persons.
- If there is a suspected security violation, change all certificates and keys immediately.
- Use password-protected certificates in the format "PKCS #12".
- Verify certificates based on the fingerprint on the server and client side to prevent "man in the middle" attacks. Use a second, secure transmission path for this.
- Before sending the device to Siemens for repair, replace the current certificates and keys with temporary disposable certificates and keys, which can be destroyed when the device is returned.

Secure/non-secure protocols and services

- Avoid or disable non-secure protocols and services, for example HTTP, Telnet and TFTP. For historical reasons, these protocols are available, however not intended for secure applications. Use non-secure protocols on the device with caution.
- Check whether use of the following protocols and services is necessary:
 - Non authenticated and unencrypted ports
 - HTTP
 - Telnet
 - SNMPv1/v2c
 - NTP
 - MRP, HRP, STP, RSTP and MSTP
 - IGMP snooping
 - LLDP
 - DCP
 - Syslog
 - DHCP Options 66/67
 - TFTP
 - GMRP and GVRP
- The following protocols provide secure alternatives:
 - HTTP → HTTPS
 - Telnet → SSH
 - SNMPv1/v2c → SNMPv3
Check whether use of SNMPv1/v2c. is necessary. SNMPv1/v2c is classified as non-secure. Use the option of preventing write access. The device provides you with suitable setting options.
If SNMP is enabled, change the community names. If no unrestricted access is necessary, restrict access with SNMP.
Use the authentication and encryption mechanisms of SNMPv3.
 - TFTP → SFTP
 - NTP → NTPsecure
- Use secure protocols when access to the device is not prevented by physical protection measures.
- If you require non-secure protocols and services, operate the device only within a protected network area.
- Restrict the services and protocols available to the outside to a minimum.
- If you use RADIUS for management access to the device, activate secure protocols and services.

3.2 Available services

List of available services

The following is a list of all available services and their ports through which the device can be accessed.

The table includes the following columns:

- **Service**
The services that the device supports
- **Default port status**
This is the status of the port in the delivery state (factory setting).
- **Configurable port/service**
Indicates whether the port number or the service can be configured via WBM / CLI.
- **Authentication**
Specifies whether the communication partner is authenticated.
If optional, the authentication can be configured as required.
- **Encryption**
Specifies whether the transfer is encrypted.
If optional, the encryption can be configured as required.

Service	Protocol / Port number	Default port status	Configurable		Authentication	Encryption
			Port	Service		
DHCPv4 Server	UDP/67	Closed	✓	✓	-	-
DHCPv4 Client (IPv4)	UDP/68	Open	-	✓	-	-
EtherNet/IP ²⁾	TCP/44818 UDP/2222 UDP/44818	Closed	-	✓	-	-
HTTP Server/Client ⁴⁾	TCP/80	Closed	✓	✓	✓	-
HTTPS WBM Server/Client	TCP/443	Open	✓	✓	✓	✓
NTP Client	UDP/123	Closed	✓	✓	-	-
NTP (secure)	UDP/123	Closed	✓	✓	✓	-
PROFINET	UDP/34964 UDP/49151 ... 49159 ¹⁾	Open	--	✓	-	-
RADIUS Client	UDP/1812 ⁵⁾ UDP/1813 ⁵⁾	Outbound only	✓	✓	✓	-
	UDP/3799	Open	✓	✓	✓	-
SFTP Server	UDP/22	Outbound only	✓	✓	✓	✓
SMTP Client	TCP/25	Closed	✓	✓	--	--
SMTP Client (secure)	TCP/465	Closed	✓	✓	✓	✓
SNMPv1/v2c ^{3) 4)}	UDP/161	Open	✓	✓	-	-
SNMPv3	UDP/161	Open	✓	✓	Optional	Optional
SNMP Traps	UDP/162	Outbound only	--	✓	-	-

Service	Protocol / Port number	Default port status	Configurable		Authentication	Encryption
			Port	Service		
SNTP Client	UDP/123	Closed	✓	✓	-	-
SSH CLI Server	TCP/22	Open	✓	✓	✓	✓
Syslog Client	UDP/514	Closed	✓	✓	-	-
Syslog (secure) Client	TCP/6514	Closed	✓	✓	-	✓
Telnet ⁴⁾	TCP/23	Closed	✓	✓	✓	-
TFTP Client	UDP/69	Outbound only	✓	✓	-	-

- 1) Port number can be configured via the WBM.
- 2) Service disabled by default.
- 3) Read-only access only.
- 4) Protocol according to Security by Default.
- 5) The port is closed by default and is displayed when a RADIUS server is configured.

The following is a list of all available Layer 2 services through which the device can be accessed.

The table includes the following columns:

- **Layer 2 service**
The Layer 2 services that the device supports.
- **Default status**
The default status of the service (open or closed).
- **Service configurable**
Indicates whether the service can be configured via WBM / CLI.

Layer 2 service	Default status	Service configurable
DCP	Setup mode ¹⁾	✓
LLDP	Open	✓
RSTP	Closed	✓
MSTP	Open	✓

- 1) Setting according to Security by Default.

Assignment of an IP address

4.1 Structure of an IP address

Address classes

IP address range	Max. number of networks	Max. number of hosts/ network	Class	CIDR
1.x.x.x through 126.x.x.x	126	16777214	A	/8
128.0.x.x through 191.255.x.x	16383	65534	B	/16
192.0.0.x through 223.255.255.x	2097151	254	C	/24
224.0.0.0 - 239.255.255.255	Multicast applications		D	
240.0.0.0 - 255.255.255.255	Reserved for future applications		E	

An IP address consists of 4 bytes. Each byte is represented in decimal, with a dot separating it from the previous one. This results in the following structure, where XXX stands for a number between 0 and 255:

XXX.XXX.XXX.XXX

The IP address is made up of two parts, the network ID and the host ID. This allows different subnets to be created. Depending on the bytes of the IP address used as the network ID and those used for the host ID, the IP address can be assigned to a specific address class.

Subnet mask

The bits of the host ID can be used to create subnets. The leading bits represent the address of the subnet and the remaining bits the address of the host in the subnet.

A subnet is defined by the subnet mask. The structure of the subnet mask corresponds to that of an IP address. If a "1" is used at a bit position in the subnet mask, the bit belongs to the corresponding position in the IP address of the subnet address, otherwise to the address of the computer.

Example of a class B network:

The standard subnet address for class B networks is 255.255.0.0; in other words, the last two bytes are available for defining a subnet. If 16 subnets must be defined, the third byte of the subnet address must be set to 11110000 (binary notation). In this case, this results in the subnet mask 255.255.240.0.

To find out whether two IP addresses belong to the same subnet, the two IP addresses and the subnet mask are ANDed bit by bit. If both logic operations have the same result, both IP addresses belong to the same subnet, for example, 141.120.246.210 and 141.120.252.108.

Outside the local area network, the distinction between network ID and host ID is of no significance, in this case packets are delivered based on the entire IP address.

Note

In the bit representation of the subnet mask, the "ones" must be set left-justified; in other words, there must be no "zeros" between the "ones".

4.2 Initial assignment of an IP address

Configuration options

An initial IP address for an IE switch cannot be assigned using Web Based Management (WBM) because this configuration tool can only be used if an IP address already exists.

The following options are available to assign an IP address to an unconfigured device:

- **DHCP** (factory setting)
- **SINEC PNI** (SINEC Primary Network Initialization)
This program for initial commissioning of network devices uses the DCP protocol to detect devices in a network and assign an IP address.
For more information, refer to PNI (<https://support.industry.siemens.com/cs/products?mfn=ps&pnid=26672&lc=en-US>)
- **STEP 7**
In STEP 7, you can configure the topology, the device name and the IP address. If you connect an unconfigured IE switch to the controller, the controller assigns the configured device name and the IP address to the IE switch automatically.
 - **STEP 7**
SCALANCE XC-300: As of V5.6.2 HF8 as HSP1118
SCALANCE XR-300: As of V5.6.2 HF8 as HSP1118
For further information on the assignment of the IP address using STEP 7 refer to the documentation "Configuring Hardware and Communication Connections STEP 7", in the section "Steps For Configuring a PROFINET IO System".
 - **STEP 7 Basic or Professional**
SCALANCE XC-300: as of V18 as HSP
SCALANCE XR-300: as of V18 as HSP
For further information on assigning the IP address using STEP 7, refer to the online help "Information system", section "Addressing PROFINET devices".
- **CLI** via the serial USB console interface
You can find the procedure for assigning the IP address via the serial USB console interface in the CLI of the device, section "General > Accessing the CLI Through the USB Console Interface".
- **NCM PC**
For further information on assigning the IP address using NCM PC, refer to the documentation "Commissioning PC stations - Manual and Quick Start", in the section "Creating a PROFINET IO system".

Note

When the product ships and after factory settings are restored, DHCP is enabled. If a DHCP server is available in the local area network, and this responds to the DHCP request of an IE switch, the IP address, subnet mask and gateway are assigned automatically when the device first starts up.

The following DHCP options are supported:

- DHCP option 3: Router IP
 - DHCP option 6: DNS server IP
 - DHCP option 12: Host name
 - DHCP option 43: Vendor-specific information
 - DHCP option 66: Assignment of a dynamic TFTP server name
 - DHCP option 67: Assignment of a dynamic boot file name
-

4.3 Address assignment with DHCP

Properties of DHCP

DHCP (Dynamic Host Configuration Protocol) is a method for automatic assignment of IP addresses. It has the following characteristics:

- DHCP can be used both when starting up a device and during ongoing operation.
- The assigned IP address remains valid only for a limited time known as the lease time. When half the period of validity has elapsed, the DHCP client can extend the period of the assigned IPv4 address. When the entire time has elapsed, the DHCP client needs to request a new IPv4 address.
- If the request for a new IP address is not successful after the lease time has expired, the IP configuration depends on the "Keep Alive" function. When Keep Alive is enabled, the IP address is kept in the event of a communication breakdown and not reset to 0.0.0.0. Keep Alive is disabled by default. When Keep Alive is disabled, the IP address is reset to 0.0.0.0 in the event of a communication breakdown.
- If an IP address was configured via DHCP and DHCP is disabled, the IP configuration depends on the "Keep Alive" function. When Keep Alive is disabled, the IP configuration is reset to 0.0.0.0 ("Not configured"). If Keep Alive is enabled, the IP address is kept and not reset to 0.0.0.0.
- If an IP address was configured via DHCP and the connection to the network is temporarily interrupted (status of the interface "Up", "Down" and "Up" again), the IP configuration first needs to be confirmed by the DHCP server. If confirmation is not possible, the IP configuration is reset to 0.0.0.0 ("Not configured") and a new IP configuration is requested from the DHCP server.
- If DHCP was active for a device, a new IP address first needs to be requested from the DHCP server after a restart.

4.3 Address assignment with DHCP

- There is normally no fixed address assignment; in other words, when a client requests an IP address again, it normally receives a different address from the previous address. It is possible to configure the DHCP server so that the DHCP client always receives the same fixed address in response to its request. The parameter with which the DHCP client is identified for the fixed address assignment is set on the DHCP client and server. The address can be assigned via the MAC address, the DHCP client ID, the PROFINET or the system name. You configure the parameter in "System > DHCP > DHCP Client (Page 197)".
- If a static IP address was configured and DHCP is enabled, the IP configuration depends on the "Keep Alive" function. If Keep Alive is disabled, the IP address is set to 0.0.0.0 when DHCP is switched on and a new IP address from the DHCP server is anticipated. When no address is assigned by the DHCP server, the switch can no longer be reached via IP.

Technical basics

5.1 PROFINET

PROFINET

PROFINET is an open standard (IEC 61158/61784) for industrial automation based on Industrial Ethernet. PROFINET uses existing IT standards and allows end-to-end communication from the field level to the management level as well as plant-wide engineering. PROFINET also has the following features:

- Use of TCP/IP
- Automation of applications with real-time requirements
 - Real-Time (RT) communication
 - Isochronous Real-Time (IRT) communication
- Seamless integration of fieldbus systems

You configure PROFINET in "System > PROFINET (Page 265)".

PROFINET IO

Within the framework of PROFINET, PROFINET IO is a communications concept for implementing modular, distributed applications. PROFINET IO is implemented by the PROFINET standard for programmable controllers (IEC 61158-x-10).

5.2 EtherNet/IP

EtherNet/IP

EtherNet/IP (Ethernet/Industrial Protocol) is an open industry standard for industrial real-time Ethernet based on TCP/IP and UDP/IP. With EtherNet/IP, Ethernet is expanded by the Common Industrial Protocol (CIP) at the application layer. In EtherNet/IP, the lower layers of the OSI reference model are adopted by Ethernet with the physical, network and transport functions.

You configure EtherNet/IP in "System > EtherNet/IP (Page 266)".

Common Industrial Protocol

The Common Industrial Protocol (CIP) is an application protocol for automation that supports transition of the field buses in Industrial Ethernet and in IP networks. This industry protocol is used by field buses/industrial networks such as DeviceNet, ControlNet and EtherNet/IP at the application layer as an interface between the deterministic fieldbus world and the automation application (controller, I/O, HMI, OPC, ...). The CIP is located above the transport layer and expands the pure transport services with communications services for automation engineering. These include services for cyclic, time-critical and event-controlled data traffic. CIP distinguishes between time-critical I/O messages (implicit messages) and individual query/response frames for configuration and data acquisition (explicit messages). CIP is object-oriented; all data "visible" from the outside is accessible in the form of objects. CIP has a common configuration basis: EDS (Electronic Data Sheet).

Electronic Data Sheet

Electronic Data Sheet (EDS) is an electronic datasheet for describing devices.

The EDS required for EtherNet/IP operation can be found in "System > Load&Save (Page 170)".

5.3 Redundancy mechanism

5.3.1 Spanning Tree

Avoiding loops on redundant connections

The spanning tree algorithm allows network structures to be created in which there are several connections between two IE switches / bridges. Spanning tree prevents loops being formed in the network by allowing only one path and disabling the other (redundant) ports for data traffic. If there is an interruption, the data can be sent over an alternative path. The functionality of the spanning tree algorithm is based on the exchange of configuration and topology change frames.

Definition of the network topology using the configuration frames

The devices exchange configuration frames known as BPDUs (Bridge Protocol Data Units) with each other to calculate the topology. The root bridge is selected and the network topology created using these frames. BPDUs also bring about the status change of the root ports.

The root bridge is the bridge that controls the spanning tree algorithm for all involved components.

Once the root bridge has been specified, each device sets a root port. The root port is the port with the lowest path costs to the root bridge.

Response to changes in the network topology

If nodes are added to a network or drop out of the network, this can affect the optimum path selection for data packets. To be able to respond to such changes, the root bridge sends configuration messages at regular intervals. The interval between two configuration messages can be set with the "Hello Time" parameter.

Keeping configuration information up to date

With the "Max Age" parameter, you set the maximum age of configuration information. If a bridge has information that is older than the time set in "Max Age", it discards the message and initiates recalculation of the paths.

New configuration data is not used immediately by a bridge but only after the period specified in the "Forward Delay" parameter. This ensures that operation is only started with the new topology after all the bridges have the required information.

5.3.1.1 RSTP, MSTP, CIST

Rapid Spanning Tree Protocol (RSTP)

One disadvantage of STP is that if there is a disruption or a device fails, the network needs to reconfigure itself: The devices start to negotiate new paths only when the interruption occurs. This can take up to 30 seconds. For this reason, STP was expanded to create the "Rapid Spanning Tree Protocol" (RSTP, IEEE 802.1w). This differs from STP essentially in that the devices are already collecting information about alternative routes during normal operation and do not need to gather this information after a disruption has occurred. This means that the reconfiguration time for an RSTP controlled network can be reduced to a few seconds. This is achieved by using the following functions:

- Edge ports (end node port)
Edge ports are ports connected to an end device.
A port that is defined as an edge port is activated immediately after connection establishment. If a spanning tree BPDU is received at an edge port, the port loses its role as edge port and it takes part in (R)STP again. If no further BPDU is received after a certain time has elapsed (3 x hello time), the port returns to the edge port status.
- Point-to-point (direct communication between two neighboring devices)

By directly linking the devices, a status change (reconfiguration of the ports) can be made without any delays.

- Alternate port (substitute for the root port)

A substitute for the root port is configured. If the connection to the root bridge is lost, the device can establish a connection over the alternate port without any delay due to reconfiguration.

5.3 Redundancy mechanism

- Reaction to events

Rapid spanning tree reacts to events, for example an aborted connection, without delay. There is no waiting for timers as in spanning tree.

- Counter for the maximum bridge hops
The number of bridge hops a package is allowed to make before it automatically becomes invalid.

In principle, therefore with rapid spanning tree, alternatives for many parameters are preconfigured and certain properties of the network structure taken into account to reduce the reconfiguration time.

Multiple Spanning Tree Protocol (MSTP)

The Multiple Spanning Tree Protocol (MSTP) is a further development of the Rapid Spanning Tree Protocol. Among other things, it provides the option of operating several RSTP instances within different VLANs or VLAN groups and, for example, making paths available within the individual VLANs that the single Rapid Spanning Tree Protocol would globally block.

Common and Internal Spanning Tree (CIST)

CIST identifies the internal instance used by the switch that is comparable in principle with an internal RSTP instance.

5.3.2 RSTP+

5.3.2.1 Properties and functions of RSTP+

The main application of RSTP+ is the redundant integration of MRP rings into an RSTP network. It is generally possible to manage such a network solely with RSTP. However, in a ring topology, MRP is the more efficient and faster method. The MRP ring redundancy mode is not affected by RSTP+ because both modes work independently of one another.

Another use case is the redundant linking of MRP rings. It is also possible to connect two RSTP networks over one MRP ring with RSTP+. This is not possible without RSTP+ because Spanning Tree is disabled at the ring ports.

Note

Multiring manager prevents the configuration of Spanning Tree

If more than one ring is configured on a device, neither RSTP or RSTP+ can be configured in parallel. This also applies if Spanning Tree has been disabled for the ring ports.

Compatibility of devices without RSTP+

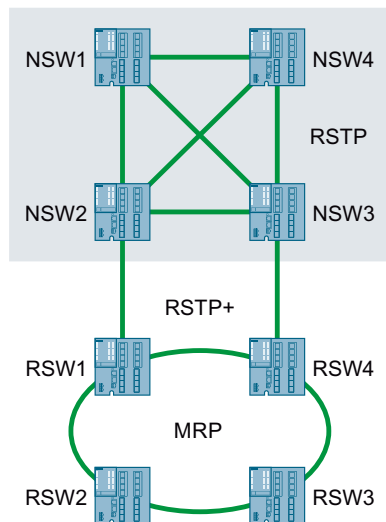
In principle, all devices at the connection points between RSTP network and MRP ring must support the RSTP+ method. All other devices in the MRP ring must forward BPDUs (Bridge Protocol Data Unit).

5.3.2.2 Topology for RSTP+

RSTP network and MRP ring

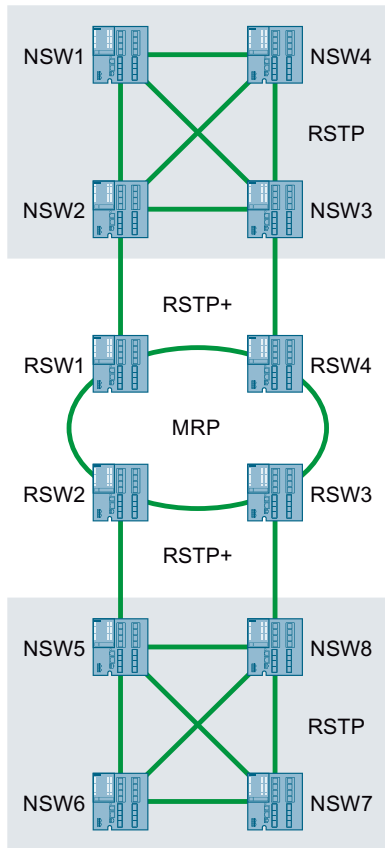
The redundant integration of MRP rings into an RSTP network is not possible without RSTP+ because parallel operation of RSTP and MRP on one port is not permitted. Only the devices of the MRP ring that are connected to the RSTP network must support RSTP+. In the example topology shown, these are the two devices RSW1 and RSW4. The other devices must forward BPDUs.

The identification of the devices in the graphics refers to the respective function of the device. "NSW" is the abbreviation for 'network switch', "RSW" is the abbreviation for 'ring switch'.



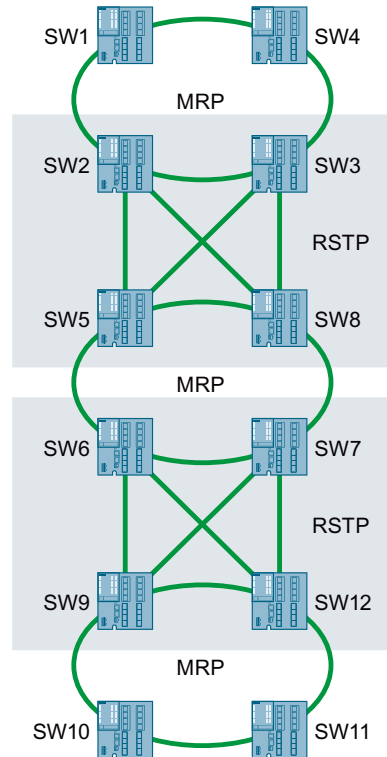
Multiple RSTP network areas and MRP ring

Another use case of RSTP+ is the connection of two or more RSTP network areas over one MRP ring. RSTP+ must be enabled for all devices in the MRP ring that are connected to one of the RSTP networks. In the example shown here, these are the devices RSW1, RSW2, RSW3 and RSW4.



Multiple MRP rings

RSTP+ can also be used to connect multiple MRP rings with each other over RSTP. RSTP+ ensures in this case that MRP still manages the ring redundancy without being affected by RSTP.

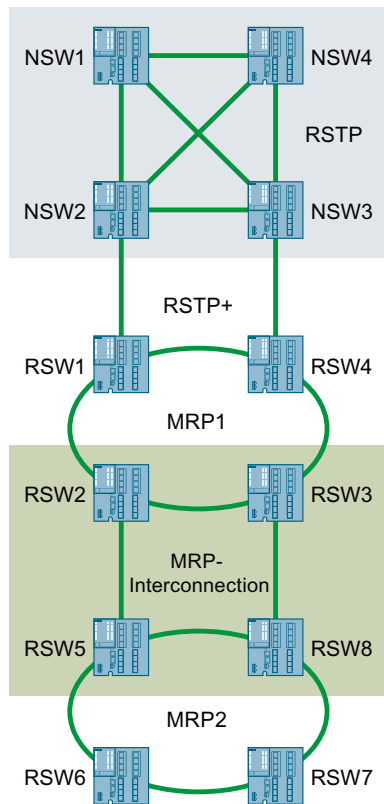


RSTP network and two MRP rings with MRP Interconnection

RSTP+ can also connect an RSTP network to two MRP rings that are linked via MRP Interconnection. In the example topology shown, the two devices RSW1 and RSW4 must support RSTP+. The devices (RSW2, RSW3, RSW5 and RSW8) involved in the connection of the two MRP rings must support MRP Interconnection. In addition, the devices RSW2 and RSW3 must forward BPDUs (Bridge Protocol Data Unit).

The following rules apply to the RSTP+ MRP Interconnection Domain ID in the example shown:

- The same RSTP+ MRP Interconnection Domain ID must be configured for the devices RSW1 and RSW4.
- The same RSTP+ MRP Interconnection Domain ID must be configured for the devices RSW2, RSW3, RSW5 and RSW8.
- The RSTP+ MRP Interconnection Domain ID of the devices RSW1 and RSW4 must differ from the RSTP+ MRP Interconnection Domain ID of the devices RSW2, RSW3, RSW5 and RSW8.



5.3.2.3 Configuring RSTP+

This section describes the procedure during configuration of RSTP+ in detail. Execute the configuration steps for all devices in which RSTP+ is to be enabled. The position numbers in the screenshots refer to the respective number of the step sequence. The description applies to devices that have not been configured yet (factory settings).

The description has three sections:

- Configure Spanning Tree: Steps 1 to 4 (Page 47)
- Enable RSTP+: Step 5 (Page 49)
- Configure ring redundancy: Steps 6 to 8 (Page 50)
- Plug cables: Step 9 (Page 50)

General configuration rules

Observe the following rules during configuration; they apply regardless of a specific network topology:

- RSTP+ can only be enabled in combination with a Spanning Tree protocol.
- RSTP+ is enabled on the switches that are at the two link points to the RSTP network in the MRP ring.
- Ring redundancy must also be configured at the two link devices. The function of the redundancy manager should not be assigned to one of the two devices of the RSTP/MRP link.

- A direct LAN connection should exist between the two ring ports of the link devices.
- For the ring nodes except for the link devices in a ring linked to an RSTP, it is advisable to enable Passive Listening at an RSTP . You enable Passive Listening on the "Layer 2 > Configuration" page.

5.3.2.4 Configuring Spanning Tree for RSTP+

In WBM, you can use the menu "Layer 2 > Spanning Tree" for the configuration of Spanning Tree.

The configuration procedure depends on the default settings of the device to be configured. For this reason, devices are divided into two groups according to their default settings:

- Group 1: Ring redundancy enabled and Spanning Tree disabled.
- Group 2: Ring redundancy disabled and Spanning Tree enabled.

For devices in the first group, you first need to disable ring redundancy and enable Spanning Tree. From step 3, configuration is the same for both groups. You can find information about predefined device settings in the section "Predefined defaults (Page 12)".

Execute steps 1 to 2 for devices with default settings in the first group or start with step 3 for devices of the second group, and continue with the configuration (steps 3 to 4) for each device for which you want to enable RSTP+.

The required port settings are made automatically during this process.

Step 1: Disable ring redundancy

Note

This step is only required for devices with default settings of Group 1.

Navigate to the menu "Layer 2 > Ring Redundancy > Ring" and clear the "Ring Redundancy" check box. Click on "Set Values".

Ring Redundancy

Ring Standby MRP Interconnection

Ring ID: 1

Ring Redundancy

Ring Redundancy Mode: -

Ring Ports: P0.1 P0.2

Domain Name: default-mrpdomain

Observer

Restart Observer

Restore Default

Ring ID	Domain Name	Ring Redundancy Mode	Ring Port 1	Ring Port 2
1	default-mrpdomain	-	P0.1	P0.2
2		-	P0.1	P0.2
3		-	P0.1	P0.2
4		-	P0.1	P0.2

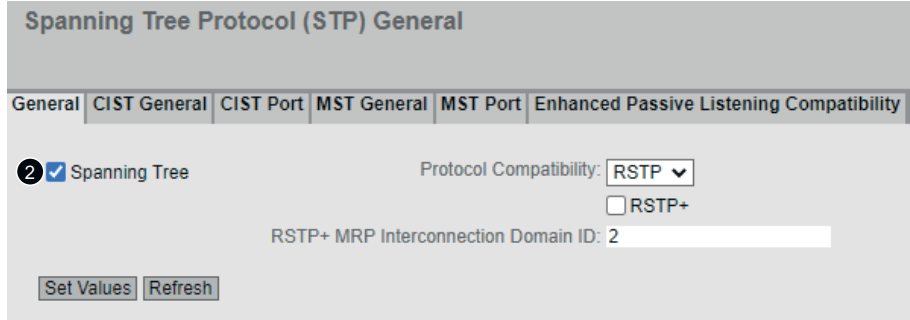
Set Values Refresh

Step 2: Enable Spanning Tree

Note

This step is only required for devices with default settings of Group 1.

Navigate to the menu "Layer 2 > Spanning Tree > General" and select the "Spanning Tree" check box.



Check the ring port settings in the menu "Layer 2 > Spanning Tree" on the page "CIST Port" or "ST Port".

The table on this page lets you configure Spanning Tree for individual ports.

Where necessary, adapt the following settings to your requirements:

- The check box for the two ring ports in the table column "Spanning Tree Status" must be selected.

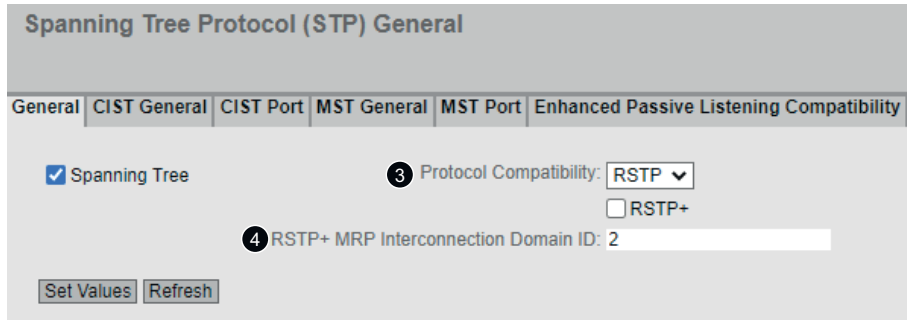
Port	Spanning Tree Status	Priority
P0.1	<input checked="" type="checkbox"/>	128
P0.2	<input checked="" type="checkbox"/>	128
P0.3	<input checked="" type="checkbox"/>	128

- The check box for the two ring ports in the table column "Restr. Role" must be cleared. This is necessary so that the behavior of the ring ports is exclusively controlled by MRP, the redundancy manager. The function of MRP is not affected by RSTP+.

Hello Time	Restr. Role
2	<input type="checkbox"/>
2	<input type="checkbox"/>
2	<input type="checkbox"/>

Step 3: Configure protocol compatibility

In the "Protocol Compatibility" drop-down list, select the item "RSTP".



Step 4: Specify the RSTP+ MRP Interconnection Domain ID

Enter a value for RSTP+ MRP Interconnection Domain ID.

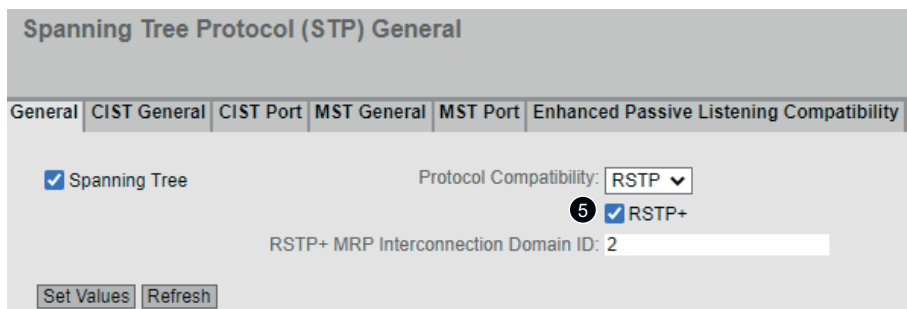
The RSTP+ MRP Interconnection Domain ID must be unique throughout the network and must differ from any MRP Interconnection Domain ID that may need to be configured. Different IDs are necessary to distinguish TCNs (Topology Change Notifications) of the RSTP network from TCNs of the MRP ring. This assignment makes it possible to only delete those FDB entries (Forwarding Database entries) that are affected by the topology change.

Each device checks whether different values were configured for these two parameters. If the IDs are identical, the device outputs an error message. The network administrator is responsible for making sure that these IDs are also unique throughout the network. An individual device cannot make such a check.

5.3.2.5 Enable RSTP+

Step 5: Enable RSTP+

In the "Layer 2 > Spanning Tree > General" menu, select the "RSTP+" check box and then click the "Set Values" button to save the configuration.



When RSTP+ is enabled, you cannot change the parameters configured previously.

5.3.2.6 Configuring Ring Redundancy for RSTP+

In WBM, you can use the menu "Layer 2 > Ring Redundancy" for configuring the ring redundancy. On the "Ring" page, execute steps 6 to 8 for each device in which you want to enable RSTP+.

The screenshot shows the "Ring Redundancy" configuration page. It includes a navigation bar with "Ring", "Standby", and "MRP Interconnection" tabs. The configuration area contains the following elements:

- Ring ID:** A dropdown menu set to "1".
- Ring Redundancy:** A checked checkbox labeled "Ring Redundancy".
- Ring Redundancy Mode:** A dropdown menu set to "MRP Client".
- Ring Ports:** Two dropdown menus, the first set to "P0.1" and the second set to "P0.2".
- Domain Name:** A dropdown menu set to "default-mrpdomain".
- Observer:** An unchecked checkbox labeled "Observer".
- Buttons:** "Restore Default", "Restart Observer", "Set Values", and "Refresh".

At the bottom, there is a table with the following data:

Ring ID	Domain Name	Ring Redundancy Mode	Ring Port 1	Ring Port 2
1	default-mrpdomain	MRP Client	P0.1	P0.2
2		-	P0.1	P0.2
3		-	P0.1	P0.2
4		-	P0.1	P0.2

Step 6: Enable ring redundancy

Select the redundant Ring 1 to be configured from the "Ring ID" drop-down list and select the "Ring Redundancy" to enable MRP on this ring.

Step 7: Assign MRP role

In the "Ring Redundancy Mode" drop-down list, select the "MRP Client", "MRP Manager" or "MRP Auto Manager" entry. The role of the redundancy manager should not be assigned to either of the two devices of the RSTP MRP link.

Step 8: Specify ring ports

Select the matching entries for the ring ports from the two drop-down lists.

Finally, click the "Set Values" button to save the configuration.

5.3.2.7 Plug cables

Step 9: Plug cables

When you have configured all devices, plug the cables according to the planned topology. The RSTP+ method is now activated.

5.3.3 HRP

HRP - High Speed Redundancy Protocol

HRP is the name of a redundancy method for networks with a ring topology. The switches are interconnected via ring ports. One of the switches is configured as the redundancy manager (RM). The other switches are redundancy clients. Using test frames, the redundancy manager checks the ring to make sure it is not interrupted. The redundancy manager sends test frames via the ring ports and checks that they are received at the other ring port. The redundancy clients forward the test frames.

If the test frames of the RM no longer arrive at the other ring port due to an interruption, the RM switches through its two ring ports and informs the redundancy clients of the change immediately. The reconfiguration time after an interruption of the ring is a maximum of 300 ms.

Standby redundancy

Standby redundancy is a method with which rings each of which is protected by high-speed redundancy can be linked together redundantly. In the ring, a master/slave device pair is configured and these monitor each other via their ring ports. If a fault occurs, the data traffic is redirected from one Ethernet connection (standby port of the master or standby server) to another Ethernet connection (standby port of the slave).

Requirements

HRP

- HRP is supported in ring topologies with up to 50 devices. Exceeding this number of devices can lead to a loss of data traffic.
- For HRP, only devices that support this function can be used in the ring.
- Devices that do not support HRP must be linked to the ring using special devices with HRP capability. Up to the ring, this connection is not redundant.
- All devices must be interconnected via their ring ports. Multimode connections up to 3 km and single mode connections up to 26 km between two IE switches are possible. At greater distances, the specified reconfiguration time may be longer.
- A device in the ring must be configured as redundancy manager by selecting the "HRP manager" setting. On all other devices in the ring, either the "HRP Client" or "Automatic Redundancy Detection" mode must be activated.
- The standby ports must be disabled in spanning tree.
- You configure HRP in Web Based Management, Command Line Interface or using SNMP.

Standby redundancy

- With standby coupling partners HRP must be set permanently.
- The ports of the standby coupling partners must be disabled in spanning tree.
- You configure standby redundancy in Web Based Management, Command Line Interface or using SNMP.

5.3.4 MRP

5.3.4.1 MRP - Media Redundancy Protocol

The "MRP" method conforms to the Media Redundancy Protocol (MRP) specified in the following standard:

IEC 62439-2:2021 Industrial communication networks - High availability automation networks Part 2: Media Redundancy Protocol (MRP)

The reconfiguration time after an interruption of the ring is a maximum of 200 ms.

Topology

The following figure shows a possible topology for devices in a ring with MRP.

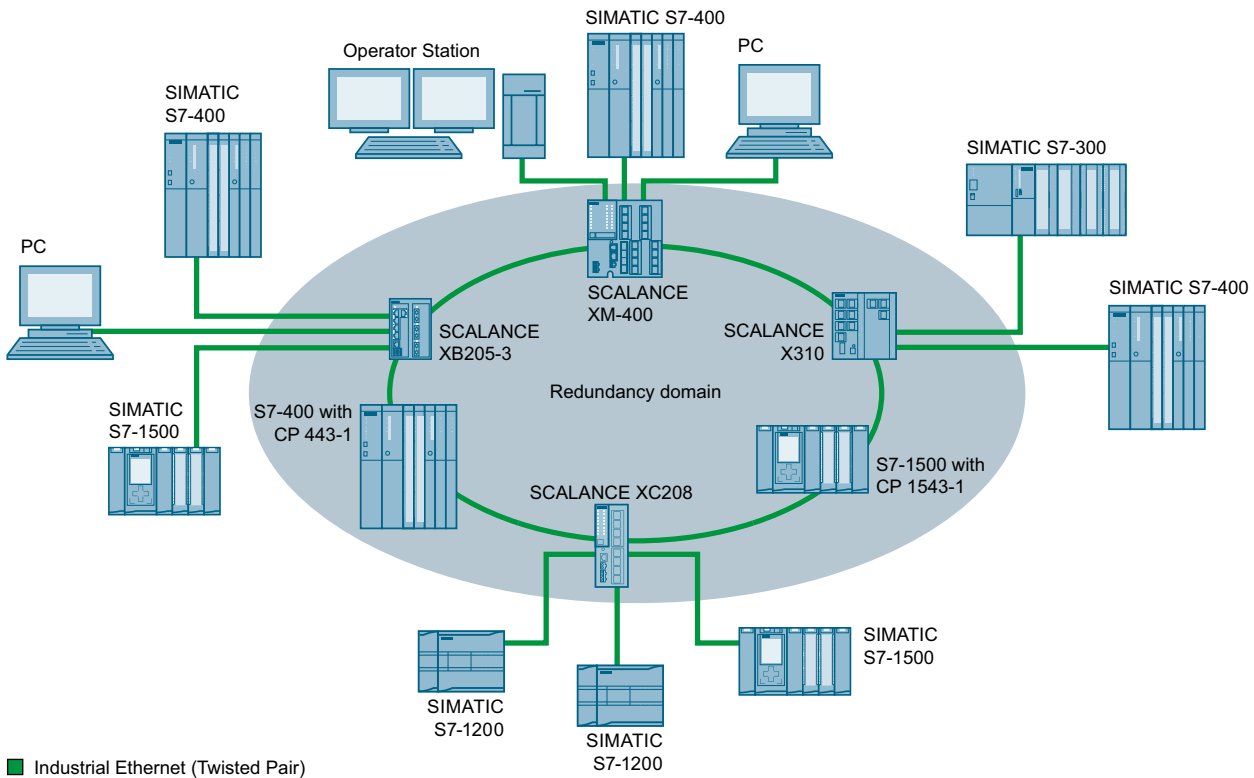


Figure 5-1 Example of a ring topology with the MRP media redundancy protocol

The following rules apply to a ring topology with media redundancy using MRP:

- All the devices connected within the ring topology are members of the same redundancy domain.
- One device in the ring is acting as redundancy manager.
- All other devices in the ring are redundancy clients.

Non MRP-compliant devices can be connected to the ring via a SCALANCE X switch or via a PC with a CP capable of MRP.

Requirements

The requirements for problem-free operation with the MRP media redundancy protocol are as follows:

- MRP is supported in ring topologies with up to 50 devices.
Exceeding this number of devices can lead to a loss of data traffic.
- The ring in which you want to use MRP may only consist of devices that support this function. These include, for example, some of the Industrial Ethernet SCALANCE X switches, some of the communications processors (CPs) for SIMATIC S7 and PG/PC or non-Siemens devices that support this function.
- All devices must be interconnected via their ring ports.
Multimode connections up to 3 km and single mode connections up to 26 km between two SCALANCE X IE switches are possible. At greater distances, the specified reconfiguration time may be longer.
- "MRP" must be enabled for all devices in the ring.
- The connection settings (transmission medium / duplex) must be set to full duplex and at least 100 Mbps for all ring ports. Otherwise there may be a loss of data traffic.
 - STEP 7: Set all the ports involved in the ring to "Automatic settings" in the "Options" tab of the properties dialog.
 - WBM: If you configure with Web Based Management, the ring ports are set automatically to autonegotiation.

5.3.4.2 Configuration in WBM

Role

The choice of role depends on the following use cases:

- You want to use MRP in a ring topology only with Siemens devices:
 - For at least one device in the ring select "Automatic Redundancy Detection" or "MRP Auto Manager".
 - For all other devices in the ring select "MRP Client" or "Automatic Redundancy Detection".
- You want to use MRP in a ring topology that also includes non-Siemens devices:
 - For exactly one device in the ring, select the role "MRP Auto Manager" or "MPR Manager".
 - For all other devices in the ring topology, select the role of "MRP client".

Note

The use of "Automatic Redundancy Detection" is not possible when using non-Siemens devices.

- You configure the devices in an MRP ring topology partly with WBM and partly with STEP 7:
 - With the devices you configure using WBM, select "MRP Client" for all devices.
 - With the devices that you configure using STEP 7, select precisely one device as "Manager" or "Manager (Auto)" and "MRP Client" for all other devices.

Note

If a device is assigned the role of "Manager" with STEP 7, all other devices in the ring must be assigned the "MRP Client" role. If there is a device with the "Manager" role and a device with the "Manager (Auto)"/"MRP Auto-Manager" in a ring, this can lead to circulating frames and therefore to failure of the network.

Configuration

In WBM, you configure MRP on the following pages:

- Configuration (Page 156)
- Ring (Page 318)

5.3.4.3 Configuration in STEP 7

Configuration in STEP 7

To create the configuration in STEP 7, select the parameter group "Media redundancy" on the PROFINET interface.

Set the following parameters for the MRP configuration of the device:

- Domain
- Role
- Ring port
- Diagnostic interrupts

These settings are described below.

Note**Valid MRP configuration**

In the MRP configuration in STEP 7, make sure that all devices in the ring have a valid MRP configuration before you close the ring. Otherwise, there may be circulating frames that will cause a failure in the network.

One device in the ring needs to be configured as "redundancy manager" and all other devices in the ring as "clients".

Note**Note factory settings**

MRP is disabled and spanning tree enabled for the following brand new IE switches and those set to the factory settings:

- SCALANCE XB-200 (EtherNet/IP variants)
- SCALANCE XC-200 (EtherNet/IP variants)
- SCALANCE XP-200 (EtherNet/IP variants)
- SCALANCE XC-300
- SCALANCE XR-300
- SCALANCE XR-300WG
- SCALANCE XC-400
- SCALANCE XM-400
- SCALANCE XR-500

To load a PROFINET configuration with MRP into one of the specified devices, disable Spanning Tree on the device. It is also possible to disable Spanning Tree only for the ring ports.

Note**Reconfiguration only when the ring is open**

First open the ring before you

- change the MRP role or
 - reconfigure ring ports.
-

Note**Starting up and restarting**

The MRP settings are still effective after a restart of the device or a power failure and hot restart as long as the power failure does not occur within 90 seconds after the configuration change.

Note

Prioritized startup

If you configure MRP in a ring, you cannot use the "prioritized startup" function in PROFINET applications on the devices involved.

If you want to use the "prioritized startup" function, then disable MRP in the configuration.

In the STEP 7 configuration, set the role of the relevant device to "Not a node in the ring".

Domain

Single MRP rings

If you want to configure a single MRP ring, leave the factory setting "mrpdomain 1" in the "Domain" drop-down list.

All devices configured in a ring with MRP must belong to the same redundancy domain. A device cannot belong to more than one redundancy domain in a single ring.

Multiple MRP rings

With the MRP multiple rings function, it is possible to control multiple MRP rings with one central redundancy manager. If you configure multiple single MRP rings, the nodes of the ring will be assigned to the individual rings with the "Domain" parameter. Set the same domain for all devices within a ring. Set different domains for different rings. Devices that do not belong to the same ring must have different domains.

If you want to configure MRP multiple rings, select a device that is capable of multiple rings as the central redundancy manager. Specify different domains for all ring instances and assign these to the corresponding ring ports of the redundancy manager. Configure the other devices as clients. The same domain must be set for all devices within a ring.

The following graphic shows a possible configuration consisting of 4 MRP multiple rings that are managed by a SCALANCE XC208 as central redundancy manager.

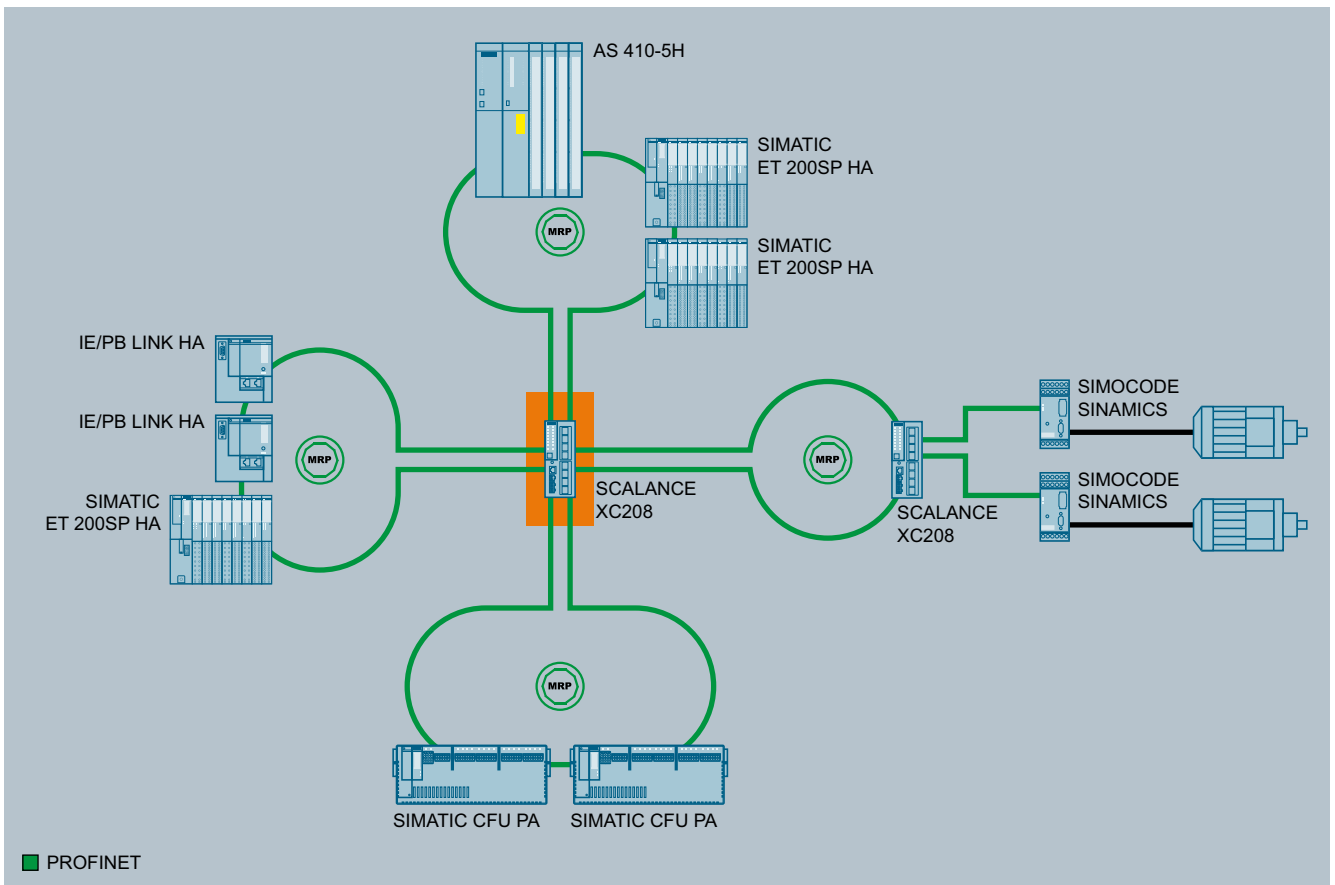


Figure 5-2 MRP multiple ring topology

Note

Suitable devices for MRP multiple rings

You can use all products from the following product lines as redundancy manager connecting multiple rings:

- SCALANCE X-300 as of firmware version V4.0
- SCALANCE X408-2 as of firmware version V4.0
- SCALANCE X414-3E as of firmware version V3.10
- SCALANCE XB-200 as of firmware version V4.3
- SCALANCE XC-200 as of firmware version V4.3
- SCALANCE XC-300 as of firmware version V1.0
- SCALANCE XP-200 as of firmware version V4.3
- SCALANCE XR-300 as of firmware version V1.0
- SCALANCE XR-300WG as of firmware version V4.3
- SCALANCE XC-400 as of firmware version V1.1
- SCALANCE XM-400 as of firmware version V6.4
- SCALANCE XR-500 as of firmware version V1.1
- SCALANCE XR-500 as of firmware version V6.4

Note

Suitable devices for MRP Interconnection

You can use all products from the following product lines as media redundancy interconnection manager and media redundancy interconnection client:

- SCALANCE XB-200 as of firmware version V4.3
 - SCALANCE XC-200 as of firmware version V4.2
 - SCALANCE XF-200BA as of firmware version V4.2
 - SCALANCE XF-200G as of firmware version V4.4
 - SCALANCE XP-200 as of firmware version V4.2
 - SCALANCE XC-300 as of firmware version V1.0
 - SCALANCE XR-300 as of firmware version V1.0
 - SCALANCE XR-300WG as of firmware version V4.3
 - SCALANCE XC-400 as of firmware version V1.1
 - SCALANCE XM-400 as of firmware version V6.3 or as of firmware version V6.2 for homogenous networks
 - SCALANCE XR-500 as of firmware version V6.3 or as of firmware version V6.2 for homogenous networks
 - SCALANCE XR-500 as of firmware version V1.1
-

Role

Note

Reconfiguration only when the ring is open

First open the ring before you reconfigure the ring ports of a ring manager.

The choice of role depends on the following use cases.

- You want to use MRP in a topology with **one ring** only with Siemens devices and without monitoring diagnostic interrupts:
Assign all devices to the "mrpdomain-1" domain and the role "Manager (Auto)".
The device that actually takes over the role of redundancy manager, is negotiated by Siemens devices automatically.
- You want to use MRP in a topology with **multiple rings** only with Siemens devices and without monitoring diagnostic interrupts:
 - Assign all instances of the device that connects the rings the role of "Manager".
 - For all other devices in the ring topology, select the role of "Client".

- You want to use MRP in a ring topology that also includes non-Siemens devices or you want to receive diagnostic interrupts relating to the MRP status from a device (see "Diagnostic interrupts"):
 - Assign precisely one device in the ring the role of "Manager (Auto)" or "MRP Manager".
 - For all other devices in the ring topology, select the role of "Client".
- You want to disable MRP:
Select the option "Not node in the ring" if you do not want to operate the device within a ring topology with MRP.

Note**Role after resetting to factory settings**

Open the ring before you reset a device in this ring to the factory settings.

With brand new Siemens devices and those reset to the factory settings the following MRP role is set:

- "Manager (Auto)"
 - CPs
- "Automatic Redundancy Detection"
 - SCALANCE X-200
 - SCALANCE XB-200 (PROFINET variants)
 - SCALANCE XC-200 (PROFINET variants)
 - SCALANCE XF-200BA
 - SCALANCE XF-200G
 - SCALANCE XP-200 (PROFINET variants)
 - SCALANCE X-300
 - SCALANCE X-400

MRP is disabled and spanning tree enabled for the following brand new IE switches and those set to the factory settings:

- SCALANCE XB-200 (EtherNet/IP variants)
 - SCALANCE XC-200 (EtherNet/IP variants)
 - SCALANCE XC-300
 - SCALANCE XP-200 (EtherNet/IP variants)
 - SCALANCE XR-300
 - SCALANCE XR-300WG
 - SCALANCE XC-400
 - SCALANCE XM-400
 - SCALANCE XR-500
-

Ring port 1 / ring port 2

Here, select the port you want to configure as ring port 1 and ring port 2.

With devices with more than 8 ports, not all ports can be selected as ring port.

The drop-down list shows the selection of possible ports for each device type. If the ports are specified in the factory, the boxes are grayed out.

NOTICE

Ring ports after resetting to factory settings

If you reset to the factory settings, the ring port settings are also reset.

Note

Reconfiguration only when the ring is open

First open the ring before you reconfigure the ring ports of a ring manager.

Diagnostic interrupts

Enable the "Diagnostic interrupts" option if you want diagnostic interrupts relating to the MRP status on the local CPU to be output.

The following diagnostic interrupts can be generated:

- Wiring or port error
Diagnostic interrupts are generated if the following errors occur at the ring ports:
 - Connection abort on a ring port
 - A neighbor of the ring port does not support MRP.
 - A ring port is connected to a non-ring port.
 - A ring port is connected to the ring port of another MRP domain.
- Status change active/passive (redundancy manager only)
If the status changes (active/passive) in a ring, a diagnostics interrupt is generated.

Parameter assignment of the redundancy is not set by STEP7 (redundancy alternatives)

This option affects all SCALANCE X switches. Select this option during configuration in STEP7 if you want to set the properties for media redundancy using alternative mechanisms such as WBM, CLI or SNMP.

If you enable this option, existing redundancy settings are retained and are not overwritten. The parameters in the "MRP configuration" box are then reset and grayed out. The entries then have no meaning.

Note

When the "Alternative redundancy" option is enabled for a device in the ring and the topology is monitored by STEP7 (controller), you must also enable the "Alternative redundancy" option for the other devices in the ring.

5.3.5 MRP Interconnection

5.3.5.1 Topology and how it works

The MRP Interconnection mode is an extension of MRP and enables redundant linking of two or more MRP rings. Isochronous real-time (IRT) networks are excluded from this. Like MRP, MRP Interconnection is specified in the standard IEC 62439-2. MRP Interconnection allows for very fast reconfiguration; the reconfiguration time is typically less than 200 milliseconds.

Topology

The diagram below shows the redundant linking of two MRP rings. A couple pair is required in each ring for a redundant coupling. A maximum of 5 couple pairs is permitted per MRP ring.

You can find information on the maximum number of active MRP Interconnection connections per device in the "Configuration limits" section.

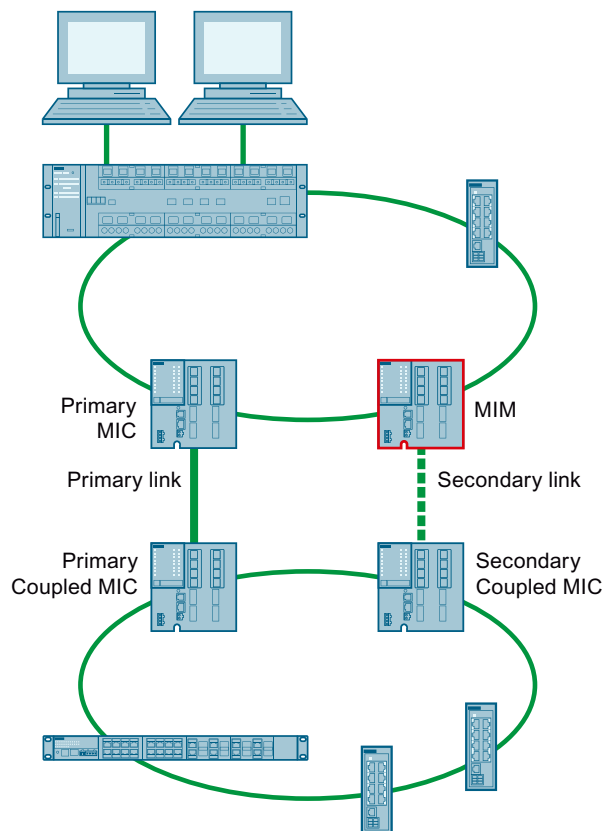


Figure 5-3 Redundant connection of two MRP rings with MRP Interconnection

Operating principle

The requirement for MRP Interconnection is that MRP is used in all rings involved. Four devices are required for the two MRP Interconnection connections:

- One Media Redundancy Interconnection Manager (MIM, shown with a red outline in the diagram)
- Three Media Redundancy Interconnection Clients (Primary MIC, Primary Coupled MIC and Secondary Coupled MIC)

Because each device is part of an MRP ring, each device also takes on one of the roles defined for MRP, i.e. MRP-Client or MRP-Manager.

Depending on the connection status of the interconnection ports, Primary MIC and Primary Coupled MIC send status messages (Link up or Link down) to the MIM. Interconnection ports are ports that are connected over the primary or secondary link. This means the MIM is always informed about the connection status between the Primary MIC and the Primary Coupled MIC ("primary link") as well as its own connection to the Secondary Coupled MIC ("secondary link"). In regular operation, the data exchange between the two rings is via primary link and the MIM blocks its interconnection port. If a Link down of the primary link is signaled to MIM, it switches its interconnection port to the "Forwarding" status, and the data exchange between the two rings is via secondary link between MIM and Secondary Coupled MIC.

5.3.5.2 Devices for MRP Interconnection

Suitable devices for MRP Interconnection

The Interconnection manager, the Interconnection clients and all ring managers must support MRP Interconnection. This is the case for the following devices:

- SCALANCE XB-200 as of firmware version V4.3
- SCALANCE XC-200 as of firmware version V4.2
- SCALANCE XC-300 as of firmware version V1.0
- SCALANCE XC-400 as of firmware version V1.1
- SCALANCE XF-200BA as of firmware version V4.2
- SCALANCE XF-200G as of firmware version V4.4
- SCALANCE XP-200 as of firmware version V4.2
- SCALANCE XR-300 as of firmware version V1.0
- SCALANCE XR-300WG as of firmware version V4.3
- SCALANCE XM-400 as of firmware version V6.3 or as of firmware version V6.2 for homogenous networks
- SCALANCE XR-500 as of firmware version V6.3 or as of firmware version V6.2 for homogenous networks
- SCALANCE XR-500 as of firmware version V1.1

IEC62439-2 Ed.2 and IEC62439-2 Ed.3

Some definitions relating to MRP Interconnection were added or edited during the transition from IEC62439-2 Edition 2 to IEC62439-2 Edition 3. For reasons of interoperability, an additional MAC address for MRP Interconnection was introduced, among other things. As a consequence, the MAC addresses to be used for MRP Interconnection have changed as compared to the requirements in the previous standard. This section describes the effect of this on the operation of SCALANCE devices.

Firmware version V6.2 for SCALANCE XM-400 and SCALANCE XR-500

MRP Interconnection based on firmware version V6.2 only works in homogenous networks of SCALANCE XM-400 and SCALANCE XR-500 when all devices have firmware version V6.2.

NOTICE

No MRP Interconnection in heterogenous networks with firmware V6.2

Activation of MRP Interconnection in heterogenous networks with SCALANCE XM-400/ SCALANCE XR-500 and firmware version V6.2 can lead to malfunctions in the network. The MRP Interconnection function should generally not be enabled in such networks.

Firmware version V6.3 for SCALANCE XM-400 and SCALANCE XR-500

As of firmware version V6.3, MRP Interconnection is released for the SCALANCE XM-400 and SCALANCE XR-500 devices and can be used without restrictions.

NOTICE

Firmware update for MRP Interconnection

For SCALANCE XM-400 and SCALANCE XR-500 devices already present in the network, an update to firmware version V6.3 or higher is essential for proper functioning of MRP Interconnection.

The MRP Interconnection function is possible with SCALANCE devices in heterogenous networks under the following conditions:

- All SCALANCE XM-400 and SCALANCE XR-500 devices have firmware version V6.3 or higher.
- All SCALANCE XC-200, SCALANCE XF-200BA and SCALANCE XP-200 devices have firmware as of version V4.2
- All SCALANCE XB-200 and SCALANCE XR300WG devices have firmware version V4.3 or higher.
- All SCALANCE XF-200G devices have firmware as of version V4.4
- All SCALANCE XC-300 and SCALANCE XR-300 devices have firmware as of version V1.0
- All SCALANCE XC-400 and SCALANCE XR-500 devices have firmware version V1.1 or higher
- All other network components fulfil the requirement of IEC 62439-2 Edition 3

Firmware version V4.2 for SCALANCE XC-200, SCALANCE XF-200BA and SCALANCE XP-200

As of firmware version V4.2, MRP Interconnection is released for the SCALANCE XC-200, SCALANCE XF-200BA and SCALANCE XP-200 devices and can be used without restrictions. The specified devices can be coupled with SCALANCE XM-400 and SCALANCE XR-500 devices as of firmware version V6.3 via MRP Interconnection.

Firmware version V4.3 for SCALANCE XB-200 and SCALANCE XR-300WG

As of firmware version V4.3, MRP Interconnection is released for the SCALANCE XB-200 and SCALANCE XR-300WG devices and can be used without restrictions. The specified devices can be coupled with SCALANCE XM-400 and SCALANCE XR-500 devices as of firmware version V6.3 via MRP Interconnection.

Firmware version V4.4 for SCALANCE XF-200G

As of firmware version V4.4, MRP Interconnection is released for the SCALANCE XF-200G devices and can be used without restrictions.

Firmware version V1.0 for SCALANCE XC-300 and SCALANCE XR-300

As of firmware version V1.0, MRP Interconnection is released for the SCALANCE XC-300 and SCALANCE XR-300 devices and can be used without restrictions.

Firmware version V1.1 for SCALANCE XC-400 and SCALANCE XR-500

As of firmware version V1.1, MRP Interconnection is released for the SCALANCE XC-300 and SCALANCE XR-300 devices and can be used without restrictions.

5.3.5.3 Configuring an MRP Interconnection connection

This following sections describe the procedure during configuration of an MRP Interconnection connection in detail. Execute the configuration steps in the order listed here to prevent network loops. During configuration, not all devices can always be reached by the configuration PC. The specified configuration order ensures that at least the devices that have not been configured yet can be reached. The position numbers in the diagrams refer to the respective number of the step sequence.

The description has three sections:

- Connecting the devices and basic configuration (step 1 to step 3)
- Configuration of ring redundancy (step 4 to step 7)
- Configuration of MRP Interconnection (step 8 to step 16)

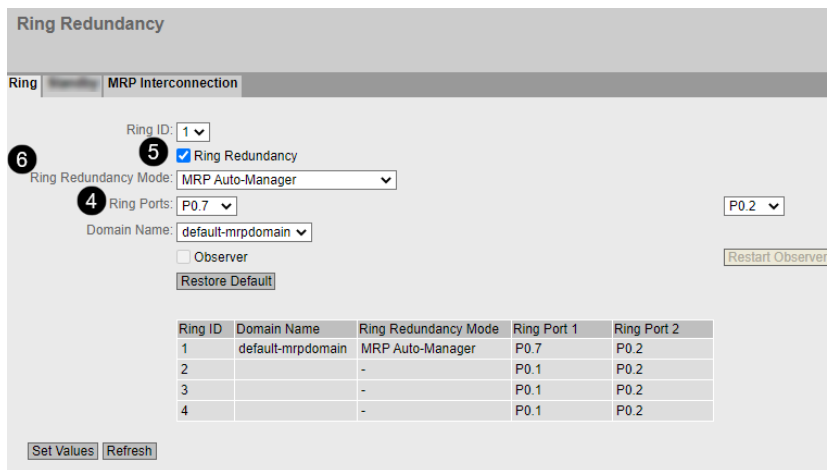
Step 3: Configure Spanning Tree

Execute the following two steps for each device if Spanning Tree is required for your network topology. Disable Spanning Tree for each device if it is not needed.

- Specify the protocol compatibility "RSTP".
(WBM menu command "Layer 2 > Spanning Tree", "General" tab, Protocol Compatibility drop-down list)
- Disable Spanning Tree for the ring ports and the MRP Interconnection ports.
(WBM menu command "Layer 2 > Spanning Tree", "CIST Port" tab, "Spanning Tree Status" table column)

5.3.5.5 Configuration of ring redundancy

In WBM, you can use the menu "Layer 2 > Ring Redundancy" for configuring the ring redundancy. In the "Ring" tab, execute steps 4 to 6 for each device.



Step 4: Specify ring ports

Select the matching entries for the ring ports from the two drop-down lists.

Note

If the selected ports have different hardware properties, the message "Port Configuration of the Ring Ports is different" is displayed. The reasons for the message can be:

- Different transmission speed (10Gigabit Ethernet port / Gigabit Ethernet Port / Fast Ethernet port)
- Different transmission mode (full duplex / half duplex)
- Different transmission media (copper cable / fiber-optic cable)

In this case, check whether the configuration is actually intended in this form. Different port properties usually limit the functions of ring ports even if data transmission is generally possible.

For detailed information on port properties, go to "System > Ports".

Step 5: Enable MRP

Select the "Ring Redundancy" check box to enable MRP.

Step 6: Assign MRP role

The following entries are available in the Ring Redundancy Mode drop-down list for the MRP mode:

- MRP Auto-Manager
- MRP Client
- MRP Manager

Configure the ring redundancy mode "MRP Auto-Manager" for two devices in each ring so that the MRP ring can be reconfigured immediately even when one device fails.

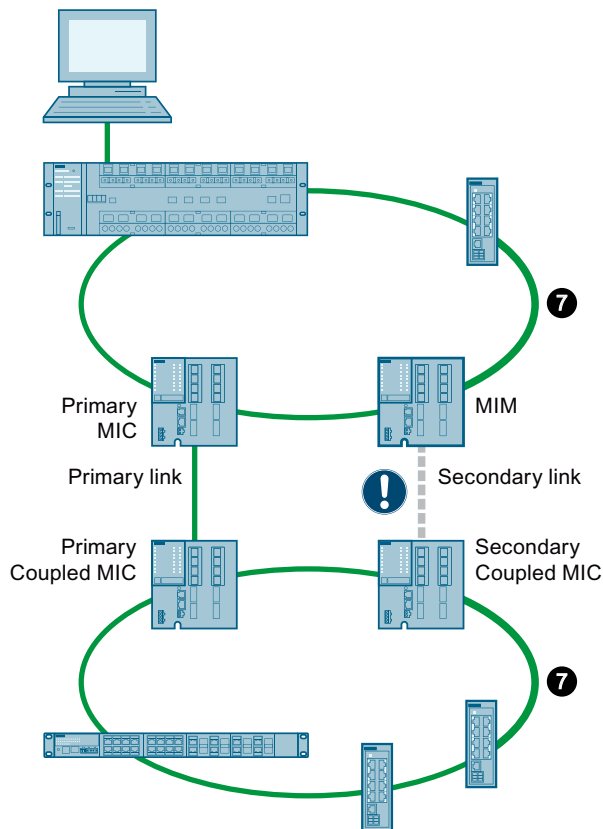
Note

If you assign the ring redundancy mode "MRP Auto-Manager" to more than one device, the device with the lowest MAC address will become the manager. The other devices automatically set themselves to "MRP Client" mode.

Finally, click the "Set Values" button to save the configuration.

Step 7: Close rings

Once you have configured all devices in both rings for MRP, close the two MRP rings by plugging the cables between the devices that have not been connected yet. Do not plug the cable between the MIM and the Secondary Coupled MIC yet.



Information on ring redundancy

You can find information on the current status of the ring redundancy in the WBM and in the CLI:

- **WBM**
"Information > Redundancy" menu, "Ring Redundancy" tab
- **CLI**
The command `show ring-redundancy` in User EXEC mode or in Privileged EXEC mode

5.3.5.6 Configuration of MRP Interconnection

Four devices are involved in the redundant linking of two rings with MRP Interconnection. When configuring these devices, you must observe a particular order so that devices which have not been configured yet can be reached by the configuration PC. Observe the following rule:

First configure the devices of the MRP Interconnection connection in the MRP ring to which the configuration PC is not connected. Start with the device for which no cable has been

plugged yet for the MRP Interconnection connection; this means you start with the device "Secondary Coupled MIC" in the example shown here.

This means the configuration sequence is as follows:

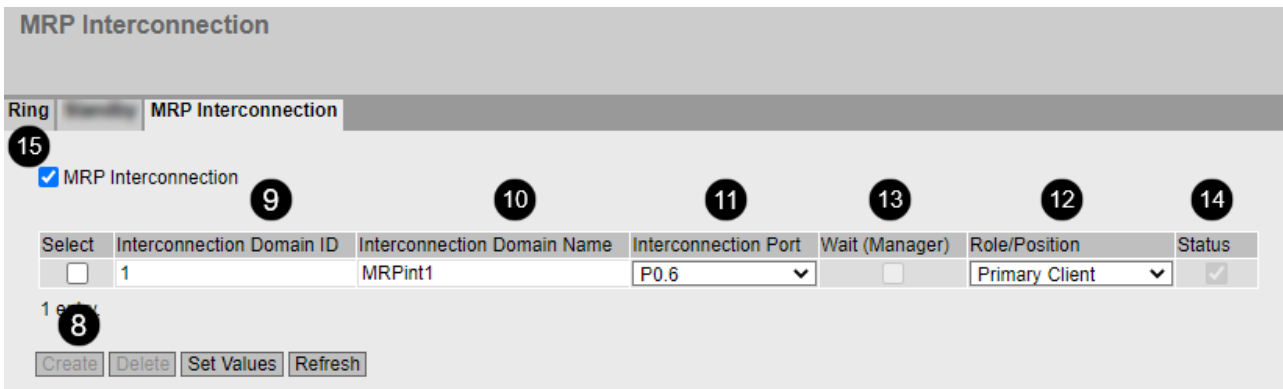
1. Secondary Coupled MIC
2. Primary Coupled MIC
3. Primary MIC
4. MIM

Note

Reachability of the devices and error message due to missing cable

- After configuration of the Secondary Coupled MIC and the Primary Coupled MIC, the two rings are disconnected and the two listed devices can initially no longer be reached.
- After configuration of the Primary MIC, the Secondary Coupled MIC and the Primary Coupled MIC as well as all other devices of the second ring can be reached again.
- After configuration of the MIM, an error message is displayed. The reason for the error is that the cable between the MIM and the Secondary Coupled MIC has not been plugged yet. This error disappears when the cable is plugged once the configuration is complete (step 16).

In WBM, you can use the menu "Layer 2 > Ring Redundancy" for configuring the MRP Interconnection. In the "MRP Interconnection" tab, execute steps 8 to 15 for each device.



Step 8: Create table entry for new connection

Click the "Create" button to create a new row in the table with the MRP Interconnection connections.

Step 9: Assign Interconnection Domain ID

Enter the Interconnection Domain ID. When specifying the ID, observe the following rules:

- The Interconnection domain ID cannot be 0.
- You need to configure the same Interconnection Domain ID for all four devices used for linking the rings.

Step 10: Assign Interconnection Domain Name

Enter any name for the Interconnection connection. You must specify a name, but the name has no effect on the configuration. The letters 'A' to 'Z' and 'a' to 'z', the numbers '0' to '9' and the '-' symbol are valid characters for this name. A hyphen cannot be used for the first or last character of the name. The name must not contain any spaces. The interconnection domain name must contain at least one character and no more than 240 characters.

Step 11: Specify the Interconnection port

From this drop-down list, select the port that is used for the MRP Interconnection connection. Be aware of the following restrictions:

- The port cannot be disabled or blocked. The "Unicast Blocking" function cannot be enabled for the port.
- The port cannot be used for a link aggregation.
- The port cannot be a monitor port of the "Mirroring" function.
- The port cannot be a Spanning Tree port.
- The port cannot be a ring port.
- The port cannot be an 802.1X Authenticator Port.
- The port cannot be an 802.1X Supplicant Port.
- In addition with SCALANCE XC-300 / XR-300 / XC-400 / XM-400 / XR-500 devices: The port cannot be a router port.

Step 12: Select the role and position of the device

You must assign a role to each device that is involved in an MRP Interconnection connection. The two roles are "Manager" and "Client". For clients, you also specify the position ("Primary" or "Secondary"). You make your selection in the drop-down list of the table column "Role/Position". In the example shown here, the devices are assigned the following roles:

Device	Role
Secondary Coupled MIC	Secondary Client
Primary Coupled MIC	Primary Client
Primary MIC	Primary Client
MIM	Manager

Step 13: Enable "Wait" option for the Manager

For devices with the "Client" role, the check boxes are cleared in this column. Select the "Wait (Manager)" check box for the device with the "Manager" role so that data transmission does not start until the primary client for MRP Interconnection is ready for operation.

Step 14: Enable MRP Interconnection connection

Select the "Status" check box to enable an MRP Interconnection connection. Observe the following rules:

- If there is not at least one enabled MRP Interconnection connection, you cannot enable the MRP Interconnection for the device.
- The following maximum values are in effect for the number of enabled MRP interconnections:
 - **Two connections**
SCALANCE XC-200, SCALANCE XP-200, SCALANCE XF-200BA as of firmware version V4.3
SCALANCE XF-200G as of firmware version V4.4
SCALANCE XC-300 and SCALANCE XR-300 as of firmware version V1.0
SCALANCE XC-400 and SCALANCE XR-500 as of firmware version V1.1
SCALANCE XM-400 and SCALANCE XR-500 as of firmware version V6.3
 - **One connection**
SCALANCE XB-200 and SCALANCE XR-300WG as of firmware version V4.3

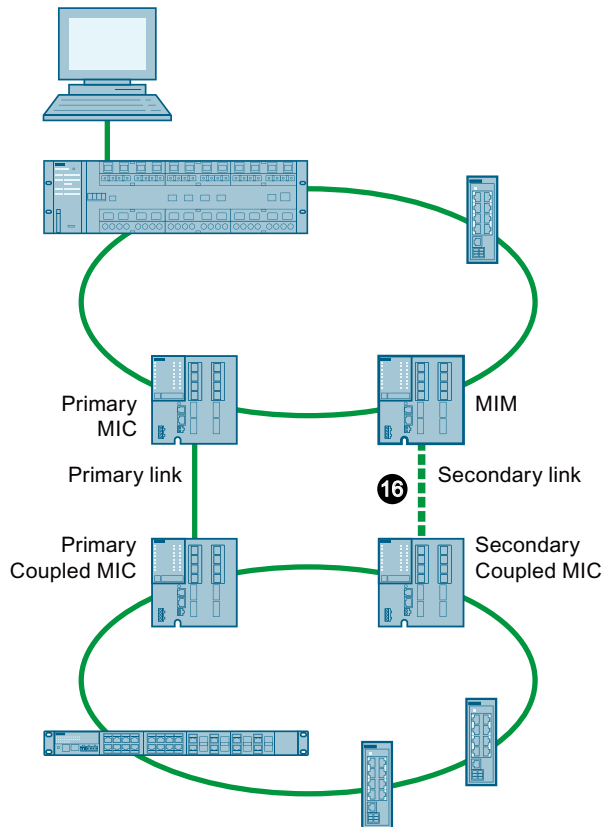
Click the "Set Values" button.

Step 15: Enable the MRP Interconnection for the device

Select the "MRP Interconnection" check box to enable the MRP Interconnection. Finally, click the "Set Values" button to save the configuration.

Step 16: Insert cable for the secondary link

Once you have configured all devices in both rings for MRP Interconnection, plug the cable for the secondary link between the MIM and Secondary Coupled MIC devices. The fault LED then no longer lights up. Afterwards, the MRP Interconnection connection is operational.



Information on MRP Interconnection

The latest information on MRP Interconnection is available in the WBM and in the CLI:

- **WBM**
"Information > Redundancy" menu, "MRP Interconnection" tab
- **CLI**
The command `show ring-redundancy` in User EXEC mode or in Privileged EXEC mode

5.3.6 Standby

General

SCALANCE X switches support not only ring redundancy within a ring but also redundant linking of rings or open network segments (linear bus). In the redundant link, rings are connected together over Ethernet connections. This is achieved by configuring a master/slave device pair in one ring so that the devices monitor each other and, in the event of a fault, redirect the data traffic from the normally used master Ethernet connection to the substitute (slave) Ethernet connection.

Standby redundancy

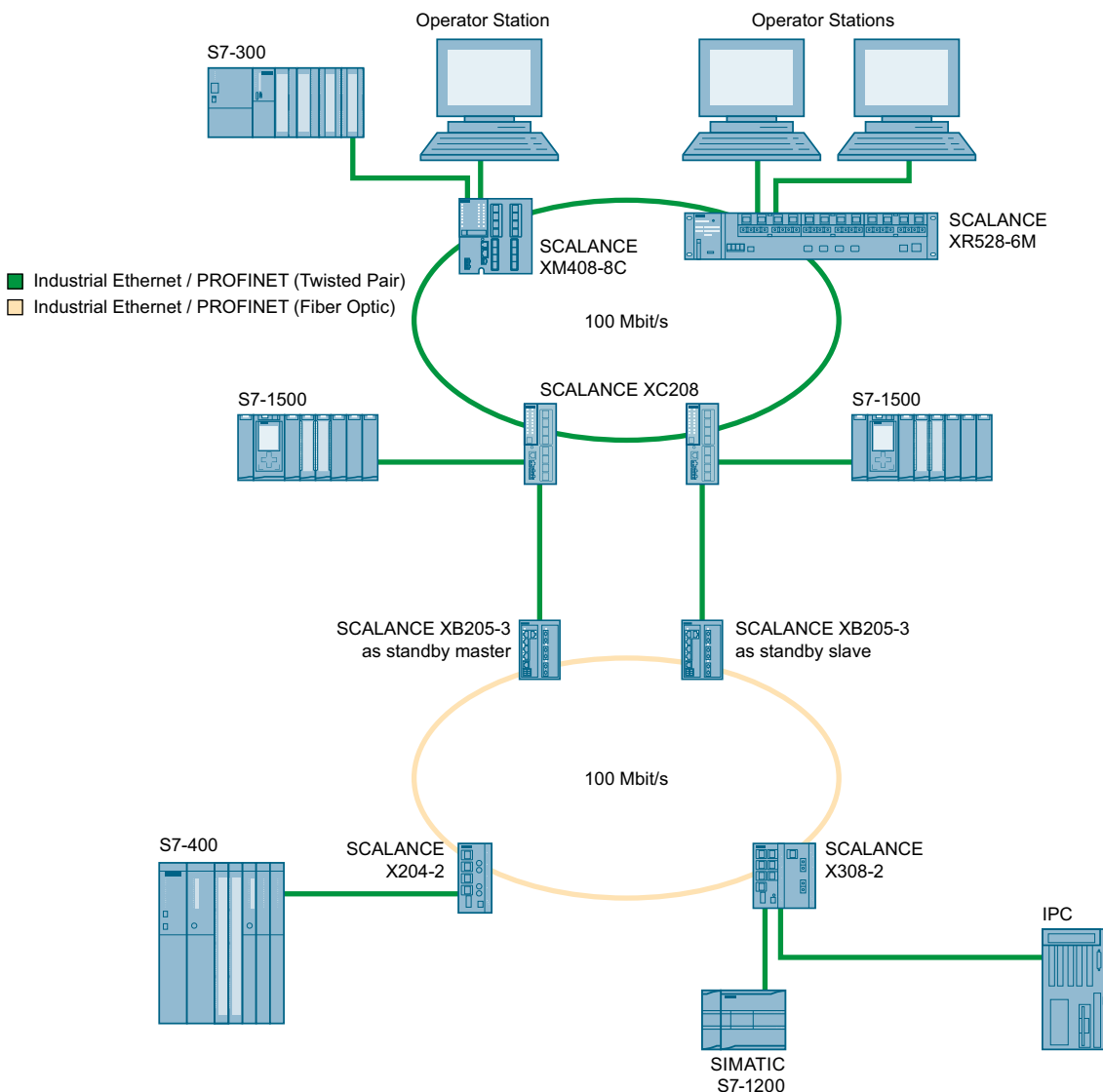


Figure 5-4 Example of a redundant link between rings

5.3 Redundancy mechanism

For a redundant link as shown in the figure, two devices must be configured as standby redundancy switches within a network segment. In this case, network segments are rings with a redundancy manager. Instead of rings, network segments might also be linear.

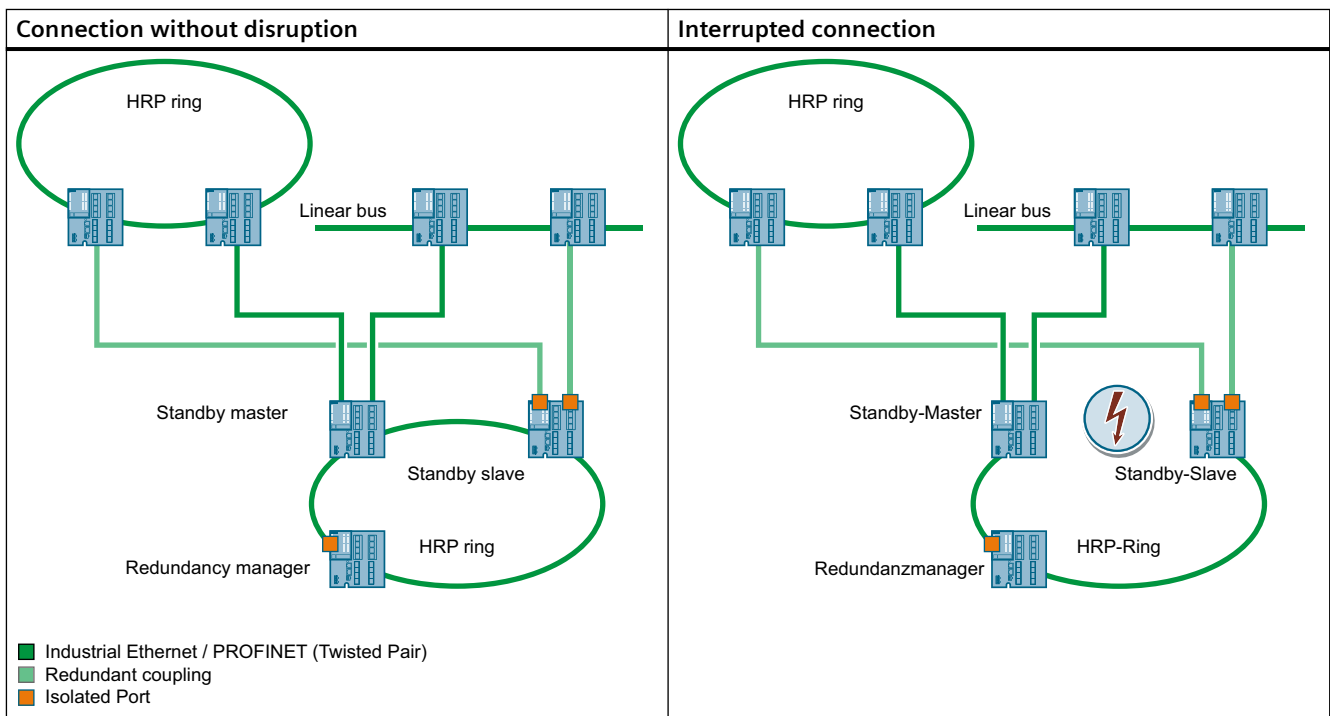
The two standby redundancy switches connected in the configuration exchange data frames with each other to synchronize their operating statuses (one device is master and the other slave). If there are no problems, only the link from the master to the other network segment is active. If this link fails (for example due to a link-down or a device failure), the slave activates its link as long as the problem persists.

Coupling of several HRP network segments

If you connect several HRP rings or links using standby redundancy, the standby master and standby slave must be located in a closed network segment. Under no circumstances may this network segment be open, i.e. a line.

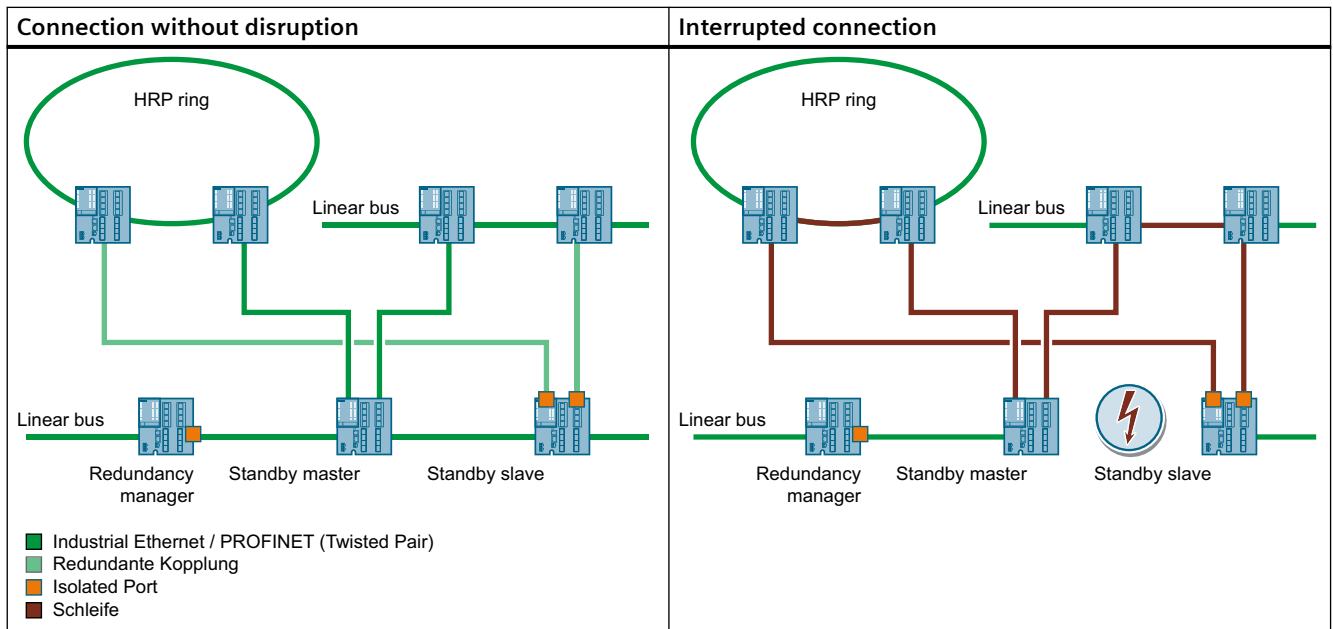
Standby master and slave in a closed network segment

If the connection between the standby master and slave is interrupted, the two devices can still communicate via the redundant link of the HRP redundancy manager.



Standby master and slave in an open network segment

If the connection between the standby master and slave is interrupted, the two devices can no longer communicate. This causes a loop via the coupled network segments.



5.4 VLAN

5.4.1 Basics

Network definition regardless of the spatial location of the nodes

VLAN (Virtual Local Area Network) divides a physical network into several logical networks that are shielded from each other. Here, devices are grouped together to form logical groups. Only nodes of the same VLAN can address each other. Since multicast and broadcast frames are only forwarded within the particular VLAN, they are also known as broadcast domains.

The particular advantage of VLANs is the reduced network load for the nodes and network segments of other VLANs.

To identify which packet belongs to which VLAN, the frame is expanded by 4 bytes (VLAN tagging (Page 76)). This expansion includes not only the VLAN ID but also priority information.

Options for the VLAN assignment

Each port of a device is assigned a VLAN ID (port-based VLAN). You configure port-based VLAN in "Layer 2 > VLAN > Port-based VLAN (Page 300)".

5.4.2 VLAN tagging

Expansion of the Ethernet frames by four bytes

For CoS (Class of Service, frame priority) and VLAN (virtual network), the IEEE 802.1Q standard defined the expansion of Ethernet frames by adding the VLAN tag.

Note

The VLAN tag increases the permitted total length of the frame from 1518 to 1522 bytes. The end nodes on the networks must be checked to find out whether they can process this length / this frame type. If this is not the case, only frames of the standard length may be sent to these nodes.

The additional 4 bytes are located in the header of the Ethernet frame between the source address and the Ethernet type / length field:

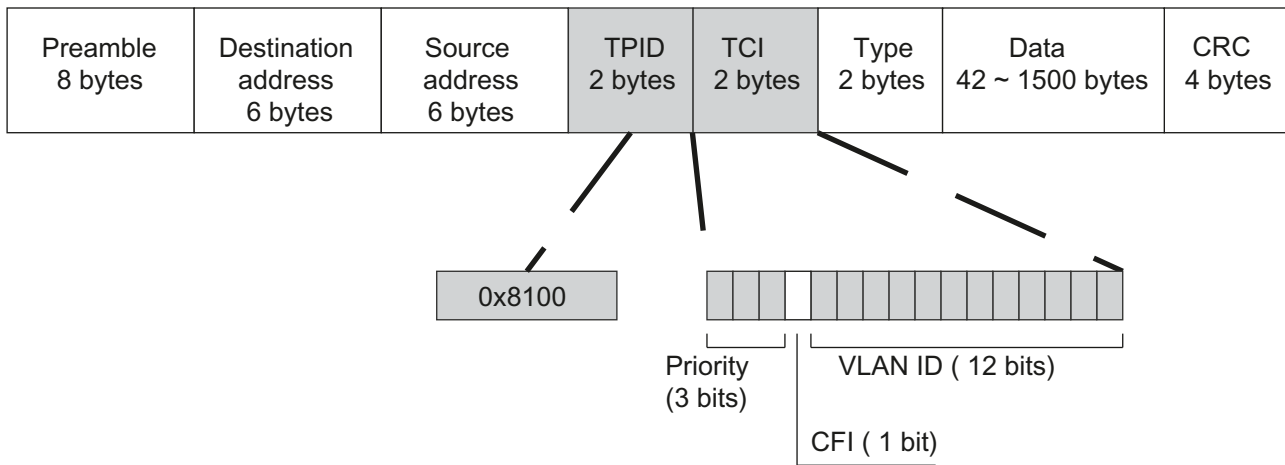


Figure 5-5 Structure of the expanded Ethernet frame

The additional bytes contain the tag protocol identifier (TPID) and the tag control information (TCI).

Tag protocol identifier (TPID)

The first 2 bytes form the Tag Protocol Identifier (TPID) and always have the value 0x8100. This value specifies that the data packet contains VLAN information or priority information.

Tag Control Information (TCI)

The 2 bytes of the Tag Control Information (TCI) contain the following information:

QoS Trust

The tagged frame has 3 bits for the priority that is also known as Class of Service (CoS), see also IEEE 802.1Q.

CoS bits	Priority	Type of the data traffic
000	0 (lowest)	Background
001	1	Best Effort
010	2	Excellent Effort
011	3	Critical Applications
100	4	Video, < 100 ms delay (latency and jitter)
101	5	Voice (language), < 10 ms delay (latency and jitter)
110	6	Internetwork Control
111	7 (highest)	Network Control

The prioritization of the data packets is possible only if there is a queue in the components in which they can buffer data packets with lower priority.

The device has multiple parallel queues in which the frames with different priorities can be processed. As default, first, the frames with the highest priority are processed. This method ensures that the frames with the highest priority are sent even if there is heavy data traffic.

Canonical Format Identifier (CFI)

The CFI is required for compatibility between Ethernet and the token Ring. The values have the following meaning:

Value	Meaning
0	The format of the MAC address is canonical. In the canonical representation of the MAC address, the least significant bit is transferred first. Standard-setting for Ethernet switches.
1	The format of the MAC address is not canonical.

VLAN ID

In the 12-bit data field, up to 4096 VLAN IDs can be formed. The following conventions apply:

VLAN ID	Meaning
0	The frame contains only priority information (priority tagged frames) and no valid VLAN identifier.
1- 4094	Valid VLAN identifier, the frame is assigned to a VLAN and can also include priority information. Default VLAN ID: 1
4095	Reserved

5.4.3 Private VLAN

With a private VLAN (PVLAN) you can divide up the layer 2 broadcast domains of a VLAN.

A private VLAN consists of the following units:

- A primary private VLAN (primary PVLAN)
The VLAN that is divided up is called primary private VLAN.
- secondary private VLANs (secondary PVLAN)
Secondary PVLANS exist only within a primary PVLAN. Every secondary PVLAN has a specific VLAN ID and is connected to the primary PVLAN.
Secondary PVLANS are divided into the following types:
 - Isolated Secondary PVLAN
Devices within an Isolated Secondary PVLAN cannot communicate with each other via layer 2.
 - Community Secondary PVLAN
Devices within a community secondary PVLAN can communicate with each other directly via layer 2. The devices cannot communicate with devices in other communities of the PVLAN via layer 2.

Note

VLAN ID with secondary PVLANS

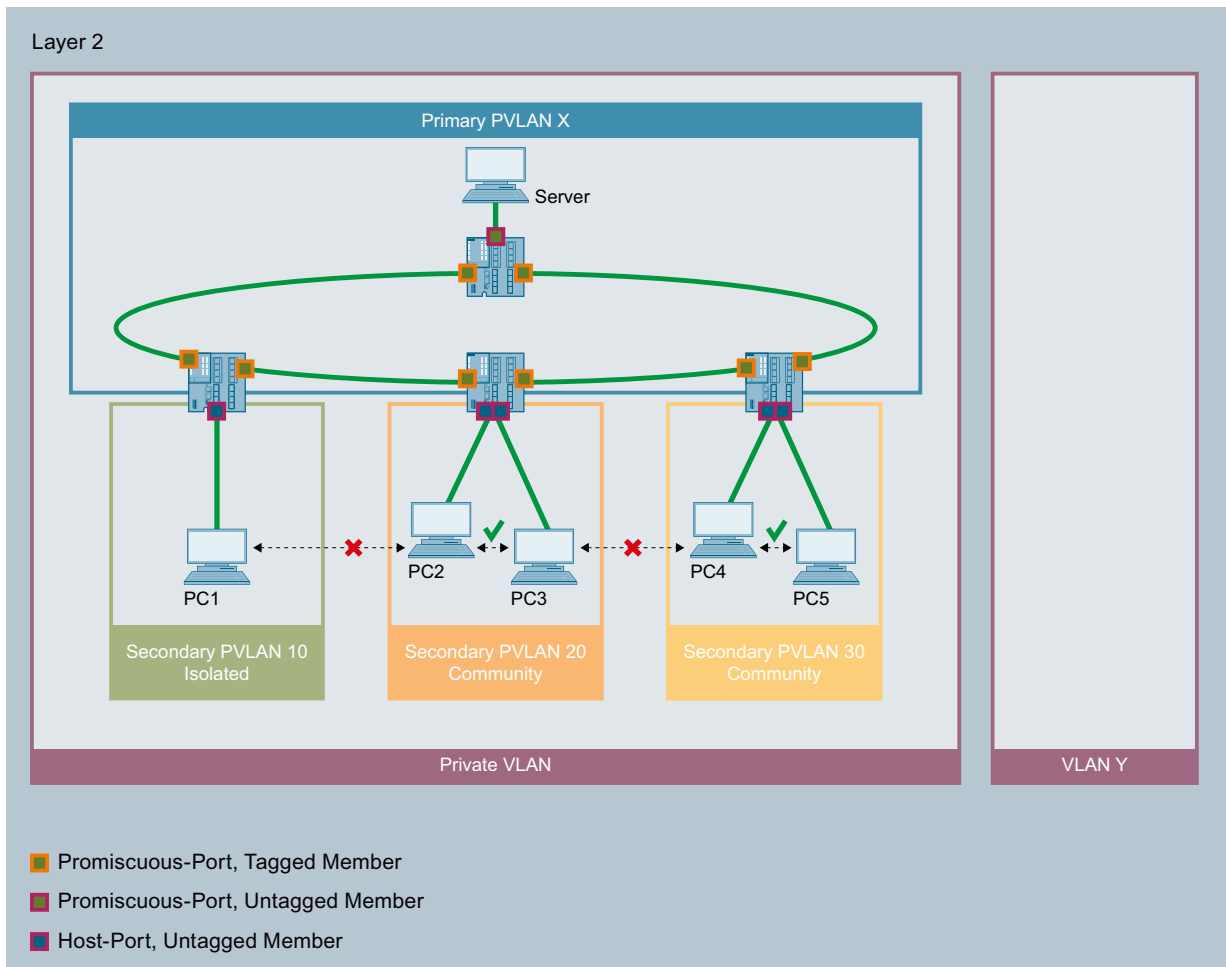
If you use the same VLAN ID for secondary PVLANS on different IE switches, the end devices in these secondary PVLANS can communicate with other via layer 2 across the different switches. The ports that connect different IE switches cannot be configured as trunk ports.

Note

Private VLAN functionality and RADIUS authentication

When VLAN assignment is enabled via RADIUS authentication for one or more ports of a VLAN, you should not configure this VLAN additionally as private VLAN.

The private VLAN functionality in connection with VLAN assignment via RADIUS authentication can result in an inconsistent system state.



In this example, the ports of the IE switches that connect them to other IE switches are promiscuous ports. These network ports are tagged members in all PVLANS: Primary PVLAN and all secondary PVLANS. The port VID of this port corresponds to VLAN1.

The ports to which the PCs are connected are host ports. The host ports are all untagged members in the primary PVLAN and in their secondary PVLAN. The port VID of this port corresponds to the secondary VLAN.

The port to which the server is connected is a promiscuous port. This promiscuous port is an untagged member in all PVLANS: Primary PVLAN and all associated secondary PVLANS. The port VID of this port corresponds to the primary VLAN.

In this example all PCs can communicate with the server. The server can communicate with all PCs. PC1 cannot communicate with any other PC. The PCs within a community secondary PVLAN can communicate with each other but not with the PCs in another secondary PVLAN.

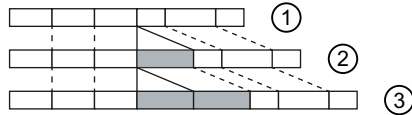
5.4.4 VLAN tunnel

With the Q-in-Q VLAN Tunnel function it is possible to forward the data traffic from different customer networks using a VLAN tunnel via a provider network. Every customer network has the full number of possible VLANs available.

5.4 VLAN

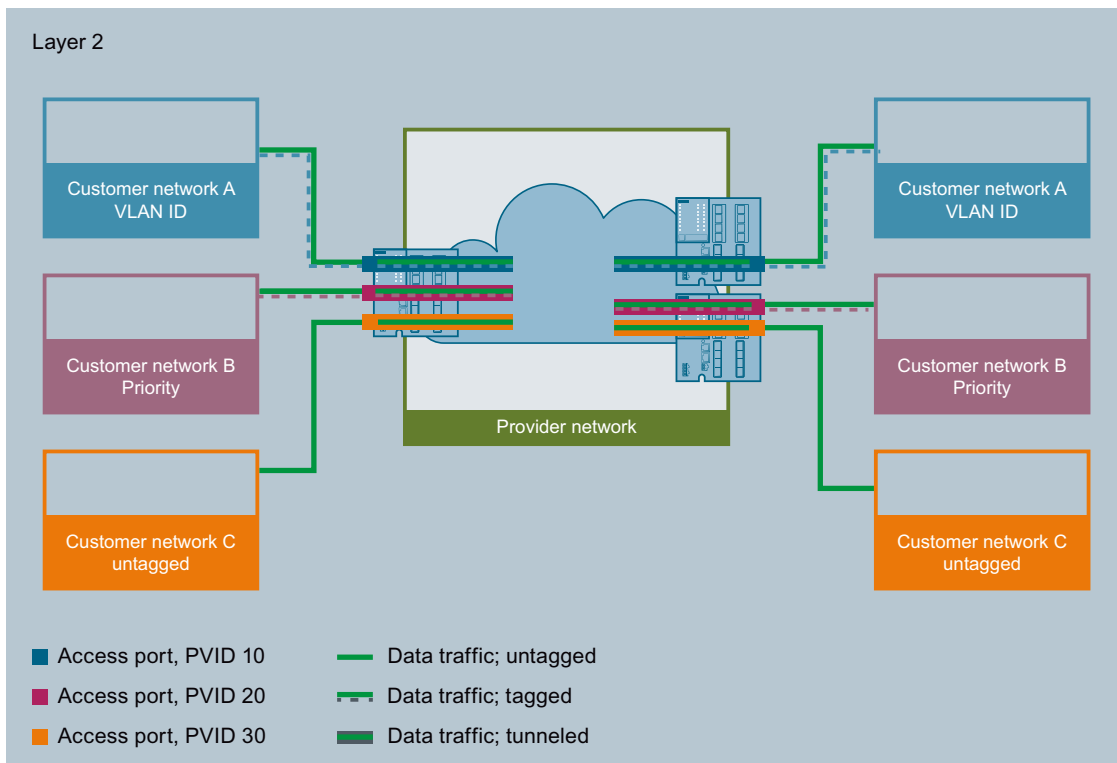
A VLAN tunnel is established between provider switches that are configured at the boundaries of a provider network. A provider switch has the following types of ports:

- Access port
 - The provider switch is connected to a customer network via an access port.
 - Incoming data traffic
 - The incoming data traffic at an access port is treated as if it were untagged ①. All incoming frames are expanded by a tag with the port VID of the access port ②. With frames that are already tagged, this means they are expanded by a second 802.1Q tag ③ the outer VLAN tag.



- Outgoing data traffic
 - With outgoing data traffic the outer tag is removed again at an access port.

- Core port
 - The provider switch is connected to a provider network via a core port.
 - Core ports are members in the port VLAN of the access port or configured with the port type "Switch-Port VLAN Trunk".



In this example, the data traffic from the customer networks A, B and C is forwarded over the provider network using a VLAN tunnel. The frames from customer network A are tagged with a VLAN ID. The frames from customer network B are tagged with a priority. The frames from customer network C are untagged.

When the frames reach the relevant access port, they are expanded by a tag with the port VID of the access port and tunneled through the provider network. As soon as the frames leave the provider network, the outer VLAN tag (PVID) is removed again. The frames are forwarded in their original form. The priority of the frame is retained.

5.5 Mirroring

The device provides the option of simultaneously channeling incoming or outgoing data streams via other interfaces for analysis or monitoring. This has no effect on the monitored data streams. This procedure is known as mirroring. In this menu section, you enable or disable mirroring and set the parameters.

Mirroring ports

Mirroring a port means that the data traffic at a port (mirrored port) of the IE switch is copied to another port (monitor port). You can mirror one or more ports to a monitor port.

If a protocol analyzer is connected to the monitor port, the data traffic at the mirrored port can be recorded without interrupting the connection. This means that the data traffic can be investigated without being affected. This is possible only if a free port is available on the device as the monitor port.

Note

Forwarding RSPAN stream

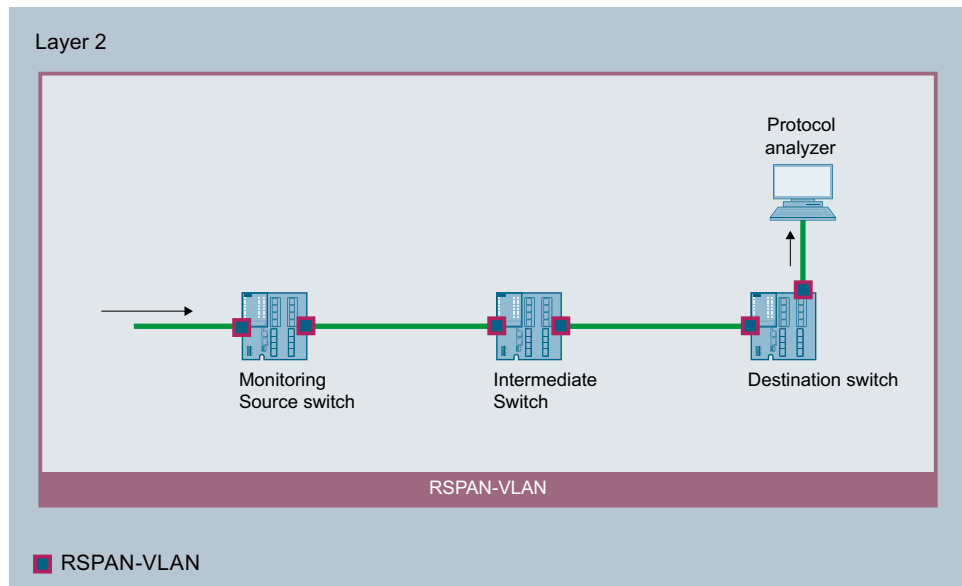
If the device is to forward RSPAN streams, two requirements must be met:

- The input and output ports need to be members of the same VLAN.
 - The "Learning" function must be disabled for the input port.
In WBM: System > Ports > Configuration > Unicast MAC Learning
In CLI: no unicast mac learning
-

RSPAN

With RSPAN (Remote Switched Port Analyzer) you can forward the data traffic of a mirroring session to the monitor port via a VLAN. On the RSPAN VLAN, the mirrored data traffic is not disturbed by other data. For problem-free function of RSPAN, automatic learning of Unicast addresses must be disabled at all affected ports or for the entire RSPAN VLAN.

Frames addressed directly to the monitoring source switch cannot be mirrored on the RSPAN destination port.



ERTM

Alternatively, the mirrored traffic can be forwarded using Encapsulated Remote Traffic Mirroring (ERTM) to a connected device on which an installed packet analyzer/sniffer is accessible via an IP address. ERTM encapsulates mirrored traffic with MAC, IP and GRE headers and forwards it in a Layer 3 network via a GRE tunnel. Encapsulated traffic is forwarded like normal Layer 3 traffic to the analyzer, which decapsulates the traffic as needed before analysis.

5.6 SNMP

Introduction

With the aid of the Simple Network Management Protocol (SNMP), you monitor and control network components from a central station, for example routers or switches. SNMP controls the communication between the monitored devices and the monitoring station.

Tasks of SNMP:

- Monitoring of network components
- Remote control and remote parameter assignment of network components
- Error detection and error notification

In versions v1 and v2c, SNMP has no security mechanisms. Each user in the network can access data and also change parameter assignments using suitable software.

For the simple control of access rights without security aspects, community strings are used.

The community string is transferred along with the query. If the community string is correct, the SNMP agent responds and sends the requested data. If the community string is not correct, the SNMP agent discards the query. Define different community strings for read and write permissions. The community strings are transferred in plain text.

Standard values of the community strings:

- public
has only read permissions
- private
has read and write permissions

Note

Because the SNMP community strings are used for access protection, do not use the standard values "public" or "private". Change these values following the initial commissioning.

Further simple protection mechanisms at the device level:

- Allowed Host
The IP addresses of the monitoring systems are known to the monitored system.
- Read Only
If you assign "Read Only" to a monitored device, monitoring stations can only read out data but cannot modify it.

SNMP data packets are not encrypted and can easily be read by others.

The central station is also known as the management station. An SNMP agent is installed on the devices to be monitored with which the management station exchanges data.

The management station sends data packets of the following type:

- GET
Request a data record from the SNMP agent
- GETNEXT
Calls up the next data record.
- GETBULK (available as of SNMPv2c)
Requests multiple data records at once, for example several rows of a table.
- SET
Contains parameter assignment data for the relevant device.

The SNMP agent sends data packets of the following type:

- RESPONSE
The SNMP agent returns the data requested by the manager.
- TRAP
If a certain event occurs, the SNMP agent itself sends traps.
- INFORM
Like a trap except that it is acknowledged by the receiver.

SNMPv1/v2c/v3 use UDP (User Datagram Protocol) and use the UDP ports 161 and 162. The data is described in a Management Information Base (MIB).

SNMPv3

Compared with the previous versions SNMPv1 and SNMPv2c, SNMPv3 introduces an extensive security concept.

SNMPv3 supports:

- Fully encrypted user authentication
- Encryption of the entire data traffic
- Access control of the MIB objects at the user/group level

5.7 Quality of Service

Quality of Service (QoS) is a method to allow efficient use of the existing bandwidth in a network.

QoS is implemented by prioritization of the data traffic. Incoming frames are sorted into a Queue according to a certain prioritization and further processed. This gives certain frames priority.

The different QoS methods influence each other and are therefore taken into account in the following order:

1. The switch first checks whether the frame contains a VLAN tag.
→ If the 1st condition is met, the switch checks the settings for the priority on the "General (Page 293)" page. The switch checks whether a value other than "Do not force" is set for the priority.
If the priority is set the switch sorts the frame into a queue according to the assignment on page "CoS queue mapping (Page 285)".
2. If the 1st condition is also not met, the frames are further processed according to the Trust mode. You configure the Trust mode on the page "QoS Trust (Page 289)".

5.8 NAT/NAPT

Note

NAT/NAPT is possible only on layer 3 of the ISO/OSI reference model. To use the NAT function, the networks must use the IP protocol.

When using the ISO protocol that operates at layer 2, it is not possible to use NAT.

With Network Address Translation (NAT), IP subnets are divided into "Inside" and "Outside". The division is from the perspective of a NAT interface. All networks that can be reached via the NAT interface itself count as "Outside" for this interface. All networks that can be reached via other IP interfaces of the same device count as "Inside" for the NAT interface.

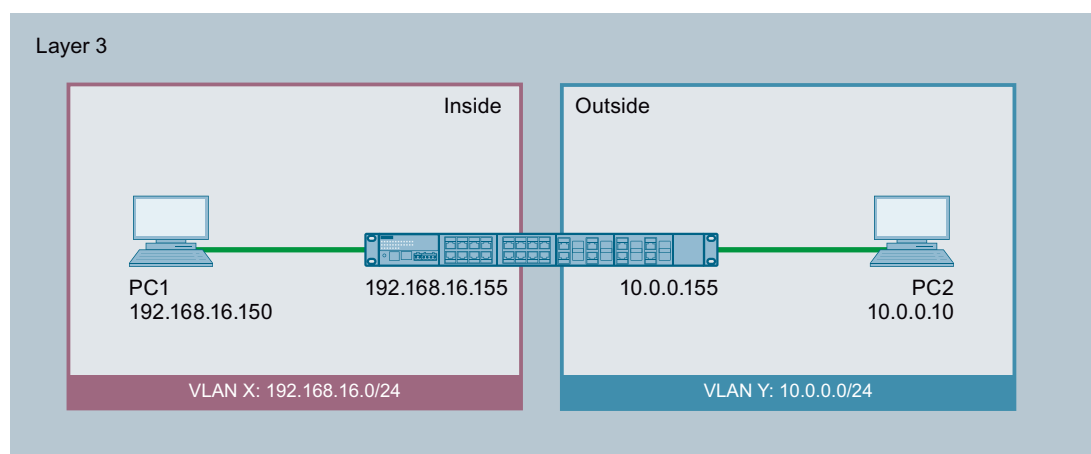
if there is routing via a NAT interface, the source or destination IP addresses of the transferred data packets are changed at the transition between "Inside" and "Outside". Whether the source or destination IP address is changed depends on the communication direction. It is always the IP address of the communications node that is located "Inside" that

is adapted. Depending on the perspective, the IP address of a communications node is always designated as "Local" or "Global".

		Perspective	
		Local	Global
Position	Inside	An actual IP address that is assigned to a device in the internal network. This address cannot be reached from the external network.	An IP address at which an internal device can be reached from the external network.
	Outside	An actual IP address that is assigned to a device in the external network. Since only "Inside" addresses are converted, there is no distinction made between outside local and outside global.	

Example

In the example two IP subnets are connected together via an IE switch. The division is from the perspective of the NAT interface 10.0.0.155. The communication of PC2 with PC1 is implemented via NAT/NAPT.



The actual IP address of PC1 (inside local) is implemented statically with NAT. For PC2, PC1 can be reached at the inside global address.

		Perspective	
		Local	Global
Position	Inside	192.168.16.150	10.0.0.7
	Outside	10.0.0.10	

The actual IP address of PC1 (inside local) is implemented with NAPT (Network Address and Port Translation).. For PC2, PC1 can be reached at the inside global address.

		Perspective	
		Local	Global
Position	Inside	192.168.16.150:80	10.0.0.7:80
	Outside	10.0.0.10:1660	

Computing capacity

Due to the load limitation of the CPU packet receipt of the device is limited to 300 packets a second. This corresponds to a maximum data through of 1.7 Mbps. This load limitation does not apply per interface but generally for all packets going the CPU.

The entire NAT communication runs via the CPU and therefore represents competition for IP communication going to the CPU, e.g. WBM and Telnet.

Note that a large part of the computing capacity is occupied if you use NAT. This can slow down access via Telnet or WBM.

NAT

With Network Address Translation (NAT), the IP address in a data packet is replaced by another. NAT is normally used on a gateway between an internal network and an external network.

With source NAT, the inside local source address of an IP packet from a device in the internal network is rewritten by a NAT device to an inside global address at the gateway.

With destination NAT, the inside global destination address of an IP packet from a device in the external network is rewritten by a NAT device to an inside local address at the gateway.

To translate the internal into the external IP address and back, the NAT device maintains a translation list. The address assignment can be dynamic or static. You configure NAT in "Layer 3 (IPv4) > NAT (Page 388)".

NAPT

In "Network Address Port Translation" (NAPT), several internal IP addresses are translated into the same external IP address. To identify the individual nodes, the port of the internal device is also stored in the translation list of the NAT device and translated for the external address.

If several internal devices send a query to the same external destination IP address via the NAT device, the NAT device enters its own external source IP address in the header of these forwarded frames. Since the forwarded frames have the same external source IP address, the NAT device assigns the frames to the devices using a different port number.

If a device from the external network wants to use a service in the internal network, the translation list for the static address assignment needs to be configured. You configure NAPT in "Layer 3 (IPv4) > NAT > NAPT (Page 393)".

NAT/NAPT and IP routing

You can enable NAT/NAPT and IP routing at the same time. In this case, you need to regulate the reachability of internal addresses from external networks with ACL rules.

Configuring with Web Based Management

6.1 Web Based Management

To access Web Based Management (WBM) of the device, make a remote connection between a client PC and a device via the network. The device has an integrated HTTPS server for the WBM. When you address a device using an Internet browser, it returns HTML pages to the client PC depending on the user input.

Requirements

- The device has an IP address.

Note

Assign an IP address to the device using DHCP or SINEC PNI.

- There is a network connection between the device and the client PC.
- The network settings of the device and of the client PC match.

Note

You can use a ping to check whether a connection exists and communication is possible.

- Access via HTTP(S) is activated on the device.
- An Internet browser is available on the client PC.
- JavaScript is activated in the Internet browser.
- The Internet browser must not be configured in such a way that it reloads the page from the server each time the page is accessed. The updating of the dynamic content of the page is ensured by other mechanisms.
- If you are using a firewall, enable the corresponding ports.
 - For access using HTTPS: TCP port 443
 - For access using HTTP: TCP port 80

WBM display

The display of the WBM was tested with the following desktop Internet browsers:

- Microsoft Edge
- Mozilla Firefox ESR
- Google Chrome

The WBM is tested with the current version of the Internet browser available at the time of firmware release.

6.2 Login

Establishing a connection to a device

Follow the steps below to establish a connection to a device using an Internet browser:

1. There is a connection between the device and the Admin PC. With the ping command, you can check whether or not a device can be reached.
2. In the address field of the web browser, enter "https://" followed by the IP address of the device to be configured or its URL, e.g. https://192.168.16.178.
Access via HTTPS is enabled as default.

Note

Information on the security certificate

Because the device can only be administered using encrypted access, it is delivered with a self-signed certificate. If certificates with signatures that the operating system does not know are used, a security message is displayed. You can display the certificate.

A message relating to the security certificate appears. Acknowledge this message and continue loading the page.

If you use a port other than the standard port, enter a colon ":" as separator between the IP address and the port number.

Example: https://192.168.16.178:49152

You change the port in "System > Configuration".

3. If there is a connection to the device, the login page of Web Based Management (WBM) is displayed.
If you wish to access the WBM via a non-secure HTTP connection, activate the HTTP server under "System > Configuration". At the next login, click on the link "Switch to insecure HTTP" on the login page or enter "http://" and the IP address of the device in the address box of the web browser.

Changing the language

1. From the drop-down list at the top right, select the language version of the WBM pages.
2. Click the "Go" button to change to the selected language.

Note

Available languages

In this version German and English are available.

Personalizing the login page

You can show an additional text on the login page.

1. Create a txt file that contains the desired text or the ASCII type. With ASCII type, pictograms, e.g. the Siemens company logo, are displayed based on the available characters. Up to 50 text lines with 255 characters each including spaces are supported.

Note

The use of the following special characters is not supported:

- Backslash (\)
 - Question mark (?)
 - Tabs: Use spaces instead of tabs
-

2. Load the text file into the device using "System > Load&Save". To do so, use the "Upload" button in the table row "LoginWelcomeMessage" regardless of the protocol used.
3. Log out. The configured text is shown below the credentials on the login page.

Logging in to WBM

You have the following options for logging in via HTTPS. You either use the login option in the center of the browser window or the login option in the upper left area of the browser window. The following steps apply, whichever of the above options you choose.

1. "Name" input box:
 - When you log in for the first time or following a "Restore Factory Defaults and Restart", enter the user preset in the factory "admin".
With this user account, you can change the settings of the device (read and write access to the configuration data).
 - Enter the user name of the created user account. You configure local user accounts and roles in "Security > Users".
2. "Password" input box:
 - When you log in for the first time or following a "Restore Factory Defaults and Restart", enter the password of the default user preset in the factory "admin": "admin".
 - Enter the password of the relevant user account.

- Click the "Login" button or confirm your input with "Enter".

Note

When you log in for the first time or following a "Restore Factory Defaults and Restart", you can rename the user preset in the factory "admin" once. Afterwards, renaming "admin" is no longer possible. Enter the new name in the corresponding input box.

When you log in for the first time or following a "Restore Factory Defaults and Restart", you are prompted to change the password on the following page:

The new password must meet the password policy "High":

- Password length: At least 8 characters, maximum 128 characters
- At least 1 uppercase letter
- At least 1 special character (special characters | § ? " ; : ß \ are not permitted)
- At least 1 number

You need to repeat the password as confirmation. The password entries must match.

- Click the "Set Values" button to complete the action.
The changes take immediate effect. Access via DCP is write-protected after the admin password is changed. The network parameters can be read with SINEC PNI or with "DCP Discovery" but cannot be changed.

Once you have logged in successfully, the start page appears.

Protection from brute force attacks

To protect against brute force attacks, login to the device is denied for a user or for the IP address of a user after multiple failed login attempts. By default, the number of login attempts is preset to 12 per user and 10 per IP address. The wait time for which the page is locked for new login attempts increases after each invalid login attempt. You can change these settings on the page "Security > Brute Force Prevention (Page 501)".

6.3 The "Information" menu

6.3.1 Start page

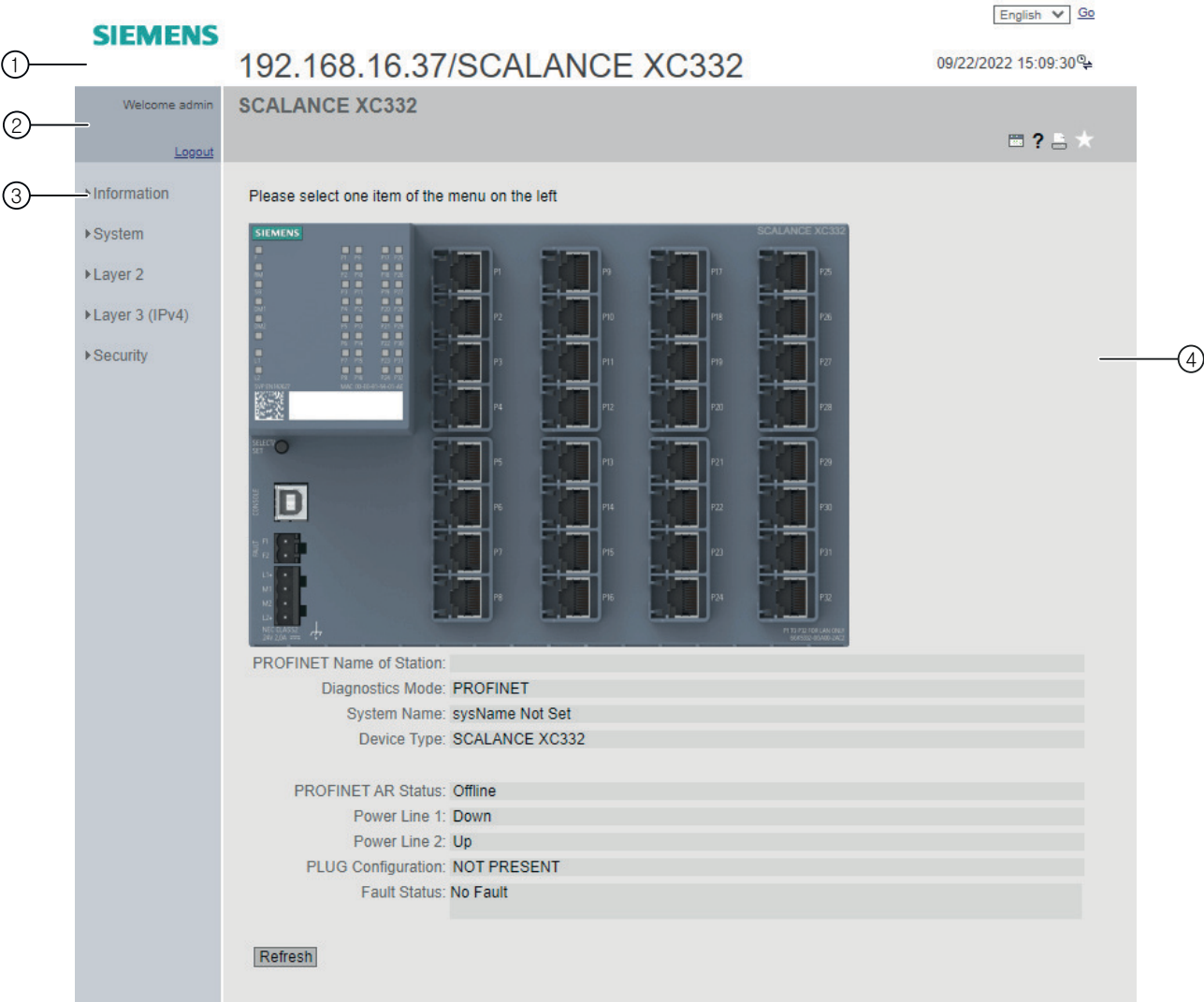
View of the Start page

When you enter the IP address of the device, the start page is displayed after a successful login. You cannot configure anything on this page.

General layout of the WBM pages

The following areas are generally available on every WBM page:

- Selection area (1): Top area
- Display area (2): Top area
- Navigation area (3): Left-hand area
- Content area (4): Middle area






Selection area (1)

The following is available in the selection area:

- Logo of Siemens AG
When you click on the logo, you arrive at the Internet page of the corresponding basic device in Siemens Industry Online Support.
- Display of: "System Location / System Name"
 - "System location" contains the location of the device.
With the settings when the device ships, the IP address of the device is displayed.
 - "System name" is the device name.
With the settings when the device ships, the device type is displayed.




You can change the content of this display with "System > General > Device".

- Drop-down list for language selection
- System date and system time with status display
You can change the content of this display under "System > System Time".
If the system time is not set, the status is . If the system time is configured, but the system time cannot be synchronized, a yellow warning triangle  can be seen. Check whether the time server can be reached. If necessary adapt your configuration. If the system time is set and/or can be synchronized, the status is .

Display area (2)

In the upper part of the display area, you can see name of the currently logged in user and the full title of the currently selected menu item.





In the lower part of the display area, you will find the following:

- **Logging out**
You can log out from any WBM page by clicking the "Logout" link.
- **LED simulation** 
Each device has one or more LEDs that provide information on the operating state of the device. Depending on its location, direct access to the device may not always be possible. Web Based Management therefore displays simulated LEDs. Unused connectors are displayed as gray LEDs. The meaning of the LED displays is described in the operating instructions.
If you click this button, you open the window for the LED simulation. You can show this window during a change of menu and move it as necessary. To close the LED simulation, click the close button in the LED simulation window.
- **Help** 
When you click this button, the help page of the currently selected menu item is opened in a new browser window. The help page contains a description of the content area. Under certain circumstances, options are described that are not available on the device.
On every search page, there is an input box for the search function at the top edge. In this input box, enter a term for which you need additional information and start the search by pressing Enter. A dialog box displays a list of WBM pages that contain the term searched for. The corresponding WBM page is opened in a new tab of the browser after clicking a list element.
- **Print** 
If you click this button, a popup window opens. The popup window contains a view of the page content optimized for printers.

Note

Printing larger tables

If you want to print large tables, please use the "Print preview" function of your Internet browser.

- **Favorites**
When the product ships, the button is disabled on all pages .
If you click this button, the symbol  changes and the currently open page or currently open tab is marked as favorite. Once you have enabled the button once, the navigation area is divided into two tabs. The first tab "Menu" contains all the available menus as previously. The second tab "Favorites" contains all the pages/tabs that you selected as favorites. On the "Favorites" tab the pages/tabs are arranged according to the structure in the "Menu" tab. If you disable all the favorites you have created, the "Favorites" tab is removed again. To do this, click the  button on the relevant pages/tabs.
You can save, upload and delete the favorites configuration of a device on the "System > Load&Save" page using HTTP or TFTP.
- **Fault **
The button is only visible in the fault state and flashes if the device has detected a fault. When you click this button, you get to the "Information > Faults" page, where you will find the description of the error that has occurred.

Navigation area (3)

In the navigation area, you have various menus available. Click the individual menus to display the submenu. The submenus contain pages on which information is available or with which you can create configurations. These pages are always displayed in the content area.

If you have created favorites, the navigation area is divided into two tabs: "Menu" and "Favorites".

Content area (4)

The content area shows a graphic of the device. The graphic always shows the device whose WBM you have called up.

The following is displayed below the device graphic:

- **PROFINET Name of Station**
Shows the PROFINET device name.
- **Diagnostics Mode**
Shows whether EtherNet/IP or PROFINET IO is enabled.
- **System Name**
Shows the name of the device.
- **Device Type**
Shows the type designation of the device.

- **PROFINET AR Status**
Shows the PROFINET application relation status.
 - Online
There is a connection to a PROFINET controller. The PROFINET controller has downloaded its configuration data to the device. The device can send status data to the PROFINET controller.
In this status, the parameters set via the PROFINET controller cannot be configured on the device.
 - Offline
There is no connection to a PROFINET controller.
- **Power Supply 1 / Power Supply 2**
 - Up
Power supply 1 or 2 is applied
 - Down:
Power supply 1 or 2 is not applied or is below the permitted voltage.
- **PLUG Configuration**
Shows the status of the configuration data on the PLUG, refer to the section "System > PLUG > Configuration".
- **Fault Status**
Shows the fault status of the device.

Buttons you require often

The pages of the WBM contain the following standard buttons:

- **Refresh the display with "Refresh"**
Web Based Management pages that display current parameters have a "Refresh" button at the lower edge of the page. Click this button to request up-to-date information from the device for the current page.

Note

If you click the "Refresh" button, before you have transferred your configuration changes to the device using the "Set Values" button, your changes will be deleted and the previous configuration will be loaded from the device and displayed here.

- **Save entries with "Set Values"**
Pages in which you can make configuration settings have a "Set Values" button at the lower edge. The button only becomes active if you change at least one value on the page. Click this button to save the configuration data you have entered on the device. Once you have saved, the button becomes inactive again.

Note

Changing configuration data is possible only with the "admin" role.

- **Create entries with "Create"**
Pages in which you can make new entries have a "Create" button at the lower edge. Click this button to create a new entry. When you create an entry the page is updated.

- **Delete entries with "Delete"**

Pages in which you can delete entries have a "Delete" button at the lower edge. Click this button to delete the previously selected entries from the device memory. When you delete an entry the page is updated.
- **Page down with "Next"**

On pages with a lot of data records the number of data records that can be displayed on a page is limited. Click the "Next" button to page down through the data records.
- **Page back with "Prev"**

On pages with a lot of data records the number of data records that can be displayed on a page is limited. Click the "Prev" button to page back through the data records.
- **Delete the display with "Clear"**

In pages with sequence logs, you can delete all table entries at the same time regardless of whether filters are selected. The display is cleared in this process. The restart counter is only reset after you have restored the device to the factory settings and restarted the device. Click the "Clear" button to completely delete the data record.
- **Button "Show all"**

You can show all entries in pages with a large number of data records. Click "Show all" to display all entries on the page. Note that displaying all messages can take some time.
- **Drop-down list for page change**

In pages with a large number of data records, you can navigate to the desired page. From the drop-down list, select the relevant page to display it.
- **"Reset Counters" button**

Click "Reset Counters" to reset all counters. The counters are also reset by a restart.

Messages

If you have enabled the "Automatic Save" mode and you change a parameter the following message appears in the display area "Changes will be saved automatically in x seconds. Press 'Write Startup Config' to save the changes immediately."

Note

Interrupting the save

Saving starts only after the timer in the message has elapsed. During the save, the message "Saving configuration data in progress. Please do not switch off the device" is displayed. How long saving takes depends on the device.

- Do not switch off the device immediately after the timer has elapsed.
-

6.3.2 Versions

Versions of hardware and software

This page shows the versions of the hardware and software of the device. You cannot configure anything on this page.

Version Information			
Hardware	Name	Revision	Order ID
Basic Device	SCALANCE XC324-4	1	6GK5 328-4TS00-2AC2
Software	Description	Version	Date
Firmware	SCALANCE XC300 Firmware	T01.00.00.00_08.01.51	09/26/2022 19:14:57
Bootloader	SCALANCE XC300 Bootloader	T01.00.00.00_01.01.01	09/02/2022 19:14:57
Firmware_Running	Current running Firmware	T01.00.00.00_08.01.51	09/26/2022 19:14:57

Description of the displayed values

Table 1 has the following columns:

- **Hardware**
 - Basic Device
Shows the basic device.
 - Px.x
x.x designates the port in which an SFP module is inserted.
- **Name**
Shows the name of the device or module.
- **Revision**
Shows the hardware version of the device.
- **Order ID**
Shows the article number of the device or described module.

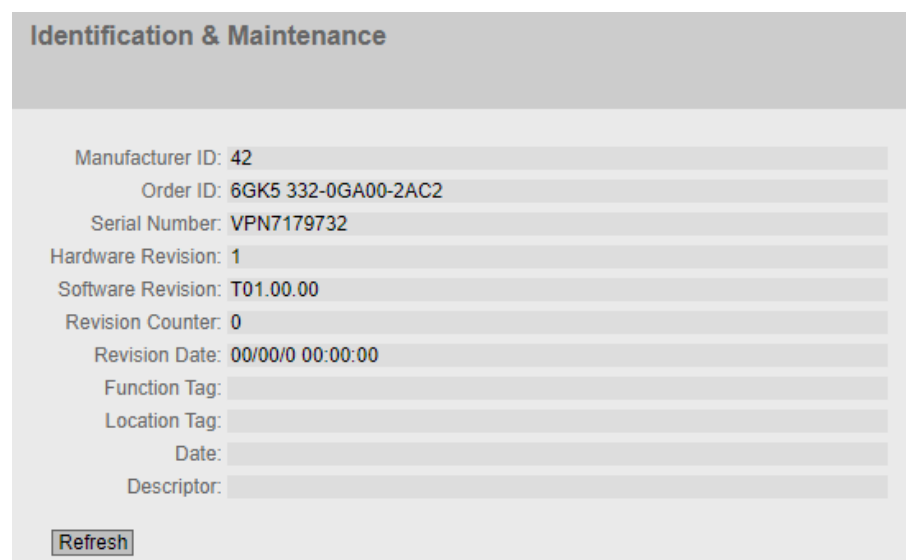
Table 2 has the following columns:

- **Software**
 - Firmware
Shows the current firmware version. If a new firmware file was downloaded and the device has not yet restarted, the firmware version of the downloaded firmware file is displayed here. After the next restart, the downloaded firmware is activated and used.
 - Bootloader
Shows the version of the boot software stored on the device.
 - Firmware_Running
Shows the firmware version currently being used on the device.
- **Description**
Shows the short description of the software.
- **Version**
Shows the version number of the software version.
- **Date**
Shows the date on which the software version was created.

6.3.3 I&M

Identification and Maintenance data

This page contains information about device-specific vendor and maintenance data such as the order number, serial number, version number etc. You cannot configure anything on this page.



The screenshot shows a web interface titled "Identification & Maintenance". It displays several fields with their corresponding values:

Manufacturer ID:	42
Order ID:	6GK5 332-0GA00-2AC2
Serial Number:	VPN7179732
Hardware Revision:	1
Software Revision:	T01.00.00
Revision Counter:	0
Revision Date:	00/00/0 00:00:00
Function Tag:	
Location Tag:	
Date:	
Descriptor:	

At the bottom left of the form, there is a "Refresh" button.

Description of the displayed values

The table has the following rows:

- **Manufacturer ID**
Shows the manufacturer ID.
- **Order ID**
Shows the order number.
- **Serial Number**
Shows the serial number.
- **Hardware Revision**
Shows the hardware version.
- **Software version**
Shows the software version.
- **Revision Counter**
Regardless of a version change, this box always displays the value "0".
- **Revision Date**
Shows the date and time of the last revision.
- **Function tag**
Shows the function tag (plant designation) of the device. The plant designation (HID) is created during configuration of the device with HW Config of STEP 7.
- **Location tag**
Shows the location tag of the device. The location identifier (LID) is created during configuration of the device with HW Config of STEP 7.
- **Date**
Shows the date created during configuration of the device with HW Config of STEP 7.
- **Descriptor**
Shows the description created during configuration of the device with HW Config of STEP 7.

6.3.4 ARP table

Assignment of MAC address and IPv4 address

With the Address Resolution Protocol (ARP), there is a unique assignment of MAC address to IPv4 address. This assignment is kept by each network node in its own separate ARP table. The WBM page shows the ARP table of the device.

Interface	MAC Address	IP Address	Media Type
vlan1	68-05-ca-19-40-bb	192.168.16.1	Dynamic

1 entry.

Description of the displayed values

The table has the following columns:

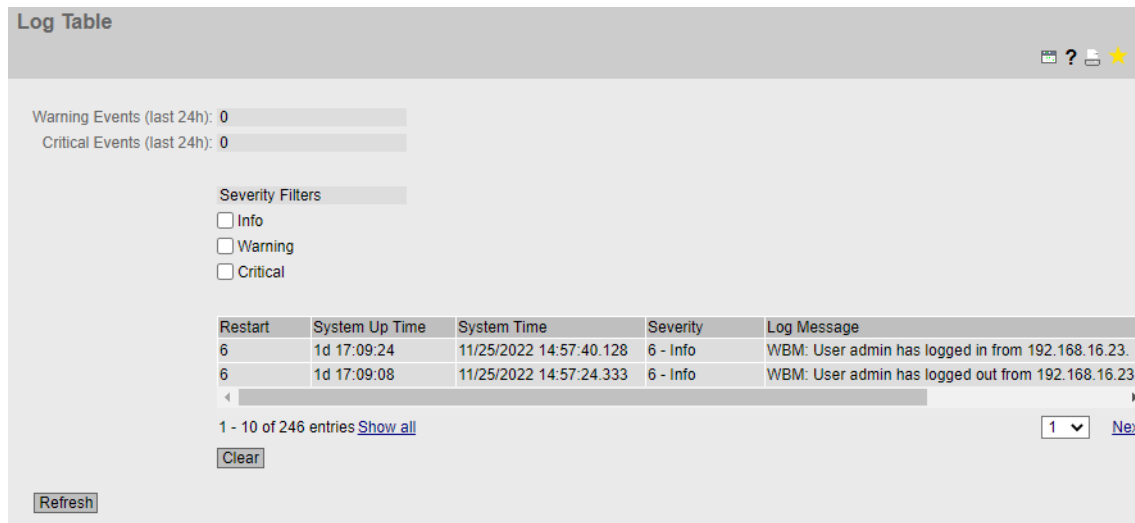
- **Interface**
Shows the interface via which the row entry was learnt.
- **MAC Address**
Shows the MAC address of the destination or source device.
- **IP Address**
Shows the IPv4 address of the destination device.
- **Media Type**
Shows the type of connection.
 - Dynamic
The device recognized the address data automatically.
 - Static
The addresses were entered as static addresses.

6.3.5 Log Table

Logging events

The device allows you to log occurring events, some of which you can specify on the page of the "System > Events" menu. This, for example, allows you to record when an authentication attempt failed or when the connection status of a port has changed.

The content of the events log table is retained even when the device is turned off.



Description of the displayed values

The page contains the following boxes:

- **'Warning' event (last 24 hr)**
Displays how many events of the "Warning" category have occurred in the last 24 hours.
- **'Critical' event (last 24 hr)**
Displays how many events of the "Critical" category have occurred in the last 24 hours.

Severity Filters

You can filter the entries in the table according to severity. Select the required entries in the check boxes above the table.

- **Info**
When this parameter is enabled, all entries of the category "Info" are displayed.
- **Warning**
When this parameter is enabled, all entries of the category "Warning" are displayed.
- **Critical**
When this parameter is enabled, all entries of the category "Critical" are displayed.

To display all entries, select either all of them or leave the check boxes empty.

The table has the following columns:

- **Restart**
Counts the number of restarts since you last reset to factory settings and shows the device restart after which the corresponding event occurred.
- **System Up Time**
Shows the time the device has been running since the last restart when the described event occurred.
- **System Time**
Shows the date and time at which the event occurred.

- **Severity**
Sorting of the entry into the categories above.
- **Log Message**
Displays a brief description of the event that has occurred.

Note

The number of entries in this table is restricted to 1200. The table can contain 400 entries for each severity. When this number is reached, the oldest entries of the relevant severity are discarded. The table remains permanently in memory.

6.3.6 Faults

Error status

if an error occurs, it is shown on this page. In addition, the red "Error" button flashes on every WBM page in the upper part of the display area. On the device, errors are indicated by red fault LED lighting up.

Internal errors of the device and errors that you configure on the following pages are indicated:

- "System > Events"
- "System > Fault Monitoring"

The calculation of the time of an error always begins after the last system start. If there are no errors present, the fault LED switches off.

The screenshot displays the 'Faults' page with the following content:

- Header: **Faults**
- Status: No. of Signaled Faults: 1
- Button: **Reset Counters**
- Table:

Fault Time	Fault Description	Clear Fault State
16s	Link down on P0.1.	Clear Fault State
17s	Warm start performed.	Clear Fault State
- Button: **Refresh**

Description

- **No. of Signaled Faults**
Indicates how often the fault LED lit up and not how many faults occurred.

6.3 The "Information" menu

The table contains the following columns:

- **Fault Time**
Shows the time the device has been running since the last system restart when the described error/fault occurred.
- **Fault Description**
Displays a brief description of the fault/error that has occurred.
- **Clear Fault State**
Some faults can be acknowledged and thus removed from the fault list, e.g. a fault of the event "Cold/Warm Start". If the "Clear Fault State" button is enabled, you can delete the error.

6.3.7 Redundancy

6.3.7.1 Spanning Tree

Introduction

The page shows the current information about the spanning tree and the settings of the root bridge.

Spanning Tree

Spanning Tree | Ring Redundancy | Standby | MRP Interconnection

Spanning Tree Mode: MSTP
Instance ID: 0
Bridge Priority: 32768
Bridge Address: d4-f5-27-cc-e5-80
Root Priority: 32768
Root Address: d4-f5-27-5a-1c-3e
Root Cost: 20000
Regional Root Priority: 32768
Regional Root Address: d4-f5-27-cc-e5-80
Regional Root Cost: 0

Port	Role	State	Oper. Version	Priority	Path Cost	Edge Type	P.T.P. Type
P0.9	Root	Forwarding	MSTP	128	20000	No Edge Port	P.T.P

Refresh

Description

The following fields are displayed:

- **Spanning Tree Mode**
Shows the set mode. You specify the mode in "Layer 2 > Configuration" and in "Layer 2 > Spanning Tree > General".
The following values are possible:
 - ' '
 - STP
 - RSTP
 - MSTP
- **Instance ID**
Shows the number of the instance. The parameter depends on the configured mode.
- **Bridge Priority / Root Priority**
Which device becomes the root bridge is decided by the bridge priority. The bridge with the highest priority (in other words, with the lowest value for this parameter) becomes the root bridge. If several devices in a network have the same priority, the device whose MAC address has the lowest numeric value will become the root bridge. The two parameters, bridge priority and MAC address, together form the bridge identifier. Since the root bridge manages all path changes, it should be located as centrally as possible due to the delay of the frames. The value for the bridge priority is a whole multiple of 4096 with a range of values from 0 to 32768.
- **Bridge address / root address**
The bridge address shows the MAC address of the device and the root address shows the MAC address of the root switch.
- **Root Cost**
Shows the path costs from the device to the root bridge.
- **Regional root priority** (available only with MSTP)
For a description, see Bridge priority / Root priority.
- **Regional root address** (available only with MSTP)
Shows the MAC address of the device.
- **Regional Root Cost** (available only with MSTP)
Shows the path costs from the regional root bridge to the root bridge.

The table has the following columns:

- **Port**
Shows the port via which the device communicates. The port is made up of the module number and the port number, for example port 0.1 is module 0, port 1.
- **Role**
Shows the status of the port. The following values are possible:
 - Disabled
The port was removed manually from the spanning tree and will no longer be taken into account by the spanning tree.
 - Designated
The port with the most favorable connection to a lower-level LAN segment. When RSTP starts, switches evaluate connections based on BPDUs. The most favorable connections are then used. Generally, all root bridge RSTP ports are Designated Ports because they are set to forwarding. The path costs and the port ID of the respective port determine which ports of the remaining nodes are selected as Designated Ports.
 - Alternate
The port with an alternative route to a network segment.
 - Backup
The port on which BPDUs from a port of the same switch that has a better connection to the root are received.
 - Root
The port that provides the best route to the root bridge.
 - Master
This port points to a root bridge located outside the MST region.
 - RSTP+
Ring ports of devices in which RSTP+ is enabled.
- **Status**
Displays the current status of the port. The values are only displayed. The parameter depends on the configured protocol. The following values are possible:
 - Discarding
The port receives BPDU frames. Other incoming or outgoing frames are discarded.
 - Listening
The port receives and sends BPDU frames. The port is involved in the spanning tree algorithm. Other outgoing and incoming frames are discarded.
 - Learning
The port actively learns the topology; in other words, the node addresses. Other outgoing and incoming frames are discarded.
 - Forwarding
Following the reconfiguration time, the port is active in the network. The port receives and sends data frames.
- **Oper. Version**
Shows the compatibility mode of Spanning Tree used by the port.

- **Priority**

If the path calculated by the spanning tree is possible over several ports of a device, the port with the highest priority (in other words the lowest value for this parameter) is selected. A value between 0 and 240 can be entered for the priority in steps of 16. If you enter a value that cannot be divided by 16, the value is automatically adapted. The default is 128.
- **Path Cost**

This parameter is used to calculate the path that will be selected. The path with the lowest value is selected. If several ports of a device have the same value, the port with the lowest port number is selected.

The calculation of the path costs is based largely on the transmission speed. The higher the achievable transmission speed is, the lower the value of the path costs.

Typical values for path costs with rapid spanning tree:

 - 10,000 Mbps = 2,000
 - 1000 Mbps = 20,000
 - 100 Mbps = 200,000
 - 10 Mbps = 2,000,000

You configure the "Cost Calc." on the pages "Layer 2 > Spanning Tree > CIST Port" and "Layer 2 > Spanning Tree > MST Port".
- **Edge Type**

Shows the type of the connection. The following values are possible:

 - Edge Port
There is an end device at this port.
 - No Edge Port
There is a spanning tree device at this port.
- **P.t.P Type**

Shows the type of the point-to-point link. The following values are possible:

 - P.t.P.
With half duplex, a point-to-point link is assumed.
 - Shared Media
With a full duplex connection, a point-to-point link is not assumed.

Note

Point-to-point connection means a direct connection between two devices. A shared media connection is, for example, a connection to a hub.

6.3.7.2 VRRP Statistics

Introduction

This page shows the statistics of the VRRP protocol and all configured virtual routers.

Virtual Router Redundancy Protocol (VRRP) Statistics

Spanning Tree | **VRRP Statistics** | VRRPv3 Statistics | Ring Redundancy | Standby | Link Check | MRP Interconnection

VRID Errors: 0
Version Errors: 0
Checksum Errors: 0

Interface	VRID	Become Master	Advertisements Received	Advertisements Interval Errors	IP TTL Errors	Prio 0 received
vlan1	34	0	0	0	0	0

< [Progress Bar] >

Reset Counters

Refresh

Continuation of table

Virtual Router Redundancy Protocol (VRRP) Statistics

Spanning Tree | VRRP Statistics | VRRPv3 Statistics | Ring Redundancy | Standby | Link Check | **MRP Interconnection**

VRID Errors: 0
Version Errors: 0
Checksum Errors: 0

Prio 0 sent	Invalid Type	Address List Errors	Invalid Auth. Type	Auth. Type Mismatch	Packet Length Errors
0	0	0	0	0	0

< [Progress Bar] >

Reset Counters

Refresh

Description of the displayed values

The following boxes are displayed:

- **VRID Errors**
Shows how many VRRP packets containing an unsupported VRID were received.
- **Version Errors**
Shows how many VRRP packets containing an invalid version number were received.
- **Checksum Errors**
Shows how many VRRP packets containing an invalid checksum were received.

The table has the following columns:

- **Interface**
Interface to which the settings relate.
- **VRID**
Shows the ID of the virtual router.
Valid values are 1 to 255.
- **Become Master**
Shows how often this virtual router changed to the "Master" status.
- **Advertisements Received**
Shows how often a VRRP packet was received that contained a bad address list.
- **Advertisement Interval Errors**
Shows how many bad VRRP packets were received whose interval does not match the value set locally.
- **IP TTL Errors**
Shows how many bad VRRP packets were received whose TTL (Time to live) value in the IP header is incorrect.
- **Prio 0 received**
Shows how many VRRP packets with priority 0 were received. VRRP packets with priority 0 are sent when a master router is shut down. These packets allow a fast handover to the relevant backup router.
- **Prio 0 sent**
Shows how many VRRP packets with priority 0 were sent. Packets with priority 0 are sent when a master router is shut down. These packets allow a fast handover to the relevant backup router.
- **Invalid Type**
Shows how many bad VRRP packets were received whose authentication type was not type 0. Type 0 means "no authentication".
- **Address List Errors**
Shows how many bad VRRP packets were received whose address list does not match the locally configured list.
- **Invalid Auth. Type**
Shows how many bad VRRP packets were received whose authentication type does not match.
- **Auth. Type Mismatch**
Shows that different authentication types are set.
- **Packet Length Errors**
Shows how many bad VRRP packets were received whose length is not correct.

6.3.7.3 VRRPv3 Statistics

Introduction

This page shows the statistics of the VRRPv3 protocol and all configured virtual routers.

Continuation of table

Advertisements Interval Errors	IP TTL Errors	Prio 0 received	Prio 0 sent	Invalid Type	Address List Errors	Packet Length Errors
0	0	0	1	0	0	0
0	0	0	1	0	0	0

Description of the displayed values

The following boxes are displayed:

- **VRID Errors**
Shows how many VRRPv3 packets containing an unsupported VRID were received.
- **Version Errors**
Shows how many VRRPv3 packets containing an invalid version number were received.
- **Checksum Errors**
Shows how many VRRPv3 packets containing an invalid checksum were received.

The table has the following columns:

- **Interfaces**
Interface to which the settings relate.
- **VRID**
Shows the ID of the virtual router. Valid values are 1 ... 255.
- **Address Type**
Shows the version of the IP protocol.

- **Become Master**
Shows how often this virtual router changed to the "Master" status.
- **Advertisements Received**
Shows how many VRRPv3 packets were received.
- **Advertisement Interval Errors**
Shows how many bad VRRPv3 packets were received whose interval does not match the value set locally.
- **IP TTL Errors**
Shows how many bad VRRPv3 packets were received whose TTL (Time to live) value in the IP header is incorrect.
- **Prio 0 received**
Shows how many VRRPv3 packets with priority 0 were received. VRRPv3 packets with priority 0 are sent when a master router is shut down. These packets allow a fast handover to the relevant backup router.
- **Prio 0 sent**
Shows how many VRRPv3 packets with priority 0 were sent. Packets with priority 0 are sent when a master router is shut down. These packets allow a fast handover to the relevant backup router.
- **Invalid Type**
Shows how many bad VRRPv3 packets were received whose value in the "Type" field of the IP header is invalid.
- **Address List Errors**
Shows how many bad VRRPv3 packets were received whose address list does not match the locally configured list.
- **Packet Length Errors**
Shows how many bad VRRPv3 packets were received whose length is not correct.

6.3.7.4 Ring Redundancy

Information on ring redundancy

On this tab, you obtain information about the status of the device in terms of ring redundancy. The text boxes on this page are read-only. If ring redundancy is not enabled, the table is empty.

Ring Redundancy ? ? ? ?

Spanning Tree | **Ring Redundancy** | **Standby** | **MRP Interconnection**

Ring ID	Domain Name	Admin Role	Oper Role	RM Status	Admin Ring Port 1	Admin Ring Port 2	Oper Ring Port 1	Oper Ring Port 2	No. of Changes to RM Active State	Max. Delay of RM Test Packets[ms]
1	default-mrpdome	Automatic Redur	MRP Auto-Mana	Active	P0.1	P0.2	P0.1	P0.2	1	0

Observer Status: -

[Reset Counters](#)

[Refresh](#)

Description

The table has the following columns:

- **Ring ID**
The ID of the ring.
- **Domain Name**
The name assigned uniquely to each ring.
- **Admin Role**
Ring redundancy mode.
- **Oper. Role**
The role of the device within the ring:
 - HRP Client
The IE switch operates as an HRP client.
 - HRP Manager
The IE switch operates as an HRP manager.
 - MRP Client
The IE switch operates as an MRP client.
 - MRP Manager
The IE switch operates as an MRP manager. The role "MRP Manager" was set for the device via WBM or the role "Manager" via STEP 7.
 - MRP Auto-Manager
The IE switch is operating as an MRP manager. Using WBM or CLI the role "MRP Auto-Manager" or using STEP 7 the role "Manager (Auto)" was set.
- **RM Status**
The "RM Status" column shows whether or not the IE switch is operating as redundancy manager and whether it has opened or closed the ring in this role.
 - Passive
The IE switch is operating as redundancy manager and has opened the ring; in other words, the line of switches connected to the ring ports is operating problem free. The "Passive" status is also displayed if the IE switch is not operating as the redundancy manager (Redundancy manager disabled).
 - Active
The IE switch is operating as redundancy manager and has closed the ring; in other words, the line of switches connected to the ring ports is interrupted (problem). The redundancy manager connects its ring ports through and restores an uninterrupted linear topology.
- **Admin Ring Port 1 and Admin Ring Port 2**
These columns show the ports that were configured as ring ports.
- **Oper. Ring Port 1 and Oper. Ring Port 2**
These columns show the ports that are used as ring ports. If media redundancy in ring topologies is completely disabled, ring ports configured last are displayed.

- **No. of Changes to RM Active State**
Shows how often the device as redundancy manager switched to the active status, i.e. closed the ring.
If the redundancy function is disabled or the device is an "HRP/MRP client", the text "Redundancy manager disabled" appears.
- **Max. Delay of RM Test Packets [ms]**
Shows the maximum delay time of the test frames of the redundancy manager.
If the redundancy function is disabled or the device is an "HRP/MRP client", the text "Redundancy manager disabled" appears.

The following fields are displayed:

- **Observer Status**
Shows the current status of the observer.

Note

The "Reset Counters" button is active when the ring redundancy mode "HRP Manager", "MRP Manager" or "MRP Auto-Manager" is configured.

6.3.7.5 Standby

Information on standby redundancy

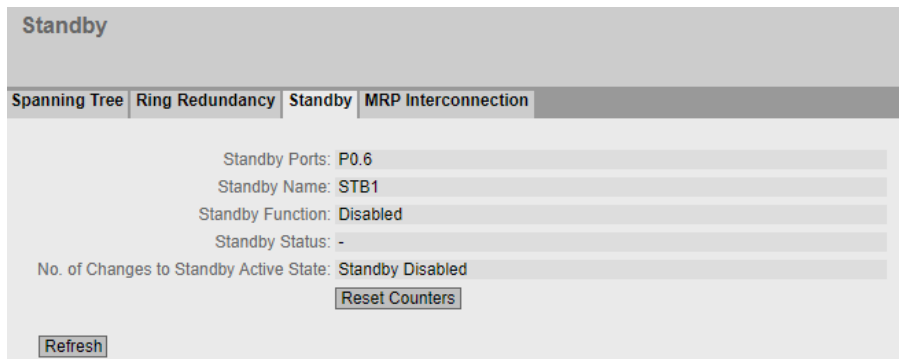
On this tab, you obtain information about the status of the device in terms of standby redundancy. The text boxes on this page are read-only.

Note**Device with the higher MAC address becomes master**

When linking HRP rings redundantly, two devices are always configured as a master/slave pair. This also applies to interrupted HRP rings = linear buses. When operating normally, the device with the higher MAC address adopts the role of master.

This type of assignment is important in particular when a device is replaced. Depending on the MAC addresses, the previous device with the slave function can take over the role of the standby master.

The Standby tab shows the status of the standby function:



Description of the displayed values

The following fields are displayed:

- **Standby ports**
Shows the standby port.
- **Standby Name**
Standby Connection Name
- **Standby Function**
 - Master
The device has a connection to the partner device and is operating as master. In normal operation, the standby port of this device is active.
 - Slave
The device has a connection to the partner device and is operating as slave. In normal operation, the standby port of this device is inactive.
 - Disabled
The standby link is disabled. The device is operating neither as master nor slave. The port configured as a standby port works as a normal port without standby function.
 - Waiting for connection
No connection has yet been established to the partner device. The standby port is inactive. In this case, either the configuration on the partner device is inconsistent (for example incorrect connection name, standby link disabled) or there is a physical fault (for example device failure, link down).
 - Connection lost
The existing connection to the partner device has been lost. In this case, either the configuration on the partner device was modified (for example a different connection name, standby link disabled) or there is a physical fault (for example device failure, link down).

- **Standby Status**
Shows the status of the standby port:
 - Active
The standby port of this device is active; in other words is enabled for frame traffic.
 - Passive
The standby port of this device is inactive; in other words is blocked for frame traffic.
 - "-":
The standby function is disabled.
- **No. of Changes to Standby Active State**
Shows how often the IE switch has changed the standby status from "Passive" to "Active". If the connection of a standby port fails on the standby master, the IE switch changes to the "active" status.
If the standby function is disabled, the text "Standby Disabled" appears in this box.

6.3.7.6 MRP Interconnection

Redundant linking of rings

Interconnection Domain ID	Interconnection Domain Name	Interconnection Port	Port State	Oper. Role/Position	Connection State	Open Count	Open Time
1	MrpIntCon1	P0.4	Not connected	Primary Client	-	0	-

Reset Counters

Refresh

Description

The following fields are displayed:

- **Interconnection Domain ID**
The ID of the MRP Interconnection connection.
- **Interconnection Domain Name**
The name of the MRP Interconnection connection.
- **Interconnection Port**
The port that is used for the MRP Interconnection connection.

- **Port Status**
Shows whether the port is enabled or disabled. Data traffic is possible only over an enabled port. The available options are as follows:
 - Forwarding
The port is in use.
 - Blocked
The port is blocked.
 - Disabled
The port is disabled.
 - Not connected
The port is not connected.
- **Oper. Role/Position**
Shows the role of the device. With the "Client" role, the position of the client is shown in addition. The available options are as follows:
 - Disabled
 - Manager
 - Primary Client
 - Secondary Client
- **Connection Status**
The status of the MRP Interconnection domain. The available options are as follows:
 - Disabled
 - Not defined
 - Open
The redundant connection is not available.
 - Close
The redundant connection is available.
- **Open Count**
Shows how often the "Open" status has occurred since the last counter reset for the MIM. For an MIC, this value is always "0".
- **Open Time**
Time since the last occurrence of the "Open" status. No value is displayed here for an MIC.

6.3.8 Ethernet Statistics

6.3.8.1 Interface Statistics

Interface statistics

The page shows the statistics from the interface table of the Management Information Base (MIB).

Note

The interface statistics specify the total number of received or sent bytes for each port. In contrast, the information for VLAN interfaces only relates to the Layer 3 data traffic of the corresponding interface.

Ethernet Statistics: Interface Statistics

Interface Statistics | Packet Size | Packet Type | Packet Error | History

Total In Errors: 0
Discarded packets (last 24h): 0
Discarded packets (last 7d): 0

	In Octet	Out Octet	In Unicast	In Non-Unicast	Out Unicast	Out Non-Unicast	In Discard	Out Discard	In Errors
P0.1	0	0	0	0	0	0	0	0	0
P0.2	0	0	0	0	0	0	0	0	0
P0.3	0	0	0	0	0	0	0	0	0

Reset Counter

Refresh

Description of the displayed values

The page contains the following boxes:

- **In Errors (total)**
Shows the sum of all received errors.
- **Discarded packets (last 24 hrs)**
Shows the sum of all discarded packets within the last 24 hours.
- **Discarded packets (last 7 days)**
Shows the sum of all discarded packets within the last 7 days.

The table has the following columns:

- **In Octet**
Shows the number of received bytes.
- **Out Octet**
Shows the number of sent bytes.
- **In Unicast**
Shows the number of received unicast frames.

6.3 The "Information" menu

- **In Non Unicast**
Shows the number of received frames that are not of the type unicast.
- **Out Unicast**
Shows the number of sent unicast frames.
- **Out Non Unicast**
Shows the number of sent frames that are not of the type unicast.
- **In Discard**
Shows the number of incoming frames that were discarded.
- **Out Discard**
Shows the number of outgoing frames that were discarded.
- **In Errors**
Shows the number of all possible RX errors, refer to the tab "Packet Error".

6.3.8.2 Packet Size

Frames sorted by length

This page displays how many frames of which length were sent and received at each port. You cannot configure anything on this page.

The displayed values are transferred by RMON.

On the page "Layer 2 > RMON > Statistics", you can set the ports for which values will be displayed.

Ethernet Statistics: Packet Size

Interface Statistics	Packet Size	Packet Type	Packet Error	History		
Port	64	65-127	128-255	256-511	512-1023	1024-max
P0.1	0	0	0	0	0	0
P0.2	0	0	0	0	0	0
P0.3	0	0	0	0	0	0
P0.4	0	0	0	0	0	0

Description of the displayed values

The table has the following columns:

- **Port**
Shows the available ports and link aggregations. The port is made up of the module number and the port number, for example, port 0.1 is module 0, port 1.

Note**Display of frame statistics**

In the statistics relating to frame lengths, note that both incoming and outgoing frames are counted.

- **Frame lengths**
The other columns after the port number contain the absolute numbers of frames according to their frame length.
The following frame lengths are distinguished:
 - 64 bytes
 - 65 - 127 bytes
 - 128 - 255 bytes
 - 256 - 511 bytes
 - 512 - 1023 bytes
 - 1024 - Max.

Note**Data traffic on blocked ports**

For technical reasons, data packets can be indicated on blocked ports.

6.3.8.3 Packet Type

Received frames sorted by Packet Type

This page displays how many frames of the types "Unicast", "Multicast", and "Broadcast" were received at each port. You cannot configure anything on this page.

The displayed values are transferred by RMON.

On the page "Layer 2 > RMON > Statistics", you can set the ports for which values will be displayed.

Ethernet Statistics: Packet Type				
Interface Statistics	Packet Size	Packet Type	Packet Error	History
Port	Unicast	Multicast	Broadcast	
P0.1	0	0	0	
P0.2	0	0	0	
P0.3	0	0	0	
P0.4	0	0	0	

Reset Counter

Refresh

Description of the displayed values

The table has the following columns:

- Port**
 Shows the available ports and link aggregations. The port is made up of the module number and the port number, for example, port 0.1 is module 0, port 1.
- Unicast / Multicast / Broadcast**
 The other columns after the port number contain the absolute numbers of the incoming frames according to their Packet Type "Unicast", "Multicast" and "Broadcast".

6.3.8.4 Packet Error

Received bad frames

This page shows how many bad frames were received per port. You cannot configure anything on this page.

The displayed values are transferred by RMON.

On the page "Layer 2 > RMON > Statistics", you can set the ports for which values will be displayed.

Ethernet Statistics: Packet Error						
Interface Statistics	Packet Size	Packet Type	Packet Error	History		
Port	CRC	Undersize	Oversize	Fragments	Jabbers	Collisions
P0.1	0	0	0	0	0	0
P0.2	0	0	0	0	0	0
P0.3	0	0	0	0	0	0
P0.4	0	0	0	0	0	0

Reset Counter

Refresh

Description of the displayed values

The table has the following columns:

- **Port**
Shows the available ports and link aggregations. The port is made up of the module number and the port number, for example, port 0.1 is module 0, port 1.
- **Error types**
The other columns after the port number contain the absolute numbers of the incoming frames according to their error type.
In the columns of the table, a distinction is made according to the following error types:
 - CRC
Packets whose content does not match the CRC checksum.
 - Undersize
Packets with a length less than 64 bytes.
 - Oversize
Packets discarded because they were too long.
 - Fragments
Packets with a length less than 64 bytes and a bad CRC checksum.
 - Jabbers
VLAN-tagged packets with an incorrect CRC checksum that were discarded because they were too long.
 - Collisions
Collisions that were detected.

6.3.8.5 History

Samples of the statistics

The page shows samples from each port with information from the RMON statistics.

On the page "Layer 2 > RMON > History", you can set the ports for which samples will be taken.

Ethernet History

Interface Statistics
Packet Size
Packet Type
Packet Error
History

Port: P0.1 ▼

Buckets: 24

Interval[s]: 3600

Sample	Sample Time	Unicast	Multicast	Broadcast	CRC	Undersize	Oversize	Fragments	Jabbers	Collisions	Utilization[%]
67	2d 18h 14m 13s	0	0	0	0	0	0	0	0	0	0
68	2d 19h 14m 25s	0	0	0	0	0	0	0	0	0	0
69	2d 20h 14m 37s	0	0	0	0	0	0	0	0	0	0
70	2d 21h 14m 49s	0	0	0	0	0	0	0	0	0	0
71	2d 22h 15m 1s	0	0	0	0	0	0	0	0	0	0

Refresh

Settings

- **Port**
Select the port for which the History will be displayed.

Description of the displayed values

- **Buckets**
Maximum number of samples that can be saved at the same time.
- **Interval [s]**
Interval after which the current status of the statistics is saved as a sample.

The table has the following columns:

- **Sample**
Number of the sample
- **Sample Time**
System up time at which the sample was taken.
- **Unicast**
Number of received unicast frames.
- **Multicast**
Number of received multicast frames.
- **Broadcast**
Number of received broadcast frames.

- **CRC**
Number of frames with a bad CRC checksum.
- **Undersize**
Number of frames that are shorter than 64 bytes.
- **Oversize**
Number of frames discarded because they are too long.
- **Fragments**
Number of frames that are shorter than 64 bytes and have a bad CRC checksum.
- **Jabbers**
Number of frames with a VLAN tag that have a bad CRC checksum and are discarded because they are too long.
- **Collisions**
Number of collisions of received frames.
- **Utilization [%]**
Utilization of the port during a sample.

6.3.9 Unicast

Status of the unicast filter table

This page shows the current content of the unicast filter table. This table lists the source addresses of unicast address frames. Entries can be made either dynamically when a node sends a frame to a port or statically by the user setting parameters.

Unicast			
VLAN ID	MAC Address	Status	Port
1	00-1b-1b-b6-32-79	Learnt	P1.1
1	68-05-ca-25-e8-62	Learnt	P1.1
1	68-05-ca-36-39-0d	Learnt	P1.1

3 entries.

Description of the displayed values

The table contains the following columns:

- **VLAN ID**
Shows the VLAN-ID assigned to this MAC address.
- **MAC Address**
Shows the MAC address of the node that the device has learned or the user has configured.

6.3 The "Information" menu

- **Status**
Shows the status of each address entry:
 - **Learnt**
The specified address was learned by receiving a frame from this node and will be deleted when the aging time expires if no further packets are received from this node.

Note

If there is a link down, learned MAC entries are deleted.

 - **Static**
Configured by the user. Static addresses are stored permanently; in other words, they are not deleted when the aging time expires or when the switch is restarted.
 - **Other**
The specified address is learnt indirectly through private VLAN.
- **Port**
Shows the port via which the node with the specified address can be reached. Frames received by the device whose destination address matches this address will be forwarded to this port.

6.3.10 Multicast

6.3.10.1 Multicast

Status of the multicast filter table

This table shows the multicast frames currently entered in the multicast filter table and their destination ports. The entries can be dynamic (the device has learned them) or static (the user has set them).

Note

The device does not learn any reserved multicast addresses, see also RFC 5771.

The screenshot shows a web interface for Multicast configuration. It has a title bar 'Multicast' with icons for help, search, and refresh. Below the title bar are two tabs: 'Multicast' and 'IGMP Groups'. The 'Multicast' tab is active and displays a table with the following data:

VLAN ID	MAC Address	Status	P0.1	P0.2	P0.3	P0.4
1	01-00-5a-00-00-00	Static	-	-	-	-

Below the table, it says '1 entry.' and there is a 'Refresh' button.

Description

The table contains the following columns:

- **VLAN ID**
Shows VLAN ID of the VLAN to which the MAC multicast address is assigned.
- **MAC Address**
Shows the MAC multicast address that the device has learned or the user has configured.
- **Status**
Shows the status of each address entry. The following information is possible:
 - Static
The address was entered statically by the user. Static addresses are stored permanently; in other words, they are not deleted when the aging time expires or when the device is restarted. These must be deleted by the user.
 - IGMP-Snooping
The destination port for this address was obtained by IGMP configuration.
 - GMRP
The destination port for this address was registered by a received GMRP frame.
- **Port List**
There is a column for each slot. Within a column, the multicast group to which the port belongs is shown:
 - M
(Member) Multicast frames are sent via this port.
 - R
(Registered) Member of the multicast group, registration was by a GMRP frame.
 - I
(IGMP) member of the multicast group, registration was by a GMRP frame.
 - –
Not a member of the multicast group. No multicast frames with the defined multicast MAC address are sent via this port.
 - F
(Forbidden) Not a member of the multicast group. This address also cannot be an address learned dynamically with GMRP or IGMP.

6.3.10.2 IGMP Groups

Status of the multicast filter table

This table shows the multicast groups currently entered in the filter table, configured and joined.

Internet Group Management Protocol (IGMP) Groups			
Multicast IGMP Groups			
Interface	Group Address	Mode	Status
vlan1	224.0.0.251	Exclude	Dynamic
vlan1	224.7.7.7	Include	Static
vlan1	239.255.255.250	Exclude	Dynamic

Refresh

Description of the displayed values

The table contains the following columns:

- **Interface**
Shows the IGMP interface.
- **Group Address**
Shows the address of the multicast group that the device has learned or the user has configured.
- **Mode**
Shows whether the recipient has specified that a multicast from a certain source should be received or rejected.
 - '-'
IGMPv1 or IGMPv2 is used or the recipient has not given any source preference or excluded any source.
 - Include
The multicast should be received from certain sources.
 - Exclude
The multicast should not be received from certain sources.
- **Status**
Shows the status of each entry. The following information is possible:
 - Static
The multicast group was configured statically.
 - Dynamic
The multicast group was learned via IGMP configuration.

6.3.11 LLDP

Status of the neighborhood table

This page shows the current content of the neighborhood table. This table stores the information that the LLDP agent has received from connected devices.

You set the interfaces via which the LLDP agent receives or sends information in the following section: "Layer 2 > LLDP".

Link Layer Discovery Protocol (LLDP) Neighbors						
System Name	Device ID	Local Interface	Hold Time[s]	Capability	Port ID	
sysName Not Set	00:1b:1b:c8:70:3a	P0.2	20	Bridge	port-002-00000	

Description

The table contains the following columns:

- **System Name**
System name of the connected device
- **Device ID**
Device ID of the connected device. The device ID corresponds to the device name, which is assigned via SINEC PNI, for example. If no device name is assigned, the MAC address of the device is displayed.
- **Local Interface**
Port at which the IE switch received the information.
- **Hold Time[s]**
Hold time in seconds
An entry remains stored on the device for the time specified here. If the IE switch does not receive any new information from the connected device during this time, the entry is deleted.
- **Capability**
Shows the properties of the connected device:
 - Router
 - Bridge
 - Telephone
 - DOCSIS Cable Device
 - WLAN Access Point
 - Repeater
 - Station
 - Other
- **Port ID**
Port of the device with which the IE switch is connected.

6.3.12 Fiber Monitoring Protocol

Monitoring optical links

With Fiber Monitoring, you can monitor optical links. The table shows the current status of the ports.

You set the values to be monitored on the following page: "Layer 2 > FMP".

Fiber Monitoring Protocol (FMP) Diagnosis				
Port	Rx Power State	Rx Power[dBm]	Power Loss State	Power Loss[dB]
P0.1	link down	-	idle	-
P0.2	ok	-21.1	ok	-5.9
P0.4	link down	-	idle	-

Description

- **Port**
Shows the optical ports that support Fiber Monitoring. This depends on the transceivers.
- **Rx Power State**
 - **disabled**
Fiber monitoring is disabled.
 - **ok**
The value for the received power of the optical link is within the set limits.
 - **maint. req.**
Check the link.
A warning is signaled.
 - **maint. dem.**
The link needs to be checked.
An alarm is signaled and the fault LED is lit.
 - **link down**
The connection to the communications partner is down. No link is detected.
- **Rx Power [dBm]**
Shows the current value of the received power. The value can have a tolerance of +/- 3 dB. If there is no connection (link down) or fiber monitoring is disabled, "-" is displayed. If fiber monitoring is not enabled on the partner port, the value 0.0 is displayed.

- **Power Loss State**
To be able to monitor the power loss of the connection the function fiber monitoring must be enabled for the optical port of the connection partner.
 - **disabled**
Fiber monitoring is disabled.
 - **ok**
The value for the power loss of the optical link is within the defined limits.
 - **maint. req.**
Check the link.
A warning is signaled.
 - **maint. dem.**
The link needs to be checked.
An alarm is signaled and the fault LED is lit.
 - **idle**
The port has no connection to another port with fiber monitoring enabled.
If no diagnostics information is received from the optical port of the connection partner for 5 cycles, the fiber monitoring connection is assumed to be interrupted. A cycle lasts 5 seconds.
- **Power Loss [dB]**
Shows the current value of the power loss. The value can have a tolerance of +/- 3 dB.
If there is no connection (link down), Fiber Monitoring is disabled or the partner port does not support Fiber Monitoring, "-" is displayed.

6.3.13 IPv4 Routing

6.3.13.1 Routing Table

Introduction

This page shows the routes currently being used.

Layer 3: IPv4 Routing Table

Routing Table | Policy Based Routing, OSPF Interfaces, OSPF Neighbors, OSPF Virtual Neighbors, OSPF LSA, OSPF Statistics, BGP Transitions, IPM Interfaces, IPM Neighbors, IPM Routes, IPM BGP, IPM BGP, BGP Cache

Destination Network	Subnet Mask	Gateway	Interface	Metric	Routing Protocol
0.0.0.0	0.0.0.0	192.168.178.1	vlan1	1	DHCP
192.168.178.0	255.255.255.0	0.0.0.0	vlan1	0	connected

2 entries.

Description of the displayed values

The table has the following columns:

- **Destination Network**
Shows the destination address of this route.
- **Subnet Mask**
Shows the subnet mask of this route.
- **Gateway**
Shows the gateway for this route. For sink routes, the information "Sink" is displayed instead of the IP address.
- **Interface**
Shows the interface for this route.
- **Metric**
Shows the metric of the route. The higher the value, the longer packets require to their destination.
- **Routing Protocol**
Shows the routing protocol from which the entry in the routing table originates. The following entries are possible:
 - DHCP: Default route, configured via DHCP
 - Connected: Connected routes
 - Static: Static routes
 - RIP: Routes via RIP
 - OSPF: Routes via OSPF
 - Other: Other routes

6.3.13.2 OSPFv2 Interfaces

Overview

This page shows the configuration of the OSPF interface.

Open Shortest Path First v2 (OSPFv2) Interfaces					
IP Address	Area ID	Interface Status	Designated Router	Backup Designated Router	Events
192.168.16.155	2.0.0.0	Designated Router	192.168.16.155	0.0.0.0	2

Description of the displayed values

The table has the following columns:

- **IP Address**
Shows the IPv4 address of the OSPF interface
- **Area ID**
Shows the area ID to which the OSPF interface belongs.
- **Interface Status**
Shows the status of the OSPF interface:
 - Down
The interface is not available.
 - Loop back
Loop back interface
 - Waiting
Startup and negotiation of the interface.
 - Point to Point
Point-to-point connection
 - Designated Router
The router is a designated router and generates network LSAs.
 - Backup D. Router
The router is the backup router for the designated router.
 - Other D. Router
The interface has started up. The router is neither a designated nor a designated backup router.
- **Designated Router**
Shows the IPv4 address of the designated router for this OSPF interface.
- **Backup Designated Router**
Shows the IPv4 address of the designated backup router for this OSPF interface.
- **Events**
Shows the number of status changes of OSPF.

6.3.13.3 OSPFv2 Neighbors

Overview

This page shows the dynamically detected neighbor routers in the relevant networks.

IP Address	Router ID	Status	Assoc. Area Type	Priority	Hello Suppr.	Retrans Queue	Events
172.25.88.17	172.25.88.1	full	Stub	1	no	0	6
172.25.88.62	0.5.2.8	full	Stub	1	no	0	6

Description of the displayed values

The table has the following columns:

- **IP Address**
Shows the IPv4 address of the neighbor router in this network.
- **Router ID**
Shows the ID of the neighbor router in IPv4 format. The two addresses can match.
- **Status**
Shows the status of the neighbor router. The status can adopt the following values:
 - unknown
Status of the neighbor router is unknown.
 - down
The neighbor router cannot be reached.
 - attempt and init
Status during the initialization
 - two-way
Two-way receipt of Hello packets. Specification of the designated router and the designated backup router.
 - exchangestart, exchange and loading
Status during exchange of the LSAs
 - full
The database is complete and synchronized within the area. The routes can now be detected.

Note

Normal status

If the partner router is a designated router or a designated backup router, the status is "full". Otherwise, the status is "two-way".

- **Assoc. Area Type**
Shows the area type via which the neighbor-neighbor relation is maintained. The following area types exist:
 - Normal
 - Stub
 - NSSA
 - Backbone
- **Priority**
Shows the priority of the neighbor router. This is only significant when selecting the designated router on a network. For virtual neighbor routers, this information is irrelevant.
- **Hello Suppr.**
Shows the suppressed Hello packets to the neighbor router. This field normally displays "no".
- **Retrans. Queue**
Shows the length of the queue with Hello packets still to be transmitted.
- **Events**
Shows the number of status changes.

6.3.13.4 OSPFv2 Virtual Neighbors

Overview

This page shows the configured virtual neighbors.

Open Shortest Path First v2 (OSPFv2) Virtual Neighbors						
IP Address	Router ID	Status	Transit Area ID	Hello Suppr.	Retrans Queue	Events
0.0.0.0	5.5.5.5	down	1.1.1.1	no	0	0

Description of the displayed values

The table has the following columns:

- **IP Address**
Shows the IPv4 address of the virtual neighbor router in this network.
- **Router ID**
Shows the router ID of the virtual neighbor router in IPv4 format.

- **Status**
Shows the status of the neighbor router. The status can adopt the following values:
 - unknown
Status of the neighbor router is unknown.
 - down
The neighbor router cannot be reached.
 - attempt and init
Brief status during initialization
 - two-way
Two-way receipt of Hello packets. Specification of the designated router and the designated backup router.
 - exchangestart, exchange and loading
Status during exchange of the LSAs
 - full
The database is complete and synchronized within the area. The routes can now be detected.

Note

Normal status

If the partner router is a designated router or a designated backup router, the status is "full". Otherwise, the status is "two-way".

- **Trans. Area ID**
Shows the ID of the area via which the virtual neighborhood relation exists.
- **Hello Suppr.**
Shows whether there are suppressed Hello packets to the virtual neighbor router.
 - No: There are no suppressed Hello packets (default)
 - Yes: There are suppressed Hello packets.
- **Retrans. Queue**
Shows the length of the queue with Hello packets still to be transmitted.
- **Events**
Shows the number of status changes.

Description

The table has the following columns:

- **Area ID**
Shows the ID of the area to which the LSA belongs. If the LSA is an external connection, '-' is displayed.
- **Link State Type**
Shows the LSA type. The following values are possible:
 - Unknown
LSA type is unknown.
 - Router
The router LSA (Type 1) is sent by the OSPF router within an area. The LSA contains information about the status of all router interfaces.
 - Network
The network LSA (Type 2) is sent by the designated router within an area. The LSA contains a list of routers connected to the network.
 - NSSA External
The NSSA external LSA (Type 7) is sent by the NSSA-ASBR (NSSA Autonomous System Border Router) within an NSSA. The NSSA-ASBR receives LSAs of Type 5 and converts the information to LSAs of Type 7. The NSSA router can forward these LSAs within an NSSA.
 - Summary
The summary LSA (Type 3) is sent by the ABR (Area Border Router) within an area. The LSA contains information about routes to other networks.
 - AS Summary
The AS summary LSA (Type 4) is sent by the ABR within an area. The LSA contains information about routes to other autonomous systems.
 - AS-External
The AS-External LSA (Type 5) is sent by the ASBR (AS Border Router) within an autonomous system. The LSA contains information about routes from one network to another.
- **Link State ID**
Shows the ID of the LSA.
- **Router ID**
Shows the ID of the router that sent this LSA.
- **Sequence Number**
Shows the sequence number of the LSA. Each time an LSA is renewed, this sequence number is incremented by one.

6.3.13.6 RIPv2 Statistics

Overview

This page shows the statistics of the RIP interface.

Description of the displayed values

Routing Information v2 (RIPv2) Statistics			
RIPv2 Statistics			
IP Address	Bad packets	Bad routes	Updates Sent
192.168.16.155	0	0	1

Refresh

The table has the following columns:

- **IP Address**
Shows the IPv4 address of the RIPv2 interface
- **Bad packets**
Number of received RIP packets that were deleted and therefore ignored.
- **Bad routes**
Number of routes of valid RIP packets that could not be taken into consideration.
- **Updates Sent**
Shows how often the router has sent its routing table to its neighbor routers.

6.3.13.7 NAT Translations

Overview

This page displays the active NAT connections.

Description of the displayed values

Network Address Translation (NAT) Translations							
NAT Translations							Last Use Time[s]
Interface	Inside Local Address	Inside Local Port	Inside Global Address	Inside Global Port	Outside Local/Global Address	Outside Local/Global Port	Last Use Time[s]
vlan1	10.0.0.2	161	140.80.100.1	161	140.80.58.23	59269	11
vlan1	10.0.0.2	49156	140.80.100.1	49156	140.80.57.72	123	46
vlan1	10.0.0.9	80	140.80.103.1	80	140.80.57.73	49620	49

0 entries.

Refresh

6.3 The "Information" menu

The table has the following columns:

- **Interface**
Shows the IP interface.
- **Inside Local Address**
Shows the actual address of the device that should be reachable from external.
- **Inside Local Port**
Shows the port that is assigned to the Inside Local Address.
- **Inside Global Address**
Shows the address at which the device can be reached from external.
- **Inside Global Port**
Shows the port that is assigned to the Inside Global Address.
- **Outside Local/Global Address**
Shows the address of the communications partner.
- **Outside Local/Global Port**
Displays the port of the external communications partner.
- **Last Use Time [s]**
Shows the time at which the last packet was transferred.

6.3.13.8 PIM interfaces

Overview

This page shows the PIM interfaces.

Protocol Independent Multicast (PIM) Protocol Interfaces				
Interface	Address	Query Interval	DR Address	DR Priority
vlan1	192.168.16.155	30	192.168.16.155	1
vlan9	10.0.0.2	30	10.0.0.2	1
vlan201	1.1.1.10	30	1.1.1.10	1

Refresh

Description of the displayed values

The table has the following columns:

- **Interface**
Shows the PIM interface.
- **Address**
Shows the IP address of the interface.

- **Query Interval**
Every PIM router or every PIM interface sends Hello packets cyclically at the specified intervals. This allows every PIM router to get to know its neighbors and the designated router can be specified.
- **DR Address**
Shows the IP address of the designated router.
- **DR Priority**
Shows the DR priority of the interface.

6.3.13.9 PIM Neighbors

Overview

This page shows the PIM neighborhood table.

Description of the displayed values

Protocol Independent Multicast (PIM) Protocol Neighbors		
Interface	Neighbor Address	DR Priority
vlan1	192.168.16.155	1
vlan9	10.0.0.2	1

Refresh

The table has the following columns:

- **Interface**
Shows the PIM interface. The PIM routers are connected together via this interface.
- **Neighbor Address**
Shows the IP address of the neighbor.
- **DR Priority**
Shows the DR priority of the interface.

6.3.13.10 PIM Routes

Overview

The page shows the PIM routing table.

Group Address	Group Mask	Source Address	Incoming Interface	Outgoing Interface	State
224.0.0.6	255.255.255.255	10.0.1.1	vlan1	vlan1	Forwarding

Description of the displayed values

Select which PIM routes should be displayed:

- All
- Outgoing

Depending on your selection not all columns are displayed in the table.

The table has the following columns:

- **Group Address**
Shows the address of the multicast group.
- **Group Mask**
Shows the subnet mask that restricts the multicast band.
- **Source Address**
 - **IP Address**
Shows the source IP address of the multicast packet.
 - *****
(* ,G) messages contain the group and the information to pass on the message in the direction of the RP.
The route is via the RP.
- **Incoming Interface**
Shows the interface via which the multicast will be received.

- **Outgoing Interfaces**
Shows the interface via which the multicast will be forwarded.
- **Status**
Shows whether or not a multicast group is used.
 - **Forwarding**
The multicast group is used.
 - **Pruned**
The multicast group is not used.

6.3.13.11 PIM RPs

Samples of the statistics

The page shows information on rendezvous points.

Protocol Independent Multicast (PIM) Rendezvous Point (RP) Tables

Routing Table Policy Based Routing IGMPv2 Interfaces IGMPv2 Neighbors IGMPv2 Virtual Neighbors IGMPv2 L/S IGMPv3 Statistics MST Translations PIM Interfaces PIM Neighbors PIM Routes **PIM RPs** PIM Sites MSTP Cache

Static

Group Address	Group Mask	RP Address	Bidirectional Multicast
224.0.0.5	255.255.255.255	10.0.0.3	Disabled
224.0.0.6	255.255.255.255	10.0.1.1	Enabled

Refresh

Description of the displayed values

Select which rendezvous points should be displayed.

- **Candidate**
Shows the IP address of the RP candidates for each multicast group within a PIM network or a PIM domain.
- **Elected**
Shows the IP address of the rendezvous point for each multicast group that was selected within a PIM network or a PIM domain.
- **Static**
Shows the static rendezvous points of the device.

Depending on your selection not all columns are displayed in the table.

6.3 The "Information" menu

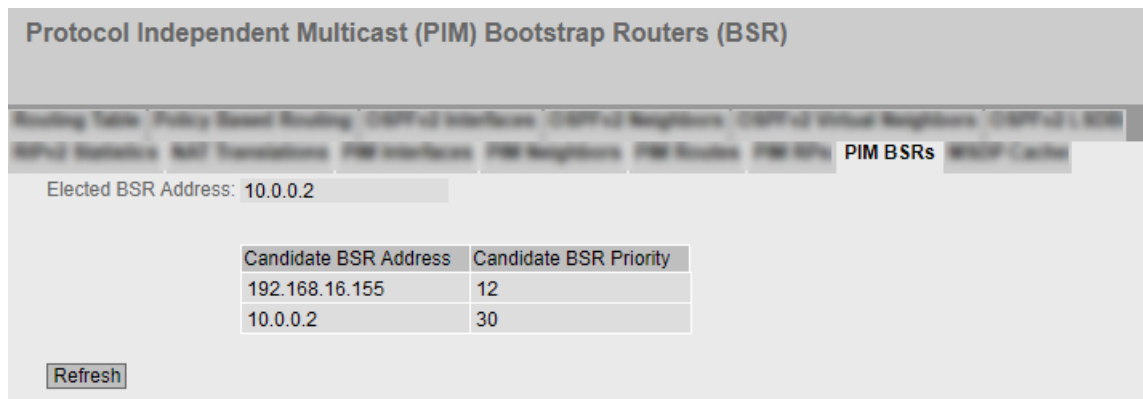
The table has the following columns:

- **Group Address**
Shows the address of the multicast group.
- **Group Mask**
Shows the subnet mask that restricts the multicast band.
- **RP Address**
Shows the IP address of the RP.
- **RP Priority**
Shows the priority of the interface as RP.
- **Bidirectional Multicast**
Shows whether the "bidirectional multicast" functionality is activated or deactivated.

6.3.13.12 PIM BSRs

Overview

The page shows information on bootstrap routers (BSR).



Description of the displayed values

The page contains the following boxes:

- **Address of the selected BSR**
Shows the IP address of the BSR that was selected within a PIM network or a PIM domain.

The table has the following columns:

- **Candidate BSR Address**
Shows the interfaces of the device that are candidates for the BSR on the PIM router.
- **Candidate BSR Priority**
Shows the priority of the BSR.

6.3.13.13 MSDP Cache

Overview

This page shows the MSDP partners.

Multicast Source Discovery Protocol (MSDP) Source-Active (SA) Cache			
Source	Group	RP	Uptime
192.168.4.202	225.0.1.1	0.0.0.0	1m 56s
192.168.4.202	225.0.1.2	0.0.0.0	1m 56s
192.168.4.202	225.0.1.3	0.0.0.0	1m 56s

Description of the displayed values

The table has the following columns:

- **Source**
Shows the source of the multicast.
- **Group**
Shows the multicast group.
- **RP**
Shows the MSDP partner.
The IP address 0.0.0.0 means that the device has taken on the role RP for the source and multicast group and sends SA messages itself. If an MSDP partner takes on this task, its IP address is shown here.
- **Uptime**
Depending on the source, the displayed value has the following significance:
 - The time for which a source has been active in its own PIM domain.
 - The time since when an MSDP partner sent an SA cache update to another PIM domain via a source.

6.3.14 DHCP Server

This page shows which IPv4 addresses were assigned to the devices by the DHCP server.

DHCP Server Bindings						
IP Address	Pool ID	Identification Method	Identification Value	Allocation Method	Binding State	Expire Time
192.168.16.90	1	Client ID	OS-EC74BA03FED2	dynamic	assigned	01/01/2000 05:21:03

1 entry.

Description

- **IP Address**
Shows the IPv4 address assigned to the DHCP client.
- **Pool ID**
Shows the number of the IPv4 address band.
- **Identification Method**
Shows the method according to which the DHCP client is identified.
- **Identification value**
Shows the MAC address of the client ID of the DHCP client.
- **Allocation Method**
Shows whether the IPv4 address was assigned statically or dynamically. You configure the static entries in "System > DHCP > Static Leases".
- **Binding State**
Shows the status of the assignment.
 - Assigned
The assignment is used.
 - Not used
The assignment is not used.
 - probing
The assignment is being checked.
 - Unknown
The status of the assignment is unknown.
- **Expire Time**
Shows until when the assigned IPv4 address is still valid. Up to this time, the DHCP client must either request a new IPv4 address or extend the lease time of the assigned IPv4 address.

6.3.15 Diagnostics

This page shows the usage values and temperature values of internal and external modules of the device. The modules are only shown if they make corresponding information available. If you add or remove a module, the display is automatically adapted. If the usage value exceeds the displayed threshold value, the status changes accordingly. With the temperature value, the status also changes when the low threshold value is undershot.

The threshold values are preset by the device and cannot be modified. If no threshold values are preset, "-" is displayed. On the "System > Events > Configuration" page, you can specify how the device signals the status change.

Diagnostics						
Usage Table						
Name	Status	Usage [%]	High Warning Threshold [%]	High Critical Threshold [%]		
CPU	OK	72	-	-		
RAM	OK	22	90	98		
FLASH:Config	OK	1	90	-		

Temperature Table						
Name	Status	Temperature [°C]	Low Critical Threshold [°C]	Low Warning Threshold [°C]	High Warning Threshold [°C]	High Critical Threshold [°C]
Chassis	OK	49	-40	-30	100	110

Description

The **Usage Table** has the following columns:

- **Name**
Shows the name of the module.
- **Status**
Depending on the relationship between the threshold values and the current usage, the following status values are displayed in ascending priority:
 - **OK**
The usage is within the preset threshold values.
 - **WARNING**
The upper threshold value of the severity level "Warning" was exceeded. The usage is still in a normal range. The operating conditions of the device should be checked.
 - **CRITICAL**
The upper threshold value of the severity level "Critical" was exceeded. The device must be checked. Overloading the device can lead to malfunctions.
 - **INVALID**
The usage could not be determined or is invalid. The "Usage [%]" box shows "-".
 - **INITIAL**
No data has been read out yet. "-" is displayed in all boxes.

- **Usage [%]**
Shows the current value for the usage of the device. The display is updated at regular intervals.
- **High Warning Threshold [%]**
If this value is exceeded, the status changes to "WARNING". You can configure that you are informed by a message.
- **High Critical Threshold [%]**
If this value is exceeded, the status changes to "CRITICAL". You can configure that you are informed by a message.

The **Temperature table** has the following columns:

- **Name**
Shows the name of the module.
The information in the row "Chassis" relates to the inner temperature of the housing.
In the case of pluggable transceivers, the port and type are specified.
- **Status**
Depending on the relationship between the threshold values and the current temperature, the following status values are displayed in ascending priority:
 - **OK**
The temperature value is within the preset threshold values.
 - **WARNING**
The low or high threshold of the severity level "Warning" was fallen below or exceeded, respectively. The temperature is still in a normal range. The device has detected a fall or rise in temperature, e.g. due to changed cooling of the cabinet. The temperature should be checked.
 - **CRITICAL**
The low or high threshold of the severity level "Critical" was fallen below or exceeded, respectively. The device must be checked. A too low or too high temperature can lead to restricted performance or damage to the device.
 - **INVALID**
The value could not be read out or is invalid. "-" is displayed in the "Temperature [°C]" box.
 - **INITIAL**
No data has been read out yet. "-" is displayed in all boxes.
- **Temperature [°C]**
Shows the current value of the temperature. The display is updated at regular intervals.
The value can have a tolerance of +/- 3 °C. Thus, the value can differ for the same devices with similar ambient conditions.
- **Low Critical Threshold [°C]**
If the value falls below this value, the status changes to "CRITICAL". You can configure that you are informed by a message.
- **Low Warning Threshold [°C]**
If the value falls below this value, the status changes to "WARNING". You can configure that you are informed by a message.

- **High Warning Threshold [°C]**
If this value is exceeded, the status changes to "WARNING". You can configure that you are informed by a message.
- **High Critical Threshold [°C]**
If this value is exceeded, the status changes to "CRITICAL". You can configure that you are informed by a message.

6.3.16 SNMP

This page displays the created SNMPv3 groups. You configure the SNMPv3 groups in "System > SNMP".

Simple Network Management Protocol v3 (SNMPv3) Groups Overview	
Group Name	User Name
Service	Mueller
Wartung	Peterson

Description

The table has the following columns:

- **Group Name**
Shows the group name.
- **User Name**
Shows the user that is assigned to the group.

6.3.17 Security

6.3.17.1 Overview

Note

The values displayed depend on the rights of the logged-in user.

This page shows the security settings and the local and external user accounts.

Security Overview

Overview | Supported Function Rights | Roles | Groups | 802.1X Port Status | MAC Authentication

Services

Telnet Server: disabled

SSH Server: enabled

SSH Fingerprint: Rsa key(md5): e2:b1:06:14:9a:0f:ea:e8:66:f1:65:42:5e:b6:3a:e1
 Rsa key(sha256): VXA5V1S6pE9ghs6L34o6u1CjEduFoQnkCjaf32uU2pE
 Ecdsa key(md5): 58:f1:3f:4c:39:d0:53:d8:16:26:ca:fd:25:6b:3d:5a
 Ecdsa key(sha256): yc/pHRszJ6zQsjA98HBmewyMhyw3T2vLY7L39s2wTAA

Web Server: HTTPS

SNMP: SNMPv1/v2c/v3

Management ACL: disabled: no access restriction

Login Authentication: Local

Password Policy: high

Local User Accounts

User Account	Role
admin	admin

External User Accounts

User Account	Role
admin	admin

Refresh

Description

Services

The "Services" list shows the security settings.

- **Telnet Server**
 You configure the setting in "System > Configuration".
 - Enabled: Unencrypted access to the CLI
 - Disabled: No unencrypted access to the CLI
- **SSH Server**
 You configure the setting in "System > Configuration".
 - Enabled: Encrypted access to the CLI
 - Disabled: No encrypted access to the CLI
- **SSH Fingerprint**
 This field shows the SSH fingerprint.
- **Web Server**
 You configure the setting in "System > Configuration"
 - HTTP/HTTPS: Access to the WBM is possible with HTTP and HTTPS.
 - HTTPS: Access to the WBM is now only possible with HTTPS.
 - HTTP: Access to the WBM is now only possible with HTTP.

- **SNMP**

You can configure the setting in "System > SNMP > General".

 - "-" (SNMP disabled)
Access to device parameters using SNMP is not possible.
 - SNMPv1/v2c/v3
Access to device parameters is possible with SNMP versions 1, 2c or 3.
 - SNMPv3
Access to device parameters is possible only with SNMP version 3.
- **Management ACL**

You configure the setting under "Security > Management ACL"

 - Enabled: Restricted access only: Access is restricted using a Management Access Control List (ACL).
 - Disabled: No access restriction: Management ACL is not enabled.
- **Login Authentication**

You configure the setting in "Security > AAA > General".

 - Local
The authentication must be made locally on the device.
 - RADIUS
The authentication must be handled via a RADIUS server.
 - Local and RADIUS
The authentication is possible both with the users that exist on the device (user name and password) and via a RADIUS server.
The user is first searched for in the local database. If the user does not exist there, a RADIUS request is sent.
 - RADIUS and fallback Local
The authentication must be handled via a RADIUS server.
A local authentication is performed only when the RADIUS server cannot be reached in the network.
- **Password Policy**

Shows which password policy is currently being used.

Local and external user accounts

You configure local user accounts and roles in "Security > Users".

When you create a local user account an external user account is generated automatically.

Local user accounts involve users each with a password for logging in on the device.

In the table "External User Accounts" a user is linked to a role. In this example, the user "Service" is linked to the "user" role. The user is defined on a RADIUS server. The role is defined locally on the device. When a RADIUS server authenticates a user, but the corresponding group is unknown or does not exist, the device checks whether or not there is an entry for the user in the table "External User Accounts". If an entry exists, the user is

6.3 The "Information" menu

logged in with the rights of the associated role. If the corresponding group is known on the device, both tables are evaluated. The user is assigned the role with the higher rights.

Note

The table "External User Accounts" is only evaluated if you have set "SiemensVSA" in the RADIUS Authorization Mode.

With CLI, you can access external user accounts.

The "Local User Accounts" and "External User Accounts" tables have the following columns:

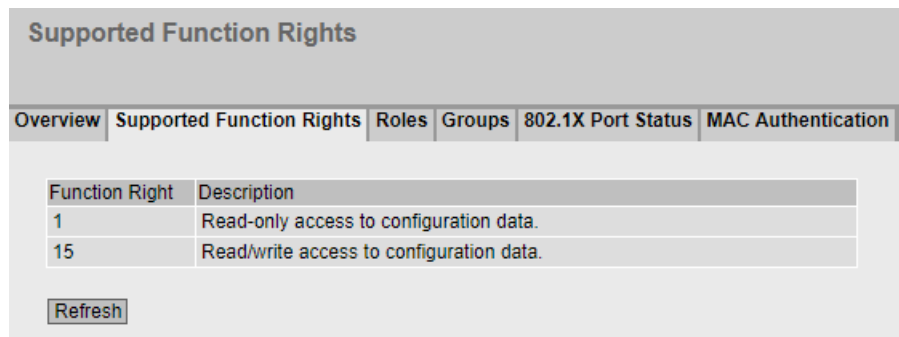
- **Account**
Shows the name of the local user.
- **Role**
Shows the role of the user. You can obtain more information on the function rights of the role in "Information > Security > Roles".

6.3.17.2 Supported Function Rights

Note

The values displayed depend on the role of the logged-on user.

The page shows the function rights available locally on the device.



Description of the displayed values

- **Function Right**
Shows the number of the function right. Different rights relating to the device parameters are assigned to the numbers.
- **Description**
Shows the description of the function right.

6.3.17.3 Roles

Note

The values displayed depend on the role of the logged-in user.

The page shows the roles valid locally on the device.

User Roles					
Overview	Supported Function Rights	Roles	Groups	802.1X Port Status	MAC Authentication
Role	Function Right	Description			
user	1	System defined role, with readonly access to configuration data of this component.			
admin	15	System defined role, with read/write access to configuration data of this component.			
default	1	Internal role, for authenticated users without group/role mapping in this component.			
everybody	0	Internal role, assigned to users when authentication failes. Access will be denied.			

[Refresh](#)

Description

The table contains the following columns:

- **Role**
Shows the name of the role.
- **Function Right**
Shows the function right of the role:
 - 1
Users with this role can read device parameters but cannot change them.
 - 15
Users with this role can both read and change device parameters.
 - 0
This is a role that the device assigns internally when a user could not be authenticated. The user is denied access to the device.
- **Description**
Shows a description of the role.

6.3.17.4 Groups

Note

The values displayed depend on the role of the logged-on user.

6.3 The "Information" menu

This page shows which group is linked to which role. The group is defined on a RADIUS server. The role is defined locally on the device.

User Groups					
Overview	Supported Function Rights	Roles	Groups	802.1X Port Status	MAC Authentication
Group	Role	Description			
Grp1	user	Admin Group			
<input type="button" value="Refresh"/>					

Description of the displayed values

The table has the following columns:

- **Group**
Shows the name of the group. The name matches the group on the RADIUS server.
- **Role**
Shows the name of the role. Users who are authenticated with the linked group on the RADIUS server receive the rights of this role locally on the device.
- **Description**
Shows a description for the link.

6.3.17.5 802.1X Port Status

This page shows the status of 802.1X authentication as well as the MAC authentication for the individual ports.

802.1X Port Status					
Overview	Supported Function Rights	Roles	Groups	802.1X Port Status	MAC Authentication
Port	802.1X Auth. Status	MAC-Auth Port Status	MAC Auth. Actual Allowed Addresses	MAC Auth. Actual Blocked Addresses	Guest VLAN Actual Allowed Addresses
P0.1	Unauthorized	Individual	0	0	0
P0.2	Authorized	-	0	0	0
<input type="button" value="Refresh"/>					

Description

The table has the following columns:

- **Port**
All ports of the device are displayed in this column.
- **802.1X Auth. Status**
The authentication status of the node. The following options are possible:
 - Authorized
Data traffic via the port is possible after successful authentication with the "802.1X" method.
 - Unauthorized
Data traffic via the port is not possible because no authentication has taken place with the "802.1X" method yet or the authentication method was not successful.
- **MAC Auth. Port Status**
Shows the status of the MAC authentication for the port. The following options are possible:
 - -
MAC authentication is disabled for the port.
 - Individual
MAC authentication is configured for the port. Clients can be authenticated individually with their MAC address.
 - Blocked
MAC authentication is configured for the port. Clients are not authenticated individually. The first client that is authenticated opens the port for all clients. No client is authenticated yet.
 - open
MAC authentication is configured for the port. Clients are not authenticated individually. The first client that is authenticated opens the port for all clients. The port was opened after successful authentication of a client.
 - Sticky
MAC authentication is configured for the port.
If a new MAC address requests on a port and the number of currently authenticated MAC addresses on the port is < the number of maximum permitted MAC addresses, the request is automatically successful.
If a new MAC address requests on a port and the number of currently authenticated MAC addresses on the port is \geq the number of maximum permitted MAC addresses, the request automatically fails.
- **MAC Auth. Actual Allowed Addresses**
Shows the number of nodes that are allowed access after successful MAC authentication.
- **MAC Auth. Actual Blocked Addresses**
Shows the number of nodes that are allowed access after failed MAC authentication.
- **Guest VLAN Actual Allowed Addresses**
Shows the number of nodes that are allowed access via the "Guest VLAN" function.

6.3.17.6 MAC Authentication Address Table

This page shows the MAC addresses for which MAC authentication was performed.

MAC-Auth. Address Table					
Overview	Supported Function Rights	Roles	Groups	802.1X Port Status	MAC Authentication
VLAN ID	MAC Address	Status	Port		
1	00-10-94-13-00-01	Authenticated	P1.6		
1	00-10-94-13-00-02	Authenticated	P1.6		
1	00-10-94-ff-00-00	Authenticated	P1.6		
1	00-10-94-ff-00-01	Authenticated	P1.6		

Description

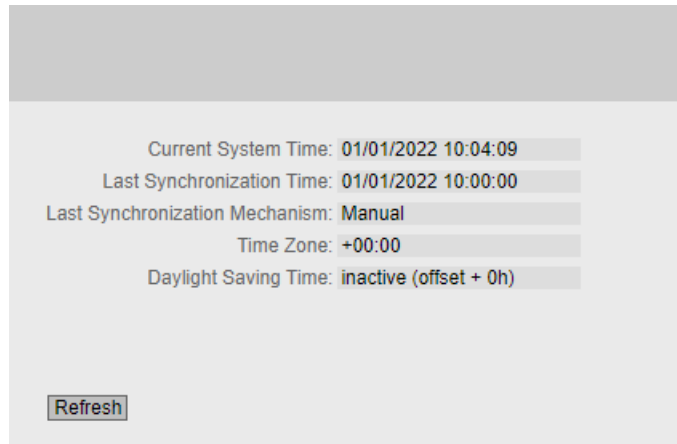
The table has the following columns:

- **VLAN ID**
Shows the VLAN ID assigned to this MAC address.
- **MAC Address**
Shows the MAC address of the node for which the authentication status is displayed.
- **Status**
The authentication status of the node. The following options are possible:
 - **Authorized**
Data traffic via the port is possible after successful authentication with the "MAC Authentication" method.
 - **Unauthorized**
Data traffic via the port is not possible because no authentication has taken place with the "MAC Authentication" method yet or the authentication method was not successful.
- **Port**
Shows the port via which the node with the specified address can be reached.

6.3.18 System time

Time-of-day synchronization in the network

This page displays the current system time.



Description

The page contains the following boxes:

- **Current System Time**
Shows the current date and current standard time received from the server. If you specify a time zone, the time information is adapted accordingly.
- **Last Synchronization Time**
Shows when the last time-of-day synchronization took place.
- **Last Synchronization Mechanism**
Shows how the last time synchronization was performed. The following methods are possible:
 - Not set
The time was not set.
 - Manual
Manual time setting
 - SNTP
Automatic time-of-day synchronization using SNTP
 - NTP
Automatic time-of-day synchronization using NTP
 - SIMATIC
Automatic time-of-day synchronization using the SIMATIC time frame
 - PTP (only for devices that support PTP.)
Automatic time-of-day synchronization with PTP

6.4 The "System" menu

- **Time Zone**
In this box, enter the time zone you are using in the format "+/- HH:MM". The time zone relates to UTC standard world time.
The time in the "Current System Time" box is adapted accordingly.
- **Daylight Saving Time (DST)**
Shows whether daylight saving time changeover is active.
 - active (offset +1 h)
The system time was changed to daylight saving time; in other words, an hour was added. You can see the current system time at the top right in the selection area of the WBM. The standard time including the time zone continues to be displayed in the "Current System Time" box.
 - inactive (offset +0 h)
The current system time is not changed.

6.4 The "System" menu

6.4.1 Configuration

System configuration

The WBM page contains the configuration overview of the access options of the device.

Specify the services that access the device. With some services, there are further configuration pages on which more detailed settings can be made.

The screenshot displays the 'System Configuration' page with the following settings:

- Telnet Server
- Telnet Port: 23
- SSH Server
- SSH Port: 22
- SSH Key Exchange Algorithm Level: High
- HTTP Server
- HTTP Port: 80
- HTTPS Server
- HTTPS Port: 443
- Minimum TLS Version: TLSv1.2
- DNS Client
- SMTP Client
- Syslog Client
- DCP Server: Read/Setup
- Time: Manual
- SNMP: SNMPv1/v2c/v3
- SNMPv1/v2 Read-Only
- SINEMA Configuration Interface
- DHCP DUID Configuration
- DUID-Type: DUID-LLT
- Link-layer Address Plus Time: 00-01-00-01-00-00-00-2E-D4-F5-27-C2-76-5B
- Vendor Enterprise Number: 00-02-00-00-10-E9-56-50-4E-37-31-37-39-37-33-32
- Link-layer address: 00-03-00-01-D4-F5-27-C2-76-5B
- Configuration Mode: Automatic Save
- Buttons: Set Values, Refresh, Write Startup Config

Description of the displayed boxes

The page contains the following boxes:

- **Telnet Server**
Enable or disable the "Telnet Server" service for unencrypted access to the CLI.
- **Telnet Port**
Standard port 23 is the default. You can optionally enter a port number in the range 1024 ... 49151 or 49500 ... 65535.
- **SSH Server**
Enable or disable the "SSH Server" service for encrypted access to the CLI.
- **SSH Port**
Standard port 22 is the default. You can optionally enter a port number in the range 1024 ... 49151 or 49500 ... 65535.

- **SSH Key Exchange Algorithm Level**
Select the level of the exchange algorithm for SSH keys from the drop-down list. The settings options are "Low" and "High". The two levels contain the following encryption algorithms:
 - Low
 - Curve25519-sha256
 - Curve25519-sha256@libssh.org
 - Ecdh-sha2-nistp256
 - Ecdh-sha2-nistp384
 - Ecdh-sha2-nistp521
 - Diffie-hellman-group16-sha512
 - Diffie-hellman-group18-sha512
 - Diffie-hellman-group14-sha256
 - Diffie-hellman-group14-sha1
 - High
 - Curve25519-sha256
 - Curve25519-sha256@libssh.org
 - Ecdh-sha2-nistp256
 - Ecdh-sha2-nistp384
 - Ecdh-sha2-nistp521

Note

If connection problems with SSH clients (TeraTerm, PuTTY, STS) occur with the setting "High", this may be because the SSH clients do not support the exchange algorithms of the setting "High".

Make sure that you are using the current versions of the SSH clients.

- **HTTP Server**
Enable or disable the "HTTP Server" service for unencrypted access to the WBM.
- **HTTP Port**
Standard port 80 is the default. You can optionally enter a port number in the range 1024 ... 49151 or 49500 ... 65535.
- **HTTPS Server**
Enable or disable the HTTPS server service for encrypted access to the WBM.
- **HTTPS Port**
Standard port 443 is the default. You can optionally enter a port number in the range 1024 ... 49151 or 49500 ... 65535.
- **Minimum TLS version**
Select the minimum TLS version to be used for the encryption from the drop-down list. Communication is not possible with devices that do not support the required TLS version.
- **DNS Client**
Enable or disable depending on whether the IE switch should operate as a DNS client. You can configure other settings in "System > DNS".
- **SMTP Client**
Enable or disable the SMTP client. You can configure other settings in "System > SMTP Client".
- **Syslog Client**
Enable or disable the Syslog client. You can configure other settings in "System > Syslog Client".

- **DCP Server**
Specify whether the device can be accessed with DCP (Discovery and Configuration Protocol):
 - "-" (disabled)
DCP is disabled. Device parameters can neither be read nor modified.
 - Read/Write
With DCP, device parameters can be both read and modified.
 - Read-Only
With DCP, device parameters can be read but cannot be modified.
 - Read/Setup
As long as the administrator's default password has not been changed, the device parameters can be both read and changed via DCP. Once the default password has been changed, the device parameters can no longer be changed via DCP.
- **Time**
Select the setting from the drop-down list. The following settings are possible:
 - Manual
The system time is set manually. You can configure other settings in "System > System Time > Manual Setting".
 - SIMATIC Time
The system time is set using a SIMATIC time transmitter. You can configure other settings in "System > System Time > SIMATIC Time Client".
 - SNTP Client
The system time is set via an SNTP server. You can configure other settings in "System > System Time > SNTP Client".
 - NTP Client
The system time is set via an NTP server. You can configure other settings in "System > System Time > NTP Client".
 - PTP Client (only for devices that support PTP)
The system time is set via PTP. You can configure other settings in "System > System Time > PTP Client".
- **SNMP**
Select the protocol from the drop-down list. The following settings are possible:
 - "-" (SNMP disabled)
Access to device parameters using SNMP is not possible.
 - SNMPv1/v2c/v3
Access to device parameters is possible with SNMP versions 1, 2c or 3. You can configure other settings in "System > SNMP > General".
 - SNMPv3
Access to device parameters is possible only with SNMP version 3. You can configure other settings in "System > SNMP > General".
- **SNMPv1/v2 Read-Only**
Enable or disable write access to SNMP variables with SNMPv1/v2c.
- **SINEMA Configuration Interface**
If the SINEMA configuration interface is enabled, you can download configurations to the IE switch via the TIA Portal.

- **DUID Type**
Specify which DUID type will be used. The DUID types are defined in RFC 3315.
 - DUID-LLT
DUID is based on the link layer address of the interface and a time stamp
 - DUID-EN
DUID is assigned by the vendor (EN = enterprise number)
 - DUID-LL
DUID is based on the link layer address of the interface
- **Link-layer Address Plus Time**
The value is based on the link layer address of the interface and a time stamp. The value is regenerated each time the factory settings are restored.
- **Vendor Enterprise Number**
The value is based on the enterprise number specific to the vendor.
- **Link-layer address**
The link-layer address is based on the MAC address.
- **Configuration Mode**
Select the mode from the drop-down list. The following modes are possible:
 - Automatic Save
Automatic backup mode. Approximately 1 minute after the last parameter change or when you restart the device, the configuration is automatically saved.
 - Trial
Trial mode. In Trial mode, although changes are adopted, they are not saved in the configuration file (startup configuration).
To save changes in the configuration file, use the "Write startup config" button. The "Write startup config" button is displayed when you set trial mode. The display area also shows the message "Trial Mode Active – Press "Write Startup Config" button to make your settings persistent" as soon as there are unsaved modifications. This message can be seen on every WBM page until the changes made have either been saved or the device has been restarted.

Note

PROFINET IO functionality of the device is switched off in "Trial" configuration mode. The device then no longer responds to PROFINET requests. Consequently, a controller does not receive any PROFINET information from the device.

SINEC NMS or SINEMA Server cannot monitor the device with the PROFINET protocol in "Trial" configuration.

Configuration procedure

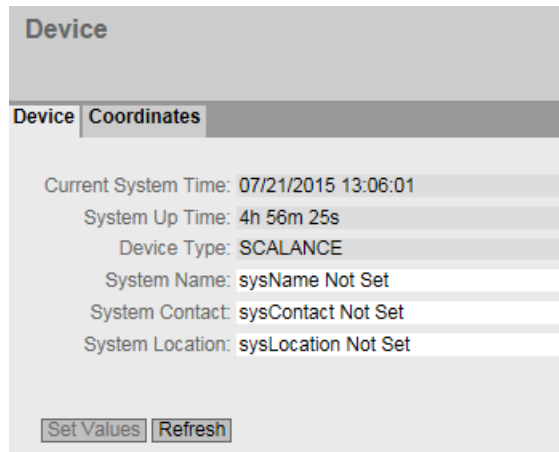
1. To use the required function, select the corresponding check box.
2. Select the options you require from the drop-down lists.
3. Click the "Set Values" button.

6.4.2 General

6.4.2.1 Device

General device information

This page contains the general device information.



The screenshot shows a web interface titled "Device" with a tabbed menu where "Coordinates" is selected. Below the menu, several fields are displayed: "Current System Time: 07/21/2015 13:06:01", "System Up Time: 4h 56m 25s", "Device Type: SCALANCE", "System Name: sysName Not Set", "System Contact: sysContact Not Set", and "System Location: sysLocation Not Set". At the bottom, there are two buttons: "Set Values" and "Refresh".

The boxes "Current System Time", "System Up Time" and "Device Type" cannot be changed.

Description

The page contains the following boxes:

- **Current System Time**
Shows the current system time. The system time is either set by the user or by a time-of-day frame: either SINEC H1 time-of-day frame, NTP or SNTP. (readonly)
- **System Up Time**
Shows the operating time of the device since the last restart. (readonly)
- **Device Type**
Shows the type designation of the device. (readonly)
- **System Name**
You can enter the name of the device. The entered name is displayed in the selection area. A maximum of 255 characters are possible.
The system name is also displayed in the CLI input prompt. The number of characters in the CLI input prompt is limited. The system name is truncated after 16 characters.
- **System Contact**
You can enter the name of a contact person responsible for managing the device. A maximum of 255 characters are possible.
- **System Location**
You can enter the location where the device is installed. The entered installation location is displayed in the selection area. A maximum of 255 characters are possible.

Note

The ASCII code 0x20 to 0x7e is used in the input boxes.

Procedure

1. Enter the contact person responsible for the device in the "System Contact" input box.
2. Enter the identifier for the location at which the device is installed in the "System Location" input box.
3. Enter the name of the device in the "System Name" input box.
4. Click the "Set Values" button.

6.4.2.2 Coordinates

Information on geographic coordinates

In the "Geographic Coordinates" window, you can enter information on the geographic coordinates. The parameters of the geographic coordinates (latitude, longitude and the height above the ellipsoid according to WGS84) are entered directly in the input boxes of the "Geographic Coordinates" window.

Getting the coordinates

Use suitable maps for obtaining the geographic coordinates of the device.

The geographic coordinates can also be obtained using a GPS receiver. The geographic coordinates of these devices are normally displayed directly and only need to be entered in the input boxes of this page.

Geographic Coordinates	
Device	Coordinates
	Latitude: e.g. DD°MM'SS"
	Longitude: e.g. DDD°MM'SS"
	Height: e.g. dddd m

Description

The page contains the following input boxes with a maximum length of 32 characters.

- **"Latitude" input box**
Geographical latitude: Here, enter the value for the northerly or southerly latitude of the location of the device.
For example, the value $+49^{\circ} 1' 31.67''$ means that the device is located at 49 degrees, 1 arc minute and 31.67 arc seconds northerly latitude.
A southerly latitude is shown by a preceding minus character.
You can also append the letters N (northerly latitude) or S (southerly latitude) to the numeric information ($49^{\circ} 1' 31.67''$ N).
- **"Longitude" input box**
Geographic longitude: Here, you enter the value of the eastern or western longitude of the location of the device.
The value $+8^{\circ} 20' 58.73''$ means that the device is located at 8 degrees, 20 minutes and 58.73 seconds east.
A western longitude is indicated by a preceding minus sign.
You can also add the letter E (easterly longitude) or W (westerly longitude) to the numeric information ($8^{\circ} 20' 58.73''$ E).
- **Input box: "Height"**
Height Here, you enter the value of the geographic height above sea level in meters.
For example, 158 m means that the device is located at a height of 158 m above sea level.
Heights below sea level (for example the Dead Sea) are indicated by a preceding minus sign.

Procedure

1. Enter the calculated latitude in the "Latitude" input box.
2. Enter the calculated longitude in the "Longitude" input box.
3. Enter the height above sea level in the "Height" input box.
4. Click the "Set Values" button.

6.4.3 Agent IP

Here, you specify the IP configuration for the device.

With devices with more than one IP interface, this call references the "Subnets > Configuration" menu item in the "Layer 3" menu and the configuration of the TIA interface there.

6.4.4 DNS

6.4.4.1 DNS-Client

The DNS (Domain Name System) server assigns a unique IP address to a domain name so that a device can be uniquely identified.

You can manually configure up to three DNS servers with IPv4 addresses on this page. Manually configured DNS servers are each assigned an index from 1 to 3. Using DHCP, the device can learn two DNS servers with IPv4 addresses. Learned DNS servers are automatically assigned an index from 4 to 5.

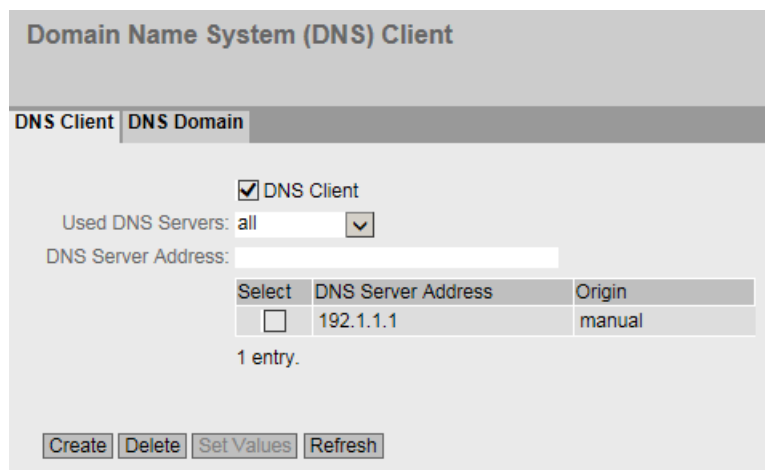
If there is more than one DNS server, the order in the table specifies the order in which the servers are queried. The top server is queried first. A total of seven DNS servers can be configured on the device. Manually configured DNS servers are given preference.

If this function is enabled, the device can communicate with a DNS server as a DNS client. You have the option of entering names in IP address fields.

Note

The "DNS Client" function can only be used if there is a DNS server in the network.

Description



The page contains the following boxes:

- **DNS Client**
Enable or disable depending on whether the device should operate as a DNS client.
- **Used DNS Servers**
Here you specify which DNS server the device uses:
 - learned only
The device uses only the DNS servers assigned by DHCP.
 - manual only
The device uses only the manually configured DNS servers. A maximum of three DNS servers can be configured.
 - all
The device uses all available DNS servers.
- **DNS Server Address**
Enter the IP address of the DNS server.

The table contains the following columns:

- **Select**
Select the check box in the row to be deleted.
- **DNS Server Address**
Shows the IP address of the DNS server.
- **Origin**
This shows whether the DNS server was configured manually or was assigned by DHCP.

Procedure

Activating DNS

1. Enable the "DNS-Client" check box.
2. Click the "Set Values" button.

Creating a DNS server

1. In the "DNS Server Address" box, enter the IP address of the DNS server.
2. Click the "Create" button.

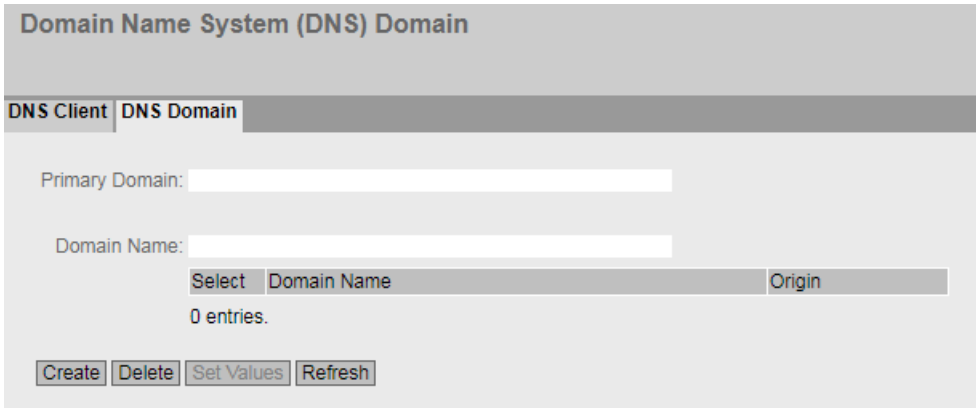
Filtering DNS servers

1. In the "Used DNS Servers" drop-down list, select which DNS servers are to be used.
2. Click the "Set Values" button.

6.4.4.2 DNS domain

On this page, you can manually define up to four domain names. The primary domain name is used first to resolve a host name.

Domain names 2 to 4 can be learned or configured manually on this page. If there is more than one DNS server, the order in the table specifies the order in which the domain names are used.



Description

The page contains the following boxes:

- **Primary Domain**
Enter the name of the primary domain. This entry is used first to resolve a host name.
- **Domain Name**
Enter the name of the other domain.

The table contains the following columns:

- **Select**
Select the check box in the row to be deleted.
- **Domain Name**
Shows the name of the other domain.
- **Origin**
Shows whether the domain name was configured manually or was assigned by DHCP.

Procedure

Specify primary domain

1. In the "Primary Domain" field, enter the name of the primary domain.
2. Click the "Set Values" button.

Specify additional domain

1. In the "Domain Name" field, enter the name of the other domain.
2. Click the "Create" button.

6.4.5 Restart

Resetting to the defaults

In this menu, there is a button with which you can restart the device and the option of resetting to the device to factory settings or resetting the default settings of various profiles.

The screenshot shows a web interface titled "Restart". It features the following elements:

- Buttons: "Restart System", "Restore Factory Defaults and Restart", "Schedule restart", "Cancel scheduled restart", "PROFINET Defaults", "EtherNet/IP Defaults", and "Industrial Ethernet Defaults".
- Input fields: "Restart in: seconds" and a "Backup:" dropdown menu.
- Footer buttons: "Set Values" and "Refresh".

Restore factory defaults

When all the settings are restored to the factory defaults, the IP address and the passwords are also lost. The device can then only be addressed via the serial interface, SINEC PNI or via DHCP.

NOTICE

Depending on the connection, a previously correctly configured device can cause circulating frames after the reset and therefore the failure of the data traffic.

Restore to defaults (profiles)

The profiles provide a preconfiguration for various use cases of the devices.

When you start a device with the default settings of a profile, the settings are reset to the factory settings and some parameters are set so that they are designed for a certain use case. In contrast to restoring the factory defaults, the users and passwords are retained after the

restart. The configured IP address is lost so that the device can then only be accessed via the serial interface, SINEC PNI or using DHCP.

NOTICE

Depending on the connection, a previously correctly configured device can cause circulating frames after the reset and therefore the failure of the data traffic.

The settings that are set specially for a profile are displayed before the restart.

The profiles can be used independently of the factory setting of the device.

Description of the displayed boxes

Note

Note the effects of the individual functions described in the sections above.

To restart the device, the buttons on this page provide you with the following options:

- **Restart**
Click this button to restart the system. You must confirm the restart in a dialog box. During a restart, the device is reinitialized, the internal firmware is reloaded, and the device runs a self-test. The settings of the start configuration are retained, e.g. the IP address of the device. The learned entries in the address table are deleted. You can leave the browser window open while the device restarts. After the restart, you will need to log in again.
- **Restore Factory Defaults and Restart**
Click this button to restore the factory defaults of the device and to restart the device. You must confirm the restart in a dialog box.
The factory defaults depend on the device.

NOTICE

When all the settings are restored to the factory defaults, the IP address and the passwords are also lost. Following this, the device can only be accessed via the serial interface using the Primary Setup Tool or using DHCP.

With the appropriate connection, a previously correctly configured device can cause circulating frames and therefore the failure of the data traffic.

- **Restart in:**
Specify the time after which the device restarts. When "Automatic Save" configuration mode is active, an additional dialog box is displayed. In this dialog box, you can specify whether the device should save the current configuration and switch to "Trial" mode. In any case, the device restarts after the specified time.

- **Backup**

The configuration backups under "System > Configuration Backup" can be selected. Before the scheduled restart, the device applies the configurations of the selected backup and continues working with them after the restart.
All configurations made up to this point that have not been saved in a backup are lost.
With the "-" setting, no file is selected and the device uses the current configuration after the restart.
- **Schedule restart**

When you click this button, a timer starts and runs backwards with the defined time. When the timer has expired, the device restarts.
The following message is also displayed in the display area: "The automatic restart starts in [...] minutes. Click 'Cancel scheduled restart' to cancel the restart". This message can be seen on every WBM page until you cancel the restart or the SCALANCE device is restarted.

Note**Unsaved configuration is lost after restart**

The scheduled restart is performed after the time has elapsed without any further message. Unsaved configuration changes are lost.

Save the current configuration via "System > Configuration Backup" before setting the timer for the restart.

- **Cancel scheduled restart**

With this button, you disable the timer for the scheduled restart.

Restart with predefined Defaults

To restart the device with a predefined profile, the buttons on this page provide you with the following options:

- **PROFINET Defaults**

Click this button to restore the default settings of the PROFINET profile and to restart the device. You must confirm the restart in a dialog box. The dialog box displays the settings specially made for operation with the PROFINET protocol.
- **EtherNet/IP Defaults**

Click this button to restore the default settings of the EtherNet/IP profile and to restart the device. You must confirm the restart in a dialog box. The dialog box displays the settings specially made for operation with the EtherNet/IP protocol.
- **Industrial Ethernet Defaults**

Click this button to restore the default settings of the Industrial Ethernet profile and to restart the device. You must confirm the restart in a dialog box. The dialog box displays the settings specially made for operation in the Industrial Ethernet environment.

6.4.6 Load & Save

Overview of the file types

The table of data types contains the following areas.

Area	File type	Description	Down-load	Save	Delete ¹⁾
Update	Firmware	<p>The firmware is signed and encrypted. This ensures that only firmware created by Siemens can be downloaded to the device.</p> <p>An installed firmware version can be updated to a previous version in this way. At the end of the download process, you can select whether the device restarts with the factory settings of the previous version or with the configuration last saved in the previous version.</p>	X	X	--

Area	File type	Description	Down-load	Save	Delete ¹⁾
Configuration	Config	This file contains the start configuration. Among other things, this device contains the definitions of the users, roles, groups and function rights. The passwords are stored the file "Users".	X	X	--
	ConfigPack	Detailed configuration information, for example, startup configuration, users, certificates, favorites, firmware of the device (if saved as well).	X	X	--
	ConfigPackBack-up	This ZIP file stores all the configuration backups you have created.	X	X	X
	LoginWelcome-Message	The txt file contains the desired text or the ASCII type. Only pure text files in ASCII format are supported.	X	X	X
	RunningCLI	Text file with CLI commands This file contains an overview of the current configuration in the form of CLI commands. Passwords are masked in this file as follows: [PASSWORD] You can download the text file. The file is not intended to be uploaded again unchanged.	--	X	--
	RunningSINEMA-Config	You save the current device configuration in this file type for transfer to STEP 7 Basic/Professional. The file can be imported in STEP 7 Basic/Professional and installed on a device with the same article number and firmware version. Before you can save a file, you must assign a password for the "RunningSINEMAConfig" in the WBM under "System > Load&Save > Passwords". You also need this password to import the file into STEP 7 Basic/Professional. See also "SINEMAConfig"	--	X	--
	Script	Text file with CLI commands You can upload a script file in a device. The CLI commands it contains are executed appropriately. CLI commands for saving and loading files cannot be executed with the CLI script file.	X	--	--
	SINEMAConfig	You load configuration data that was exported via STEP 7 Basic/Professional for transfer to the WBM with this file type. To load a file, you must assign a password for the "SINEMAConfig" under "System > Load&Save > Passwords". You also need this password to export the file from STEP 7 Basic/Professional. See also "RunningSINEMAConfig"	X	--	--
	Users	File with user names and passwords	X	X	--
WBM Fav	WBM favorite pages This file contains the favorites that you created in the WBM.. You can download this file and upload it in other devices.	X	X	X	

6.4 The "System" menu

Area	File type	Description	Down-load	Save	Delete ¹⁾
Certificate & Key	HTTPSCert	<p>Default HTTPS certificates including key</p> <p>The preset and automatically created HTTPS certificates are self-signed.</p> <p>We strongly recommend that you create your own HTTPS certificates and make them available. We recommend that you use HTTPS certificates signed either by a reliable external or by an internal certification authority. The HTTPS certificate checks the identity of the device and controls the encrypted data exchange.</p> <p>The following file types can be loaded into the device.</p> <ul style="list-style-type: none"> • .pem To successfully load an HTTPS certificate with this data type into the device, the certificate must include the unencrypted private key. • .p12 For HTTPS certificates with this file type, the private key is encrypted and secured with a password. To load the certificate successfully into the device, enter the password specified for the file on the WBM page "Passwords (Page 186)". P12 certificates that are encrypted with RC2-40-CBC are not supported. <p>It is recommended that you use password-protected certificates in the PKCS#12 format.</p> <p>The following certificates are supported:</p> <ul style="list-style-type: none"> • RSA certificates with a key length of 2048 bits and 4096 bits. • ECDSA certificates that were generated with secp521r1 (NIST P-521). ECDSA certificates with a key length of 256 bits are present on the device in the delivery state. 	X	X	X
	SSHPrivate-KeyECDSA	<p>SSH private key (ECDSA)</p> <p>The SSH key ecdsa-sha2-nistp521 is supported.</p> <p>There are files to which access is password-protected. To successfully load the file into the device, enter the password specified for the file on the WBM page "Passwords (Page 186)".</p>	X	X	X
	SSHPrivateKeyRSA	<p>SSH private key (RSA) with and without password</p> <p>The following SSH keys are supported:</p> <ul style="list-style-type: none"> • rsa-sha2-512 • rsa-sha2-256 <p>There are files to which access is password-protected. To successfully load the file into the device, enter the password specified for the file on the WBM page "Passwords (Page 186)".</p>	X	X	X

Area	File type	Description	Down-load	Save	Delete ¹⁾
Services & log	Debug	This file contains information for Siemens Support. It is encrypted and can be sent by e-mail to Siemens Support without any security risk.	--	X	X
	DebugExt	This file contains more detailed information for Siemens Support. It is encrypted and can be sent by e-mail to Siemens Support without any security risk. Saving the file may take some time.	--	X	--
	LogFile	File with entries from the event log table	--	X	--
	StartupInfo	Startup log file This file contains the messages that were entered in the log file during the last startup.	--	X	--
Information	EDS	Electronic Data Sheet (EDS) Encoder data set for describing devices in the EtherNet/IP mode	--	X	--
	GSDML	PROFINET information on the device properties	--	X	--
	MIB	Private MSPS MIB file "Scalance_m_msp.mib"	--	X	--
License	LicenseCondi-tions	The ZIP file contains the licensing conditions and copy-right information	--	X	--

¹⁾ Deletion is only possible via HTTP/HTTPS.

6.4.6.1 HTTP

Loading and saving data via HTTP

The WBM allows you to store device data in an external file on your client PC or to load such data from an external file from the client PC to the devices. This means, for example, that you can also load new firmware from a file located on your client PC.

Note

This WBM page is available both for connections using HTTP and for connections using HTTPS.

Firmware

The firmware is signed and encrypted. This ensures that only firmware created by Siemens can be downloaded to the device.

Note

Incompatibility with previous firmware versions with/without PLUG inserted

During the installation of a previous version, the configuration data can be lost. In this case, the device starts up with the factory settings after the firmware has been installed.

In this situation, if a PLUG is inserted in the device, following the restart, this has the status "Not Accepted" since the PLUG still has the configuration data of the previous more up-to-date firmware. This allows you to return to the previous, more up-to-date firmware without any loss of configuration data. If the original configuration on the PLUG is no longer required, the PLUG can be deleted or rewritten manually using the WBM page "System > PLUG".

Configuration files

Note

Configuration files and trial mode/Automatic Save mode

In Automatic Save mode, the data is saved automatically before the configuration files (ConfigPack and Config) are transferred.

In Trial mode, although the changes are adopted, they are not saved in the configuration files (ConfigPack and Config). Use the "Write Startup Config" button on the "System > Configuration" WBM page to save changes in the configuration files.

CLI script file

You can download existing CLI configurations (RunningCLI) and upload your own CLI scripts (Script).

Note

The downloadable CLI script is not intended to be uploaded again unchanged.

Exchange of configuration data with STEP 7 Basic/Professional using a file

You use the two file types "RunningSINEMAConfig" and "SINEMAConfig" to exchange configuration data between a device (WBM) and STEP 7 Basic/Professional via a file.

Requirements:

- Same article number
- Same firmware version
- Password
You assign the password in the WBM under "System > Load&Save > Passwords".

You can use the file types as follows:

- For offline diagnostics
You can save the faulty configuration of a device as "RunningSINEMAConfig" via the WBM and import it in STEP 7 Basic/Professional. No connection to a real device is required for the diagnostics in STEP 7 Basic/Professional. You can export a corrected configuration and load it as "SINEMAConfig" again using the WBM.
- For configuration
No connection to a real device is required to configure a device in STEP 7 Basic/Professional. You can export the configuration and load it as "SINEMAConfig" to the real device using the WBM.

Load and Save via HTTP

HTTP | TFTP | SFTP | Passwords

Update

Type	Description	Load	Save	Delete
Firmware	Firmware Update	Load	Save	

Configuration

Type	Description	Load	Save	Delete
Config	Startup Configuration	Load	Save	
ConfigPack	Startup Config, Users, Certificates and WBM favourites	Load	Save	
ConfigPackBackup	ConfigPackBackup	Load	Save	Delete
LoginWelcomeMessage	Login Welcome Message	Load	Save	Delete
RunningCLI	'show running-config all' CLI settings		Save	
RunningSINEMAConfig	SINEMA Running Configuration		Save	
Script	Script	Load		
SINEMAConfig	SINEMA Offline Configuration	Load		
Users	Users and Passwords	Load	Save	
WBM Fav	WBM favourite pages	Load	Save	Delete

Certificate & Key

Type	Description	Load	Save	Delete
HTTPSCert	HTTPS Certificate	Load	Save	Delete
SSHPrivateKeyECDSA	SSH Private Key (ECDSA)	Load	Save	Delete
SSHPrivateKeyRSA	SSH Private Key (RSA)	Load	Save	Delete

Service & Log

Type	Description	Load	Save	Delete
Debug	Debug Information for Siemens Support		Save	Delete
DebugExt	Extended Debug Information for Siemens Support		Save	
LogFile	Event Log (ASCII)		Save	
StartupInfo	Startup Information		Save	

Information

Type	Description	Load	Save	Delete
EDS	EtherNet/IP Device Description		Save	
GSDML	PROFINET Device Description		Save	
MIB	SCALANCE XNG MSPS MIB		Save	

License

Type	Description	Load	Save	Delete
LicenseConditions	ZIP File with Open Source Software License Conditions		Save	

Description

The table has the following columns:

- **Type**
Shows the file type.
- **Description**
Shows the short description of the file type.
- **Load**
With this button, you can upload files to the device. The button can be enabled, if this function is supported by the file type.
- **Save**
With this button, you can download files from the device. The button can only be enabled if this function is supported by the file type and the file exists on the device.
- **Delete**
With this button, you can delete files from the device. The button can only be enabled if this function is supported by the file type and the file exists on the device.

Note

Following a firmware update, delete the cache of your Internet browser.

Configuration procedure

Uploading data using HTTP

1. Start the upload function by clicking the one of the "Load" buttons.
A dialog for uploading a file opens.
2. Select the required file and confirm the upload.
The file is uploaded.
3. If a restart is necessary, a message to this effect will be output. Click the "OK" button and a restart will follow. If you click the "Abort" button, there is no device restart. The changes only take effect after a restart.

Downloading data using HTTP

1. Start the download by clicking the one of the "Save" buttons.
2. Select a storage location and a name for the file.
3. Save the file.
The file is downloaded and saved.

Deleting files using HTTP

1. Start the delete function by clicking the one of the "Delete" buttons.
The file is deleted.

Reusing configuration data

If several devices are to receive the same configuration and the IP addresses are assigned using DHCP, the effort for configuration can be reduced by saving and reading in the configuration data.

Follow the steps below to reuse configuration data:

1. Save the configuration data of a configured device on your PC.
2. Load these configuration files onto all other devices you want to configure in this way.
3. If individual settings are necessary for specific devices, these must be made online on the relevant device.

Note

Configuration data has a checksum. If you edit the files, you can no longer upload them to the IE switch.

Updating firmware

1. Load a new firmware version into the device with the "Load" button.
2. Confirm the device restart at the end of the update process.
The device restarts with the settings saved in the last version.

Updating firmware to a previous version

You have the option to load an older firmware version into the device if a newer version is running on the device.

Note**Downgrade from V1.1 to V1.0**

This function is not available with layer 3 devices. These devices are approved as of V1.1.

1. Click "Load".
2. In the dialog window, select the file with the previous version of the currently loaded firmware.
3. In the dialog displayed at the end of the load process, select one of the options:
 - Restart with rollback configuration
The device restarts with the last saved configuration.
 - Restart with factory defaults
The device is reset to the factory settings of the version to be loaded and then restarts.
 - Do not restart
You must manually perform a restart on the page "System > Restart".

6.4.6.2 TFTP

Loading and saving data via a TFTP server

On this page, you can configure the TFTP server and the file names. The WBM also allows you to store device data in an external file on a TFTP server or to load such data from an external file from the TFTP server to the devices. This means, for example, that you can also load new firmware from a file located on a TFTP server.

Firmware

The firmware is signed and encrypted. This ensures that only firmware created by Siemens can be downloaded to the device.

Note

Incompatibility with previous firmware versions with/without PLUG inserted

During the installation of a previous version, the configuration data can be lost. In this case, the device starts up with the factory settings after the firmware has been installed.

In this situation, if a PLUG is inserted in the device, following the restart, this has the status "Not Accepted" since the PLUG still has the configuration data of the previous more up-to-date firmware. This allows you to return to the previous, more up-to-date firmware without any loss of configuration data. If the original configuration on the PLUG is no longer required, the PLUG can be deleted or rewritten manually using the WBM page "System > PLUG".

Configuration files

Note

Configuration files and trial mode/Automatic Save mode

In Automatic Save mode, the data is saved automatically before the configuration files (ConfigPack and Config) are transferred.

In Trial mode, although the changes are adopted, they are not saved in the configuration files (ConfigPack and Config). Use the "Write Startup Config" button on the "System > Configuration" WBM page to save changes in the configuration files.

CLI script file

You can download existing CLI configurations (RunningCLI) and upload your own CLI scripts (Script).

Note

The downloadable CLI script is not intended to be uploaded again unchanged.

Exchange of configuration data with STEP 7 Basic/Professional using a file

You use the two file types "RunningSINEMAConfig" and "SINEMAConfig" to exchange configuration data between a device (WBM) and STEP 7 Basic/Professional via a file.

Requirements:

- Same article number
- Same firmware version
- Password
You assign the password in the WBM under "System > Load&Save > Passwords".

You can use the file types as follows:

- For offline diagnostics
You can save the faulty configuration of a device as "RunningSINEMAConfig" via the WBM and import it in STEP 7 Basic/Professional. No connection to a real device is required for the diagnostics in STEP 7 Basic/Professional. You can export a corrected configuration and load it as "SINEMAConfig" again using the WBM.
- For configuration
No connection to a real device is required to configure a device in STEP 7 Basic/Professional. You can export the configuration and load it as "SINEMAConfig" to the real device using the WBM.

Load and Save via TFTP

HTTP | TFTP | SFTP | Passwords

TFTP Server Address: 0.0.0.0
TFTP Server Port: 69

Update

Type	Description	Filename	Actions
Firmware	Firmware Update	firmware_SCALANCE_XC300.sfw	Select action

Configuration

Type	Description	Filename	Actions
Config	Startup Configuration	config_SCALANCE_XC300.conf	Select action
ConfigPack	Startup Config, Users, Certificates and WBM favourites	configpack_SCALANCE_XC300.zip	Select action
ConfigPackBackup	ConfigPackBackup	configbackup_SCALANCE_XC300.zip	Select action
LoginWelcomeMessage	Login Welcome Message	login_welcome_message.txt	Select action
RunningCLI	'show running-config all' CLI settings	RunningCLI.txt	Select action
RunningSINEMAConfig	SINEMA Running Configuration	sinema_config_running.zip	Select action
Script	Script	Script.txt	Select action
SINEMAConfig	SINEMA Offline Configuration	sinema_config.zip	Select action
Users	Users and Passwords	users.enc	Select action
WBM Fav	WBM favourite pages	wbmfav.txt	Select action

Certificate & Key

Type	Description	Filename	Actions
HTTPSCert	HTTPS Certificate	https_cert	Select action
SSHPrivateKeyECDSA	SSH Private Key (ECDSA)	sshprivatekeyecdsa	Select action
SSHPrivateKeyRSA	SSH Private Key (RSA)	sshprivatekeyrsa	Select action

Service & Log

Type	Description	Filename	Actions
Debug	Debug Information for Siemens Support	debug_SCALANCE_XC300.bin	Select action
DebugExt	Extended Debug Information for Siemens Support	DebugExt.bin	Select action
LogFile	Event Log (ASCII)	logfile_SCALANCE_XC300.csv	Select action
StartupInfo	Startup Information	startup_SCALANCE_XC300.log	Select action

Information

Type	Description	Filename	Actions
EDS	EtherNet/IP Device Description	EDS_SCALANCE_X300_MSPS.zip	Select action
GSDML	PROFINET Device Description	gsdml_SCALANCE_XC300.zip	Select action
MIB	SCALANCE XNG MSPS MIB	scalance_xng_msp.mib	Select action

License

Type	Description	Filename	Actions
LicenseConditions	ZIP File with Open Source Software License Conditions	OSS_Readme.zip	Select action

Set Values Refresh

Description

The page contains the following boxes:

- **TFTP Server Address**
Here, you enter the IP address or the FQDN (Fully Qualified Domain Name) of the TFTP server with which you exchange data.
- **"TFTP Server Port"**
Here, enter the port of the TFTP server over which data exchange will be handled. If necessary, you can change the default value 69 to your own requirements.

The table has the following columns:

- **Type**
Shows the file type.
- **Description**
Shows the short description of the file type.
- **Filename**
A file name is preset here for every file type.

Note

Changing the file name

You can change the file name preset in this column. After clicking the "Set Values" button, the changed name is saved on the device and can also be used with the Command Line Interface.

- **Actions**
Select the action from the drop-down list. The selection depends on the selected file type, for example you can only save the log file.
The following actions are possible:
 - **Save file**
With this selection, you save a file on the TFTP server.
 - **Load file**
With this selection, you load a file from the TFTP server.

Configuration procedure

Loading or saving data using TFTP

1. Enter the IP address or the FQDN of the TFTP server in the "TFTP Server Address" input box.
2. Enter the server port of the TFTP server to be used in the in the "TFTP Server Port" input box.
3. If applicable, enter the name of a file in which you want to save the data or take the data from in the "File name" input box.
4. Select the action you want to execute from the "Actions" drop-down list.
5. Click the "Set Values" button to start the selected actions.
6. If a restart is necessary, a message to this effect will be output. Click the "OK" button to run the restart. If you click the "Abort" button, there is no device restart. The changes only take effect after a restart.

Reusing configuration data

If several devices are to receive the same configuration and the IP addresses are assigned using DHCP, the effort for configuration can be reduced by saving and reading in the configuration data.

Follow the steps below to reuse configuration data:

1. Save the configuration data of a configured device on your PC.
2. Load these configuration files onto all other devices you want to configure in this way.
3. If individual settings are necessary for specific devices, these must be made online on the relevant device.

Note that the configuration data is coded when it is saved. This means that you cannot edit the files with a text editor.

Updating firmware

1. Load a new firmware version into the device with the "Load" button.
2. Confirm the device restart at the end of the update process.
The device restarts with the settings saved in the last version.

Updating firmware to a previous version

You have the option to load an older firmware version into the device if a newer version is running on the device.

Note

Downgrade from V1.1 to V1.0

This function is not available with layer 3 devices. These devices are approved as of V1.1.

1. Click "Load".
2. In the dialog window, select the file with the previous version of the currently loaded firmware.
3. In the dialog displayed at the end of the load process, select one of the options:
 - Restart with rollback configuration
The device restarts with the last saved configuration.
 - Restart with factory defaults
The device is reset to the factory settings of the version to be loaded and then restarts.
 - Do not restart
You must manually perform a restart on the page "System > Restart".

6.4.6.3 SFTP

Loading and saving data via an SFTP server

SFTP (SSH File Transfer Protocol) transfers the files encrypted. On this page, you configure the access data for the SFTP server.

The WBM also allows you to store device data in an external file on your client PC or to load such data from an external file from the PC to the devices. This means, for example, that you can also load new firmware from a file located on your Admin PC.

On this page, the certificates required to establish a secure VPN connection can also be loaded.

Firmware

The firmware is signed and encrypted. This ensures that only firmware created by Siemens can be downloaded to the device.

Configuration files

Note

Configuration files and Trial mode /Automatic Save

In "Automatic Save" mode, the data is saved automatically before the configuration files (ConfigPack and Config) are transferred.

In "Trial" mode, although the changes are adopted, they are not saved in the configuration files (ConfigPack and Config). Use the "Write Startup Config" button on the "System > Configuration" WBM page to save changes in the configuration files.

CLI script file

You can download existing CLI configurations (RunningCLI) and upload your own CLI scripts (Script).

Note

The downloadable CLI script is not intended to be uploaded again unchanged.

CLI commands for saving and loading files cannot be executed with the CLI script file (Script).

Exchange of configuration data with STEP 7 Basic/Professional using a file

You use the two file types "RunningSINEMAConfig" and "SINEMAConfig" to exchange configuration data between a device (WBM) and STEP 7 Basic/Professional via a file.

Requirements:

- Same article number
- Same firmware version
- Password
You assign the password in the WBM under "System > Load&Save > Passwords".

You can use the file types as follows:

- For offline diagnostics
You can save the faulty configuration of a device as "RunningSINEMAConfig" via the WBM and import it in STEP 7 Basic/Professional. No connection to a real device is required for the diagnostics in STEP 7 Basic/Professional. You can export a corrected configuration and load it as "SINEMAConfig" again using the WBM.
- For configuration
No connection to a real device is required to configure a device in STEP 7 Basic/Professional. You can export the configuration and load it as "SINEMAConfig" to the real device using the WBM.

Load and Save via SFTP

HTTP | **TFTP** | **SFTP** | Passwords

SFTP Server Address: 0.0.0.0
 SFTP Server Port: 22
 SFTP User:
 SFTP Password:
 SFTP Password Confirmation:

Update

Type	Description	Filename	Actions
Firmware	Firmware Update	firmware_SCALANCE_XC300.sfw	Select action

Configuration

Type	Description	Filename	Actions
Config	Startup Configuration	config_SCALANCE_XC300.conf	Select action
ConfigPack	Startup Config, Users, Certificates and WBM favourites	configpack_SCALANCE_XC300.zip	Select action
ConfigPackBackup	ConfigPackBackup	configbackup_SCALANCE_XC300.zip	Select action
LoginWelcomeMessage	Login Welcome Message	login_welcome_message.txt	Select action
RunningCLI	'show running-config all' CLI settings	RunningCLI.txt	Select action
RunningSINEMAConfig	SINEMA Running Configuration	sinema_config_running.zip	Select action
Script	Script	Script.txt	Select action
SINEMAConfig	SINEMA Offline Configuration	sinema_config.zip	Select action
Users	Users and Passwords	users.enc	Select action
WBM Fav	WBM favourite pages	wbmfav.txt	Select action

Certificate & Key

Type	Description	Filename	Actions
HTTPSCert	HTTPS Certificate	https_cert	Select action
SSHPrivateKeyECDSA	SSH Private Key (ECDSA)	sshprivatekeyecdsa	Select action
SSHPrivateKeyRSA	SSH Private Key (RSA)	sshprivatekeyrsa	Select action

Service & Log

Type	Description	Filename	Actions
Debug	Debug Information for Siemens Support	debug_SCALANCE_XC300.bin	Select action
DebugExt	Extended Debug Information for Siemens Support	DebugExt.bin	Select action
LogFile	Event Log (ASCII)	logfile_SCALANCE_XC300.csv	Select action
StartupInfo	Startup Information	startup_SCALANCE_XC300.log	Select action

Information

Type	Description	Filename	Actions
EDS	EtherNet/IP Device Description	EDS_SCALANCE_X300_MSPS.zip	Select action
GSDML	PROFINET Device Description	gsdml_SCALANCE_XC300.zip	Select action
MIB	SCALANCE XNG MSPS MIB	scalance_xng_msp.mib	Select action

License

Type	Description	Filename	Actions
LicenseConditions	ZIP File with Open Source Software License Conditions	OSS_Readme.zip	Select action

Set Values Refresh

Description

The page contains the following boxes:

- **SFTP Server Address**
Enter the IP address or the FQDN of the SFTP server with which you exchange data.
- **SFTP Server Port**
Enter the port of the SFTP server via which data exchange will be handled. If necessary, you can change the default value 22 to your own requirements.
- **SFTP User**
Enter the user for access to the SFTP server. This assumes that a user with the corresponding rights has been created on the SFTP server.
- **SFTP Password**
Enter the password for the user
- **SFTP Password Confirmation**
Confirm the password.

The table has the following columns:

- **Type**
Shows the file type.
- **Description**
Shows the short description of the file type.
- **Filename**
A file name is preset here for every file type.

Note

Changing the file name

You can change the file name preset in this column. After clicking the "Set Values" button, the changed name is saved on the device and can also be used with the Command Line Interface.

- **Actions**
Select the action from the drop-down list. The selection depends on the selected file type, for example you can only save the log file.
The following actions are possible:
 - **Save file**
With this selection, you save a file on the SFTP server.
 - **Load file**
With this selection, you load a file from the SFTP server.

Procedure

Loading or saving data using SFTP

1. Enter the address of the SFTP server in "SFTP Server Address".
2. Enter the port of the SFTP server to be used in "SFTP Server Port".
3. Enter the user data (user name and password) required for access to the SFTP server.

4. If applicable, enter the name of a file in which you want to save the data or take the data from in "Filename".

Note**Files whose access is password protected**

To be able to load these files on the device successfully, you need to enter the password specified for the file in "System" > "Load&Save" > "Passwords".

5. Select the action you want to execute from the "Actions" drop-down list.
6. Click "Set Values" to start the selected action.
7. If a restart is necessary, a message to this effect will be output. Click the "OK" button to run the restart. If you click the "Abort" button, there is no device restart. The changes only take effect after a restart.

Reusing configuration data

If several identical devices are to receive the same configuration and the IP addresses are assigned using DHCP, the effort for reconfiguration can be reduced by saving and reading in the configuration data.

Follow the steps below to reuse configuration data:

1. Save the configuration data of a configured device on your PC.
2. Load these configuration files onto all other devices you want to configure in this way.
3. If individual settings are necessary for specific devices, these must be made online on the relevant device.

Note

Configuration data has a checksum. If you change the data, you can no longer upload it to the IE switch.

Updating firmware

1. Load a new firmware version into the device with the "Load" button.
2. Confirm the device restart at the end of the update process.
The device restarts with the settings saved in the last version.

Updating firmware to a previous version

You have the option to load an older firmware version into the device if a newer version is running on the device.

Note**Downgrade from V1.1 to V1.0**

This function is not available with layer 3 devices. These devices are approved as of V1.1.

6.4 The "System" menu

1. Click "Load".
2. In the dialog window, select the file with the previous version of the currently loaded firmware.
3. In the dialog displayed at the end of the load process, select one of the options:
 - Restart with rollback configuration
The device restarts with the last saved configuration.
 - Restart with factory defaults
The device is reset to the factory settings of the version to be loaded and then restarts.
 - Do not restart
You must manually perform a restart on the page "System > Restart".

6.4.6.4 Passwords

There are files to which access is password-protected. For example to be able to use the HTTPS certificate, you need to specify the corresponding password on this WBM page.

Type	Description	Setting	Password	Password Confirmation	Status
Config	Startup Configuration	<input type="checkbox"/>			-
ConfigPack	Startup Config, Users, Certificates and WBM favourites	<input type="checkbox"/>			-
HTTPS Cert	HTTPS Certificate	<input type="checkbox"/>			-
RunnmgSINEMAConfig	SINEMA Running Configuration	<input type="checkbox"/>			Required
SINEMAConfig	SINEMA Offline Configuration	<input type="checkbox"/>			Required
SSHPrivateKeyECDSA	SSH Private Key (ECDSA)	<input type="checkbox"/>			-
SSHPrivateKeyRSA	SSH Private Key (RSA)	<input type="checkbox"/>			-

Description

The table has the following columns:

- **Type**
Shows the file type.
- **Description**
Shows the short description of the file type.
- **Setting**
When enabled, the file is used. Can only be enabled if the password is configured.
- **Password**
Enter the password for the file.

- **Password Confirmation**
Confirm the password.
- **Status**
Shows whether the current settings for the file match the device.
 - valid
The "Setting" check box is selected, and the password matches the file.
 - invalid
The "Setting" check box is selected but the password does not match the file or no file has been loaded yet.
 - ' '
The password cannot be evaluated or is not yet being used. The "Setting" check box is not selected.
 - Required
A password is needed to use the specified file type. The "Setting" check box is not selected.

Procedure

1. Enter the password in "Password".
2. To confirm the password, enter the password again in "Password Confirmation".
3. Enable the "Setting" option.
4. Click the "Set Values" button.

6.4.7 Events

6.4.7.1 Configuration

Selecting system events

On this page, you specify how a device reacts to system events. By enabling the appropriate options, you specify how the device reacts to events. To enable or disable the options, click the relevant check boxes of the columns.

Event Configuration

Configuration | Severity Filters

Signaling Contact Method: conventional ▾

Signaling Contact Status: open ▾

Log Table Alarm Threshold: 350

	E-mail	Trap	Log Table	Syslog	Fault	Copy To Table
All Events	No Change ▾	No Change ▾	No Change ▾	No Change ▾	No Change ▾	Copy To Table

Event	E-mail	Trap	Log Table	Syslog	Fault
Cold/Warm Start	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Link Change	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Authentication Failure	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
RMON Alarm	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Power Change	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
RM State Change	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Spanning Tree Change	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Fault State Change	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Standby State Change	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
VRRP State Change	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Loop Detection	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Diagnostics Alarms	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
OSPF State Change	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
802.1X Port Authentication State Change	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
FMP Status Change	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
CLI Script File	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Secure NTP	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Configuration Change	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
MRP Interconnection State Change	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Service Information	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
DHCP Server Log	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	

Set Values | Refresh

Description of the displayed boxes

The page contains the following boxes:

- **"Signaling Contact Method" drop-down list**

Select the reaction of the signaling contact from the drop-down list. The following reactions are possible:

 - conventional
Default setting for the signaling contact. An error/fault is displayed by the fault LED and the signaling contact is opened. When the error/fault state no longer exists, the fault LED goes off and the signaling contact is closed.
 - User Defined
The way the signaling contact works does not depend on the error/fault that has occurred. The signaling contact can be opened or closed as required by user actions.
- **"Signaling Contact Status" drop-down list**

Select the status of the signaling contact from the drop-down list. The following states are possible:

 - Closed
Signaling contact is closed.
 - Open
Signaling contact is opened.
- **Log Table Alarm Threshold**

Set the limit for the entries for each severity. A maximum of 350 entries are possible for each severity.
If the specified limit will be reached with the next entry, an alarm message is output, e.g. if 350 is specified, the message that the limit has been reached is output after entry 349.

The table has the following columns:

- **Event**

The column contains the following values:

- Cold/Warm Start
The device was turned on or restarted by the user.
- Link Change
This event occurs only when the port status is monitored and has changed, see "System > Fault Monitoring > Link Change".
- Authentication Failure
This event occurs when access is attempted with an incorrect password.
- RMON Alarm
An alarm or event has occurred relating to the remote monitoring of the system.
- Power Change
This event occurs only when power supply lines 1 and 2 are monitored. It indicates that there was a change to line 1 or line 2. See "System > Fault Monitoring > Power Supply".
- RM State Change
The redundancy manager has recognized an interruption or restoration of the ring and has switched the line over or back.
- Spanning Tree Change
The STP or RSTP or MSTP topology has changed.
- Fault State Change
The fault status has changed. The fault status can relate to the activated port monitoring, the response of the signaling contact or the power supply monitoring.
- Standby State Change
A device with an established standby connection (master or slave) has activated or deactivated the link to the other ring (standby port). The data traffic was redirected from one Ethernet connection (standby port of the master) to another Ethernet connection (standby port of the slave).
- VRRP State Change (only with routing using VRRP)
The state of the virtual router has changed.
- Loop Detection
A loop was detected in the network segment.
- Diagnostics Alarms
A diagnostics value has fallen below or exceeded a certain limit.
- OSPF State Change
The status of OSPF has changed.
- 802.1X Port Authentication State Change
This event occurs with 802.1X authentications.
- FMP Status Change
The value of the received power or the power loss has exceeded or fallen below a certain limit.
- CLI script file
An error was detected in the CLI script:

- Secure NTP
An error occurred when using Secure NTP, e.g. a key with the wrong length was specified.
- Configuration Change
The configuration was saved retentively.
- MRP Interconnection State Change
This event is triggered when the redundant connection is no longer available. The cause can be either the loss of the primary or the secondary MRP Interconnection connection.
- Service Information
For certain events, entries are made in the log table even without configuration. For these events, you can configure additional subsequent actions here (e-mail, trap, syslog).
- DHCP Server Log
DHCP events are logged. The prerequisite is that the DHCP server is enabled on the device.
- **E-Mail**
The device sends an e-mail. This is only possible if the SMTP server is set up and the "SMTP client" function is enabled.
- **Trap**
The device sends an SNMP trap. This is only possible if "SNMPv1 Traps" is enabled in "System > Configuration".
- **Log table**
The device writes an entry in the event log table, see "Information > Log Table"
- **Syslog**
The device writes an entry to the system log server. This is only possible if the system log server is set up and the "Syslog client" function is enabled.
- **Faults**
The device triggers an error. The error LED lights up

Configuration procedure

1. Select the check box in the row of the required event. Select the event in the column under the following actions:
 - E-mail
 - Trap
 - Log Table
 - Syslog
 - Faults
2. Click the "Set Values" button.

6.4.7.2 Severity Filters

Setting the Severity Filters

On this page, you configure the severity for the sending of system event notifications.

Client Type	Severity
E-mail	Info
Log Table	Info
Syslog	Info

Set Values Refresh

Description

The table has the following columns:

- **Client Type**
Select the client type for which you want to make settings:
 - E-mail
Sending of system event messages by e-mail
 - Log Table
Entry of system events in the log table
 - Syslog
Sending of system event messages to a syslog server
- **Severity**
Select the desired severity. The following settings are possible:
 - **Critical**
System events with the severity Critical are processed.
 - **Warning**
System events with the severity Warning or higher are processed: This means events of the categories "Warning" and "Critical".
 - **Info**
System events with the severity Info or higher are processed: This means events of the categories "Info", "Warning" and "Critical".

Procedure

Follow the steps below to configure the required level:

1. Select the required values from the drop-down lists of the second table column after the client types.
2. Click the "Set Values" button.

6.4.8 SMTP Client

6.4.8.1 General

Network monitoring with e-mails

If events occur, the device can automatically send an e-mail, e.g. to the service technician. The e-mail contains the identification of the sending device, a description of the cause in plain text, and a time stamp. This allows centralized network monitoring to be set up for networks with few nodes based on an e-mail system.

Simple Mail Transfer Protocol (SMTP) Client General

General Receiver

SMTP Client

SMTP Server Address:

Select	Status	SMTP Server Address	Sender Address	Username	Password	Password Confirmation	Port	Security	Test	Test Result
<input type="checkbox"/>	<input checked="" type="checkbox"/>	192.168.16.10	Device1@auto.de				465	SSL/TLS	Test	Connection with server failed
<input type="checkbox"/>	<input checked="" type="checkbox"/>	192.168.16.200	Device1@auto.de				25	None	Test	
<input type="checkbox"/>	<input checked="" type="checkbox"/>	192.168.16.220					25	None	Test	

3 entries.

Requirements for sending e-mails

- "E-mail" is activated for the relevant event in "System > Events > Configuration".
- The desired severity is configured under "System > Events > Severity level".
- At least one entry exists under "System > SMTP Client > Receiver" and the setting "Send" is activated.

Description

The page contains the following boxes:

- **SMTP Client**
Enable or disable the SMTP client.
- **SMTP Server Address**
Enter the IP address or the FQDN of the SMTP server.

The table contains the following columns:

- **Select**
Select the check box in a row to be deleted.
 - **Status**
Specify whether this SMTP server will be used.
 - **SMTP Server Address**
Shows the SMTP server IP address.
 - **Sender Email Address**
Enter the e-mail address of the sender that is specified in the e-mail.
 - **User Name**
If necessary, enter the user name used for authentication on the SMTP server.
 - **Password**
If necessary, enter the password used for authentication on the SMTP server.
 - **Password Confirmation**
Repeat the password.
 - **Port**
Enter the port via which your SMTP server can be reached.
Factory settings:
 - 25 (None)
 - 465 (SSL/TLS and StartTLS)
 - **Security**
Specify whether transfer of the e-mail from the device to the SMTP server is encrypted. This is only possible when the SMTP server supports the selected setting.
-
- Note**
- 2-factor authentication (2FA)**
- 2-factor authentication is not supported.
-
- SSL/TLS
 - StartTLS
 - None: The e-mail is transferred unencrypted.
- **Test**
Sends a test email to the configured receivers.
 - **Test Result**
Shows whether the e-mail was sent successfully or not. If sending was not successful, the message contains possible causes.

Procedure

Configuring the SMTP server

1. Enable the "SMTP Client" function.
2. Enter the IP address of the SMTP server in "SMTP Server Address".

3. Click the "Create" button. A new entry is generated in the table.
4. Enter the name of the sender that will be included in the e-mail for "Sender Email Address".
5. Enter the user name and password if the SMTP server prompts you to log in.
6. Under "Security", specify whether transfer to the SMTP server is encrypted.
7. Enable the SMTP server entry.
8. Click the "Set Values" button.

Note

Depending on the properties and configuration of the SMTP server, it may be necessary to adapt the "Sender E-Mail Address" input for the e-mails. Check with the administrator of the SMTP server.

Testing the configuration of the SMTP server

1. Configure receivers
 - Click the "Receiver" tab.
 - Select the desired SMTP server under "SMTP server".
 - Enter the desired address under "E-mail address of the SMTP recipient".
 - Click the "Create" button. A new entry is generated in the table. The setting "Send" is enabled by default.
2. Sending a test e-mail
 - Click the "General" tab.
 - Click the "Test" button next to the SMTP server entry. The device sends a test email to every configured receiver.
 - Check the test result. If sending was not successful, the message contains possible causes.

6.4.8.2 Recipient

On this page, you specify who receives an e-mail when an event occurs.

Simple Mail Transfer Protocol (SMTP) Client Receiver

General
Receiver

SMTP Server: ▼

SMTP Receiver Email Address:

Select	SMTP Server	Send	SMTP Receiver Email Address
<input type="checkbox"/>	192.168.16.10	<input checked="" type="checkbox"/>	service@device.de

1 entry.

Create
Delete
Set Values
Refresh

Description

The page contains the following boxes:

- **SMTP Server**
Specify the SMTP server via which the e-mail is sent.
- **Email address of the SMTP receiver**
Enter the e-mail address to which the device sends an e-mail.

The table contains the following columns:

- **Select**
Select the check box in a row to be deleted.
- **SMTP Server**
Shows the IP address of the SMTP server to which the entry relates.
- **Send**
When enabled, the device sends an email to this receiver.
- **Email address of the SMTP receiver**
Shows the e-mail address to which the device sends an e-mail if a fault occurs.

Procedure

Configuring an SMTP receiver

1. Select the required "SMTP server".
2. Enter the email address of the SMTP receiver.
3. Click the "Create" button. A new entry is generated in the table.
4. Activate the "Send" option for the entry.
5. Click the "Set Values" button.

6.4.9 DHCPv4

6.4.9.1 DHCP Client

Setting of the DHCP mode

If the device is configured as a DHCP client, it starts a DHCP request. As response, the device receives an IPv4 address from the DHCP server. The server manages an address range from which it assigns IPv4 addresses. It is also possible to configure the server so that the client always receives the same IPv4 address in response to its request.

The screenshot shows the 'Dynamic Host Configuration Protocol (DHCP) Client' configuration page. It features a navigation bar with tabs for 'DHCP Client', 'DHCP Client Options', 'DHCP Server', 'Port-IP Address Mapping', 'Port Range', 'DHCP Options', and 'Relay Agent Information'. The 'DHCP Client' tab is active. Below the navigation bar, there are sub-tabs for 'Static Leases' and 'Host Options'. The main configuration area includes a 'Keep Alive' checkbox, a 'DHCP Client Configuration Request (Opt.66, 67):' dropdown menu set to 'setup', and a 'DHCP Mode:' dropdown menu set to 'via MAC Address'. Below these options is a table with three columns: 'Interface', 'DHCP', and 'IAID Value'. The table contains one row for 'vlan1' with a checkbox in the 'DHCP' column and the value '00-00-00-3D' in the 'IAID Value' column. At the bottom left, there are 'Set Values' and 'Refresh' buttons.

Interface	DHCP	IAID Value
vlan1	<input type="checkbox"/>	00-00-00-3D

Description

The page contains the following boxes:

- **Keep Alive**
Keep Alive is disabled by default. If Keep Alive is disabled, the IP address is reset to 0.0.0.0 when the connection to the DHCP server is lost or after the lease time expires. If the function is enabled, the IP address is kept alive and is not reset to 0.0.0.0 when the connection to the DHCP server is lost or after the lease time expires.
- **DHCP client configuration file request (opt. 66, 67)**
When enabled, the DHCP client uses the options to download the configuration file (option 67) from the TFTP server (option 66). After the restart, the device uses the data from the configuration file.

NOTICE
<p>Security hazard - risk of unauthorized access and/or misuse</p> <p>The function can potentially be used to change the functionality of the device and thus cause the failure of data traffic. Users with malicious intent could cause the device to load a manipulated configuration file in order to change the configuration to their benefit.</p> <p>To prevent unauthorized access and/or misuse, disable the function if you are not using it (Off).</p> <p>In a device with default setting (Setup), no configuration file is loaded from the DHCP server even if the options 66 and 67 are still contained in the DHCP queries of the DHCP client after the first login with the default user profile admin and the assignment of a new password.</p>

- **Setup**
Default setting. The function depends on the status of the device. In the delivery state and after reset to default settings, the function behaves as with the setting **On** and the function is enabled for all DHCP client interfaces. The following events trigger a status change of the device: The first login with the default user profile admin and the associated assignment of a new password as well as the loading of a configuration file. Afterwards, the device is in the secure operating state and the function behaves as with the **Off** option: The option is disabled for all DHCP client interfaces. The status changes automatically.
- **On**
The function is enabled. The DHCP client requests a configuration file with the next DHCP query.
- **Off**
The function is disabled. The DHCP client does not request a configuration file.

- **DHCP Mode**
Specify the type of identifier with which the DHCP client logs on with its DHCP server:
 - via MAC Address
Default setting. Identification is based on the MAC address.
 - via DHCP Client ID
Identification is based on a freely defined DHCP client ID.
 - via System Name
Identification is based on the system name. If the system name is 255 characters long, the last character is not used for identification.
 - via PROFINET Name of Station
The identification runs via the PROFINET device name.
 - via IAID and DUID
The identification runs via the IAID (Identity Association Identifier) and the DUID (DHCP Unique Identifier).
- **DHCP Client ID**
The input box appears if you select the DHCP mode "via DHCP client ID". Enter a DHCP Client ID.

The table has the following columns:

- **Interface**
Interface to which the setting relates.
- **DHCP**
Enable or disable the DHCP client for the relevant interface.
- **IAID Value**
Value with which the interface (DHCP client) identifies itself on the DHCP server.

RADIUS authentication and DHCP

Only after it has been assigned an IP address can the SCALANCE X start the RADIUS authentication. The DHCP server, therefore, must be reachable via a port that must not be authenticated by the RADIUS server.

The authentication process can be delayed for the following reasons:

- The first configured RADIUS server is unreachable.
- A fallback to MAC authentication takes place.

Procedure

Follow the steps below to configure the IP address using the DHCP client ID:

1. Select the identification method in the "DHCP Mode" drop-down list.
If you select the DHCP mode "via DHCP Client ID" an input box appears.
In the enabled input box "DHCP client ID" enter a string to identify the device. This is then evaluated by the DHCP server.
2. Select the "DHCP Client Configuration Request (Opt. 66, 67)", if you want the DHCP client to use options 66 and 67 to download and then enable a configuration file.

3. Enable the "DHCP" option in the table.
4. Click the "Set Values" button.

Note

If a configuration file is downloaded, this can trigger a system restart. If the currently running configuration and the configuration in the downloaded configuration file differ, the system restarts.

Make sure that the option "DHCP Client Configuration Request (Opt. 66, 67)" is no longer set.

6.4.9.2 DHCP Client Options

On this page, you specify which additional DHCP options the client uses.

Description

The page contains the following boxes:

- **Interface**
Select the interface for which the option should apply.
- **Option Code**
Select the desired DHCP option.
- **Value**
Enter the value for the option.

The table has the following columns:

- **Select**
Select the check box in the row to be deleted.
- **Interface**
Displays the interface for which the option should apply.

- **Option Code**
Shows the number of the DHCP option.
- **Value**
Enter the DHCP parameter that is transferred from the DHCP client to the server. The content depends on the DHCP option.
 - DHCP option 60 (vendor class):
The server compares this value with the pool name. If they match, the corresponding pool is selected.

Procedure

Creating a DHCP option

1. Select an interface.
2. Select an Option Code.
3. Enter a value.
4. Click the "Create" button.

Deleting a DHCP option

1. Enable the "Select" check box in the row to be deleted.
Repeat this for all entries you want to delete.
2. Click the "Delete" button.
The entry is deleted.

6.4.9.3 DHCP Server

You can operate the device as a DHCP server. This allows IP addresses to be assigned automatically to the connected devices. The IP addresses are either distributed dynamically from an address band (pool) you have specified or a specific IP address is assigned to a particular device.

Both with the dynamic and static assignment a pool is selected based on the following criteria:

1. With the DHCP query option 82 is enabled.
The DHCP server checks whether there is a pool with option 82. You configure this criterion in the "Relay Agent Information" tab.
2. The DHCP query was received via a relay agent.
The DHCP server checks whether the relay agent is located in the subnet of a pool.
3. The port via which the DHCP query was received is enabled in the Port Range.
The DHCP server checks whether the IP interface of the port is located in the subnet of a pool. You configure this criterion on the page "Layer 3 (IPv4) > Subnets". In addition, the DHCP server checks whether the DHCP client applies DHCP option 60 (vendor class) to select a relevant pool. You can find more information in the section "DHCP Client Options (Page 200)".

During configuration make sure that the selection of the pool based on the criteria named is possible. If the criteria match several pools, only one pool is selected. The other pools for which the same criteria match are never selected.

6.4 The "System" menu

On this page, specify the address band from which the connected device receives any IP address. You configure the static assignment of the IP addresses in "Static Leases".

Note

Deleting DHCP server assignments

If you deactivate or delete an IPv4 address band or turn the DHCP server off and on again, the DHCP server bindings are deleted, see "Information > DHCP Server".

Select	Pool ID	Name	Interface	Enable	Subnet	Lower IP Address	Upper IP Address	Lease Time [sec]
<input type="checkbox"/>	1	pool_1	vian1	<input type="checkbox"/>	192.168.16.175/32	192.168.16.175	192.168.16.175	3600

Requirement

- The connected devices are configured in such a way that they obtain the IP address from a DHCP server.

Description

The page contains the following boxes:

- **DHCP Server**
Enable or disable the DHCP server on the device.

Note

To avoid conflicts with IPv4 addresses, only one device may be configured as a DHCP server in the network.

If you want to operate a DHCP server on the devices of a VRRP group, note the information in the section "Layer 3 (IPv4) > VRRP/VRRPv3 > Router".

- **Probe address with ICMP Echo before offer**
When enabled, the DHCP server checks whether an IP address has already been assigned. To do this, the DHCP server sends ICMP echo messages (ping) to this IPv4 address. If no reply is received, the IPv4 address is assigned.

Note

This check is not made with static assignments.

Note

If there are devices in your network on which the echo service is disabled as default, there may be conflicts with the IPv4 addresses. To avoid this, assign these devices an IPv4 address outside the IPv4 address band used by the DHCP server.

The table has the following columns:

- **Select**
Select the check box in the row to be deleted.
- **Pool ID**
Shows the number of the IPv4 address band. If you click the "Create" button, a new row with a unique number is created (pool ID).
- **Name**
Shows the name of the IPv4 address band. When you create a new entry, the name "pool_x" is entered automatically, where x stands for a consecutive number. You can change the name.
- **Interface**
Select an IP interface or a router port. The IPv4 addresses are assigned dynamically via this interface.
- **Enable**
Specify whether or not this IPv4 address band will be used.

Note

If you enable the IPv4 address band, its settings in this and the other DHCP tabs are grayed out and can no longer be edited.

- **Subnet**
Enter the network address range that will be assigned to the devices. Use the CIDR notation.

- **Lower IP Address**
Enter the IPv4 address that specifies the start of the dynamic IPv4 address band. The IPv4 address must be within the network address range you configured for "Subnet".
- **Upper IP address**
Enter the IPv4 address that specifies the end of the dynamic IPv4 address band. The IPv4 address must be within the network address range you configured for "Subnet".
- **Lease Time (sec)**
Specify for how many seconds the assigned IPv4 address remains valid. When half the period of validity has elapsed, the DHCP client can extend the period of the assigned IPv4 address. When the entire time has elapsed, the DHCP client needs to request a new IPv4 address.

Procedure

Enable DHCP server globally

1. Select the "DHCP Server" check box.
2. Click the "Set Values" button.

Configuring a DHCP pool

1. Click the "Create" button.
A new row with a unique number (Pool ID) is created.
2. Select an IP interface.
3. Click the "Set Values" button.
In the "Port-IP Address Mapping" tab a new row for the pool ID is created. In the "Port" column, all ports can be selected that currently belong to the selected VLAN.
In the "Port Range" tab a new row for the pool ID is created. In the row, all ports are enabled that currently belong to the selected VLAN.
The standard options for the pool are created in the "DHCP Options" tab.

4. You have the following options for configuring the pool:

Configuring a DHCP pool for an IPv4 address band

- Enter the subnet, the lower and the upper IPv4 address.
- Enter the lease time.
- Click the "Set Values" button.

Configuring a DHCP pool for an IPv4 address and assigning it to a certain port

- Change to the "Port-IP Address Mapping" tab.
- Select the required port.
In the "Port Range" tab only the selected port is enabled.
- Enter the IPv4 address and the subnet mask.
- Click the "Set Values" button.
In the "DHCP Server" tab the boxes "Subnet", "Lower IP Address" and "Upper IP Address" are filled accordingly.
- Configure the lease time in the "DHCP Server" tab.

5. Make the settings you require for the pool in the other DHCP tabs.

Enabling the DHCP pool

1. In the "DHCP Server" tab select the "Enable" check box.
2. Click the "Set Values" button.

Deleting a DHCP pool**Note**

You can only delete entries that are not enabled.

1. Enable the "Select" check box in the row to be deleted.
Repeat this for all entries you want to delete.
2. Click the "Delete" button.
The entry is deleted.

6.4.9.4 Port-IP Address Mapping

On this page, you assign exactly one IP address to a certain port.

After you have created a pool in the "DHCP Server" tab, a new row is created in the table on this page. In the corresponding drop-down list, select which port is assigned to this port.

The configuration on this page has effects on the tabs "DHCP Server" and "Port Range".

DHCP Server Port-IP Address Mapping

DHCP Client	DHCP Client Options	DHCP Server	Port-IP Address Mapping	Port Range	DHCP Options	Relay Agent Information	Static Leases	Host Options								
			<table border="1"> <thead> <tr> <th>Pool ID</th> <th>Port</th> <th>IP Address</th> <th>Subnet Mask</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>P9.2</td> <td>192.168.16.175</td> <td>255.255.255.255</td> </tr> </tbody> </table>	Pool ID	Port	IP Address	Subnet Mask	1	P9.2	192.168.16.175	255.255.255.255					
Pool ID	Port	IP Address	Subnet Mask													
1	P9.2	192.168.16.175	255.255.255.255													

Set Values Refresh

Description

This table contains the following columns:

- **Pool ID**
Shows the number of the IPv4 address band. A line is created for every address band.
- **Port**
Select the setting from the drop-down list. You have the following setting options:
 - Px.y
Specify the port via which IPv4 address will be assigned. You can only select ports located in the corresponding VLAN.
If you select a port, only this port is enabled in the "Port Range" tab.
 - Not Selected
With this setting, in the "Port Range" tab no ports or more than one port are selected.
If you select the setting "Not Selected", all ports in the "Port Range" tab are disabled.

6.4 The "System" menu

- **IP Address**
Enter an IPv4 address.
In the "DHCP Server" tab, the boxes "Lower IP Address" and "Upper IP Address" are filled accordingly.
- **Subnet Mask**
Enter a corresponding subnet mask.
In the "DHCP Server" tab, the "Subnet" box is filled accordingly.

Procedure

Assign an IP address to the port

1. Select the required port.
2. Enter the IPv4 address and the subnet mask.
3. Click the "Set Values" button.
In the "Port Range" tab only the selected port is enabled for the relevant DHCP pool.
In the "DHCP Server" tab, the boxes "Subnet", "Lower IP Address" and "Upper IP Address" are filled accordingly for the relevant DHCP pool.

6.4.9.5 Port Range

On this page, you define the ports via which the IPv4 addresses of an address band are assigned. After you have created an IPv4 address band in the "DHCP Server" tab, a new line is created in this tab and all ports selected that are currently located in the corresponding VLAN. If you add ports to the VLAN later, the ports are not automatically enabled in this tab.

DHCP Server Port Range																		
DHCP Client	DHCP Client Options	DHCP Server	Port-IP Address Mapping				Port Range				DHCP Options	Relay Agent Information	Static Leases	Host Options				
Pool ID	Interface	All ports	P0.1	P0.2	P0.3	P0.4	P1.1	P1.2	P1.3	P1.4	P2.1	P2.2	P2.3	P2.4	P3.1	P3.2	P3.3	P3.4
1	vlan1	No Change	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Description

This table contains the following columns:

- **Pool ID**
Shows the number of the IPv4 address band. A line is created for every address band.
- **Interface**
Shows the assigned IP interface.

- **All ports**
Select the setting from the drop-down list. You have the following setting options:
 - Enabled
The check box is enabled for all ports of the relevant VLAN.
 - Disabled
The check box is disabled for all ports of the relevant VLAN.
 - No Change
The table remains unchanged.
- **Px.y**
Specify the ports via which IPv4 addresses of the address band will be assigned.
You can only select ports located in the corresponding VLAN.

Note**Effects on other tabs**

If you enable precisely one port this is selected in the "Port-IP Address Mapping" tab.

If you enable no port or more than one port in the "Port-IP Address Mapping" tab, the setting "Not Selected" is selected.

Procedure

Configuring individual ports

1. Enable or disable the check box for the required ports.
2. Click the "Set Values" button.

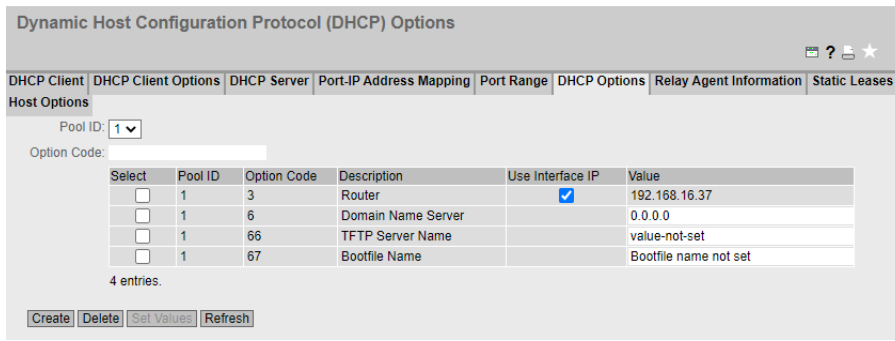
Configuring all ports

1. Select the required entry in the "All ports" drop-down list.
2. Click the "Set Values" button.

6.4.9.6 DHCP Options

On this page, you specify which DHCP options the DHCP server supports. The various DHCP options are defined in RFC 2132.

The DHCP options 1, 3, 6, 66 and 67 are created automatically when the IPv4 address band is created. Except for the DHCP option 1, the options can be deleted. With DHCP option 1, the subnet mask that you entered for the address band in "DHCP Server" is set automatically. With the DHCP option 3, you can set the internal IPv4 address of the DHCP server as a DHCP parameter using a check box.



Description

The page contains the following boxes:

- **Pool ID**
Select the required IPv4 address band.
- **Option Code**
Enter the number of the required DHCP option. The various DHCP options are defined in RFC 2132. The supported DHCP options are listed in the following paragraph.

The table has the following columns:

- **Select**
Select the check box in the row to be deleted.
- **Pool ID**
Shows the number of the IPv4 address band.
- **Option Code**
Shows the number of the DHCP option.
- **Description**
Shows a description of the DHCP option.

- **Use Interface IP**
If you enable the check box, the IPv4 address is used as the default gateway that is assigned to the IP interface of the address band. If the check box is cleared, you can enter an IPv4 address.
- **Value**
Enter the DHCP parameter that is transferred to the DHCP client. The content depends on the DHCP option.
 - DHCP option 3 (default gateway)
Enter the DHCP parameter as an IPv4 address, for example, 192.168.100.2.
 - DHCP option 6 (DNS server)
Enter the DHCP parameter as an IPv4 address, for example, 192.168.100.2. You can specify up to three IPv4 addresses separated by commas.
 - DHCP option 12 (host name)
Enter the host name in the string format.
 - DHCP option 15 (domain name)
Enter the name of the domain in which the client is located.
 - DHCP option 43 (vendor-specific information)
Enter the information in string format.
 - DHCP option 66 (TFTP server)
Enter the DHCP parameter as an IPv4 address or as FQDN, e.g. 192.168.100.2.
 - DHCP option 67 (boot file name)
Enter the name of the boot file in the string format.

Supported DHCP options

The following DHCP options are supported:

- Option 1
- Option 3
- Option 6
- Option 12
- Option 15
- Option 43
- Option 66
- Option 67

Procedure

Creating a DHCP option

1. Select a Pool ID.
2. Enter the option code.
3. Click the "Create" button.

6.4 The "System" menu

4. Enter a value.
5. If applicable, select the "Use Interface IP" check box for option 3.
6. Click the "Set Values" button.

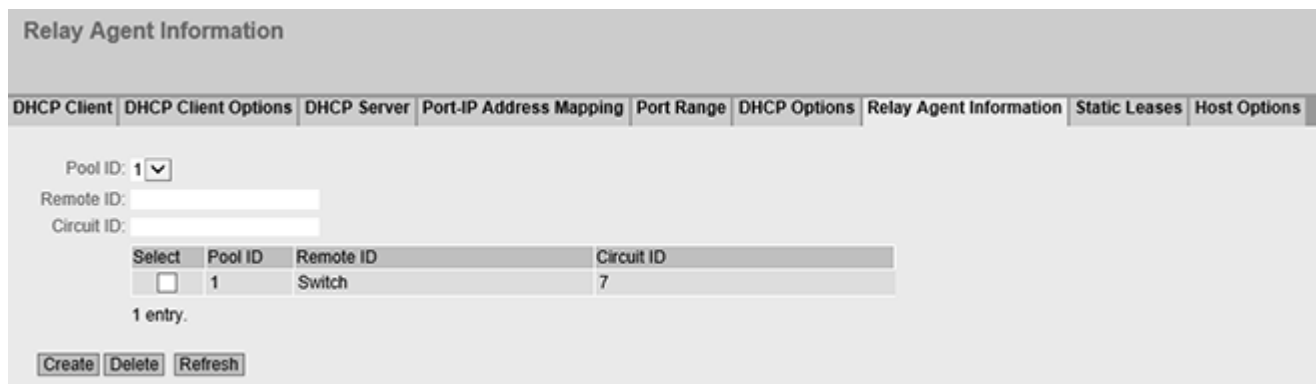
Deleting a DHCP option

1. Enable the "Select" check box in the row to be deleted.
Repeat this for all entries you want to delete.
2. Click the "Delete" button.
The entry is deleted.

6.4.9.7 Relay Agent Information

On this page you define that devices with a certain remote ID and circuit ID are assigned the IPv4 addresses from a specific address band.

If you create such an entry for an address band, the ports of the address band only react to DHCP queries via a DHCP Relay Agent (option 82). You can create additional address bands for the same IP interfaces so that ports react to different requests.



Description

The page contains the following boxes:

- **Pool ID**
Select the required IPv4 address band.
- **Remote ID**
Enter the remote ID.
- **Circuit ID**
Enter the circuit ID.

The table has the following columns:

- **Select**
Select the check box in the row to be deleted.
- **Pool ID**
Shows the number of the IPv4 address band.

- **Remote ID**
Shows the remote ID.
- **Circuit ID**
Shows the circuit ID.

Procedure

Creating an entry

1. Select a Pool ID.
2. Enter the remote ID.
3. Enter the circuit ID.
4. Click the "Create" button.

Deleting an entry

1. Enable the "Select" check box in the row to be deleted.
Repeat this for all entries you want to delete.
2. Click the "Delete" button.
The entry is deleted.

6.4.9.8 Static Leases

On this page you define that DHCP clients are assigned a preset IPv4 address depending on their client ID or MAC address.

Static Leases

[DHCP Client](#) | [DHCP Client Options](#) | [DHCP Server](#) | [Port-IP Address Mapping](#) | [Port Range](#) | [DHCP Options](#) | [Relay Agent Information](#) | [Static Leases](#) | [Host Options](#)

Pool ID:

Client Identification Method:

Value:

Select	Pool ID	Identification Method	Value	IP Address	Comment
<input type="checkbox"/>	1	Client ID	65756767	0.0.0.0	

1 entry.

Description

The page contains the following boxes:

- **Pool ID**
Select the required IPv4 address band.
- **Client identification method**
Select the method according to which a client is identified.
 - Ethernet MAC
The client is identified by its MAC address.
 - Client ID
The client is identified by a freely defined DHCP client ID.
 - DUID
The client is identified via the DUID.
- **Value**
Enter the MAC address (Ethernet MAC), the client ID (Client ID) or DUID (DUID) of the client.

The table has the following columns:

- **Select**
Select the check box in the row to be deleted.
- **Pool ID**
Shows the number of the IPv4 address band.
- **Identification Method**
Shows whether the client is identified by its MAC address, the client ID or DUID.
- **Value**
Shows the MAC address or client ID of the client.
- **IP Address**
Specify the IPv4 address that will be assigned to the client. The IPv4 address must be within the IPv4 address band.
- **Comment**
If necessary, enter a comment.

Procedure

Creating static leases

1. Select a Pool ID.
2. Select the Client identification method.
3. Enter the value.
4. Click the "Create" button.
5. Specify the IPv4 address that will be assigned to the client.
6. Click the "Set Values" button.

Deleting static leases

1. Enable the "Select" check box in the row to be deleted.
Repeat this for all entries you want to delete.
2. Click the "Delete" button.
The entry is deleted.

6.4.9.9 Host Options

On this page, you can specify DHCP options for devices to which you have assigned a static IP address. With the DHCP options, the DHCP server provides the clients with additional configuration parameters.

Dynamic Host Configuration Protocol (DHCP) Host Options

DHCP Client	DHCP Client Options	DHCP Server	Port-IP Address Mapping	Port Range	DHCP Options	Relay Agent Information	Static Leases	Host Options
-------------	---------------------	-------------	-------------------------	------------	--------------	-------------------------	---------------	--------------

Pool ID:

Client: Client ID:

Option Code:

Select	Pool ID	Identification Method	Value	Option Code	Option Value
<input type="checkbox"/>	1	Client ID	65756767	Host Name (12)	<input type="text"/>

1 entry.

Description

The page contains the following boxes:

- **Pool ID**
Select the required IPv4 address band.
- **Client**
Select the device for which you want to set a DHCP option.
- **Option Code**
Select the DHCP option from this drop-down list. The following options are available:
 - Host Name (12)
 - TFTP Server Name (66)
 - Bootfile Name (67)

The table has the following columns:

- **Select**
Select this check box to mark a row that you want to delete.
- **Pool ID**
Shows the number of the IPv4 address band.

6.4 The "System" menu

- **Identification Method**
Shows how the client is identified. The following options are possible:
 - MAC
 - Client ID
 - DUID
- **Value**
Shows the value for the "Identification Method" that was assigned under "Static Leases".
- **Option Code**
Shows the DHCP option.
- **Option Value**
Depending on the selected option code, enter the host name, the name of the TFTP server or boot file.

Procedure

Define option

1. Select a Pool ID.
2. Select the client.
3. Select the Option Code.
4. Click the "Create" button. An additional row is created in the table.
5. Enter the Option Value for the DHCP option in the newly created row.
6. Click the "Set Values" button.

Delete option

1. Select the check box of the row you want to delete.
2. Click the "Delete" button.

6.4.9.10 DHCP snooping

You can prevent attacks from malicious DHCP servers with DHCP snooping. DHCP snooping evaluates received DHCP messages and filters or restricts messages from non-trustworthy sources.

On this page, you can configure each port for DHCP snooping functionality.

Dynamic Host Configuration Protocol (DHCP) Snooping

DHCP Client | DHCP Client Options | DHCP Server | Port-IP Address Mapping | Port Range
 DHCP Options | Relay Agent Information | Static Leases | Host Options | DHCP Snooping

Setting: No Change [Copy to Table]

Port	Setting
P0.1	disabled
P0.2	disabled
P0.3	disabled
P0.4	disabled
P0.5	disabled

[Set Values] [Refresh]

Description

Table 1 has the following columns:

- **1st column**
Shows that the settings are valid for all ports of table 2.
- **Setting**
Select the setting from the drop-down list. You have the following setting options:
 - Disabled (default setting)
The snooping function is disabled. Messages concerning DHCP packets are ignored.
 - Client
Port that is connected to the DHCP client.
Messages that are received from the DHCP server are logged on this port.
 - Client-React
Port that is connected to the DHCP client. If messages from the DHCP server are received on this port, this is logged and the port is disabled.
 - Server
Port that is connected to the DHCP server.
Messages that are received from the DHCP client are logged on this port.
 - Server-React
Port that is connected to the DHCP server. If messages from the DHCP client are received on this port, this is logged and the port is disabled.
 - No Change
Table 2 remains unchanged.
- **Copy to Table**
If you click the button, the setting is adopted for all ports of table 2.

6.4 The "System" menu

Table 2 has the following columns:

- **Port**
Shows all available ports. The port is made up of the module number and the port number, for example port 0.1 is module 0, port 1.
- **Setting**
Select the setting from the drop-down list.

Configuration procedure

1. Select the desired setting for DHCP snooping from the "Setting" drop-down list. Repeat the process for every port for which you want to enable or disable the function.
2. Click the "Set Values" button.

6.4.10 SNMP

You should also refer to the chapter "Technical Basics", section "SNMP (Page 82)".

6.4.10.1 General

Configuration of SNMP

Note

Delete SNMPv3 configuration

To delete the SNMPv3 configuration, follow these steps:

1. Delete all SNMPv3 views except for the predefined views **SIMATICNETRD** and **SIMATICNETWR**.
 2. Delete all SNMPv3 Access.
 3. Delete all entries in the "SNMPv3 User to Group mapping" table.
 4. Delete all SNMPv3 Users.
-

On this page, you make the basic settings for SNMP. Enable the options according to the function you want to use.

Simple Network Management Protocol (SNMP) General

General	SNMPv3 Users	SNMPv3 User to Group mapping	SNMPv3 Access	SNMPv3 Views	Notifications
----------------	---------------------	-------------------------------------	----------------------	---------------------	----------------------

SNMP: ▼

SNMPv1/v2c Read Only

SNMPv1/v2c Read Community String:

SNMPv1/v2c Read/Write Community String:

SNMPv3 User Migration

SNMP Engine ID:

SNMP Agent Listen Port:

Description

The page contains the following boxes:

- **SNMP**

Select the SNMP protocol from the drop-down list. The following settings are possible:

- "-" (disabled)
SNMP is disabled.
- SNMPv1/v2c/v3
SNMPv1/v2c/v3 is supported.

Note

Note that SNMP in versions 1 and 2c does not have any security mechanisms.

- SNMPv3
Only SNMPv3 is supported.

- **SNMPv1/v2c Read Only**

If you enable this option, SNMPv1/v2c can only read the SNMP variables.

Note

Community String

For security reasons, do not use the default values "public" or "private". Change the community strings following the initial installation.

The recommended minimum length for community strings is 6 characters.

For security reasons, only limited access to objects of the SNMPCommunityMIB is possible with the SNMPv1/v2c Read Community String. With the SNMPv1/v2c Read/Write Community String, you have full access to the SNMPCommunityMIB.

- **SNMPv1/v2c Read Community String**
Enter the community string for read access of the SNMP protocol.
- **SNMPv1/v2c Read/Write Community String**
Enter the community string for read and write access of the SNMP protocol.
- **SNMPv3 User Migration**
 - **Enabled**
If the function is enabled, an SNMP engine ID is generated that can be migrated. You can transfer configured SNMPv3 Users to a different device.
If you enable this function and load the configuration of the device on another device, configured SNMPv3 Users are retained.
 - **Disabled**
If the function is disabled, a device-specific SNMP Engine ID is generated. To generate the ID, the agent MAC address of the device is used. You cannot transfer this SNMP user configuration to other devices.
If you load the configuration of the device on another device, all configured SNMPv3 Users are deleted.
- **SNMP Engine ID**
Shows the SNMP Engine ID.
- **SNMP Agent Listen Port**
Specify the port at which the SNMP agent waits for the SNMP queries. Standard port 161 is the default. You can optionally enter the standard port 162 or a port number in the range 1024 ... 49151 or 49500 ... 65535.

Procedure

1. Select the required option from the "SNMP" drop-down list:
 - "-" (disabled)
 - SNMPv1/v2c/v3
 - SNMPv3
2. Select the "SNMPv1/v2c Read Only" check box if you only want read access to SNMP variables with SNMPv1/v2c.
3. Enter the required character string in the "SNMPv1/v2c Read Community String" input box.
4. Enter the required character string in the "SNMPv1/v2c Read/Write Community String" input box.
5. If necessary, enable the SNMPv3 User Migration.
6. Click the "Set Values" button.

6.4.10.2 SNMPv3 Users

User-specific security settings

On the WBM page, you can create new SNMPv3 users and modify or delete existing users. The user-based security model works with the concept of the user name; in other words, a user ID is added to every frame. This user name and the applicable security settings are checked by both the sender and recipient.

Simple Network Management Protocol (SNMP) v3 Users

General | **SNMPv3 Users** | SNMPv3 User to Group mapping | SNMPv3 Access | SNMPv3 Views | Notifications

User Name:

Select	User Name	Authentication Protocol	Privacy Protocol	Authentication Password	Authentication Password Confirmation	Privacy Password	Privacy Password Confirmation
<input type="checkbox"/>	Miller	MD5	DES	*****	*****	*****	*****

1 entry.

Description

The page contains the following boxes:

- **User Name**
Enter a freely selectable user name. After you have entered the data, you can no longer modify the name.

The table has the following columns:

- **Select**
Select the row you want to delete.
- **User Name**
Shows the created users.
- **Authentication Protocol**
Specify the authentication protocol for which a password will be stored. The following settings are available:
 - None
 - MD5
 - SHA
- **Privacy Protocol**
Specify the encryption protocol for which a password will be stored. This drop-down list is only enabled when an authentication protocol has been selected. The following settings are available:
 - None
 - DES
 - AES

- **Authentication Password**

Enter the authentication password in the first input box. This password must have at least 1 character, the maximum length is 32 characters.

Note

Length of the password

As an important measure to maximize security, we recommend that the password has a minimum length of 6 characters and that it contains special characters, uppercase/lowercase letters, numbers.

- **Authentication Password Confirmation**

Confirm the password by repeating the entry.

- **Privacy Password**

Enter your encryption password. This password must have at least 1 character, the maximum length is 32 characters.

Note

Length of the password

As an important measure to maximize security, we recommend that the password has a minimum length of 6 characters and that it contains special characters, uppercase/lowercase letters, numbers.

- **Privacy Password Confirmation**

Confirm the encryption password by repeating the entry.

Procedure

Create a new user

1. Enter the name of the new user in the "User Name" input box.
2. Click the "Create" button. A new entry is generated in the table.
3. Select the authentication algorithm for "Authentication Protocol". In the relevant input boxes, enter the authentication password and the confirmation.
4. Select the algorithm in "Privacy Protocol". In the relevant input boxes, enter the encryption password and the confirmation.
5. Click the "Set Values" button.

Delete user

1. Enable "Select" in the row to be deleted.
Repeat this for all users you want to delete.
2. Click the "Delete" button. The entry is deleted.

6.4.10.3 SNMPv3 User to Group mapping

Configuration of group members

You assign users to SNMPv3 groups on this WBM page. Each user can only be a member of one group.

Simple Network Management Protocol (SNMP) v3 Groups

General
SNMPv3 Users
SNMPv3 User to Group mapping
SNMPv3 Access
SNMPv3 Views
Notifications

Group Name:

User Name:

Select	Group Name	User Name
<input type="checkbox"/>	Service	Miller

1 entry.

Create
Delete
Set Values
Refresh

Description

The page contains the following boxes:

- **Group Name**
Enter the group that will be assigned to the user.
- **User Name**
Select the user to be a member of the specified group. The drop-down list only contains users that are not yet assigned to a group.

The table has the following columns:

- **Select**
Select the row you want to delete.
- **Group Name**
Displays the SNMPv3 group. A group name can only be changed later if no access rights have been defined for the group yet.
- **User Name**
Shows the user that is a member of this group.

6.4.10.4 SNMPv3 Access

Security settings and assigning permissions

SNMP version 3 allows permissions to be assigned, authentication, and encryption at protocol level. The security level and read/write permissions are assigned according to groups. The settings automatically apply to every member of a group.

Note

Different access permissions for different security levels can be assigned to a group. If no access permission is defined for a security level, no access to the device is possible for members of the group using this security level.

Simple Network Management Protocol (SNMP) v3 Access

General	SNMPv3 Users	SNMPv3 User to Group mapping	SNMPv3 Access	SNMPv3 Views	Notifications
---------	--------------	------------------------------	---------------	--------------	---------------

Group Name:

Security Level:

Select	Group Name	Security Level	Read View Name	Write View Name	Notify View Name
<input type="checkbox"/>	Service	no Auth/no Priv	SIMATICNETRD	SIMATICNETWR	SIMATICNETRD

1 entry.

Description

The page contains the following boxes:

- **Group Name**
Select the name of the group.
- **Security Level**
Select the security level (authentication, encryption) for which you want to define the access permissions of the group:
 - **No Auth/no Priv**
No authentication enabled/no encryption enabled.
 - **Auth/no Priv**
Authentication enabled/no encryption enabled.
 - **Auth/Priv**
Authentication enabled/encryption enabled.

The table has the following columns:

- **Select**
Select the row you want to delete.
- **Group Name**
Shows the name of the SNMPv3 group.
- **Security Level**
Shows the security level to which this access permission applies.
- **Read View Name**
Enter an SNMPv3 view that grants read access to members of the group with the specified Security Level.
- **Write View Name**
Enter an SNMPv3 view that grants write access to members of the group with the specified Security Level.

Note

For write access to work, you also need to enable read access.

- **Notification View Name**
Enter an SNMPv3 view for which SNMP notification to members of the group with the defined security level should be used.

Procedure

Creating a new group

1. Select the name of the group for which you are configuring SNMP access.
2. Select the required security level from the "Security Level" drop-down list.
3. Click the "Create" button to create a new entry.
4. In the "Read View Name" field, enter the SNMPv3 view for read access.
5. In the "Write View Name" field, enter the SNMPv3 view for write access.
6. In the "Notification View Name" field, enter the SNMPv3 view for notifications.
7. Click the "Set Values" button.

Modifying a group

Once a group name and the security level have been specified, they can no longer be modified after the group is created. If you want to change the group name or the security level, you will need to delete the group and create it and configure it with the new name.

Deleting a group

1. Enable "Select" in the row to be deleted.
Repeat this for all groups you want to delete.
2. Click the "Delete" button. The entries are deleted.

6.4.10.5 SNMPv3 Views

Configuration of SNMPv3 views

You configure the parameters of SNMP views on this WBM page.

Simple Network Management Protocol (SNMP) v3 Views

General | SNMPv3 Users | SNMPv3 User to Group mapping | SNMPv3 Access | SNMPv3 Views | Notifications

View Name:

MIB Tree:

Select	View Name	MIB Tree	View Type
<input type="checkbox"/>	MY_RD	org	Included <input type="text" value="v"/>
<input type="checkbox"/>	MY_RD	private	Included <input type="text" value="v"/>
<input type="checkbox"/>	MY_WR	1.3.6.1.3.6.18.1.1.1.83.73.77	Included <input type="text" value="v"/>
<input type="checkbox"/>	SIMATICNETRD	iso	Included <input type="text" value="v"/>
<input type="checkbox"/>	SIMATICNETRD	1.3.6.1.6.3.18.1.1	Excluded <input type="text" value="v"/>
<input type="checkbox"/>	SIMATICNETRD	1.3.6.1.6.3.18.1.1.1.83.73.77.65.84.73.67.78.69.84.82.68	Included <input type="text" value="v"/>
<input type="checkbox"/>	SIMATICNETWR	iso	Included <input type="text" value="v"/>

7 entries.

Note

Controlling the SNMPv1 and SNMPv2c access

The preconfigured **SIMATICNETRD** and **SIMATICNETWR** views are used internally to control the SNMPv1 and SNMPv2c access. If you delete or change these views, this directly affects the SNMPv1 and SNMPv2c access.

Description

The page contains the following boxes:

- **View Name**
Select the name of the view that you want to configure. An SNMPv3 view always needs to be assigned to an SNMPv3 access. For this reason, you need to enter a new SNMPv3 view in the table in the "SNMP Access" tab.
- **MIB Tree**
Select the Object Identifier (OID) of the MIB area that is to be used for the SNMPv3 view. The following options are possible:
 - iso
 - std
 - member-body
 - org
 - mgmt
 - private
 - snmpV2

The drop-down list only contains the OIDs that are usually used. If the configuration of a specific OID that is not listed is necessary, you can configure this via the CLI with the `snmp view` command. This OID is then also displayed in the WBM in the overview table.

The table has the following columns:

- **Select**
Select the row you want to delete.
- **View Name**
The name of the SNMPv3 view.
- **MIB Tree**
The OID of the MIB area for the SNMPv3 view.
- **View Type**
The available options are as follows:
 - **Included**
The MIB OID and its lower-level nodes are part of the SNMPv3 view. Access to the corresponding MIB objects is possible.
 - **Excluded**
The MIB OID and its lower-level nodes are not part of the SNMPv3 view. Access to the corresponding MIB objects is not possible.

6.4.10.6 Notifications

SNMP traps and SNMPv3 notifications

If an alarm event occurs, a device can send SNMP notifications (traps and inform notifications) to up to ten different management stations at the same time. Notifications are only sent for events that were specified in the "Events" menu.

Simple Network Management Protocol (SNMP) Notifications

General | **SNMPv3 Users** | SNMPv3 User to Group mapping | SNMPv3 Access | SNMPv3 Views | Notifications

SNMPv1 Traps

SNMPv1/v2c Trap Community String: public

SNMPv3 Notify User: -

SNMPv3 Notify Security Level: no Auth/no Priv

Notification Receiver Type: SNMPv1 Trap

Notification Receiver Address:

Select	Notification Receiver Address	Notification Receiver Type	SNMP Engine ID	Notification
<input type="checkbox"/>	192.168.178.107	SNMPv1 Trap	-	<input type="checkbox"/>

1 entry.

Description

The page contains the following boxes:

- **SNMPv1 Traps**
Enable or disable sending of SNMPv1 traps. This setting affects all receivers of SNMPv1 traps and has no effects on receivers of SNMPv2c or SNMPv3 notifications.
- **SNMPv1/v2c Trap Community String**
Enter the community string for sending SNMPv1/v2c notifications.
- **SNMPv3 Notify User**
Select the user to which SNMPv3 notifications are to be sent.
- **SNMPv3 Notify Security Level**
Select the security level (authentication, encryption) to be used for SNMPv3 notification. The following options are possible:
 - no Auth/no Priv
No authentication enabled / no encryption enabled.
 - Auth/no Priv
Authentication enabled / no encryption enabled.
 - Auth/Priv
Authentication enabled / encryption enabled.

- **Notification Receiver Type**
The receiver type defines the SNMP version and the type of notification. SNMP inform notifications must be acknowledged by the receiver, SNMP traps do not. The following options are possible:
 - SNMPv1 Trap
 - SNMPv2c Trap
 - SNMPv2c Inform
 - SNMPv3 Trap
 - SNMPv3 Inform
- **Notification Receiver Address**
Enter the IP address of the receiver station to which the device sends SNMP notifications. You can specify up to ten different receivers servers.

The table has the following columns:

- **Select**
Select the row you want to delete.
- **Notification Receiver Address**
If necessary, change the IP address of the stations.
- **Notification Receiver Type**
Shows the defined receiver type.
- **SNMP Engine ID**
The ID of the SNMP engine to which SNMPv3 inform notifications are sent. You can only configure this parameter for the "SNMPv3-Inform" receiver type.
- **Notification**
Enable or disable the sending of SNMP notifications. Stations that are entered but not selected do not receive any SNMP notifications.

Note

If a table row is grayed out, the corresponding notification was configured via the CLI and can only be deleted via the CLI.

Procedure

Configuring a notification

1. Select the receiver for SNMPv3 notifications in the "SNMPv3 Notify User" drop-down list.
2. Select the security level for SNMPv3 notifications in the "SNMPv3 Notify Security Level" drop-down list.
3. Select the receiver type in the "Notification Receiver Type" drop-down list.
4. In "Notification Receiver Address", enter the IP address of the station to which the device should send traps or notifications.
5. Click the "Create" button to create a new trap entry.

6.4 The "System" menu

- 6. Activate "Notification" in the required row.
- 7. Click the "Set Values" button.

Deleting a trap entry

- 1. Enable "Select" in the row to be deleted.
- 2. Click the "Delete" button. The entry is deleted.

6.4.11 System Time

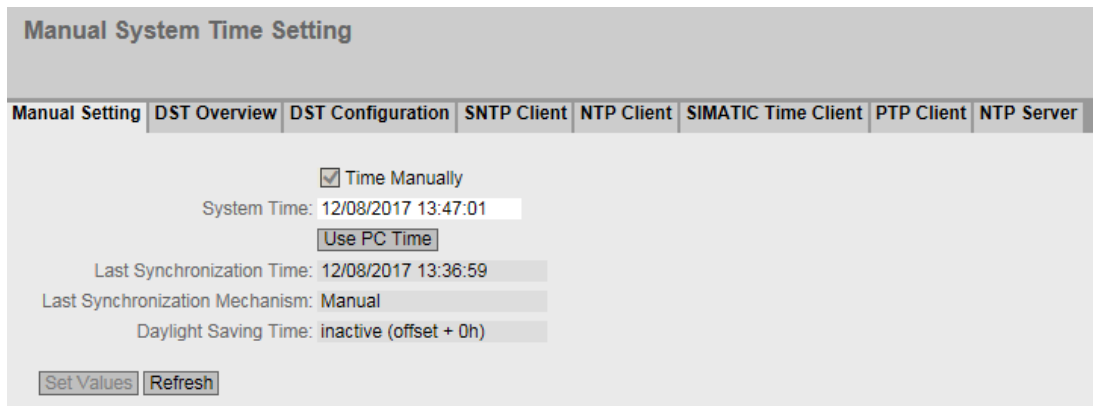
There are different methods that can be used to set the system time of the device. Only one method can be active at any one time.

If one method is activated, the previously activated method is automatically deactivated.

6.4.11.1 Manual Setting

Manual setting of the system time

On this page, you set the date and time of the system yourself. For this setting to be used, enable "Time Manually".



Description

The page contains the following boxes:

- **Time Manually**
Enable or disable the manual time setting. If you enable the option, the "System Time" input box can be edited.
- **System Time**
Enter the date and time in the format "MM/DD/YYYY HH:MM:SS".
- **Use PC Time**
Click the button to use the time setting of the PC.

- **Last Synchronization Time**
Shows when the last time-of-day synchronization took place. If no time-of-day synchronization was possible, the box displays "Date/time not set".
- **Last Synchronization Mechanism**
Shows how the last time synchronization was performed.
 - Not set
The time was not set.
 - Manual
Manual time setting
 - SNTP
Automatic time-of-day synchronization with SNTP
 - NTP
Automatic time-of-day synchronization with NTP
 - SIMATIC
Automatic time-of-day synchronization using the SIMATIC time frame
 - PTP
Automatic time-of-day synchronization with PTP. This display is only possible for devices that support PTP.
- **Daylight Saving Time (DST)**
Shows whether the daylight saving time changeover is active.
 - active (offset +1 h)
The system time was changed to daylight saving time; in other words an hour was added. You can see the current system time at the top right in the selection area of the WBM. The set time continues to be displayed in the "System Time" box.
 - inactive (offset +0 h)
The current system time is not changed.

Procedure

1. Enable the "Time Manually" option.
2. Click in the "System Time" input box.
3. In the "System Time" input box, enter the date and time in the format "MM/DD/YYYY HH:MM:SS".
4. Click the "Set Values" button.
The date and time are adopted and "Manual" is entered in "Last Synchronization Mechanism" box.

6.4.11.2 DST Overview

Daylight saving time switchover

On this page, you can create new entries for the daylight saving time changeover. The table provides an overview of the existing entries.

Daylight Saving Time (DST) Overview									
Manual Setting	DST Overview	DST Configuration	SNTP Client	NTP Client	SIMATIC Time Client	PTP Client	NTP Server		
Select	DST No	Name	Year	Start Date	End Date	Recurring Date	State	Type	
<input type="checkbox"/>	1	DST 2018	2018	03/25 02:00	10/28 03:00	-	enabled	Date	
1 entry.									
<input type="button" value="Create"/> <input type="button" value="Delete"/> <input type="button" value="Refresh"/>									

Settings

The page contains the following boxes:

- Select**
 Select the row you want to delete.
- DST No.**
 Shows the number of the entry.
 If you create a new entry, a new line with a unique number is created.
- Name**
 Shows the name of the entry.
- Year**
 Shows the year for which the entry was created.
- Start Date**
 Shows the month, day and time for the start of daylight saving time.
- End Date**
 Shows the month, day and time for the end of daylight saving time.
- Recurring Date**
 With an entry of the type "Recurring", the period in which daylight saving time is active is displayed consisting of week, day, month and time of day.
 With an entry of the type "Date" a "-" is displayed.

- **Status**
Shows the status of the entry:
 - Enabled
The entry was created correctly.
 - Invalid
The entry was created new and the start and end date are identical.
- **Type**
Shows how the daylight saving time changeover is made:
 - Date
A fixed date is entered for the daylight saving time changeover.
 - Recurring
A rule was defined for the daylight saving time changeover.

Procedure

Creating an entry

1. Click the "Create" button.
A new entry is created in the table.
2. Click on the required entry in the "DST No" column.
You change to the "DST Configuration" page.
3. Select the required type in the "Type" drop-down list.
Depending on the selected type, various settings are available.
4. Enter a name in the "Name" box.
5. If you have selected the type "Date", fill in the following boxes.
 - Year
 - Day (for start and end date)
 - Hour (for start and end date)
 - Month (for start and end date)
6. If you have selected the type "Recurring", fill in the following boxes.
 - Hour (for start and end date)
 - Month (for start and end date)
 - Week (for start and end date)
 - Day (for start and end date)
7. Click the "Set Values" button.

Deleting an entry

1. Enable "Select" in the row to be deleted.
2. Click the "Delete" button. The entry is deleted.

6.4.11.3 DST Configuration

Configuring the daylight saving time switchover

On this page, you can configure the entries for the daylight saving time changeover. As result of the changeover to daylight saving or standard time, the system time for the local time zone is correctly set.

You can define a rule for the daylight saving time changeover or specify a fixed date.

Settings

Note

The content of this page depends on the selection in the "Type" box.

The boxes "DST No.", "Type" and "Name" are always shown.

- **DST No.**
Select the type of the entry.
- **Type**
Select how the daylight saving time changeover is made:
 - Date
You can set a fixed date for the daylight saving time changeover.
This setting is suitable for regions in which the daylight saving time changeover is not governed by rules.
 - Recurring
You can define a rule for the daylight saving time changeover.
This setting is suitable for regions in which the daylight saving time always begins or ends on a certain weekday.
- **Name**
Enter a name for the entry.
The name can be a maximum of 16 characters long.

Settings with "Date" selected

DST Configuration

Manual Setting | DST Overview | **DST Configuration** | SNTP Client | NTP Client | SIMATIC Time Client | PTP Client | NTP Server

DST No: 1

Type: Date

Name: DST 2018

Year: 2018

Start Date

Day: 25

Hour: 02:00

Month: March

End Date

Day: 28

Hour: 03:00

Month: October

Set Values Refresh

You can set a fixed date for the start and end of daylight saving time.

- **Year**
Enter the year for the daylight saving time changeover.
- **Start Date**
Enter the following values for the start of daylight saving time:
 - Day
Specify the day.
 - Hour
Specify the hour.
 - Month
Specify the month.
- **End Date**
Enter the following values for the end of daylight saving time:
 - Day
Specify the day.
 - Hour
Specify the hour.
 - Month
Specify the month.

Settings with "Recurring" selected

You can create a rule for the daylight saving time changeover.

- **Start Date**
Enter the following values for the start of daylight saving time:
 - Hour
Specify the hour.
 - Month
Specify the month.
 - Week
Specify the week.
You can select the first to fourth or the last week of the month.
 - Day
Specify the weekday.
- **End Date**
Enter the following values for the end of daylight saving time:
 - Hour
Specify the hour.
 - Month
Specify the month.
 - Week
Specify the week.
You can select the first to fourth or the last week of the month.
 - Day
Specify the weekday.

6.4.11.4 SNTP Client

Time-of-day synchronization in the network

SNTP (Simple Network Time Protocol) is used for synchronizing the time in the network. The time frames are sent by an SNTP server in the network.

Simple Network Time Protocol (SNTP) Client

Manual Setting | DST Overview | DST Configuration | **SNTP Client** | NTP Client | SIMATIC Time Client | PTP Client | NTP Server

SNTP Client

Current System Time: 12/08/2017 13:51:18

Last Synchronization Time: 12/08/2017 13:36:59

Last Synchronization Mechanism: Manual

Time Zone: +00:00

Daylight Saving Time: inactive (offset + 0h)

SNTP Mode: Poll

Poll Interval[s]: 64

SNTP Server Address:

Select	SNTP Server Address	SNTP Server Port	Primary
<input type="checkbox"/>	10.0.0.7	123	<input checked="" type="checkbox"/>

1 entry.

Create | Delete | Set Values | Refresh

Description

The page contains the following boxes:

- **SNTP Client**
Enable or disable automatic time-of-day synchronization using SNTP.
- **Current System Time**
Shows the current date and current normal time received by the IE switch. If you specify a time zone, the time information is adapted accordingly.
- **Last Synchronization Time**
Shows when the last time-of-day synchronization took place.

- **Last Synchronization Mechanism**

Shows how the last time synchronization was performed. The following methods are possible:

 - Not set
The time was not set.
 - Manual
Manual time setting
 - SNTP
Automatic time-of-day synchronization with SNTP
 - NTP
Automatic time-of-day synchronization with NTP
 - SIMATIC
Automatic time-of-day synchronization using the SIMATIC time frame
 - PTP
Automatic time-of-day synchronization with PTP. This display is only possible for devices that support PTP.
- **Time Zone**

In this box, enter the time zone you are using in the format "+/- HH:MM". The time zone relates to UTC standard world time.
The time in the "Current System Time" box is adapted accordingly.
- **Daylight Saving Time (DST)**

Shows whether the daylight saving time changeover is active.

 - active (offset +1 h)
The system time was changed to daylight saving time; in other words an hour was added. You can see the current system time at the top right in the selection area of the WBM. The normal time including the time zone continues to be displayed in the "Current System Time" box.
 - inactive (offset +0 h)
The current system time is not changed.

- **SNTP Mode**

Select the synchronization mode from the drop-down list. The following types of synchronization are possible:

 - Listen
With this mode, the device is passive and receives SNTP frames that deliver the time of day. Settings in the input boxes "SNTP Server Address" and "SNTP Server Port" have no effect in this mode.
In this mode, only IPv4 addresses are supported.

Note

SNTP Client in Listen mode and NTP Server cannot be enabled at the same time.

 - Poll
If you select this mode, the input box "Poll Interval[s]" is displayed to allow further configuration. In this mode the settings in the input boxes "SNTP Server Address" and "SNTP Server Port" are taken into account. With this type of synchronization, the device is active and sends a time query to the SNTP server.
IPv4 addresses are supported in this mode.
- **Poll Interval[s]**

Here, enter the interval between two-time queries. In this box, you enter the query interval in seconds. Possible values are 16 to 16284 seconds.
 - **SNTP Server Address**

Enter the IP address or the FQDN (Fully Qualified Domain Name) of the SNTP server.
 - **SNTP Server Port**

Enter the port of the SNTP server.
The following ports are possible:

 - 123 (standard port)
 - 1025 to 36564
 - **Primary**

A check mark is set for the SNTP server that you create first. If several SNTP servers have been created, the primary server is queried first.

Procedure

1. Click the "SNTP Client" check box to enable the automatic time setting.
2. In the "Time Zone" input box, enter the local time difference to world time (UTC). The input format is "+/-HH:MM" (for example +02:00 for CEST), because the SNTP server always sends the UTC time. This time is then recalculated as the local time based on the specified time zone. You configure the daylight saving time switchover on the pages "System > System Time > DST Overview" and "System > System Time > DST Configuration". You also need to take this into account when completing the "Time Zone" input box.

6.4 The "System" menu

3. Select one of the following options from the "SNTP Mode" drop-down list:
 - Poll
For this mode, you need to configure the following:
 - time zone difference (step 2)
 - query interval (step 4)
 - time server (step 5)
 - Port (step 7)
 - complete the configuration with step 8.
 - Listen
For this mode, you need to configure the following:
 - time difference to the time sent by the server (step 2)
 - time server (step 5)
 - port (step 7)
 - complete the configuration with step 8.
4. In the "Poll Interval[s]" input box, enter the time in seconds after which a new time query is sent to the time server.
5. In the "SNTP Server Address" input box, enter the IP address or the FQDN of the SNTP server whose frames will be used to synchronize the time of day.
6. Click the "Create" button.
A new row is inserted in the table for the SNTP server.
7. In the "SNTP Server Port" column, enter the port via which the SNTP server is available. The port can only be modified if the IPv4 address or the FQDN name of the SNTP server is entered.
8. Click the "Set Values" button to transfer your changes to the device.

6.4.11.5 NTP Client

Automatic time-of-day setting with NTP

If you require time-of-day synchronization using NTP, you can make the relevant settings here.

Network Time Protocol (NTP) Client

Manual Setting | DST Overview | DST Configuration | SNTP Client | **NTP Client** | SIMATIC Time Client | PTP Client | NTP Server

NTP Client
 Secure NTP Client only
 Current System Time: 09/29/2022 15:32:45
 Last Synchronization Time: 09/28/2022 17:04:18
 Last Synchronization Mechanism: Manual
 Time Zone: +00:00
 Daylight Saving Time: inactive (offset + 0h)

NTP Server Index: 1

Select	NTP Server Index	NTP Server Address	NTP Server Port	Poll Interval	Key ID	Hash Algorithm	Key	Key Confirmation
<input type="checkbox"/>	1	0.0.0.0	123	64	1	DES		

1 entry.

Create | Delete | Set Values | Refresh

Description

The page contains the following boxes:

- **NTP Client**
Select this check box to enable automatic time-of-day synchronization with NTP.
- **Secure NTP Client only**
When enabled, the device receives the system time from a secure NTP server. The setting applies to all server entries.
To enable the secure NTP client, the parameters for authentication (key ID, hash algorithm, key) must be configured.

Note

We highly recommend using a secure NTP server.

- **Current System Time**
Shows the current date and current normal time received by the IE switch. If you specify a time zone, the time information is adapted accordingly.
- **Last Synchronization Time**
Shows when the last time-of-day synchronization took place.
- **Last Synchronization Mechanism**
Shows how the last time synchronization was performed. The following methods are possible:
 - Not set
The time was not set.
 - Manual
Manual time setting
 - SNTP
Automatic time-of-day synchronization with SNTP
 - NTP
Automatic time-of-day synchronization with NTP
 - SIMATIC
Automatic time-of-day synchronization using the SIMATIC time frame
 - PTP
Automatic time-of-day synchronization with PTP. This display is only possible for devices that support PTP.
- **Time Zone**
In this box, enter the time zone you are using in the format "+/- HH:MM". The time zone relates to UTC standard world time.
The time in the "Current System Time" box is adapted accordingly.

- **Daylight Saving Time (DST)**
Shows whether the daylight saving time changeover is active.
 - active (offset +1 h)
The system time was changed to daylight saving time; in other words an hour was added. You can see the current system time at the top right in the selection area of the WBM. The normal time including the time zone continues to be displayed in the "Current System Time" box.
 - inactive (offset +0 h)
The current system time is not changed.
- **NTP Server Index**
Select the index of the NTP server. You can specify up to four NTP servers or Secure NTP servers. The NTP servers are queried in the order of the NTP Server Index. The system time is applied by the server with the highest classification. If time frames of an NTP server with a smaller stratum value are received, this time is applied. The switchover to the time with the smaller stratum takes about 30 minutes.

The table has the following columns:

- **Select**
Select the check box in the row to be deleted.
- **NTP Server Index**
The index of the NTP server.
- **NTP Server Address**
Enter the IP address, the FQDN (Fully Qualified Domain Name) or the host name of the NTP server.
- **NTP Server Port**
Enter the port of the NTP server.
The following ports are possible:
 - 123 (standard port)
 - 1025 to 36564
- **Poll Interval[s]**
Here you enter the interval between two time queries. The greater the interval, the less accurate the time of the device. Possible values are 64 to 1024 seconds.

The following boxes are only relevant for a secure NTP client. If the "Secure NTP Client only" check box is not selected, these boxes are grayed out:

- **Key ID**
Enter the ID of the authentication key.
- **Hash Algorithm**
Specify the format for the authentication key.
- **Key**
Enter the authentication key. The key can only contain printable ASCII characters.
- **Key Confirmation**
Enter the authentication key for confirmation.

Procedure

Time-of-day synchronization via NTP server

1. Click the "NTP Client" check box to enable the automatic time setting using NTP.
2. In the "Time Zone" input box, enter the local time difference to world time (UTC). The input format is "+/-HH:MM" (for example +02:00 for CEST, the Central European Summer Time), because the NTP server always sends the UTC time. This time is then recalculated as the local time based on the specified time zone. You configure the daylight saving time switchover on the pages "System > System Time > DST Overview" and "System > System Time > DST Configuration". You also need to take this into account when completing the "Time Zone" input box.
3. Select the "NTP Server Index".
4. Click the "Create" button.
A new row is inserted in the table for the NTP server.
5. In the "NTP Server Address" input box, enter the IP address, the FQDN or the host name of the NTP server whose frames will be used to synchronize the time of day.
6. In the "NTP Server Port" column, enter the port via which the NTP server is available. The port can only be modified if the IPv4 address or the FQDN name of the NTP server is entered.
7. In the "Poll Interval" column, enter the time in seconds after which a new time query is sent to the time server.
8. Click the "Set Values" button.

Time-of-day synchronization via a secure NTP server

To synchronize the time of day via a secure NTP server, the following additional steps are necessary:

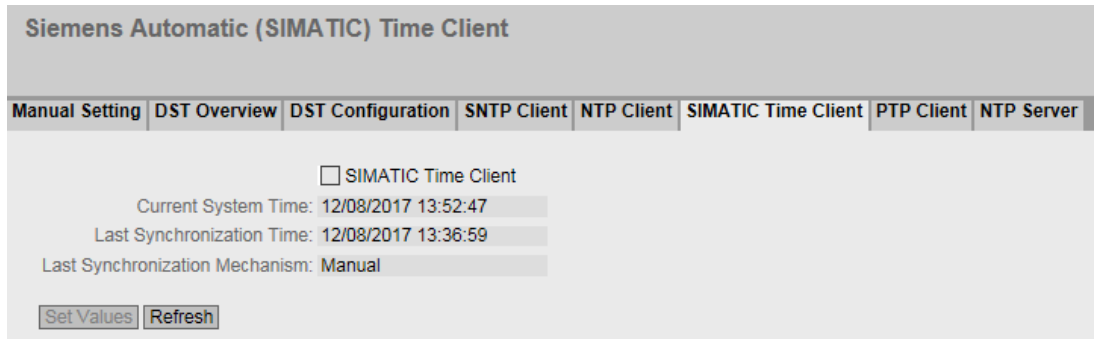
1. Click in the "Secure NTP Client only" check box to enable automatic time setting via secure NTP.
2. Configure the authentication.
 - In "Key ID", enter the ID of the authentication key.
 - In "Hash Algorithm", select the required format.
 - In "Key", enter the authentication key.

With these entries, the NTP client authenticates itself on the secure NTP server. These entries must be present on the secure NTP server.

3. Click the "Set Values" button.

6.4.11.6 SIMATIC Time Client

Time setting via SIMATIC Time Client



Description

The page contains the following boxes:

- **SIMATIC Time Client**
Select this check box to enable the device as a SIMATIC time client.
- **Current System Time**
Shows the current system time.
- **Last Synchronization Time**
Shows when the last time-of-day synchronization took place.
- **Last Synchronization Mechanism**
Shows how the last time synchronization was performed. The following methods are possible:
 - Not set
The time was not set.
 - Manual
Manual time setting
 - SNTP
Automatic time-of-day synchronization with SNTP
 - NTP
Automatic time-of-day synchronization with NTP
 - SIMATIC
Automatic time-of-day synchronization using the SIMATIC time frame
 - PTP
Automatic time-of-day synchronization with PTP. This display is only possible for devices that support PTP.

Procedure

1. Click the "SIMATIC Time Client" check box to enable the SIMATIC Time Client.
2. Click the "Set Values" button.

6.4.11.7 PTP Client

Automatic time-of-day setting with PTP

If you require time-of-day synchronization using PTP, you can make the relevant settings here.

Note

Time synchronization via PTP is only possible when the domain number of the device matches the domain number of the time transmitter. You configure the domain number of the device in the menu Layer 2 > PTP > TC General.

IEEE 1588 Precision Time Protocol (PTP) Client

Manual Setting	DST Overview	DST Configuration	SNTP Client	NTP Client	SIMATIC Time Client	PTP Client	NTP Server
----------------	--------------	-------------------	-------------	------------	---------------------	------------	------------

PTP Client

Current System Time: 12/08/2017 13:53:42

Last Synchronization Time: 12/08/2017 13:36:59

Last Synchronization Mechanism: Manual

Time Zone: +00:00

Daylight Saving Time: inactive (offset + 0h)

Set Values
Refresh

Description

The page contains the following boxes:

- **PTP Client**
Select this check box to enable automatic time-of-day synchronization with PTP.
- **Current System Time**
Shows the current date and current normal time obtained due to time synchronization in the network. If you specify a time zone, the time information is adapted accordingly.
- **Last Synchronization Time**
Shows when the last time-of-day synchronization took place.

- **Last Synchronization Mechanism**

Shows how the last time synchronization was performed. The following methods are possible:

 - Not set
The time was not set.
 - Manual
Manual time setting
 - SNTP
Automatic time-of-day synchronization with SNTP
 - NTP
Automatic time-of-day synchronization with NTP
 - SIMATIC
Automatic time-of-day synchronization using the SIMATIC time frame
 - PTP
Automatic time-of-day synchronization with PTP
- **Time Zone**

In this box, enter the time zone you are using in the format "+/- HH:MM". The time zone relates to UTC standard world time.
The time in the "Current System Time" box is adapted accordingly.
- **Daylight Saving Time (DST)**

Shows whether the daylight saving time changeover is active.

 - active (offset +1 h)
The system time was changed to daylight saving time; in other words an hour was added. You can see the current system time at the top right in the selection area of the WBM. The normal time including the time zone continues to be displayed in the "Current System Time" box.
 - inactive (offset +0 h)
The current system time is not changed.

Procedure

1. Click the "PTP Client" check box to enable the automatic time setting using PTP.
2. Specify the a time zone, if applicable.
3. Click the "Set Values" button.

6.4.11.8 NTP Server

On this WBM page, you configure the device as an NTP server or as an NTP server of the type "NTP (secure)". The other devices can call up the time made available by the device via this NTP server. This means that the supplied devices are not dependent on a connection to an external time server.

Note

Time synchronization

To ensure that the device synchronizes the connected devices to a correct time, it should also be configured as client for a protocol for time synchronization (NTP, SNTP, PTP or SIMATIC time-of-day frames).

The NTP server does not send cyclic messages with time information on its own, but only responds to corresponding requests. Settings in the function as a client (time zone and daylight saving time) do not influence the time information that the device sends as a server.

Network Time Protocol (NTP) Server

Manual Setting | DST Overview | DST Configuration | SNTP Client | NTP Client | SIMATIC Time Client | PTP Client | NTP Server

NTP Server

Interface: vlan1 v

Select	Interface	Listen	Server Port	Secure	Key ID	Hash Algorithm	Key	Key Confirmation
<input type="checkbox"/>	vlan1	<input checked="" type="checkbox"/>	123	<input type="checkbox"/>	1	DES	v	

1 entry.

Create
Delete
Set Values
Refresh

Description

The page contains the following boxes:

- **NTP Server**

Enable or disable the service of the NTP server.

Note

SNTP Client in Listen mode and NTP Server cannot be enabled at the same time.

- **Interface**

Specify the interface for which the NTP server will be configured. When you create a new row in the table, time-of-day synchronization with NTP is activated for the corresponding interface by default ("Listen" column).

The table has the following columns:

- **Select**
Select the row you want to delete.
- **Interface**
The name of the interface for which an NTP server is configured.
- **Listen**
If you select this check box, the time is synchronized via NTP for the corresponding interface.
- **Server Port**
Specify the port of the NTP server.
The following ports are possible:
 - 123 (standard port)
 - 1025 to 36564
- **Secure**
When this is enabled, the NTP server becomes an NTP server of the type "NTP (secure)".

The device only uses the contents of the following columns when it synchronizes via "NTP (secure)".

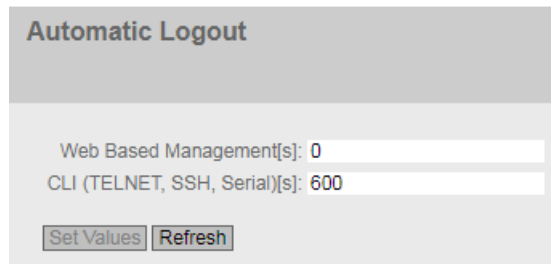
- **Key ID**
Enter the ID of the authentication key.
- **Hash Algorithm**
Specify the format for the authentication key.
- **Key**
Enter the authentication key. The length depends on the hash algorithm.
The following minimum lengths are recommended for the hash algorithm:
 - DES: ASCII 8 characters
 - MD5: ASCII 16 characters
 - SHA1: ASCII 20 characters
- **Key Confirmation**
Enter the authentication key for confirmation.

6.4.12 Automatic logout

Setting Automatic Logout

On this page, set the time intervals after which there is an automatic logout from the WBM or CLI following user inactivity.

If you have been logged out automatically, you will need to log in again.



Automatic Logout

Web Based Management[s]: 0

CLI (TELNET, SSH, Serial)[s]: 600

Configuration

1. Enter a value of 60-3600 seconds in the "Web Based Management[s]" input box. If you enter the value 0, Automatic Logout is disabled.
2. Enter a value of 60-600 seconds in the "CLI (TELNET, SSH, Serial)[s]" input box. If you enter the value 0, Automatic Logout is disabled.
3. Click the "Set Values" button.

6.4.13 Configuration of the SELECT/SET button


Description of the SELECT/SET button

The "SELECT/SET" button is used for the following:

- Changing the display mode,
- Resetting to factory defaults,
- Defining the fault mask and the LED display.

You will find a detailed description of the individual functions available with the buttons in the device operating instructions.

On this page, the functionality of the SELECT/SET button can be restricted or fully disabled.



SELECT/SET Button Configuration


Restore Factory Defaults


Set Fault Mask

Description of the displayed boxes

The following functions are possible:

- **Restore Factory Defaults**
Enable or disable the "Restore Factory Defaults" function with the SELECT/SET button.

 CAUTION
<p>Button function "Restore Factory Defaults" active during startup</p> <p>If you have disabled this function in your configuration, disabling is only valid during operation. When restarting, for example after power down, the function is active until the configuration is loaded so that the device can inadvertently be reset to the factory settings. This may cause unwanted disruption in network operation since the device needs to be reconfigured if this occurs. An inserted PLUG is also deleted and returned to the status as shipped.</p>

 CAUTION
<p>Resetting with WBM and CLI</p> <p>If you have disabled the "Restore Factory Defaults" function in your configuration, the disabling does not apply to the CLI command <code>restart</code> or to the WBM page "System > Restart". This means that the device can inadvertently be reset to the factory defaults. This may cause unwanted disruption in network operation since the device then needs to be reconfigured. An inserted PLUG is also deleted and returned to the status as shipped.</p>

- **Set Fault Mask**
Enable or disable the function "Define fault mask via the LED display" with the SELECT/SET button.

Configuration procedure

1. To use the required functionality, select the corresponding check box.
2. Click the "Set Values" button.

6.4.14 Syslog Client

Syslog according to RFC 3164 is used for transferring short, unencrypted text messages over UDP in the IP network. This requires a Syslog server.

Requirements for sending log entries

- The Syslog function is enabled on the device.
- The Syslog function is enabled for the relevant event.

- There is a Syslog server in your network that receives the log entries. Since this is a UDP connection, there is no acknowledgment to the sender.
- The IP address or the FQDN of the Syslog server is entered on the device.

System Logging (Syslog) Client

Syslog Client

Syslog Server Address:

Select	Syslog Server Address	Server Port	TLS
<input type="checkbox"/>	192.168.16.100	514	<input type="checkbox"/>

1 entry.

Description

The page contains the following boxes:

- **Syslog Client**
Enable or disable the Syslog function.
- **Syslog Server Address**
Enter the IP address of the Syslog server.

This table contains the following columns

- **Select**
Select the row you want to delete.
- **Syslog Server Address**
Shows the IP address or the FQDN of the Syslog server.
- **Server Port**
Enter the port of the Syslog server being used.
- **TLS**
When this check box is selected, communication with the Syslog server is encrypted.

Procedure

Enabling function

1. Select the "Syslog Client" check box.
2. Click the "Set Values" button.

Creating a new entry

1. In the "Syslog Server Address" input box, enter the IP address or the FQDN of the Syslog server on which the log entries will be saved.
2. Click the "Create" button. A new row is inserted in the table.

6.4 The "System" menu

3. In the "Server Port" input box, enter the number of the UDP port of the server.
4. Click the "Set Values" button.

Note

The default setting of the server port is 514.

Changing the entry

1. Delete the entry.
2. Create a new entry.

Deleting an entry

1. Select the check box in the row to be deleted.
2. Click the "Delete" button. All selected entries are deleted and the display is refreshed.

6.4.15 Ports

6.4.15.1 Overview

Overview of the port configuration

The page shows the configuration of the data transfer for all ports of the device. You cannot configure anything on this page.

Ports Overview									
Overview Configuration									
Port	Port Name	Port Type	Status	OperState	Link	Mode	MTU	Negotiation	Maximum Nodes
P0.1		Switch-Port VLAN Hybrid	enabled	up	up	1G FD	1514	enabled	0
P0.2		Switch-Port VLAN Hybrid	enabled	down	down	1G FD	1514	enabled	0
P0.3		Switch-Port VLAN Hybrid	enabled	down	down	1G FD	1514	enabled	0
P0.4		Switch-Port VLAN Hybrid	enabled	down	down	1G FD	1514	enabled	0
P0.5		Switch-Port VLAN Hybrid	enabled	down	down	1G FD	1514	enabled	0

(Continuation of table)

Maximum Nodes	Learnt Nodes	MAC Address	Blocked by	Unicast MAC Learning
0	0	d4-f5-27-cc-e5-81	Link down	enabled
0	0	d4-f5-27-cc-e5-82	Link down	enabled
0	0	d4-f5-27-cc-e5-83	Link down	enabled
0	0	d4-f5-27-cc-e5-84	Link down	enabled

Description of the displayed boxes

The table has the following columns:

- **Port**
Shows the available ports. If you click on the port, the corresponding configuration page is opened. The port is made up of the module number and the port number, for example port 0.1 is module 0, port 1.
- **Port Name**
Shows the name of the port.
- **Port Type**
Shows the type of the port. The following types are possible:
 - Switch-Port VLAN Hybrid
 - Switch-Port VLAN Trunk
 - Router-Port
 - Switch-Port PVLAN Host
 - Switch-Port PVLAN Promiscuous
 - Switch-Port VLAN Access
- **Status**
Shows whether the port is enabled or disabled. Data traffic is possible only over an enabled port.
- **OperState**
Displays the current operating state. The operating status depends on the configured "Status" and the "Link". The following options are possible:
 - up
You have configured the status "enabled" for the port, and the port has a valid connection to the network.
 - down
You have configured the status "disabled" or "Link down" for the port, or the port has no connection.
 - not present
With modular devices, this status is displayed when, for example, no media module is inserted.
- **Link**
Shows the connection status to the network. With the connection status, the following is possible:
 - up
The port has a valid link to the network, a "Link Integrity Signal" is being received.
 - down
The link is down, for example, because the connected device is turned off.
- **Mode**
Shows the transfer parameters of the port.
- **MTU (Maximum Transmission Unit)**
Shows the packet size.

6.4 The "System" menu

- **Negotiation**
Shows whether the automatic configuration is enabled or disabled.
- **Maximum Nodes**
Shows the number of learnt MAC addresses after which a warning is output. If the value "0" is displayed, this function is disabled. With a value greater than "0", this function is enabled.
- **Learnt Nodes**
The number of MAC addresses that were learned for this port.
- **MAC Address**
Shows the MAC address of the port.

- **Blocked by**
Shows why the port is in the "blocked" status:
 - -
The port is not blocked.
 - Ring Redundancy
The port belongs to a redundancy manager. When the redundancy manager is in the "Passive" status, one of the ring ports is in the "blocking" status.
 - Spanning Tree
The port has the status "Discarding" in the spanning tree. The port is part of a spanning tree but is located in a redundant path and disabled for data traffic.
 - Loop Detection
A loop was detected, and the status "disable" was configured for the port as reaction to a loop.
 - Link Aggregation Member
The port is part of a link aggregation and was disabled by LACP.
 - Link Aggregation (LoopD)
The port is part of a link aggregation. A loop was detected and the status "disable" was configured for the link aggregation as reaction to a loop.
 - Link Aggregation (STP)
The port is part of a link aggregation. The link aggregation was switched to the status "Discarding" by the spanning tree.
 - Admin down
The status "disabled" is configured for the port, see "System > Ports > Configuration".
 - Link down
The "enabled" status is configured for the port but there is no connection, see "System > Ports > Configuration".
 - Spannungsversorgung aus
The status "Link down" or "Power down" is configured for the port; see "System > Ports > Configuration".
 - Standby
Standby redundancy is enabled on the device. The port is a standby port with the status "Passive".
 - MRP-Interconnection
The port is an MRP Interconnection port with the status "blocking".
- **Unicast MAC Learning**
Shows whether the learning of unicast addresses is enabled or disabled for a port.

6.4.15.2 Configuration

Configuring ports

With this page, you can configure all the ports of the device.

Description

The table has the following rows:

- **Port**
Select the port to be configured from the drop-down list. The port is made up of the module number and the port number, for example port 0.1 is module 0, port 1.
- **Status**
Specify whether the port is enabled or disabled.
 - **Enabled**
The port is enabled. Data traffic is possible only over an enabled port.
 - **Disabled**
The port is disabled but the connection remains.
 - **Link down**
The port is disabled and the connection to the partner device is terminated.
 - **Power down**
The port is disabled.

- **Port Name**
Enter a name for the port.
- **MAC Address**
Shows the MAC address of the port.
- **Mode Type**
From this drop-down list, select the transmission speed and the transfer mode of the port. If you set the mode to "Auto negotiation", these parameters are automatically negotiated with the connected end device. This must also be in the "Auto negotiation" mode for this purpose.

Note

Before the port and partner port can communicate with each other, the settings must match at both ends.

- **Mode**
Shows the transmission speed and the transmission mode of the port. The transmission speed can be 10 Mbps, 100 Mbps, 1000 Mbps or 10 Gbps. As the transmission mode, you can configure full duplex (FD) or half duplex (HD).
- **Negotiation**
Shows whether the automatic configuration of the connection to the partner port is enabled or disabled.
- **MTU**
Enter the packet size.

- **Port Type**
Select the type of port from the drop-down list.

Note

Private VLAN functionality and RADIUS authentication

When VLAN assignment is enabled via RADIUS authentication for one or more ports of a VLAN, you should not configure this VLAN additionally as private VLAN.

The private VLAN functionality in connection with VLAN assignment via RADIUS authentication can result in an inconsistent system state.

- **Switch-Port VLAN Hybrid**
The port sends tagged and untagged frames. It is not automatically a member of a VLAN.
 - **Switch-Port VLAN Trunk**
The port only sends tagged frames and is automatically a member of all VLANs.
 - **Router-Port**
The port is a layer 3 interface. It does not support layer 2 functions.
 - **Switch-Port PVLAN Host**
Host ports belong to a secondary PVLAN.
Connect devices to host ports that are only intended to communicate with certain devices of the PVLAN.
 - **Switch-Port PVLAN Promiscuous**
Promiscuous ports belong to a primary PVLAN.
Connect devices to promiscuous ports that are intended to communicate with all devices of the PVLAN.
 - **Switch-Port VLAN Access**
Access ports belong to a provider switch that supports the function Q-in-Q VLAN-Tunnel.
Connect a customer network to access ports.
- **Nodes Monitoring**
When this check box is selected, a warning is output when the maximum number of nodes is exceeded. When it is selected, the value in the "Maximum number of nodes" input box is automatically set to "1"; when cleared, the value is automatically set to "0".
 - **Maximum Nodes**
The number of learned MAC addresses after which a warning is output. If the value in this input box is greater than "0", the "Node monitoring" check box is selected automatically. The value "0" clears the "Node monitoring" check box automatically.

- **Operating Status**

Displays the current operational status. The operating status depends on the configured "Status" and the "Link". The following options are possible:

 - **up**

You have configured the status "Enabled" for the port and the port has a valid connection to the network.
 - **down**

You have configured the status "Disabled" or "Link down" for the port or the port has no connection.
 - **not present**

With modular devices, this status is displayed when, for example, no media module is inserted.
- **Link**

Shows the connection status to the network. The following options are possible:

 - **up**

The port has a valid link to the network, a link integrity signal is being received.
 - **down**

The link is down, for example because the connected device is turned off.

- **Blocked by**
Shows why the port is in the "blocked" status:
 - -
The port is not blocked.
 - **Ring Redundancy**
The port belongs to a redundancy manager. When the redundancy manager is in the "Passive" status, one of the ring ports is in the "blocking" status.
 - **Spanning Tree**
The port has the status "Discarding" in the spanning tree. The port is part of a spanning tree but is located in a redundant path and disabled for data traffic.
 - **Loop Detection**
A loop was detected, and the status "disable" was configured for the port as reaction to a loop.
 - **Link Aggregation Member**
The port is part of a link aggregation and was disabled by LACP.
 - **Link Aggregation (LoopD)**
The port is part of a link aggregation. A loop was detected and the status "disable" was configured for the link aggregation as reaction to a loop.
 - **Link Aggregation (STP)**
The port is part of a link aggregation. The link aggregation was switched to the status "Discarding" by the spanning tree.
 - **Admin down**
The status "disabled" is configured for the port, see "System > Ports > Configuration".
 - **Link down**
The "enabled" status is configured for the port but there is no connection, see "System > Ports > Configuration".
 - **Power down**
The status "Link down" or "Power down" is configured for the port; see "System > Ports > Configuration".
 - **Standby**
Standby redundancy is enabled on the device. The port is a standby port with the status "Passive".
 - **MRP-Interconnection State Change**
The port is an MRP Interconnection port and is in the "Blocked" state.
- **Unicast MAC Learning**
Enable or disable the learning of unicast addresses for a port. These unicast addresses are entered in the FDB as dynamically learned addresses.

Changing the port configuration

Click the appropriate box to change the configuration.

Note

Optical ports only work with the full duplex mode and at maximum transmission rate. As a result, the following settings cannot be made for optical ports:

- Automatic configuration
 - Transmission speed
 - Transmission mode
-

Note

With various automatic functions, the device prevents or reduces the effect on other ports and priority classes (Class of Service) if a port is overloaded. This can mean that frames are discarded even when flow control is enabled.

Port overload occurs when the device receives more frames than it can send, for example as the result of different transmission speeds.

Configuration procedure

1. Change the settings according to your configuration.
2. Click the "Set Values" button.

6.4.16 Fault Monitoring

6.4.16.1 Power Supply

Settings for monitoring the power supply

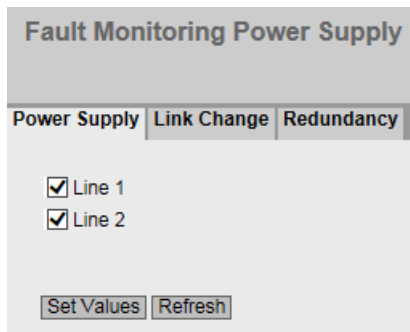
Configure whether or not the power supply should be monitored by the messaging system. Depending on the hardware variant, there are one or two power connectors (Supply 1 / Supply 2). With a redundant power supply, configure the monitoring separately for each individual feed-in line.

A fault is then signaled by the message system when there is no power on a monitored connection (supply 1 or supply 2) or when the applied voltage is too low.

Note

You will find the permitted operating voltage limits in the operating instructions of the device.

A fault causes the signaling contact to trigger and the fault LED on the device to light up and, depending on the configuration, can trigger a trap, an e-mail, or an entry in the event log table.



Procedure

1. Click the check box in front of the line name you want to monitor to enable or disable the monitoring function.
2. Click the "Set Values" button.

6.4.16.2 Link Change

Configuration of fault monitoring of status changes on connections

On this page, you configure whether or not an error message is triggered if there is a status change on a network connection.

If connection monitoring is enabled, an fault is signaled when:

- There should be a link on a port and the link is missing.
- There should not be a link on the port and a link is detected.
- The link on a port frequently changes.

A fault causes the signaling contact to trigger and the fault LED on the device to light up and, depending on the configuration, can trigger a trap, an e-mail, or an entry in the event log table.

Description of the displayed boxes

The page contains the following boxes:

- **Flap Count**
Configure the maximum number of allowed changeovers between "Link up" and "Link down" within the flap time.
- **Flap Reaction**
Select what happens when the error occurs:
 - Notifications
A persistent error message is triggered that needs to be acknowledged by the user.
 - Notify power down
A persistent error message is triggered that needs to be acknowledged by the user and the port is disabled.

Acknowledge the error message manually under "Information > Error".
Activate the port manually under "System > Ports > Configuration".
- **Flap Time [s]**
Configure the time interval in which the maximum number of allowed changeovers between "Link up" and "Link down" is monitored.
If a port changes between "Link up" and "Link down" within the flap time more often than the value of the flap count, the fault is triggered.

Table 1 has the following columns:

- **1st column**
Shows that the settings are valid for all ports.
- **Setting**
Select the setting from the drop-down list. You have the following setting options:
 - "-" (disabled)
 - Up
 - Down
 - Flap: See the explanation below
 - No Change: The setting in table 2 remains unchanged.
- **Copy to Table**
If you click the button, the setting is adopted for all ports of table 2.

Table 2 has the following columns:

- **Port**
Shows the available ports and link aggregations. The port is made up of the module number and the port number, for example port 0.1 is module 0, port 1.
- **Setting**
Select the setting from the drop-down list. You have the following options:
 - "-" (disabled)
Error handling is not triggered.
 - Up
Error handling is triggered when the port changes to the active status.
(From "Link down" to "Link up")
 - Down
Error handling is triggered when the port changes to the inactive status.
(From "Link up" to "Link down")
 - Flap
Error handling is triggered if the port changes between "Link up" and "Link down" more often than the value of the flap count within the flap time.

Configuration procedure

Configure error monitoring for a port

1. Adjust the values for the flap monitoring.
2. From the relevant drop-down list, select the options of the slots / ports whose connection status you want to monitor.
3. Click the "Set Values" button.

Configure error monitoring for all ports

1. Adjust the values for the flap monitoring.
2. Select the required setting from the drop-down list of the "Setting" column.

3. Click the "Copy to Table" button. The setting is adopted for all ports of table 2.
4. Click the "Set Values" button.

6.4.16.3 Redundancy

On this page, you configure whether or not an error message is triggered if there is a status change on a redundant connection.



Setting

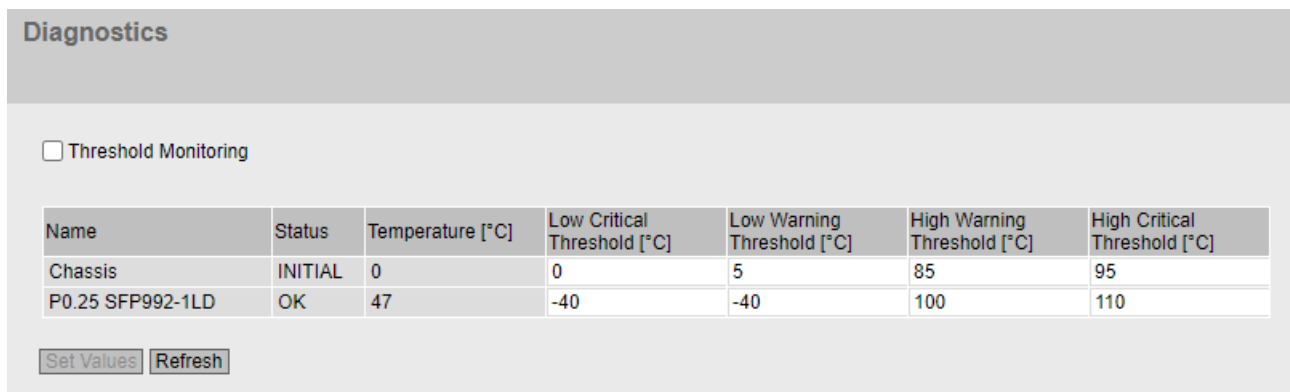
- **Redundancy Lost**
When the check box is selected, the error LED is activated for the respective ring manager in case of a ring switchover (MRP or HRP, blocked port is closed).

6.4.17 Diagnostics

On this page, you can configure thresholds for internal and external modules of the device. The modules are only shown if they make diagnostics information available. If you add or remove a module, the display is automatically adapted.

If the diagnostic value falls below or exceeds the configured thresholds, the status changes accordingly.

On the "System > Events > Configuration" page, you can specify how the device signals the status change.



Description

The page contains the following boxes:

- **Threshold Monitoring**

Enable or disable the monitoring of the thresholds.

If the monitoring is enabled, the events are only triggered if the threshold is exceeded for more than 15 minutes.

The table contains the following columns:

- **Name**

Shows the name of the module.

The information in the row "Chassis" relates to the inner temperature of the housing.

In the case of pluggable transceivers, the port and type are specified.

- **Status**

Depending on the relationship between the threshold values and the current temperature the following statuses are displayed in ascending priority.

- OK

The temperature value is within the preset threshold values.

- WARNING

The low or high threshold of the severity level "Warning" was fallen below or exceeded, respectively. The temperature is still in a normal range. The device has detected a fall or rise in temperature, for example, due to changed cooling of the cabinet. The device should be checked.

- CRITICAL

The low or high threshold of the severity level "Critical" was fallen below or exceeded, respectively. The device must be checked. A too low or too high temperature can lead to restricted performance or damage to the device.

- INVALID

The value could not be read out or is invalid. In the "Temperature [°C]" box "-" is displayed.

- INITIAL

No data has been read out yet.

- **Temperature [°C]**

Shows the current value of the temperature. The display is updated at regular intervals.

The value can have a tolerance of +/- 3 °C. Thus, the value can differ for the same devices with similar ambient conditions.

- **Lower Threshold [°C] (Critical)**

If the value falls below this value, the status changes to "CRITICAL". You can configure that you are informed by a message.

- **Lower Threshold [°C] (Warning)**

If the value falls below this value, the status changes to "WARNING". You can configure that you are informed by a message.

- **Upper Threshold [°C] (Warning)**

If the value exceeds this value, the status changes to "WARNING". You can configure that you are informed by a message.

- **Upper Threshold [°C] (Critical)**

If the value exceeds this value, the status changes to "CRITICAL". You can configure that you are informed by a message.

6.4.18 PROFINET

Settings for PROFINET

On this page, you configure the mode of PROFINET.

PROFINET

PROFINET Device Diagnostics: On

PROFINET Device Diagnostics for next boot: On ▾

PROFINET AR Status: Offline

PROFINET Name of Station:

Description

The page contains the following boxes:

- **PROFINET Device Diagnostics**
Shows whether PROFINET is enabled ("On") or disabled ("Off").
- **PROFINET Device Diagnostics for next boot**
Set whether PROFINET will be enabled ("On") or disabled ("Off") after the next device restart.

Note

PROFINET and EtherNet/IP

When PROFINET is turned on, EtherNet/IP is turned off. The switchover from PROFINET and EtherNet/IP has no effect on DCP.

Note

PROFINET AR Status

If a PROFINET connection is established; in other words, the PROFINET AR status is "Online", you cannot disable PROFINET.

- **PROFINET AR Status**
This box shows the status of the PROFINET connection; in other words whether the device is connected to a PROFINET controller "Online " or "Offline".
Here, online means that a connection to a PROFINET controller exists, that it has downloaded its configuration data to the device and that the device can send status data to the PROFINET controller. In this status that is also known as "in data exchange", the parameters set via the PROFINET controller cannot be configured.

6.4 The "System" menu

- **PROFINET Name of Station**
This box displays the PROFINET device name according to the configuration in HW Config of STEP 7 or via the CLI with the `pnio station-name` command.
- **Restart with PROFINET Defaults**
Click this button to restore the default settings of the PROFINET profile and to restart the device. You must confirm the restart in a dialog box. The dialog box displays the settings specially made for operation with the PROFINET protocol.

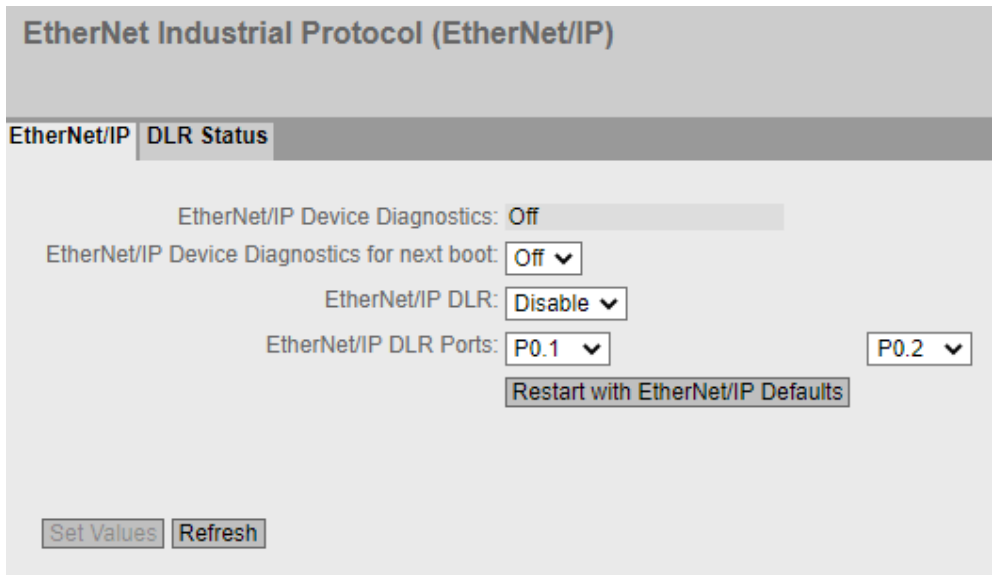
NOTICE
By resetting the settings to the default settings of a profile, the IP address is also lost. The device can then only be addressed via the serial interface, SINEC PNI or via DHCP.
With the appropriate connection, a previously correctly configured device can cause circulating frames after the reset and therefore the failure of the data traffic.

6.4.19 EtherNet/IP

6.4.19.1 EtherNet/IP

EtherNet Industrial Protocol (EtherNet/IP)

On this page, you configure the EtherNet/IP protocol.



Description

The page contains the following boxes:

- **EtherNet/IP Device Diagnostics**
Shows whether EtherNet/IP is enabled ("On") or disabled ("Off").
- **EtherNet/IP Device Diagnostics for next boot**
Set whether EtherNet/IP will be enabled ("On") or disabled ("Off") after the next device restart.

Note

EtherNet/IP and PROFINET

When EtherNet/IP is turned on, PROFINET is turned off. The switchover from EtherNet/IP and PROFINET has no effect on DCP.

Note

PROFINET AR Status

If a PROFINET connection is established; in other words the PROFINET AR status is "Online", you cannot enable EtherNet/IP.

- **EtherNet/IP DLR**
Set whether the Device Level Ring (DLR) protocol is activated ("Enable") or deactivated ("Disable").
- **EtherNet/IP DLR Ports**
Select the two DLR ports in the drop-down lists.
- **Restart with EtherNet/IP Defaults**
Click this button to restore the default settings of the EtherNet/IP profile and to restart the device. You must confirm the restart in a dialog box. The dialog box displays these settings specially made for operation with the EtherNet/IP protocol.

NOTICE
<p>Failure of the data traffic after resetting to default settings</p> <p>By resetting all the settings to the default settings of a profile, the IP address is also lost. The device can then only be addressed via the serial interface, SINEC PNI or via DHCP.</p> <p>With the appropriate attachment, a previously correctly configured device can cause circulating frames after the reset and therefore the failure of the data traffic.</p>

6.4.19.2 DLR Status

Device Level Ring status

This page displays information on the Device Level Ring (DLR) protocol. You cannot configure parameters on this page.

EtherNet/IP	DLR Status
	Supervisor IP Address: 0.0.0.0
	Supervisor MAC Address: 00-00-00-00-00-00
	Ring Topology: Linear
	Ring State: Fault
	Node State: Idle
	Network Status: Normal
	VLAN ID: 0
	Ring Port 1 Status: Down
	Ring Port 2 Status: Down

Description

The page contains the following boxes:

- **Supervisor IP Address**
The IP address of the device that takes on the function of the DLR supervisor.
- **Supervisor MAC Address**
The MAC address of the device that takes on the function of the DLR supervisor.
- **Ring Topology**
The topology of the network of the two DLR ports.
- **Ring State**
Shows whether the DLR ring is working properly.
- **Node State**
Shows the state of the DLR supervisor.
- **Network Status**
Shows the functionality of the network.

- **VLAN ID**
The VLAN ID for EtherNet/IP. The VLAN ID "0" is not supported. The VLAN ID "0" is only displayed in the WBM when EtherNet/IP DLR is not enabled and as long as no supervisor has been recognized. With SCALANCE XC-300/XR-300, the DLR VLAN is independent of the VLAN configuration of the device.
- **Ring Port 1 Status**
The port status of DLR port 1.
- **Ring Port 2 Status**
The port status of DLR port 2.

6.4.20 PLUG

6.4.20.1 Configuration

NOTICE
<p>Do not remove or insert the PLUG during operation.</p> <p>A PLUG may only be removed or inserted when the device is turned off.</p> <p>The device checks whether a PLUG is inserted at one second intervals. If the PLUG is removed during operation, loss of data may occur.</p>

Information about the PLUG configuration

This page provides detailed information about the configuration stored on the PLUG. It is also possible to reset the PLUG to "Factory settings" or to load it with new contents.

Note

The action is only executed after you click the "Set Values" button.

The action cannot be undone.

If you decide against executing the function after making your selection, click the "Refresh" button. As a result the data of this page is read from the device again and the selection is canceled.

PLUG Configuration (CLP)

Configuration

State: NOT PRESENT

Device Group: -

Device Type: -

Configuration Revision: -

File System: -

File System Size: -

File System Usage: -

Info String: -

Firmware on PLUG

Modify PLUG: Select action

Description

The table has the following rows:

- **State**
Shows the status of the PLUG. The following are possible:
 - ACCEPTED
There is a PLUG with a valid and suitable configuration in the device.
 - NOT ACCEPTED
Invalid or incompatible configuration on the inserted PLUG.
 - NOT PRESENT
No PLUG is inserted in the device.
 - FACTORY
PLUG is inserted and does not contain a configuration. This status is also displayed when the PLUG was formatted during operation.
- **Device Group**
Shows the SIMATIC NET product line that used the PLUG previously.
- **Device Type**
Shows the device type within the product line that used the PLUG previously.
- **Configuration Revision**
The version of the configuration structure. This information relates to the configuration options supported by the device and has nothing to do with the concrete hardware configuration. This revision information does not therefore change if you add or remove additional components (modules or extenders), it can, however, change if you update the firmware.
- **File System**
Displays the type of file system on the PLUG.
- **File System Size**
Displays the maximum storage capacity of the file system on the PLUG in bytes.
- **File System Usage**
Displays the storage space in use in the file system of the PLUG in bytes.
- **Info String**
Shows additional information about the device that used the PLUG previously, for example, article number, type designation, and the versions of the hardware and software. The displayed software version corresponds to the version in which the configuration was last changed. With the "NOT ACCEPTED" status, further information on the cause of the problem is displayed.

6.4 The "System" menu

- **Firmware on PLUG**
The setting is enabled by default.
When enabled, the firmware will be stored on the PLUG. This means that automatic firmware updates/downgrades can be made with the PLUG. The "Info" field shows whether or not the firmware is stored on the PLUG. You can find more information on this in the section "Configuration License PLUG (CLP) (Page 26)".
- **Modify PLUG**
Select the required setting from the drop-down list. You have the following options for changing the configuration on the PLUG:
 - Write current configuration to PLUG
This option is available only if the status of the PLUG is "NOT ACCEPTED" or "FACTORY".
The configuration in the internal flash memory of the device is copied to the PLUG.
 - Erase PLUG to factory default
Deletes all data from the PLUG and performs low-level formatting.

Procedure

Requirement:

- User with administrator rights

Modifying the PLUG configuration

1. If you want to save the firmware on the PLUG, select the check box "Firmware on PLUG".
2. Click the "Set Values" button.

6.4.21 Ping

Reachability of an address in an IPv4 network

With the ping function, you can check whether a certain IPv4 address is reachable in the network.



The screenshot shows a web-based interface for the Ping utility. At the top, the title "Ping" is displayed. Below the title, there are two input fields: "Destination Address:" and "Repeat: 3". To the right of the "Repeat:" field is a "Ping" button. Below these fields is a large, empty rectangular area labeled "Ping Output:". At the bottom left of the interface is a "Clear" button.

Description

The table has the following columns:

- **Destination Address**
Enter the IPv4 address of the device.
- **Repeat**
Enter the number of ping requests.
- **Ping**
Click this button to start the ping function.
- **Ping Output**
This box shows the output of the ping function.

6.4.22 DCP Discovery

On this page, you can select an interface and search for devices that are reachable via the interface and support DCP. DCP Discovery only searches for devices located in the same subnet as the interface. The reachable devices are listed in a table. In the table, you can check and adapt the network parameters of the devices. To identify and configure the devices, the Discovery Configuration Protocol (DCP) is used.

Note

DCP Discovery

The function is only available with the VLAN associated with the TIA interface. You configure the TIA interface under "System > Agent IP".

Discovery and Set via PROFINET Discovery and Configuration Protocol (DCP)

Timeout[s]: 5

Blink Own LEDs

Interface: vlan1

Discover

Port	MAC Address	Device Type	Device Name	IP Address	Mask Address	Gateway Address	Name Status	IP Status	Timeout[s]	Blink
P0.8	00-1b-1b-38-5c-90	SCALANCE W-700		192.168.16.177	255.255.255.0	0.0.0.0	None	Discovered/IP	5	Blink
P0.8	00-1b-1b-40-91-23	SCALANCE X-500		192.168.16.150	255.255.255.0	0.0.0.0	None	Discovered/IP	5	Blink
P0.8	00-1b-1b-9a-31-94	SCALANCE M-800		192.168.16.48	255.255.255.0	0.0.0.0	None	Discovered/IP	5	Blink
P0.8	00-1b-1b-9a-32-2e	SCALANCE M-800		192.168.16.50	255.255.255.0	0.0.0.0	None	Discovered/IP	5	Blink
P0.8	00-1b-1b-9a-3c-b2	SCALANCE M-800		192.168.16.46	255.255.255.0	0.0.0.0	None	Discovered/IP	5	Blink
P0.8	00-1b-1b-a5-5d-98	SCALANCE W-700		192.168.16.107	255.255.255.0	0.0.0.0	None	Discovered/IP	5	Blink
P0.8	00-1b-1b-af-a2-00	SCALANCE X-400		192.168.16.26	255.255.255.0	0.0.0.0	None	Discovered/IP	5	Blink
P0.8	00-1b-1b-b6-32-79	SCALANCE S-600		192.168.16.42	255.255.255.0	0.0.0.0	None	Discovered/IP	5	Blink
P0.8	00-1b-1b-c7-f5-a2	SCALANCE W-700		192.168.16.7	255.255.255.0	0.0.0.0	None	Discovered/IP	5	Blink
P0.8	00-1b-1b-c8-70-3a	SCALANCE X-300		192.168.16.33	255.255.255.0	192.168.16.33	None	Discovered/IP	5	Blink

1 - 10 of 33 entries [Show all](#)

1 Next

Set Values Refresh

Requirement:

To adapt network parameters, DCP requires write access to the device. If access is write-protected, the network parameters cannot be configured.

On the SCALANCE devices, you configure access under "System > Configuration".

Description

The page contains the following boxes:

- **Timeout[s]**
Select the period of time for which the LEDs should flash.
- **Blink Own LEDs**
Start flashing the LEDs of the device.

- **Interface**
Select the required interface.
- **Discover**
Starts the search for devices reachable via the selected interface.
On completion of the search, the reachable devices are listed in the table. The table is limited to 100 entries.

The table has the following columns:

- **Port**
Shows the port via which the device can be reached.
- **MAC Address**
Shows the MAC address of the device.
- **Device Type**
Shows the product line or product group to which the device belongs.
- **Device Name**
Adapt the PROFINET device name if necessary. The device name must be DNS-compliant. If the device name is not used, the box is empty.
- **IP Address**
If necessary, adapt the IPv4 address of the device.
The IPv4 address should be unique within your network and should match the network. The IPv4 address 0.0.0.0 means that no IPv4 address has yet been set.
- **Subnet mask**
If necessary, adapt the subnet mask of the device.
- **Gateway Address**
Adapt the IPv4 address of the gateway if necessary.
- **Status Device Name**
 - None: The device name is not used.
 - Discovered: The set device name is used.
 - Configured: The device was assigned a new device name.
- **IP Status**
 - Discovered/IP: The device uses a static IPv4 address.
 - Discovered/DHCP: The device has obtained the IPv4 address from a DHCP server.
 - Configured: The device was assigned a new IPv4 address.
- **Timeout[s]**
Specify the time for flashing. When the time elapses, flashing stops.
- **Blink**
Makes the port LEDs of the selected device flash.

Configuration procedure

1. Select the TIA interface.
2. To show all devices that can be reached via the TIA interface, click the "Discover" button.

6.4 The "System" menu

3. Adapt the desired properties.
4. Click the "Set Values" button.
The status of the modified properties changes to "Configured".
5. To ensure that the properties were applied correctly, click the "Discover" button again.
The status of the modified properties changes to "Discovered".

6.4.23 Port Diagnostics

6.4.23.1 Cable Tester

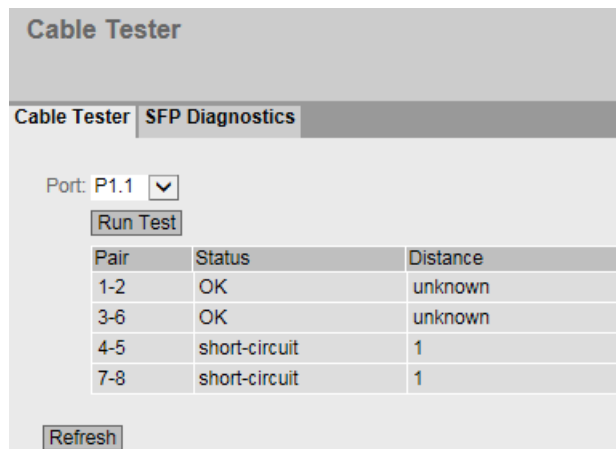
With this page, each individual Ethernet port can run independent fault diagnostics on the cable. This test is performed without needing to remove the cable, connect a cable tester and install a loopback module at the other end. Short-circuits and cable breaks can be localized to within a few meters.

Note

Please note that this test is permitted only when no data connection is established on the port to be tested.

If, however, there is a data connection to the port to be tested, this is briefly interrupted.

Automatic re-establishment of the connection can fail and then needs to be done manually.



Description

The page contains the following boxes:

- **Port**
Select the required port from the drop-down list.
- **Run Test**
Activates error diagnostics. The result is shown in the table.

The table contains the following columns:

- **Pair**
Shows the wire pair in the cable.

Note**Wire pairs**

Wire pairs 4-5 and 7-8 of 10/100 Mbps network cables are not used.

1000 Mbps or gigabit Ethernet uses all 4 wire pairs.

The wire pair assignment - pin assignment is as follows (DIN 50173):

Pair 1 = pin 4-5

Pair 2 = pin 1-2

Pair 3 = pin 3-6

Pair 4 = pin 7-8

- **Status**
Displays the status of the cable.
- **Distance**
Displays the distance to the open cable end, cable break, or short-circuit in meters. The value for the distance has a tolerance of +/-3 m.
If the status is "OK", the length is specified with "unknown".

6.4.23.2 SFP Diagnostics

On this page, you run independent error diagnostics for each individual SFP port. This test is performed without needing to remove the cable, connect a cable tester or install a loopback module at the other end.

Note

Note that this test is permitted only when no data connection is established on the port to be tested. If, however, there is a data connection to the port to be tested, this is briefly interrupted. Automatic re-establishment of the connection can fail; in this case, the connection needs to be re-established manually.

Small Form-factor Pluggable (SFP) Transceiver Diagnostics

Cable Tester
SFP Diagnostics

Port: P0.4 ▼

Name: SIEMENS

Model: SFP992-1

Revision: 1

Serial: NM0001MC1S0065

Nominal Bit Rate[MBit/s]: 10300

Max. Link (single mode)[m]: 80

Max. Link (50.0/125um)[m]: 80

Max. Link (62.5/125um)[m]: 30

	Current	Low	High
Temperature[°C]:	34.14	-5.0	75.0
Voltage[V]:	3.21	3.0	3.55
Current[mA]:	5.20	2.92	9.10
Rx Power[uW]:	0.0	63.0	891.2
Rx Power[dBm]:	-99.9	-12.0	0.5
Tx Power[uW]:	436.0	316.2	891.2
Tx Power[dBm]:	-3.6	-5.0	0.5

Refresh

Description

The page contains the following boxes:

- **Port**
Select the required port from the drop-down list.
- **Refresh**
Refreshes the display of the values of the set port. The result is shown in the table.

The values are shown in the following boxes:

- **Name**
Shows the name of the interface.
- **Model**
Shows the type of interface.
- **Revision**
Shows the hardware version of the SFP.
- **Serial**
Shows the serial number of the SFP.
- **Nominal Bit Rate [Mbps]**
Shows the nominal bit rate of the interface.

- **Max. Link (single mode)[m]**
Shows the maximum distance in meters that is possible with this medium.
- **Max. Link (50.0/125um)[m]**
Shows the maximum distance in meters that is possible with this medium.
- **Max. Link (62.5/125um)[m]**
Shows the maximum distance in meters that is possible with this medium.

The following table shows the values of the SFP transceiver used in this port:

Note**Deviations of the displayed values from the technical specifications**

The values displayed for the minimum and maximum send or receive power can vary slightly from the values specified in the operating instructions. The values displayed on the WBM page are relevant.

- **Temperature[°C]**
Shows the temperature of the interface.
- **Voltage[V]**
Shows the voltage applied to the interface in volts [V].
- **Current[mA]**
Shows the current consumption of the interface in milliamperes.
- **Rx Power[μW]/Rx Power[dBm]**
Shows the receive power of the interface in microwatts/decibel milliwatts.
- **Tx Power[μW]/Tx Power[dBm]**
Shows the transmit power of the interface in microwatts/decibel milliwatts.
- **Current column**
Shows the current value.
- **Low column**
Shows the lowest value.
- **High column**
Shows the highest value.

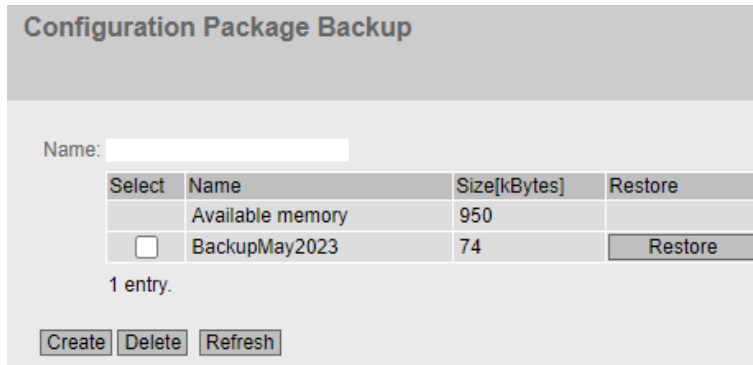
6.4.24 Configuration Backup

Backup

On this page, you can create backups of the configuration and save them on the device. The backups are created in "ConfigPack" format and include users with passwords, certificates and favorites in addition to the configuration. You can restore these backups directly from the device. After the restore, the device restarts. The maximum number depends on the size of the backup and the available memory space.

6.4 The "System" menu

On the "System > Load&Save > HTTP/TFTP/SFTP" page, you can save the created backups in ZIP format under "ConfigPackBackup" on your client PC to be able to load them from there later. You can find more detailed information in the section "Load & Save (Page 170)".



Description

The page contains the following boxes:

- **Name**
Enter a name for the backup.

The table contains the following columns:

- **Select**
Select the row you want to delete.
- **Name**
Shows the name of the backup.
- **Size [KB]**
The first row "Available memory" shows how much memory is available for backups on the device. When you create a backup, the available memory space is reduced accordingly. The other rows show the size of each backup.
- **Restore**
Click the "Restore" button to load the relevant backup on the device.

Procedure

1. Enter the required name.
2. Click the "Create" button.
The current configuration is saved as a configuration backup. Saving the backup may take some time. A new row is created for the backup. The size of the backup is displayed and subtracted from the available memory space.

6.5 The "Layer 2" menu

6.5.1 Configuration

Configuring layer 2

On this page, you create a basic configuration for the functions of layer 2. On the configuration pages of these functions, you can make more detailed settings. You can also check the settings on the configuration pages.

Note

The displayed parameters partially depend on the function or device.

The screenshot shows a web interface titled "Layer 2 Configuration". It contains several configuration options:

- Dynamic MAC Aging
- Redundancy Type: RSTP+
- Redundancy Mode: Standby MRP Interconnection Passive Listening
- RMON
- Dynamic Multicast:
- GVRP Mirroring Loop Detection
- PTP:

At the bottom of the form are two buttons: "Set Values" and "Refresh".

Description

- **Dynamic MAC Aging**
Enable or disable the "Aging" mechanism. You can configure other settings in "Layer 2 > Dynamic MAC Aging".
- **Redundancy Type**
The following settings are available:
 - "-" (disabled)
The redundancy function is disabled.
 - Spanning Tree
If you select this option, you specify the required redundancy mode in the "Redundancy Mode" drop-down list.
 - Ring
If you select this option, you specify the required redundancy mode in the "Redundancy Mode" drop-down list.
 - Ring with RSTP
If you select this option, the compatibility mode for Spanning Tree is set permanently to RSTP. In the "Redundancy Mode" drop-down list, you specify the redundancy mode of the ring redundancy.
You can change the current setting in the "Ring Redundancy" and "Spanning Tree" menus.

Note

Restriction relating to ports with the "Ring with RSTP" option

If you have enabled the "Ring with RSTP" option, the following ports must not be included in the Spanning Tree:

- Ring ports
 - Standby ports
 - Standby coupling ports
 - MRP Interconnection ports
-

- **RSTP+**
Enables RSTP+. You can only select this check box when MRP is configured as redundancy mode.

- **Redundancy Mode**

If you select "Ring" or "Ring with RSTP" in the "Redundancy Type" drop-down list, the following options are then available:

- Automatic Redundancy Detection
Select this setting to create an automatic configuration of the redundancy mode. In the "Automatic Redundancy Detection" mode, the device automatically detects whether there is a device with the "HRP Manager" role in the ring. If there is, the device adopts the role "HRP client".
If no HRP manager is found, all devices with the "Automatic Redundancy Detection" or "MRP Auto Manager" setting negotiate among themselves to establish which device adopts the role of "MRP Manager". The device with the lowest MAC address will always become the "MRP Manager". The other devices automatically set themselves to "MRP Client" mode.
- MRP Auto-Manager
In the "MRP Auto Manager" mode, the devices negotiate among themselves to establish which device will adopt the role of "MRP Manager". The device with the lowest MAC address will always become the "MRP Manager". The other devices automatically set themselves to "MRP Client" mode.
In contrast to the setting "Automatic Redundancy Detection", the devices are not capable of detecting whether an HRP manager is in the ring.
- MRP Client
The device adopts the role of MRP client.
- MRP Manager
The device adopts the role of MRP Manager. The device cannot take on the client role automatically.
- HRP Client
The device adopts the HRP Client role.
- HRP Manager
The device adopts the role of HRP manager.
When you configure an HRP ring, one device must be set as HRP Manager. For all other devices, "HRP Client" or "Automatic Redundancy Detection" must be set.

If you select "Spanning Tree" in the "Redundancy Type" drop-down list, the following options are then available:

- STP
Enables the Spanning Tree Protocol (STP). Typical reconfiguration times with Spanning Tree are between 20 and 30 seconds. You can configure other settings in "Layer 2 > Spanning Tree".
- RSTP
Enables the Rapid Spanning Tree Protocol (RSTP). If a Spanning Tree frame is detected at a port, this port reverts from RSTP to Spanning Tree. You can configure other settings in "Layer 2 > Spanning Tree".

Note

When using RSTP, loops involving duplication of frames or frames being overtaken may occur briefly. If this is not acceptable in your specific application, you need to use the slower standard Spanning Tree mechanism.

- MSTP
Enables the Multiple Spanning Tree Protocol (MSTP). You can configure other settings in "Layer 2 > Spanning Tree".

If you select "Ring with RSTP" in the "Redundancy Type" drop-down list, the current redundancy mode of the Spanning Tree and ring redundancy is displayed.

- **Standby**
Enable or disable the standby redundancy function. You can find other settings in "Layer 2 > Ring Redundancy".
- **MRP Interconnection**
Enable or disable the MRP Interconnection function. You can find other settings under "Layer 2 > Ring Redundancy > MRP Interconnection". You can only enable MRP Interconnection when the following requirements are met:
 - Ring redundancy is enabled.
 - "MRP Auto-Manager" or "MRP Client" is used as ring redundancy mode.
 - There is an activated MRP Interconnection connection.

Note

Configure the ring redundancy mode "MRP Auto-Manager" for two devices in each ring so that the MRP ring can be reconfigured immediately even when one device fails.

- **Passive Listening**
Enable or disable the passive listening function.
With passive listening, you can connect Spanning Tree networks to MRP/HRP rings. The ring nodes forward Spanning Tree BPDUs and therefore react to topology changes. When a topology change frame is received, the MAC address table is deleted.
- **RMON**
If you select this check box, Remote Monitoring (RMON) allows diagnostics data to be collected on the device, prepared and read out using SNMP by a network management station that also supports RMON. This diagnostic data, for example port-related load trends, allow problems in the network to be detected early and eliminated. Some of the "Ethernet Statistics Counters" are part of the RMON function. If you disable RMON, the "Ethernet statistics counter" in "Information > Ethernet Statistics" is no longer updated.
- **Dynamic Multicast**
The following settings are possible:
 - "-" (disabled)
 - IGMP Snooping
Enables IGMP (Internet Group Management Protocol). You can configure other settings in "Layer 2 > Multicast > IGMP".
 - GMRP
Enables GMRP (GARP Multicast Registration Protocol). You can configure other settings in "Layer 2 > Multicast > GMRP".

Note

GMRP and IGMP cannot be operated at the same time.

- **GVRP**
Enable or disable "GVRP" (GARP VLAN Registration Protocol). You can configure other settings in "Layer 2 > VLAN > GVRP".
- **Mirroring**
Enable or disable port mirroring. You can configure other settings in "Layer 2 > Mirroring".
- **Loop Detection**
Enable or disable the loop detection function. This allows loops in the network to be detected. You will find other settings in "Layer 2 > Loop Detection"
- **PTP**
The following settings are possible:
 - off
The device does not forward PTP messages.
 - transparent
The device does not synchronize itself with a time master but forwards PTP messages between the time master and the slaves to be synchronized.
 You will find other settings under "Layer 2 > PTP".

6.5.2 QoS (Quality of Service)

6.5.2.1 CoS queue mapping

CoS queue

Here, CoS priorities are assigned to certain queues (Traffic Queues).

Class of Service (CoS) Mapping

CoS Map	DSCP Map	QoS Trust																		
<table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr style="background-color: #f2f2f2;"> <th>COS</th> <th>Queue</th> </tr> </thead> <tbody> <tr><td>0</td><td>2 <input type="button" value="v"/></td></tr> <tr><td>1</td><td>1 <input type="button" value="v"/></td></tr> <tr><td>2</td><td>3 <input type="button" value="v"/></td></tr> <tr><td>3</td><td>4 <input type="button" value="v"/></td></tr> <tr><td>4</td><td>5 <input type="button" value="v"/></td></tr> <tr><td>5</td><td>6 <input type="button" value="v"/></td></tr> <tr><td>6</td><td>7 <input type="button" value="v"/></td></tr> <tr><td>7</td><td>8 <input type="button" value="v"/></td></tr> </tbody> </table>			COS	Queue	0	2 <input type="button" value="v"/>	1	1 <input type="button" value="v"/>	2	3 <input type="button" value="v"/>	3	4 <input type="button" value="v"/>	4	5 <input type="button" value="v"/>	5	6 <input type="button" value="v"/>	6	7 <input type="button" value="v"/>	7	8 <input type="button" value="v"/>
COS	Queue																			
0	2 <input type="button" value="v"/>																			
1	1 <input type="button" value="v"/>																			
2	3 <input type="button" value="v"/>																			
3	4 <input type="button" value="v"/>																			
4	5 <input type="button" value="v"/>																			
5	6 <input type="button" value="v"/>																			
6	7 <input type="button" value="v"/>																			
7	8 <input type="button" value="v"/>																			
<input type="button" value="Set Values"/> <input type="button" value="Refresh"/>																				

Description of the displayed boxes

The table has the following columns:

- **CoS**
Shows the CoS priority of the incoming packets.
- **Queue**
From the drop-down list, select the forwarding queue (send priority) that is assigned to the CoS priority.
The higher the number of the queue, the higher the send priority.
With queues 1 - 6 frames with a lower priority are occasionally processed even if there are frames with high priority in the queue.
With queues 7 - 8 only frames with a high priority are processed as long as there are frames with high priority in the queue.

The service classes (CoS) are assigned to the queues as follows:

- CoS 0 → Queue 2
- CoS 1 → Queue 1
- CoS 2 → Queue 3
- CoS 3 → Queue 4
- CoS 4 → Queue 5
- CoS 5 → Queue 6
- CoS 6 → Queue 7
- CoS 7 → Queue 8

Steps in configuration

1. For each value in the "CoS" column, select the forwarding queue from the "Queue" drop-down list.
2. Click the "Set Values" button.

6.5.2.2 DSCP Mapping

DSCP Mapping

On this page, DSCP settings are assigned to various queues (Traffic Queues).

Differentiated Services Code Point (DSCP) Mapping

CoS Map | **DSCP Map** | QoS Trust

DSCP min	DSCP max	Queue	Copy to Table
0	63	1	Copy to Table

DSCP	Queue
0	2
1	2
2	2
3	2
4	2

Set Values Refresh

Description of the displayed values

Table 1 has the following columns:

- DSCP min**
 From the drop-down list, select the minimum value for a range of DSCP codes to which you wish to assign a queue.
- DSCP max**
 From the drop-down list, select the maximum value for a range of DSCP codes to which you wish to assign a queue.
- Queue**
 From the drop-down list, select the forwarding queue (send priority) that is assigned to the range of DSCP codes.
- Copy to Table**
 When you click the button, the selected forwarding queue (send priority) is assigned to the DSCP codes in the specified range.

Table 2 has the following columns:

- **DSCP**
Shows the DSCP priority of the incoming packets.
- **Queue**
From the drop-down list, select the forwarding queue (send priority) that is assigned to the DSCP value.
The higher the queue number, the higher the send priority.
With queues 1 - 6 frames with a lower priority are occasionally processed even if there are frames with high priority in the queue.
With queues 7 - 8 only frames with a high priority are processed as long as there are frames with high priority in the queue.

The DSCP codes are assigned to the queues as follows:

- DSCP codes 0 - 7 → Queue 2
- DSCP codes 8 - 15 → Queue 1
- DSCP codes 16 - 23 → Queue 3
- DSCP codes 24 - 31 → Queue 4
- DSCP codes 32 - 39 → Queue 5
- DSCP codes 40 - 47 → Queue 6
- DSCP codes 48 - 55 → Queue 7
- DSCP codes 56 - 63 → Queue 8

Configuration procedure

1. For each value in the "DSCP" column, select the forwarding queue from the "Queue" drop-down list.
2. Click the "Set Values" button.

6.5.2.3 QoS Trust

Specifying the subnet priority

On this page you can set the method according to which frames to be forwarded are prioritized port by port.

Quality of Service (QoS) Trust Mode		
CoS Map DSCP Map QoS Trust		
Port	Trust Mode	Copy to Table
All ports	No Change	Copy to Table
Port	Trust Mode	
P0.1	Trust COS-DSCP	
P0.2	Trust COS-DSCP	
P0.3	Trust COS-DSCP	

Set Values Refresh

Description of the displayed values

Table 1 has the following columns:

- **Port**
Shows that the setting is valid for all ports of table 2.
- **Trust Mode**
Select the setting from the drop-down list. You have the following setting options:
 - No Trust
 - Trust COS
 - Trust DSCP
 - Trust COS-DSCP
 - No Change
Table 2 remains unchanged.
- **Copy to Table**
If you click the button, the setting is adopted for all ports of table 2.

Table 2 has the following columns:

- **Port**
Shows the configurable ports.
The port is made up of the module number and the port number, for example port 0.1 is module 0, port 1.
- **Trust Mode**
Select the required mode from the drop-down list:

Note

You configure the prioritization of the receiving port on the page "Layer 2 > VLAN > Port Based VLAN".

You configure the assignment of the following priorities to a queue on the page "Layer 2 > QoS > CoS Map":

- Receiving port
- VLAN tag
- Broadcast and agent frame

You configure the assignment of the DSCP prioritization to a queue on the page "Layer 2 > QoS > DSCP Map".

- No Trust
The switch sorts the incoming frames into a queue according to the prioritization of the receiving port.
If there is a DSCP value in the IP header, this is ignored. If a VLAN tag exists, its priority value is replaced by the priority value of the receiving port.
- Trust COS
If an incoming frame contains a VLAN tag, the switch sorts it into a queue according to this prioritization.
If the frame does not contain a VLAN tag, the switch sorts the frame into a queue according to the prioritization of the receiving port.
If there is a DSCP value in the IP header, this is ignored.
- Trust DSCP
If an incoming frame contains a DSCP prioritization, the switch sorts it into a queue according to this prioritization.
If the frame does not contain a DSCP prioritization, the switch sorts the frame into a queue according to the prioritization of the receiving port.
If the frame contains a VLAN tag, this is ignored.
- Trust COS-DSCP
With an incoming frame, there is a sequential check of which prioritization it contains.
If it contains a DSCP prioritization, it is handled as in the "Trust DSCP" mode.
If it contains no DSCP prioritization, the switch checks whether it contains a VLAN tag. If it contains a VLAN tag, the switch sorts it into a queue according to this prioritization.
If the frame contains neither a DSCP prioritization nor a VLAN tag, the switch sorts the frame into a queue according to the prioritization of the receiving port.

Configuration procedure

1. Select the required Trust Mode from the drop-down list.
2. Click the "Set Values" button.

6.5.3 Rate Control

Limiting the transfer rate of incoming and outgoing data

On this page, you configure the load limitation (maximum number of data packets per second) for the individual ports. For incoming data traffic, you also specify the category of telegrams to which the overall transmission rate should apply.

Rate Control

	Limit Ingress Unicast (DLF)	Limit Ingress Broadcast	Limit Ingress Multicast	Limit Ingress Unicast	Total Ingress Rate pkts/s	Egress Rate kb/s	Copy to Table
All ports	No Change <input type="button" value="v"/>	No Change <input type="button" value="v"/>	No Change <input type="button" value="v"/>	No Change <input type="button" value="v"/>	No Change	No Change	<input type="button" value="Copy to Table"/> <input type="button" value="↕"/>

Port	Limit Ingress Unicast (DLF)	Limit Ingress Broadcast	Limit Ingress Multicast	Limit Ingress Unicast	Total Ingress Rate pkts/s	Egress Rate kb/s
P0.1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	0	0
P0.2	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	0	0
P0.3	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	0	0
P0.4	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	0	0
P1.1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	0	0

Description of the displayed values

Table 1 has the following columns:

- **1st column**
Shows that the settings are valid for all ports.
- **Limit Ingress Unicast (DLF) / Limit Ingress Broadcast / Limit Ingress Multicast / Limit Ingress Unicast**
Select the required setting in the drop-down list.
 - enabled: Enables the function.
 - disabled: Disables the function
 - No Change: The setting in table 2 remains unchanged
- **Total Ingress Rate [pkts/s]**
Specify the maximum number of incoming packets processed by the device. If "No Change" is entered, the entry in the table remains unchanged.

- **Egress Rate kb/s**
Specify the data rate for all outgoing frames. If "No Change" is entered, the entry in the table remains unchanged
- **Copy to Table**
When you click the button, the settings are adopted for all ports of table 2.

Table 2 has the following columns:

- **Port**
Shows the slot and the port to which the other information relates. This field cannot be configured. The port is made up of the module number and the port number, for example port 0.1 is module 0, port 1.
- **Limit Ingress Unicast(DLF)**
Enable or disable the data rate for limiting incoming unicast frames with an unresolvable address (Destination Lookup Failure).
- **Limit Ingress Broadcast**
Enable or disable the data rate for limiting incoming broadcast frames.
- **Limit Ingress Multicast**
Enable or disable the data rate for limiting incoming multicast frames.
- **Limit Ingress Unicast**
Enable or disable the data rate for limiting incoming unicast frames with resolvable address.
- **Total Ingress Rate [pkts/s]**
Specify the maximum number of incoming packets processed by the device.

Note

The device limits data traffic to the entered value only if at least one check box in the following columns has been selected:

- Limit Ingress Broadcast
- Limit Ingress Multicast
- Limit Ingress Unicast

If no check box has been selected, incoming data traffic is not limited even if there is an entry in the "Total Ingress Rate pkts/s" field. If multiple check boxes have been selected, the total of data packets from all activated categories is decisive for limiting the data traffic.

- **Egress Rate kb/s**
Specify the data rate for all outgoing frames.

Note

Rounding of the values, deviation from desired value

When you input the rate values, note that the WBM rounds to correct values.

If values are configured for Total Ingress Rate and Egress Rate, the actual values in operation can deviate slightly from the set values.

Configuration procedure

1. Enter the relevant values in the columns "Total Ingress Rate" and "Egress rate" in the row of the port being configured.
2. To use the limitation for the incoming frames, select the check box in the row. For outgoing frames, the value in the "Egress Rate" column is used.
3. Click the "Set Values" button.

6.5.4 VLAN

6.5.4.1 General

VLAN configuration page

On this page, you configure the VLANs.

Note

Changes to the TIA interface

If the device is configured via TIA and the TIA interface is changed, the configuration PC can no longer access the device.

Virtual Local Area Network (VLAN) General

General

Bridge Mode: Customer

VLAN ID:

Select	VLAN ID	Name	Status	Private VLAN Type	Primary VLAN ID	Transparent	Learning	Priority	Update Priority
<input type="checkbox"/>	1		Static	-		<input type="checkbox"/>	<input checked="" type="checkbox"/>	Do not force	<input type="checkbox"/>
<input type="checkbox"/>	7		Static	-		<input type="checkbox"/>	<input checked="" type="checkbox"/>	Do not force	<input type="checkbox"/>

2 entries.

Create Delete Set Values Refresh

Important rules for VLANs

Make sure you keep to the following rules when configuring and operating your VLANs:

- Frames with the VLAN ID "0" are handled as untagged frames but retain their priority value.
- As default, all ports on the device send frames without a VLAN tag to ensure that the end node can receive these frames.
- With SCALANCE X devices, the VLAN ID "1" is the default on all ports.

- If an end node is connected to a port, outgoing frames should be sent without a tag (static access port). If, however, there is a further switch at this port, the frame should have a tag added (trunk port).
- With a trunk port, the VLAN assignment is dynamic. Static configurations can only be created if, in addition to the trunk port property, the port is also entered statically as a member in the VLANs involved. An example of a static configuration is the assignment of the multicast groups in certain VLANs.

Description

The page contains the following boxes:

- **Bridge mode**
Select the role of the device. The roles are as follows:
 - Customer
If you operate the device with the "Customer" role, it behaves like a standard IE switch.
 - Provider
If you operate the device with the "Provider" role, in addition to the properties of the "Customer" role, it provides the option of managing external VLAN tags. With this role you can use the function Q-in-Q VLAN tunnel.
- **VLAN ID**
Enter the VLAN ID in the "VLAN ID" input box.
Range of values: 1 ... 4094

The table has the following columns:

- **Select**
Select the row you want to delete.
- **VLAN ID**
Shows the VLAN ID. The VLAN ID (a number between 1 and 4094) can only be assigned once when creating a new data record and can then no longer be changed. To make a change, the entire data record must be deleted and created again. Up to 257 VLANs can be defined.
- **Name**
Enter a name for the VLAN. The name only provides information and has no effect on the configuration. The length is a maximum of 32 characters.
- **Status**
Shows the status type of the entry in the internal port filter table.
 - Static
The address of the user was entered statically
 - GVRP
The configuration was registered by a GVRP frame. This is, however, only possible if GVRP was enabled for the device.

- **Private VLAN Type**
Shows the type of the PVLAN.
 - -
These VLANs are not private VLANs.
 - Primary
With this type, you define a primary PVLAN. In a PVLAN you can only define one primary PVLAN. The primary PVLAN uses the VLAN ID of the VLAN.
 - Isolated
With this type, you define a secondary PVLAN. Devices within an Isolated Secondary PVLAN cannot communicate with each other via layer 2. The secondary PVLAN has a specific VLAN ID.
 - Community
With this type, you define a secondary PVLAN. The devices in this secondary PVLAN can communicate with each other via layer 2. The secondary PVLAN has a specific VLAN ID.
- **Primary VLAN ID**
For secondary PVLANS, shows the ID of the corresponding primary PVLAN.
- **Transparent**
When you select this check box, you switch a VLAN to the transparent mode. The prerequisite is that ports are not members of other VLANs. Ports that were assigned to this VLAN as members or untagged members now become transparent ports.
This means the following:
 - The port VLAN ID of the transparent ports is set to the ID of this VLAN.
 - Untagged frames that are received at these ports are also forwarded to all other transparent ports without tag.
 - Frames tagged with VLAN ID "0" and that are received at these ports are forwarded to all other transparent ports once again tagged with VLAN ID "0".
The VLAN ID "0" is used for the prioritization of PROFINET frames.
 - Frames tagged with the VLAN ID of the transparent VLAN and that are received at these ports are forwarded to all transparent ports once again tagged with the VLAN ID of the transparent VLAN.
 - Frames of the switch only receive the VLAN ID "0" in transparent mode. If the "Transparent" check box is not selected, the PROFINET IO frames of the switch is not tagged.
 - All ports that were not members or untagged members in the relevant VLAN are automatically set to the "Forbidden" status.
 - As long as a VLAN is configured as a transparent VLAN, the ports belonging to this VLAN cannot be modified.
 - You can only configure one a transparent VLAN.

Note

If you disable the transparent mode for a VLAN again, the previously written port configuration is retained.

- **Learning**
With this check box, you enable the learning of unicast addresses for a VLAN.
- **Priority**
Select a priority to apply to all incoming frames of this VLAN as new Class of Service (CoS). The frames are processed further by the switch depending on the selected priority, regardless of the port priority or the prioritization in untagged frames. The VLAN tags contained in the frame are not changed. If you select "Do not force", the priority of the frames remains unchanged. The frames are prioritized according to the port priority or the VLAN tag.
- **Update Priority**
When you select this check box, the value set in the "Priority" column is applied to the Tag Control Information (TCI) as new Class of Service.

Configuration procedure

1. Enter an ID in the "VLAN ID" input box.
2. Click the "Create" button. A new entry is generated in the table. As default, the boxes have "-" entered.
3. Enter a name for the VLAN under Name.
4. Switch the VLAN to the transparent or standard compliant mode.
5. Specify the use of the port in the VLAN. If, for example you select M, the port is a member of the VLAN. The frame sent in this VLAN is forwarded with the corresponding VLAN tag.
6. Click the "Set Values" button.

6.5.4.2 Port Assignment

List of ports

You specify the use of the ports on this page.

Virtual Local Area Network (VLAN) Port Assignment

General | **Port Assignment** | GVRP | Port Based VLAN

VLAN ID	Name	P0.1	P0.2	P0.3	P0.4	P0.5
1		U	U	U	U	U
7		M	-	-	u	-

2 entries.

Set Values Refresh

Description

The table has the following columns:

- **VLAN ID**
Shows the VLAN ID. The VLAN ID (a number between 1 and 4094) can only be assigned once when creating a new data record and can then no longer be changed. To make a change, the entire data record must be deleted and created again. Up to 257 VLANs can be defined.
- **Name**
Enter a name for the VLAN. The name only provides information and has no effect on the configuration. The length is a maximum of 32 characters.
- **List of ports**
Specify the use of the port. The following options are available:
 - **"_"**
The port is not a member of the specified VLAN.
With a new definition, all ports have the identifier "-".
 - **F**
The port is not a member of the specified VLAN and it is not possible for the VLAN to be registered dynamically at this port using GVRP. If a port in a VLAN has this option, it cannot become a member of this VLAN even if it is configured as a trunk port.
You can configure further settings in "Layer 2 > VLAN > Port-based VLAN".
 - **M**
The port is a member of the VLAN. Frames sent in this VLAN are forwarded with the corresponding VLAN tag.
 - **Q**
The port is tunnel port. Frames from different customer networks are forwarded using a VLAN tunnel via a provider network.
You define this port under "Layer 2 > Provider bridge > Tunnel ports (Page 306)".
 - **R**
The port is a member of the VLAN. A GVRP frame is used for the registration.
 - **T**
This port is a trunk port, making it a member in all VLANs.
You create this port under "System > Ports > Configuration".
 - **U (uppercase)**
The port is an untagged member of the VLAN. Frames sent in this VLAN are forwarded without the VLAN tag. Frames without a VLAN tag are sent from this port.
 - **u (lowercase)**
The port is an untagged member of the VLAN, but the VLAN is not configured as a port VLAN. Frames sent in this VLAN are forwarded without the VLAN tag.

Configuration procedure

1. In the row for a VLAN, click on the field for the port whose usage you want to configure. A button for opening a drop-down list is displayed.
2. Open the drop-down list and select one of the following settings:
 - "-"
 - **u** (lowercase)
You cannot select the setting "U" (uppercase). After "u" is selected, "U" is automatically displayed in the table if the PVID of the port matches the VLAN ID.
 - **M**
 - **F**
3. Click the "Set Values" button.

6.5.4.3 GVRP

Configuration of GVRP functionality

Using GVRP frame, a different device can register at the port of the device for a specific VID. A different device, can, for example be an end device or a switch. The device can also send GVRP frames via this port.

On this page, you can enable each port for GVRP functionality.

GARP VLAN Registration Protocol (GVRP)

General
Port Assignment
GVRP
Port Based VLAN

GVRP

	Setting	Copy to Table
All ports	No Change ▾	Copy to Table

Port	Setting	
P0.1	<input type="checkbox"/>	▲
P0.2	<input checked="" type="checkbox"/>	■
P0.3	<input type="checkbox"/>	▼

Set Values
Refresh

Timer

The following timers are set in the protocols mentioned above. The timer values are not configurable.

Timer	Description	Factory setting
Join-time	Time in milliseconds that passes between the transfer of two PDUs (Protocol Data Unit)	200 ms
Leave-time	Time period of the timer in milliseconds before the device changes its GARP status The timer starts and runs backwards with the defined time as soon as the device sends or receives a "Leave-all-time" message. The timer is stopped when the device receives a Join message.	600 ms
Leave-all-time	Time period of the timer in milliseconds before all devices change their GARP status	10000 ms

In devices connected via Layer 2, the same values must be set for the GARP/GMRP timers. If different values are set with the GARP/GMRP timers, GARP applications such as GMRP and GVRP cannot be executed successfully.

Description of the displayed boxes

The page contains the following box:

- **GVRP**
Enable or disable the GVRP function.

Table 1 has the following columns:

- **1st column**
Shows that the settings are valid for all ports of table 2.
- **Setting**
Select the setting from the drop-down list. You have the following setting options:
 - Enabled
Enables the sending of GVRP frames.
 - Disabled
Disables the sending of GVRP frames.
 - No change
No change to table 2.
- **Copy to Table**
If you click the button, the setting is adopted for all ports of table 2.

Table 2 has the following columns:

- **Port**
Shows the available ports. The port is made up of the module number and the port number, for example, port 0.1 is module 0, port 1.
- **Setting**
Enable or disable the sending GVRP frames.

Configuration procedure

1. Click "GVRP" check box.
2. Click the check box after the port in the "Setting" column to enable or disable GVRP for this port.
Repeat this for every port for which you want to enable or disable the function.
3. Click the "Set Values" button.

6.5.4.4 Port Based VLAN

Processing received frames

On this page, you specify the configuration of the port properties for receiving frames.

Port Based Virtual Local Area Network (VLAN) Configuration

? ☆

General | **Port Assignment** | **GVRP** | **Port Based VLAN**

	Priority	Port VID	Acceptable Frames	Ingress Filtering	Copy to Table
All ports	No Change ▾	No Change ▾	No Change ▾	No Change ▾	Copy to Table

Port	Priority	Port VID	Acceptable Frames	Ingress Filtering
P0.1	0 ▾	VLAN1 ▾	All ▾	<input type="checkbox"/>
P0.2	0 ▾	VLAN1 ▾	All ▾	<input type="checkbox"/>
P0.3	0 ▾	VLAN1 ▾	All ▾	<input type="checkbox"/>
P0.4	0 ▾	VLAN1 ▾	All ▾	<input type="checkbox"/>
P0.5	0 ▾	VLAN1 ▾	All ▾	<input type="checkbox"/>

Description of the displayed boxes

Table 1 has the following columns:

- **Port**
Shows that the settings are valid for all ports.
- **Priority // Port-VID / Acceptable Frames / Ingress Filtering**
Select the setting in the drop-down list. If "No Change" is selected, the entry in table 2 remains unchanged.
- **Copy to Table**
If you click the button, the setting is adopted for all ports of table 2.

Table 2 has the following columns:

- **Port**
Shows the available ports and link aggregations. The port is made up of the module number and the port number, for example, port 0.1 is module 0, port 1.
- **Priority**
From the drop-down list, select the priority given to untagged frames.
The CoS priority (Class of Service) used in the VLAN tag. If a frame is received without a tag, it will be assigned this priority. This priority specifies how the frame is further processed compared with other frames.
There are a total of eight priorities with values 0 to 7, where 7 represents the highest priority (IEEE 802.1p Port Priority).
- **Port VID**
Select the VLAN ID from the drop-down list. Only VLAN IDs defined on the "VLAN > General" page can be selected.
If a received frame does not have a VLAN tag, it has a tag with the VLAN ID specified here added to it and is sent according to the rules at the port.
- **Acceptable Frames**
Specify which types of frames will be accepted. The following alternatives are possible:
 - Tagged Frames Only
The device discards all untagged frames. Frames tagged with "0" are treated like untagged frames. The device forwards all tagged frames. Otherwise, the forwarding rules apply according to the configuration.
 - Untagged and Priority Tagged Only
The device discards all tagged frames. The device forwards all untagged frames as well as frames with VLAN = 0 and a priority (Priority Tagged Frames). Otherwise, the forwarding rules apply according to the configuration.
If you have configured the Bridge mode "Provider" this means that the device treats all incoming frames like untagged frames.
 - All
The device forwards all frames.
- **Ingress Filtering**
Specify whether the VID of received frames is evaluated
You have the following options:
 - Enabled
The VLAN ID of received frames decides whether they are forwarded: To forward a VLAN tagged frame, the receiving port must be a member in the same VLAN. Frames from unknown VLANs are discarded at the receiving port.
 - Disabled
All frames are forwarded.

Configuration procedure

1. In the row of the port to be configured, click on the relevant cell in the table to configure it.
2. Enter the values to be set in the input boxes as follows.

3. Select the values to be set from the drop-down lists.
4. Click the "Set Values" button.

See also

General (Page 293)

6.5.5 Private VLAN

6.5.5.1 General

Private VLAN configuration page

On this page you define the types of the PVLANS and assign secondary PVLANS to a primary PVLAN.

VLAN ID	Private VLAN Type	Primary VLAN ID
1	-	-
10	Primary	-
11	Isolated	10
12	Community	10

Set Values Refresh

Description

The table has the following columns:

- **VLAN ID**
Shows the VLAN ID.
- **Private VLAN Type**
Specify the type of PVLAN:
 - -
These VLANs are not private VLANs.
 - Primary
With this type, you define a primary PVLAN. In a PVLAN you can only define one primary PVLAN. The primary PVLAN uses the VLAN ID of the VLAN.
 - Isolated
With this type, you define a secondary PVLAN. Devices within an Isolated Secondary PVLAN cannot communicate with each other via layer 2. The secondary PVLAN has a specific VLAN ID.
 - Community
With this type, you define a secondary PVLAN. The devices in this secondary PVLAN can communicate with each other via layer 2. The secondary PVLAN has a specific VLAN ID.
- **Primary VLAN ID**
For secondary PVLANS select the VLAN ID of the primary PVLAN.

Configuration procedure

1. Create the required VLANs on the page "Layer 2 > VLAN > General".

Note

All secondary PVLANS must be known on all IE switches of a PVLAN. Even if an IE switch has no host port in a secondary PVLAN, the secondary PVLAN must be known on the IE switch.

2. Change to the page "Layer 2 > Private VLAN > General". A line is created there for every VLAN.
3. On this page, you specify the "Private VLAN Type".
4. Click the "Set Values" button.
5. For the secondary PVLANS specify the corresponding primary PVLAN.
6. Click the "Set Values" button.

7. For the required ports select the corresponding port type on the page "System > Ports > Configuration":
 - Switch-Port PVLAN Promiscuous
 - Switch-Port PVLAN Host
8. Specify the use of the ports on the page "Layer 2 > VLAN > Port Assignment".
 - For promiscuous ports that are connected to other promiscuous ports, select the setting "M" in all PVLANS.
 - For promiscuous ports that are connected to an end device, select the setting "u" (lower case) in all PVLANS.
Change to the page "Layer 2 > VLAN > Port Based VLAN" and select the VLAN ID of the Primary VLAN for these ports under "Port VID".
 - For host ports in the primary PVLAN and in its secondary PVLAN, select the setting "u" (lower case)
Change to the page "Layer 2 > VLAN > Port Based VLAN" and select the VLAN ID of the Secondary VLAN for these ports under "Port VID".

With incoming untagged frames, the port VLAN-ID of the VLAN is set by entering the port with the setting "U" (upper case).

6.5.5.2 IP Interface Mapping

Private VLAN configuration page

On this page you specify from which secondary PVLANS the IP interface of the primary PVLAN will be reachable.

Configure the IP interface assignment for all functions for which an end device needs to communicate from the secondary PVLAN via the IP interface of the primary PVLAN.

Examples:

- An end device in the secondary PVLAN is configured as DHCP client. A remote DHCP server is set up. A PVLAN switch is configured as DHCP relay agent. Configure an IP interface in the primary PVLAN of the DHCP relay agent. Assign the secondary PVLANS containing DHCP clients to this IP interface.
- A PVLAN switch is configured as router. Configure an IP interface in the primary PVLAN of the router. Assign the secondary PVLANS containing end devices that use the router as a gateway to this IP interface.

Private Virtual Local Area Network (VLAN) IP Interface Mapping

General IP Interface Mapping

Interface:

Secondary VLAN ID:

Select	Interface	Secondary VLAN ID
<input type="checkbox"/>	vlan10	11
<input type="checkbox"/>	vlan10	12

2 entries.

Description of the displayed boxes

The page contains the following boxes:

- **Interface**
Select the primary PVLAN with an IP interface.
- **Secondary VLAN ID**
Select a secondary VLAN ID from which the IP interface of the primary PVLAN will be reachable.

The table has the following columns:

- **Select**
Select the row you want to delete.
- **Interface**
Shows the IP interface.
- **Secondary VLAN-ID**
Shows the secondary VLAN-ID of the secondary PVLAN from which the IP interface of the primary PVLAN is reachable.

Steps in configuration

1. Create an IP interface for the primary PVLAN.
2. Select the primary PVLAN with an IP interface.
3. Select a secondary VLAN ID.
4. Click the "Create" button.

6.5.6 Provider Bridge

6.5.6.1 Tunnel ports

Configuration page for tunnel ports

On this page, you enable the Q-in-Q VLAN tunnel function. Frames received by a tunnel port are expanded by an external VLAN tag, the PVID of the port.

Port	Setting	Copy to Table
All ports	No Change	Copy to Table

Port	Setting
P0.1	<input type="checkbox"/>
P0.2	<input checked="" type="checkbox"/>
P0.3	<input type="checkbox"/>
P0.4	<input type="checkbox"/>

Set Values Refresh

Description of the displayed boxes

Table 1 has the following columns:

- **1st column**
Shows that the settings are valid for all ports of table 2.
- **Setting**
Select the setting from the drop-down list. You have the following setting options:
 - Enabled
Enables the Q-in-Q VLAN tunnel function on all ports.
 - Disabled
Disables the Q-in-Q VLAN tunnel function on all ports.
 - No Change
Table 2 remains unchanged.
- **Copy to Table**
When you click the button, the settings are adopted for all ports of table 2.

Table 2 has the following columns:

- **Port**
Shows all available ports. The port is made up of the module number and the port number, for example, port 0.1 is module 0, port 1.
- **Setting**
Enable or disable the function for this port.

Steps in configuration

To configure a port as a tunnel port proceed as follows:

1. Change to the page "Layer 2 > VLAN > General".
2. Configure the Bridge mode "Provider".
3. Click the "Set Values" button.
The layer 2 port settings (VLAN, Spanning Tree) are restored to the factory defaults and the device is restarted.
4. Change to the page "Layer 2 > VLAN > General".
5. Enter the required VLAN ID.
6. Click the "Create" button.
7. Change to the page "Layer 2 > VLAN > Port Based VLAN".
8. For the port select the port VID of the created VLAN.
9. For the port in "Acceptable Frames" select the setting "Untagged and Priority Tagged Only".
10. Click the "Set Values" button.
11. Change to the page "Layer 2 > VLAN > Port Mapping".
12. For the port in the required VLAN, select the setting "U" (uppercase).
13. For the port in all other VLANs, select the setting "-".
14. Click the "Set Values" button.
15. Disable the following protocols on the port:
 - On the page "Layer 2 > VLAN > GVRP" the check box beside "Setting".
 - On the page "Layer 2 > Spanning Tree > CIST Port" the check box beside "Spanning Tree Status".
 - On the page "Layer 2 > Multicast > GMRP" the check box beside "Setting".
16. Change to the page "System > Ports > Configuration"
17. Select the required port.
18. Select the port type "Switch-Port VLAN Access".
19. Click the "Set Values" button.
20. Change to the page "Layer 2 > Provider-Bridge > Tunnel-Ports".

21. Select the check box for the required port.
22. Click the "Set Values" button.
 On the page "Layer 2 > VLAN > Port Mapping", the setting is changed automatically to "Q" after you save.

6.5.7 Mirroring

6.5.7.1 General

On this page, you can enable/disable the "Mirroring" function and create mirroring sessions. You can also enable the "Mirroring" function via PROFINET IO. In this case, a configuration via the WBM page is not possible.

Note

You need to disable port mirroring if you want to connect an end device to the monitor port.

Mirroring General

General
Destinations
Port
VLAN
MAC Flow
IP Flow

Mirroring
 Monitor Barrier

Select	Session ID	Session Type	Status	Hardware Index
<input type="checkbox"/>	1	VLAN	active	0
<input type="checkbox"/>	2	Port Based	active	0
<input type="checkbox"/>	3	MAC ACL	inactive	0
<input type="checkbox"/>	4	IP ACL	inactive	0
<input type="checkbox"/>	5	Port Based	active	0

5 entries.

Create
Delete
Set Values
Refresh

Note the data rate

If the maximum data rate of the mirrored port is higher than that of the monitor port, data may be lost and the monitor port no longer reflects the data traffic at the mirrored port. Several ports can be mirrored to one monitor port at the same time.

Note

It cannot be guaranteed when mirroring the data traffic that all packets are mirrored. This depends primarily on the load on the mirrored ports and on the number of sessions. To achieve maximum precision, a limit of one session is recommended.

Description

The page contains the following boxes:

- **Mirroring**
Click this check box to enable or disable mirroring.
 - **Monitor Barrier**
Click this check box to enable or disable Monitor Barrier
-

Note**Effects of monitor barrier**

If you enable this option, management of the switch via the monitor port is no longer reachable. The following port-specific functions are changed:

- The DCP forwarding is turned off.
- LLDP is turned off.
- Unicast, multicast and broadcast blocking are turned on.
- With ports for which loop detection is enabled, the port status is changed to "Blocked".

The previous statuses of these functions are no longer restored after disabling monitor barrier again. They are reset to the default values and may need to be reconfigured.

You can reconfigure these functions manually even if monitor barrier is turned on. The data traffic on the monitor port is, however, also allowed again. If you do not require this, make sure that only the data traffic you want to monitor is forwarded to the interface.

If mirroring is disabled, the listed port-specific functions are reset to the default values. This reset takes place regardless of whether the functions were configured manually or automatically by enabling "monitor barrier".

The table for the basic settings contains the following boxes:

- **Select**
Select the row you want to delete.
- **Session ID**
The Session ID is assigned automatically when a new entry is created.

- **Session Type**
Select the required entry from the drop-down list:
 - -
None
 - Port Based
Port-based mirroring
 - VLAN
VLAN-based mirroring
 - MAC ACL
Mirroring of the MAC Access Control List
 - IP ACL
Mirroring of the IP Access Control List

Note

You can create up to four session of the type "VLAN", "MAC ACL" or "IP ACL" and up to five of the type "Port-based".

Note

If you change the "Session Type" of an existing session, all previous configurations of this session are lost.

- **Status**
Shows whether or not mirroring is enabled.
The status does not change to "enabled" until you configure settings for the mirroring source and destination in additional tabs and enable mirroring on this page.
In the case of ERTM, a mirroring session only becomes active after a connection has been established to the destination IP or the next hop gateway on the way to the destination.
- **Hardware Index**
If in a VLAN you select more than one source port for the port-based egress mirroring, unknown unicast and multicast frames as well as broadcast frames are forwarded only once to the destination port. With several sessions, the corresponding frames are only visible in one session. They are only mirrored on the destination port with the lowest hardware index.

Procedure

Creating a mirroring session

1. Activate mirroring.
2. Click the "Create" button to create a further entry in the table.
The session ID is assigned automatically. Depending on the session type selected, you can create one or more mirroring sessions.
3. Select a "Session Type".
4. Click the "Set Values" button.
5. Change to the following tabs to make further detailed settings for the relevant session ID.

Deleting a mirroring session

1. Click the check box in the first column to select the row.
2. Click the "Delete" button to delete the selected rows.

6.5.7.2 Targets

On this page, you configure the destination port to which the mirrored data is sent for each created session.

Destinations

General	Destinations	Port	VLAN	MAC Flow	IP Flow																								
<table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr style="background-color: #f2f2f2;"> <th>Session ID</th> <th>Dest. Port</th> <th>RSPAN VLAN ID</th> <th>ERTM Remote IP Address</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>P0.5</td> <td>VLAN1</td> <td></td> </tr> <tr> <td>2</td> <td>P0.3</td> <td>VLAN1</td> <td></td> </tr> <tr> <td>3</td> <td>P0.7</td> <td>VLAN1</td> <td></td> </tr> <tr> <td>4</td> <td>P0.10</td> <td>VLAN1</td> <td></td> </tr> <tr> <td>5</td> <td>-</td> <td>-</td> <td>140.80.57.2</td> </tr> </tbody> </table>						Session ID	Dest. Port	RSPAN VLAN ID	ERTM Remote IP Address	1	P0.5	VLAN1		2	P0.3	VLAN1		3	P0.7	VLAN1		4	P0.10	VLAN1		5	-	-	140.80.57.2
Session ID	Dest. Port	RSPAN VLAN ID	ERTM Remote IP Address																										
1	P0.5	VLAN1																											
2	P0.3	VLAN1																											
3	P0.7	VLAN1																											
4	P0.10	VLAN1																											
5	-	-	140.80.57.2																										
<input type="button" value="Set Values"/> <input type="button" value="Refresh"/>																													

Description

The table for the basic settings contains the following boxes:

- **Session ID**
Displays the session IDs you created on the "General" page.
- **Dest. Port**
Select the desired destination port from the drop-down list.
- **RSPAN VLAN-ID**
Select a VLAN for the RSPAN traffic from the drop-down list.
- **ERTM Remote IP Address** (Encapsulated Remote Traffic Mirroring)
Enter the IP address of a connected device on which the mirrored packets are to be received. Devices with an IP address, e.g. a PC or a hard disk, are suitable for this. The prerequisite is that the device is reachable via IP (Layer 3). The destination port is determined dynamically. Information on how to use the installed tool for recording and analyzing data traffic, e.g. Wireshark, can be obtained from the tool provider.

Procedure**Configuring a destination port for port-based mirroring**

1. Create a VLAN for the RSPAN data traffic on all devices involved.
2. Select a mirroring session on the "Mirroring > General" page and the entry "Port Based" for "Session Type".

6.5 The "Layer 2" menu

3. From the drop-down list, select the destination port to which the traffic is to be sent.
4. Click the "Set Values" button to save the selected settings.

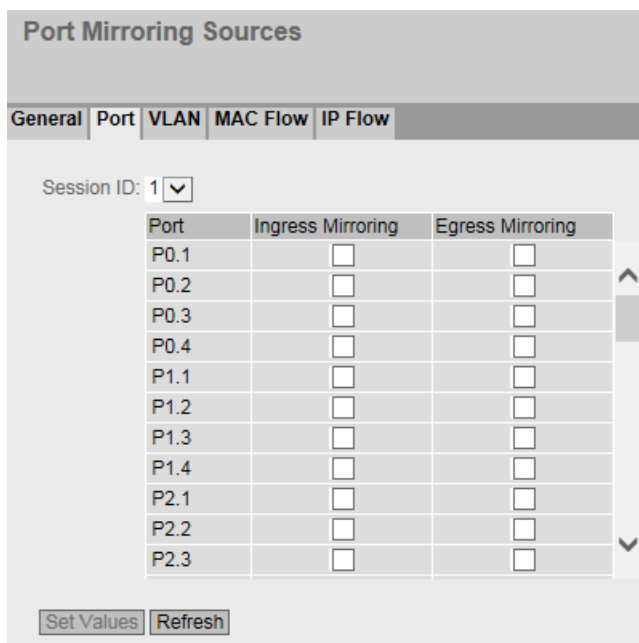
Configuring mirroring with the ERTM remote IP address

1. Select a mirroring session on the "Mirroring > General" page and the entry "Port Based" for "Session Type".
2. Enter the IP address of the connected PC.
3. Click the "Set Values" button to save the selected settings.

6.5.7.3 Port

Mirroring ports

You can only configure the settings on this page if you have already generated a session ID with the session type "Port-based" on the "General" tab.



Description of the displayed boxes

The page contains the following drop down list:

- **Session ID**
Select the session you want to monitor. Up to 5 parallel sessions are possible and their ports must not overlap.

The table has the following columns:

- **Port**
Shows the available ports. The port is made up of the module number and the port number, for example port 0.1 is module 0, port 1.
- **Ingress Mirroring**
Enable or disable listening in on incoming packets at the required port.
- **Egress Mirroring**
Enable or disable listening in on outgoing packets at the required port.

Note

Egress mirroring is always VLAN-tagged, regardless of whether the port is a tagged or untagged member of a VLAN.

Configuration procedure

1. In the "Session ID" drop-down list, select the session you created earlier on the "General" tab.
2. In the table, click the check box of the row after the port to be mirrored.
Select whether you want to monitor incoming or outgoing packets.
To monitor the entire data traffic of the port, select both check boxes.
3. Click the "Set Values" button.

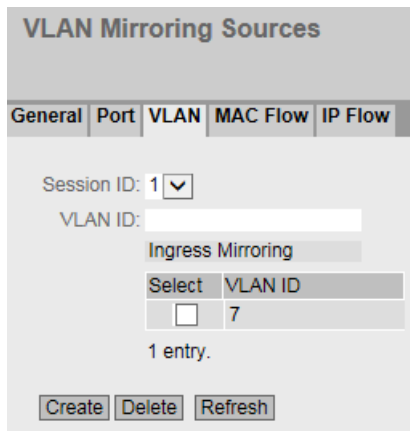
6.5.7.4 VLAN

VLAN sources of the port mirroring

You can only configure the settings on this page if you have already generated a session ID with the session type "VLAN" on the "General" tab.

On this page, you specify the VLAN whose incoming data traffic will be mirrored to the monitor port.

It can happen that data packets are visible on the monitor port that were not received in the defined VLAN. These data packets come from functions that are enabled on the device, e.g. SIMATIC time client. To avoid these data packets when VLAN mirroring, disable the relevant functions on the device before a recording.



Description of the displayed boxes

The page contains the following boxes:

- **Session ID**
Select the session you want to monitor. Only one session is possible.
- **VLAN ID**
Enter the VLAN ID in the "VLAN ID" input box.
Range of values: 1 ... 4094

The table "Ingress Mirroring " has the following columns:

- **Select**
Select the row you want to delete.
- **VLAN ID**
Shows the VLAN ID for which the incoming frames are mirrored. The VLAN ID (a number between 1 and 4094) can only be assigned once when creating a new data record and can then no longer be changed. To make a change, the entire data record must be deleted and created again.

6.5.7.5 MAC Flow

ACL filter for port mirroring

You can only configure the settings on this page if you have already generated a session ID with the session type "MAC ACL" on the "General" tab.

The ACL filter decides which data is available at the monitor port.

MAC Flow Mirroring Sources

General | Port | VLAN | MAC Flow | IP Flow

Session ID: 1

ACL Filter Number	Ingress Mirroring	Source MAC Address	Dest. MAC Address	Ingress Interfaces	Egress Interfaces
1	<input type="checkbox"/>	00-00-00-00-00-00	00-00-00-00-00-00	P0.1	P0.1

Description of the displayed boxes

- **Session ID**
Select the session you want to monitor. Only one session is possible.
- **ACL Filter Number**
Shows the number of the ACL filter.
- **Ingress Mirroring**
Shows whether incoming packets are mirrored.

Note

Rules

The selected rule only becomes active when you specify with which ACL rules the incoming packets will be filtered for at least one interface. You configure the settings in "Security > MAC ACL > Ingress Rules".

- **Source MAC**
Shows the MAC address of the sender.
- **Dest. MAC**
Shows the MAC address of the recipient.
- **Ingress Interfaces**
Shows all interfaces to which this rule applies. The ACL filter decides which incoming data streams are mirrored on the monitor port (destination port).
- **Egress Interfaces**
Shows all interfaces to which this rule applies.

6.5.7.6 IP Flow

ACL filter for port mirroring

You can only configure the settings on this page if you have already generated a session ID with the session type "IP ACL" on the "General" tab.

The ACL filter decides which data is available at the monitor port.

IP Flow Mirroring Sources							
General Port VLAN MAC Flow IP Flow							
Session ID: <input type="text" value="1"/>							
ACL Filter Number	Ingress Mirroring	Source IP Address	Source Subnet Mask	Dest. IP Address	Dest. Subnet Mask	Ingress Interfaces	Egress Interfaces
1	<input type="checkbox"/>	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	P0.1	P0.1
2	<input type="checkbox"/>	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	P0.1	
3	<input type="checkbox"/>	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0		
4	<input type="checkbox"/>	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0		
6	<input type="checkbox"/>	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0		

Description of the displayed boxes

- **Session ID**
Select the session you want to monitor. Only one session is possible.
- **ACL Filter Number**
Shows the number of the ACL filter.
- **Ingress Mirroring**
Shows whether incoming packets are mirrored.

Note

Rules

The selected rule only becomes active when you specify with which ACL rules the incoming packets will be filtered for at least one interface. You configure the settings in "Security > IP ACL > Ingress Rules".

- **Source IP**
Shows the IPv4 address of the destination device.
- **Source Subnet Mask**
Shows the subnet mask of the sender.
- **Dest. IP**
Shows the IPv4 address of the recipient.
- **Dest. Subnet Mask**
Shows the subnet mask of the recipient.
- **Ingress Interfaces**
Shows all interfaces to which this rule applies. The ACL filter decides which incoming data streams are mirrored on the monitor port (destination port).
- **Egress Interfaces**
Shows all interfaces to which this rule applies.

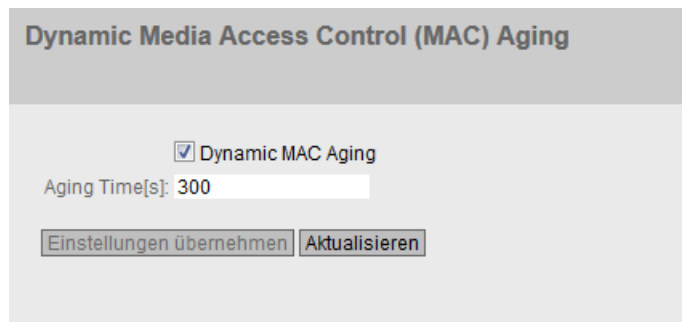
6.5.8 Dynamic MAC Aging

Protocol settings and switch functionality

The device automatically learns the source addresses of the connected nodes. This information is used to forward data frames to the nodes specifically involved. This reduces the network load for the other nodes.

If a device does not receive a frame whose source address matches a learnt address within a certain time, it deletes the learnt address. This mechanism is known as "Aging". Aging prevents frames being forwarded incorrectly, for example when an end device is connected to a different switch port.

If the check box is not enabled, a device does not delete learnt addresses automatically.



Dynamic Media Access Control (MAC) Aging

Dynamic MAC Aging

Aging Time[s]: 300

Description of the displayed boxes

The page contains the following boxes:

- **Dynamic MAC Aging**
Enable or disable the function for automatic aging of learned MAC addresses.
- **Aging Time[s]**
Enter the time in seconds. After this time, a learned address is deleted if the device does not receive any further frames from this sender address.
Range of values: 10 - 630 (seconds)
Factory setting: 300 seconds

Note

The actual Aging Time may be longer than the configured value. If the configured Aging Time is 30 seconds, it may take up to 60 seconds for a learnt address to be cleared.

Configuration procedure

1. Select the "Dynamic MAC Aging" check box.
2. Enter the time in seconds in the "Aging Time[s]" input box.
3. Click the "Set Values" button.

6.5.9 Ring Redundancy

6.5.9.1 Ring

Rules for ring redundancy

Factory settings

- The factory setting defines MSTP as the redundancy method.
- The factory setting defines ports P0.1 and P0.2 as ring ports.

Enabling redundancy

You can enable ring redundancy as follows:

- using the WBM
- using the CLI
- using a PROFINET configuration download

Configuration of ring redundancy

Ring Redundancy

Ring | Standby | MRP Interconnection

Ring ID:

Ring Redundancy

Ring Redundancy Mode:

Ring Ports:

Domain Name:

Observer

Ring ID	Domain Name	Ring Redundancy Mode	Ring Port 1	Ring Port 2
1	default-mrpdomain	-	P0.1	P0.2
2		-	P0.1	P0.2
3		-	P0.1	P0.2
4		-	P0.1	P0.2

- **Ring ID**
Select the ID of the ring you want to configure.
- **Ring Redundancy**
If you enable the "Ring Redundancy" check box, you turn ring redundancy on. The ring ports set on this page are used.

- **Ring Redundancy Mode**

Here, you set the mode of the ring redundancy.

Note

If you configure multiple redundant rings, you need to select the "MRP Manager" ring redundancy mode for each ring.

The following modes are available:

- **Automatic Redundancy Detection**
Select this setting to create an automatic configuration of the redundancy mode.
In "Automatic Redundancy Detection" mode, the device automatically detects whether there is a device with the "HRP Manager" role in the ring. If this is the case, the device adopts the role of "HRP Client".
If no HRP manager is found, all devices with the "Automatic Redundancy Detection" or "MRP Auto-Manager" setting negotiate among themselves to establish which device adopts the role of "MRP Manager". The device with the lowest MAC address will always become "MRP Manager". The other devices automatically set themselves to "MRP Client" mode.
- **MRP Auto-Manager**
In the "MRP Auto-Manager" mode, the devices negotiate among themselves to establish which device will adopt the role of "MRP Manager". The device with the lowest MAC address will always become "MRP Manager". The other devices automatically set themselves to "MRP Client" mode.
In contrast to the "Automatic Redundancy Detection" setting, the devices are not capable of detecting whether an HRP manager is in the ring.
- **MRP Client**
The device adopts the MRP Client role.
- **HRP Client**
The device adopts the HRP Client role.
- **HRP Manager**
The device adopts the HRP Manager role.
When you configure an HRP ring, one device must be set as HRP Manager. For all other devices, "HRP Client" or "Automatic Redundancy Detection" must be set.
- **MRP Manager**
The device adopts the role of MRP Manager. The device cannot take on the client role automatically. "MRP Client" must be set for all other devices.

- **Ring ports**

Here, you set the ports to be used as ring ports in ring redundancy. You need to configure the Agent VLAN ID in the value range 1 ... 4094.

The ring port you select in the left-hand drop-down menu is the "Isolated Port" in HRP.

With MRP when the link is established, it is decided which port will become the "Isolated Port".

Note

Forwarding RSPAN stream

If the device is to forward RSPAN streams, two requirements must be met:

- Input port and output port must belong to the same port group.
 - The "Learning" function must be disabled for the input port.
In WBM: System > Ports > Configuration > Unicast MAC Learning
In CLI: no unicast mac learning
-

H-Sync

H-Sync is a Layer 2 protocol with which process data is synchronized via PROFINET in systems with redundant control.

The two controllers are connected redundantly via an MRP ring. The controllers must be directly connected with one another on a path. Both controllers are configured as "MRP Auto-Manager", so one of the controllers becomes MRP manager. All other devices in the ring are MRP clients. The two controllers send H-Sync frames in both directions of the ring (Provider). H-Sync frames that they receive are not forwarded (Consumer). All other devices in the ring only forward the H-Sync frames between their ring ports in both directions (Forwarder). The H-Sync frames are filtered on all other ports.

H-Sync is a transparent protocol for the IE switches.

You only configure H-Sync via STEP 7 Basic or Professional. However, note that settings deviating from the following rules can result in complications in configuration:

- Redundancy mode: MRP Client
- Ring ports:
 - Use the ring ports preset in the factory.
 - Use Port 1 and Port 2.

- **Domain Name**

Select a domain name from the drop-down list. Each name can only be assigned to one ring.

Note

If you configure multiple redundant rings, you cannot use the "default-mrpdomain" domain name for any of the rings.

- **Observer**

Enable or disable the observer. The "Observer" function is only available in HRP rings.

The ring port selected in the left-hand drop-down menu is connected to the "Isolated Port" of an HRP manager.

The observer monitors malfunctions of the redundancy manager or incorrect configurations of an HRP ring.

If the observer is enabled, it can interrupt the connected ring if errors are detected. To do this, the observer switches a ring port to the "blocking" status. When the error is resolved, the observer enables the port again.

- **Restart Observer**
If numerous errors occur in quick succession, the observer no longer enables its port automatically. The ring port remains permanently in the "blocking" status. This is signaled by the error LED and a message text.
After the errors have been eliminated, you can enable the port again using the "Restart Observer" button.
- **Restore Default**
This button is only functional if multiple redundant rings are active. Click this button to reset the ring redundancy configuration to the factory settings.

The table has the following columns:

- **Ring ID**
The ID of the ring.
- **Domain Name**
The name of the redundancy domain.
- **Ring Redundancy Mode**
The redundancy mode that is used in this ring. If "-" is displayed, ring redundancy is not enabled.
- **Ring Port 1**
The first ring port of the ring.
- **Ring Port 2**
The second ring port of the ring.

Restoring factory settings

If you have restored the factory defaults, ring redundancy is disabled and the default ports are used as the ring ports. This can lead to circulating frames and failure of the data traffic if other settings were used in a previous configuration.

Changing over the status of the ring ports with the redundancy manager

If you configure a redundancy manager, set the status of the ring ports. With HRP the first ring port changes to the "blocking" status and the second ring port to the "forwarding" status. As long as ring redundancy is enabled, you cannot change the status of these ring ports.

Note

Make sure that you first open the ring so that there are no circulating frames.

Changing ring ports

You can change the ring ports without needing to open the ring.

To change the ring ports, follow the steps below:

1. Change to the page "Layer 2 > Spanning Tree > CIST Port".
2. Disable the ports in the spanning tree you want to configure as ring ports.

6.5 The "Layer 2" menu

3. Change to the page "Layer 2 > Ring Redundancy > Ring".
4. Select the new ring ports.
5. Change the cable connections.
6. Change to the page "Layer 2 > Spanning Tree > CIST Port".
7. Enable the ports in the spanning tree that are no longer ring ports.

6.5.9.2 Standby

Redundant linking of rings

Standby redundancy allows the redundant linking of HRP rings.

To establish a standby connection, configure two neighboring devices within a ring as standby master or standby slave. The standby master and the standby slave must be connected via parallel cables to two devices in another ring.

In problem-free operation, messages are exchanged between the two rings via the master. If the master's line is disturbed, the slave takes over the forwarding of messages between the two rings.

Enable standby redundancy for both standby partners and select the ports via which the device is connected to the rings you want to link to.

For the "Standby Connection Name", a name unique within the ring must be assigned for both partners. This identifies the two modules that belong together as standby partners.

Note

To be able to use the function, HRP must be activated.

Note

When the connection of standby master and standby slave in a line topology is restored after an interruption, increased data traffic may occur temporarily.

Standby Redundancy

Ring
Standby
MRP Interconnection

Standby

Standby Connection Name:

Force device to Standby Master
 Wait for Standby Partner

Partner detect timeout[ms]:

Port	Setting
P0.1	<input type="checkbox"/>
P0.2	<input type="checkbox"/>
P0.3	<input type="checkbox"/>

Description of the displayed boxes

- **Standby**
Enable or disable the standby function.

Note

If two devices are linked by standby, the "Standby" function must be enabled on both devices.

- **Standby Connection Name**
This name defines the master/slave device pair. Both devices must be located in the same ring. Here, enter the name for the standby connection. This must be identical to the name entered on the standby partner. You can select any name to suit your purposes, however, you can only use the name for one pair of devices in the entire network.

- **Force device to Standby Master**

If you select this check box, the device is configured as a standby master regardless of its MAC address.

- If this check box is not selected for either of the devices for which the standby master is enabled, then assuming that no error has occurred, the device with the higher MAC address adopts the role of standby master.
- If the option is selected for both devices or if the "Force device to Standby Master" property is supported by only one device, the standby master is also selected based on the MAC address.

This type of assignment is important in particular when a device is replaced. Depending on the MAC addresses, the previous device with the slave function can take over the role of the standby master.

Note

If the option "Force device to Standby Master" is enabled on both devices of a standby coupling, this can lead to circulating frames and therefore to failure of the data traffic. Enable the "Force device to Standby Master" option only on one device of a standby coupling.

- **Wait for Standby Partner**

- Enabled
A standby connection is enabled only after the standby master and the standby slave as well as their standby partners have established a connection. This ensures that the redundant connection is really available before communication via a standby connection is enabled.
- Disabled
A standby connection is enabled even if the standby master has not yet established a connection to the standby slave.
This can lead to circulating frames and failure of the data traffic if another standby connection has already been enabled. Multiple standby connections can, for example, result due to configuration errors if different standby connection names were assigned to the standby master and standby slave.

- **Partner detect timeout [ms]**

The input box is only shown if the "Wait for Standby Partner" check box is cleared. In this case, you can define how long the device waits before establishing a standby connection. After this period of time, a standby connection is enabled even if the standby master has not yet established a connection to the standby slave.

- **Port**

Select the port to be standby port. The link to the other ring is via the standby port. The standby port is involved in the redirection of data traffic. In there are no problems, only the standby port of the master is enabled and handles the data traffic into the connected HRP ring or HRP bus.

If the master or the Ethernet connection of the standby port of the master fails, the standby port of the master will be disabled and the standby port of the slave enabled. As a result, a functioning Ethernet connection to the connected network segment (HRP ring or HRP linear bus) is restored.

6.5.9.3 MRP Interconnection

Redundant linking of rings

On this page, you create, delete and configure MRP Interconnection connections.

MRP Interconnection

Ring Standby **MRP Interconnection**

MRP Interconnection

Select	Interconnection Domain ID	Interconnection Domain Name	Interconnection Port	Wait (Manager)	Role/Position	Status
<input type="checkbox"/>	1	MrpIntCon1	P0.2	<input type="checkbox"/>	Primary Client	<input checked="" type="checkbox"/>

1 entry.

Description

The page contains the following boxes:

- **MRP Interconnection**
Select this check box to activate MRP Interconnection for the device. You can only enable MRP Interconnection when the following requirements are met:
 - Ring redundancy is enabled.
 - "MRP Auto-Manager" or "MRP Client" is used as ring redundancy mode.
 - There is an activated MRP Interconnection connection.

Note

Configure the ring redundancy mode "MRP Auto-Manager" for two devices in each ring so that the MRP ring can be reconfigured immediately even when one device fails.

The table has the following columns:

- **Select**
Select the row you want to delete.
- **Interconnection Domain ID**
Specify the ID of the MRP Interconnection connection. When specifying the ID, observe the following rules:
 - The Interconnection ID cannot be 0.
 - You need to configure the same Interconnection ID for all four devices used for linking the rings.

- **Interconnection Domain Name**

Enter any name for the MRP Interconnection connection. You can also define different names for the four devices used for linking the rings. The letters 'A' to 'Z' and 'a' to 'z', the numbers '0' to '9' and the '-' symbol are valid characters for this name. A hyphen cannot be used for the first or last character of the name. The interconnection name must contain at least one character and no more than 240 characters.
- **Interconnection Port**

From this drop-down list, select the port that is used for the MRP Interconnection connection. Be aware of the following restrictions:

 - The port cannot be disabled or blocked. The "Unicast Blocking" function cannot be enabled for the port.
 - The port cannot be used for a link aggregation.
 - The port cannot be a monitor port of the "Mirroring" function.
 - The port cannot be a Spanning Tree port.
 - The port cannot be a ring port.
 - The port cannot be a router port.
 - The port cannot be an 802.1X Authenticator Port.
 - The port cannot be an 802.1X Supplicant Port.
- **Wait (Manager)**

For devices with the "Client" role, you cannot select the check boxes in this column. When you select this check box for the device with the "Manager" role, the MRP Interconnection Manager waits with data transmission until the primary client for MRP Interconnection is ready. When the check box is not selected, the MRP Interconnection Manager starts data transmission after a waiting time of 200 milliseconds, regardless of the operating state of the primary clients.
- **Role/Position**

There are two roles: "Manager" and "Client". For clients, you also specify the position ("Primary" or "Secondary"). This drop-down list therefore offers the following selection options:

 - Manager
 - Primary Client
 - Secondary Client
- **Status**

Check this check box to enable the MRP Interconnection connection. Observe the following rules:

 - If no MRP Interconnection connection is activated, you cannot enable the MRP Interconnection for the device.
 - A maximum of two MRP Interconnection connections can be active at the same time.

Configuration procedure

Note

You can find a detailed step-by-step description of the MRP Interconnection configuration in the section Technical basics → Redundancy mechanism → MRP Interconnection.

Requirements for the configuration

1. Plug the cables according to the planned topology, except for the following connections:
 - One connection line in each ring, which means the rings must not be closed yet.
 - The two devices intended for the secondary link (MIM and Secondary Coupled MIC) must not be connected yet.
2. Assign an IP address for each device to use the WBM.

Requirements for the configuration when Spanning Tree is required for the network topology

1. Configure the protocol compatibility "RSTP" for Spanning Tree.
2. Disable Spanning Tree for the ring ports and the MRP Interconnection ports.

Configuration of ring redundancy

Configure the following parameters for each device for ring redundancy:

1. Specify the ring ports.
2. Enable MRP.
3. Assign an MRP role to the device. Configure the ring redundancy mode "MRP Auto-Manager" for two devices in each ring so that the MRP ring can be reconfigured immediately even when one device fails.

Once you have configured all devices in both rings for MRP, close the two MRP rings by plugging the cables between the devices that have not been connected yet. Do not plug the cable between the MIM and the Secondary Coupled MIC yet.

Configuration of MRP Interconnection

When configuring these devices, you must observe a particular order so that the devices can be reached by the configuration PC at any time. First configure the devices of the MRP Interconnection connection in the MRP ring to which the configuration PC is not connected. Start with the device for which no cable has been plugged yet for the MRP Interconnection connection. You must execute the following steps for each device:

1. Click the "Create" button to create a new row in the table with the MRP Interconnection connections.
2. Configure the parameters for the MRP Interconnection connection according to the description above.
3. Select the "MRP Interconnection" check box to enable the MRP Interconnection.

6.5 The "Layer 2" menu

Once you have configured all devices in both rings for MRP Interconnection, plug the cable for the secondary link between the MIM and Secondary Coupled MIC devices. Afterwards, the MRP Interconnection connection is operational.

Note

Reconfiguration

Open the ring before you reconfigure the topology to prevent circulating frames.

6.5.10 Spanning tree

6.5.10.1 General

General settings of Spanning Tree

This is the basic page for spanning tree. Select the compatibility mode from the drop-down list.

On the configuration pages of these functions, you can make further settings.

Depending on the compatibility mode, you can configure the corresponding function on the relevant configuration page.

Spanning Tree Protocol (STP) General

General | CIST General | CIST Port | **MST General** | MST Port | Enhanced Passive Listening Compatibility

Spanning Tree Protocol Compatibility: RSTP ▾

RSTP+

RSTP+ MRP Interconnection Domain ID: 5

Set Values Refresh

Description of the displayed boxes

The page contains the following boxes:

- **Spanning Tree**
Enable or disable Spanning Tree.
- **Protocol Compatibility**
Select the protocol compatibility.
Ports with an activated ring protocol cannot participate in RSTP. Therefore, on the "Layer 2 > Ring Redundancy (Page 318)" pages, disable all ring protocols and MRP Interconnection connections with the "Status" check box.
The following settings are available:
 - STP
 - RSTP
Rapid Spanning Tree Protocol
With RSTP, Spanning Tree and an MRP ring can be active on the same device, but not on the same port. Only with RSTP+ can Spanning Tree also be active on an MRP ring port.
 - MSTP
Multiple Spanning Tree Protocol
- **RSTP+**
enables the linking of a network segment in which Spanning Tree is activated with an MRP ring.
Make sure that the following requirements have been met before selecting this check box:
 - MRP must be enabled as the redundancy method.
 - If ring redundancy is activated, you need to disable the ring ports for Spanning Tree.When you activate RSTP+, the ring ports become both part of the MRP ring and part of the Spanning Tree network segment. Without RSTP+, the ring ports do not belong to the Spanning Tree network segment.
- **RSTP+ MRP Interconnection Domain ID**
Configure the MRP Interconnection domain ID for RSTP+ here. This value must not match the MRP Interconnection domain ID configured for the active MRP Interconnection connection.

Note

Multiring manager prevents the configuration of Spanning Tree

If more than one ring is configured on a device, neither RSTP or RSTP+ can be configured in parallel. This also applies if Spanning Tree has been disabled for the ring ports.

Configuration procedure

1. Select the "Spanning Tree" check box.
2. From the "Protocol Compatibility" drop-down list, select the type of compatibility.
3. Click the "Set Values" button.

6.5.10.2 CIST General

MSTP-CIST configuration

The page consists of the following parts.

- The left-hand side of the page shows the configuration of the device.
- The central part shows the configuration of the root bridge that can be derived from the spanning tree frames received by an device.
- The right-hand side shows the configuration of the regional root bridge that can be derived from the MSTP frames. The displayed data is only visible if you have enabled "Spanning Tree" on the "General" page and if "MSTP" is set for "Protocol Compatibility". This also applies to the "Bridge Max Hop Count" parameter. If the device is a root bridge, the information on the left and right matches.

Common Internal Spanning Tree (CIST) General

General	CIST General	CIST Port	MST General	MST Port	Enhanced Passive Listening Compatibility
Bridge Priority: 32768	Root Priority: 0	Regional Root Priority: 0	Bridge Address: 00-00-00-00-00-00	Root Address: 00-00-00-00-00-00	Regional Root Address: 00-00-00-00-00-00
Root Port: -	Root Cost: 0	Regional Root Cost: 0	Topology Changes: 0	Last Topology Change: -	Region Name: 00:1b:1b:40:91:23
Bridge Hello Time[s]: 2	Root Hello Time[s]: 2	Region Version: 0	Bridge Forward Delay[s]: 15	Root Forward Delay[s]: 15	
Bridge Max Age[s]: 20	Root Max Age[s]: 20		Bridge Max Hop Count: 20		
<input type="button" value="Reset Counters"/>					
<input type="button" value="Set Values"/> <input type="button" value="Refresh"/>					

Description of the displayed boxes

The page contains the following boxes:

- **Bridge Priority / Root Priority**
The Bridge Priority decides which device becomes the Root Bridge. The Bridge with the highest priority becomes the Root Bridge. The lower the value, the higher the priority. If several devices in a network have the same priority, the device whose MAC address has the lowest numeric value will become the root bridge. The two parameters, bridge priority and MAC address, together form the bridge identifier. Since the root bridge manages all path changes, it should be located as centrally as possible due to the delay of the frames. The value for the bridge priority is a whole multiple of 4096. Range of values: 0 - 61440
- **Bridge Address / Root Address**
The bridge address shows the MAC address of the device and the root address shows the MAC address of the root bridge.

- **Root port**
Shows the port via which the switch communicates with the root bridge.
- **Root Cost**
The path costs from this device to the root bridge.
- **Topology Changes / Last Topology Change**
The entry for the device shows the number of reconfiguration actions due to the spanning tree mechanism since the last startup. For the root bridge, the time since the last reconfiguration is displayed as follows:
 - Seconds: Unit "sec" after the number
 - Minutes: Unit min after the number
 - Hours: Unit hr after the number
- **Bridge hello time [s] / Root hello time [s]**
Each bridge sends configuration frames (BPDUs) regularly. The interval between two configuration frames is the "Hello Time".
Factory setting: 2 seconds

Note

The setting of the "Bridge Hello Time" is only possible with the Protocol compatibility RSTP. If the "Protocol compatibility MSTP is set, the "Hello Time" parameter on the page "Layer 2 > Spanning Tree > CIST Port" page is used.

- **Bridge Forward Delay[s] / Root Forward Delay[s]**
New configuration data is not used immediately by a bridge but only after the period specified in the Forward Delay parameter. This ensures that operation is only started with the new topology after all the bridges have the required information.
Factory setting: 15 seconds
- **Bridge Max Age[s] / Root Max Age[s]**
If the BPDU is older than the specified "Max Age" it is discarded.
Factory setting: 20 seconds
- **Regional root priority**
For a description, see Bridge Priority / Root Priority
- **Regional Root Address**
The MAC address of the device.
- **Regional Root Cost**
The path costs from this device to the root bridge.
- **Bridge Max Hop Count**
This parameter specifies how many MSTP nodes a BPDU may pass through. If an MSTP BPDU is received and has a hop count that exceeds the value configured here, it is discarded. The default for this parameter is 20.

6.5 The "Layer 2" menu

- Region Name**
 Enter the name of the MSTP region to which this device belongs. As default, the MAC address of the device is entered here. This value must be the same on all devices that belong to the same MSTP region.
- Region Version**
 Enter the version number of the MSTP region in which the device is located. This value must be the same on all devices that belong to the same MSTP region.

Configuration procedure

- Enter the data required for the configuration in the input boxes.
- Click the "Set Values" button.

6.5.10.3 CIST Port

MSTP-CIST port configuration

When the page is called, the table displays the current status of the configuration of the port parameters.

To configure them, click the relevant cells in the port table.

Common Internal Spanning Tree (CIST) Port

General | CIST General | **CIST Port** | MST General | MST Port | Enhanced Passive Listening Compatibility

Spanning Tree Status Copy to Table
 All ports No Change Copy to Table

Port	Spanning Tree Status	Priority	Cost Calc.	Path Cost	State	Fwd. Trans.
P0.1	<input checked="" type="checkbox"/>	128	0	20000	Disabled	0
P0.2	<input type="checkbox"/>	128	0	20000	Disabled	0
P0.3	<input type="checkbox"/>	128	0	20000	Disabled	0
P0.4	<input checked="" type="checkbox"/>	128	0	20000	Disabled	0

Set Values Refresh

(Continuation of table)

Edge-Typ	Edge	P.t.P.-Typ	P.t.P.	Hello Time	Eingeschränkte Rolle	Eingeschränktes TCN	Limitiertes TCN	BPDU Guard
Auto	<input type="checkbox"/>	-	<input type="checkbox"/>	2	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Auto	<input type="checkbox"/>	-	<input type="checkbox"/>	2	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Auto	<input type="checkbox"/>	-	<input type="checkbox"/>	2	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Auto	<input type="checkbox"/>	-	<input type="checkbox"/>	2	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Description

Table 1 has the following columns:

- **1st column**
Shows that the settings are valid for all ports of table 2.
- **Spanning Tree Status**
Select the setting from the drop-down list. You have the following setting options:
 - Enabled
Port is integrated in the spanning tree.
 - Disabled
Port is not integrated in the spanning tree.
 - No Change
Table 2 remains unchanged.
- **Copy to Table**
If you click the button, the setting is adopted for all ports of table 2.

Table 2 has the following columns:

- **Port**
Shows the available ports. The port is made up of the module number and the port number, for example port 0.1 is module 0, port 1.
- **Spanning Tree Status**
Specify whether or not the port is integrated in the spanning tree.

Note

If you disable the "Spanning Tree Status" option for a port, this may cause the formation of loops. The topology must be kept in mind.

- **Priority**
Enter the priority of the port. The priority is only evaluated when the path costs are the same. The value must be divisible by 16. If the value that cannot be divided by 16, the value is automatically adapted.
Range of values: 0 - 240.
The default is 128.
- **Cost Calc.**
Enter the path cost calculation. If you enter the value "0" here, the automatically calculated value is displayed in the "Path costs" box.

- **Path Cost**

This parameter is used to calculate the path that will be selected. The path with the lowest value is selected as the path. If several ports of a device have the same value for the path costs, the port with the lowest port number is selected.

If the value in the "Cost Calc." box is "0", the automatically calculated value is shown.

Otherwise, the value of the "Cost Calc." box is displayed.

The calculation of the path costs is largely based on the transmission speed. The higher the achievable transmission speed is, the lower the value of the path costs.

Typical values for path costs with rapid spanning tree:

- 10,000 Mbps = 2,000
- 1000 Mbps = 20,000
- 100 Mbps = 200,000
- 10 Mbps = 2,000,000

The values can, however, also be set individually.

- **Status**

Displays the current status of the port. The values are only displayed and cannot be configured. The "Status" parameter depends on the configured protocol. The following values are possible:

- Disabled
The port only receives and is not involved in STP, MSTP and RSTP.
- Discarding
In the "Discarding" mode, BPDU frames are received. Other incoming or outgoing frames are discarded.
- Listening

In this status, BPDUs are both received and sent. The port is involved in the spanning tree algorithm.
- Learning
Stage prior to the "Forwarding" status, the port is actively learning the topology (in other words, the node addresses).
- Forwarding
Following the reconfiguration time, the port is active in the network; it receives and forwards data frames.

- **Fwd. Trans**

Specifies the number of changes from the "Discarding" status to the "Forwarding" status.

- **Edge Type**

Specify the type of "edge port". You have the following options:

 - "-"
Edge port is disabled. The port is treated as a "no Edge Port".
 - Admin
Select this option when there is always an end device on this port. Otherwise a reconfiguration of the network will be triggered each time a connection is changed.
 - Auto
Select this option if you want a connected end device to be detected automatically at this port. When the connection is established the first time, the port is treated as a "no Edge Port".
 - Admin/Auto
Select these options if you operate a combination of both on this port. When the connection is established the first time, the port is treated as an "Edge Port".
- **Edge**

Shows the status of the port.

 - Enabled

An end device is connected to this port.
 - Disabled
There is a Spanning Tree or Rapid Spanning Tree device at this port.

With an end device, a switch can change over the port faster without taking into account spanning tree frames. If a spanning tree frame is received despite this setting, the port automatically changes to the "Disabled" setting.
- **P.t.P. Type**

Select the required option from the drop-down list. The selection depends on the port that is set.

 - "-"
Point to point is calculated automatically. If the port is set to half duplex, a point-to-point link is not assumed.
 - P.t.P.

Even with half duplex, a point-to-point link is assumed.
 - Shared Media
Even with a full duplex connection, a point-to-point link is not assumed.

Note

Point-to-point connection means a direct connection between two devices. A shared media connection is, for example, a connection to a hub.

- **P.t.P.**

A selected check box indicates that the operating state of the port corresponds to the configuration in the "P.t.P. Type" column.

- **Hello Time**
Enter the interval after which the bridge sends configuration frames (BPDUs). As default, 2 seconds is set.
Range of values: 1-2 seconds

Note

The port-specific setting of the Hello time is only possible with Protocol compatibility MSTP. If the Protocol Compatibility RSTP is set, the "Bridge Hello Time" parameter on the "Layer 2 > Spanning Tree > CIST General" page is used.

- **Restr. Role**
If this check box is selected, the corresponding port is not selected as root port, regardless of the priority value. If the check box is selected, the port with the lowest priority also does not become the root port. Only activate this option if you wish to restrict the impact of bridges outside of the administered range to the Spanning Tree topology.
- **Restr. TCN**
If this check box is selected, the corresponding port does not forward either received or detected topology changes (Topology Change Notifications) to other ports. Only activate this option if you wish to restrict the impact of bridges outside of the administered range to the Spanning Tree topology.
- **Limited TCN**
If this check box is selected, the corresponding port accepts received and detected topology changes, but does not forward topology changes to other ports. You can only select the check box in this column if the following requirements are met:
 - RSTP+ must be enabled.
 - The "Restr. TCN" check box must be cleared for this port.If the specified requirements are not met, the check box in this column is shown grayed out.
- **BPDU Guard**
Enables BPDU protection at the selected port. If Spanning Tree BPDU packets are received at this port, the port is disabled. The event is logged and the administrator is notified.

Configuration procedure

1. In the input cells of the table row, enter the values of the port you are configuring.
2. From the drop-down lists of the cells of the table row, select the values of the port you are configuring.
3. Click the "Set Values" button.

6.5.10.4 MST General

Multiple Spanning Tree configuration

With MSTP, in addition to RSTP, several VLANs can be managed in a LAN with separate RSTP trees.

Multiple Spanning Tree (MST) General

General | CIST General | CIST Port | **MST General** | MST Port | Enhanced Passive Listening Compatibility

MSTP Instance ID:

Select	MSTP Instance ID	Root Address	Root Priority	Bridge Priority	VLAN ID
<input type="checkbox"/>	1	00-00-00-00-00-00	0	32768	

1 entry.

Description

The page contains the following box:

- **MSTP Instance ID**
Enter the number of the MSTP instance.
Permitted values: 1 - 64

The table has the following columns:

- **Select**
Select the row you want to delete.
- **MSTP instance ID**
Shows the number of the MSTP instance.
- **Root Address**
Shows the MAC address of the root bridge.
- **Root Priority**
Shows the priority of the root bridge.
- **Bridge Priority**
Enter the bridge priority in this box. The value for the bridge priority is a whole multiple of 4096 with a range of values from 0 to 61440.
- **VLAN ID**
Enter the VLAN ID. Here, you can also specify ranges with Start ID, "-", End ID. Several ranges or IDs are separated by ",".
Permitted values: 1- 4094

Procedure

Creating a new entry

1. Enter the number of the MSTP instance in the "MSTP Instance ID" box.
2. Click the "Create" button.
3. Enter the ID of the VLAN in the "VLAN ID" box.
4. Enter the priority of the bridge in the "Bridge Priority" box.
5. Click the "Set Values" button.

Deleting entries

1. Use the check box at the beginning of the relevant row to select the entries to be deleted.
2. Click the "Delete" button to delete the selected entries from memory. The entries are deleted from the memory of the device and the display on this page is updated.

6.5.10.5 MST Port

Configuration of the Multiple Spanning Tree port parameters

On this page, you set the parameters for the ports of the configured multiple spanning tree instances.

Multiple Spanning Tree (MST) Port

General | CIST General | CIST Port | **MST General** | MST Port | Enhanced Passive Listening Compatibility

MSTP Instance ID: 1

		MSTP Status	Copy to Table	
All ports	No Change	<input type="checkbox"/>	<input type="button" value="Copy to Table"/>	

Port	MSTP Instance ID	MSTP Status	Priority	Cost Calc.	Path Cost	State	Fwd. Trans.
P0.1	1	<input checked="" type="checkbox"/>	128	0	200000	Forwarding	1
P0.2	1	<input checked="" type="checkbox"/>	128	0	200000	Discarding	0
P0.3	1	<input checked="" type="checkbox"/>	128	0	200000	Discarding	0
P0.4	1	<input checked="" type="checkbox"/>	128	0	200000	Discarding	0

Description of the displayed boxes

The page contains the following box:

- **MSTP Instance ID**
In the drop-down list, select the ID of the MSTP instance.

Table 1 has the following columns:

- **1st column**
Shows that the settings are valid for all ports.
- **MSTP Status**
Select the setting from the drop-down list. You have the following setting options:
 - Enabled
 - Disabled
 - No Change: Table 2 remains unchanged.
- **Copy to Table**
If you click the button, the setting is adopted for all ports of table 2.

Table 2 has the following columns:

- **Port**
Shows all available ports and link aggregations.
- **MSTP Instance ID**
ID of the MSTP instance.
- **MSTP Status**
Select the check boxes of the ports that belong to this instance.
- **Priority**
Enter the priority of the port. The priority is only evaluated when the path costs are the same. The value must be divisible by 16. If the value that cannot be divided by 16, the value is automatically adapted.
Range of values: 0 - 240.
Factory setting: 128
- **Cost Calc.**
Enter the path cost calculation in the input box. If you enter the value "0" here, the automatically calculated value is displayed in the next box "Path Costs".
- **Path cost**
The path costs from this port to the root bridge. The path with the lowest value is selected as the path. If several ports of a device have the same value, the port with the lowest port number will be selected.
If the "Cost Calc." is "0", the automatically calculated value is shown. Otherwise, the value of the "Cost Calc." box is displayed.
The calculation of the path costs is largely based on the transmission speed. The higher the achievable transmission rate, the lower the value for the path costs will be.
Typical values for rapid spanning tree are as follows:
 - 10,000 Mbps = 2,000
 - 1000 Mbps = 20,000
 - 100 Mbps = 200,000
 - 10 Mbps = 2,000,000The values can, however, also be set individually.

6.5 The "Layer 2" menu

- **Status**
Displays the current status of the port. The values are only displayed and cannot be configured. The following is possible for status:
 - **Discarding**
The port exchanges MSTP information but is not involved in the data traffic.
 - **Blocked**
In the blocking mode, BPDU frames are received.
 - **Forwarding**
The port receives and sends data frames.
- **Fwd. Trans.**
Specifies the number of status changes Discarding - Forwarding or Forwarding - Discarding for a port.

Steps in configuration

1. In the input cells of the table row, enter the values of the port you are configuring.
2. From the drop-down lists of the cells of the table row, select the values of the port you are configuring.
3. Click the "Set Values" button.

6.5.10.6 Enhanced Passive Listening Compatibility

Spanning Tree and ring redundancy

If you enable Enhanced Passive Listening Compatibility, topology change notifications will be sent via RSTP edge ports. In conjunction with the "Edge Type" function (see "Layer 2 > Spanning Tree > CIST Port"), this parameter is necessary to link Spanning Tree networks with HRP rings. Otherwise, no TCN frames are sent via edge ports; however, this is necessary for the Passive Listening function on ring nodes.

Enabling the function

On this page, you can enable the "Enhanced Passive Listening Compatibility" function.

Enhanced Passive Listening Compatibility

General | CIST General | CIST Port | MST General | MST Port | **Enhanced Passive Listening Compatibility**

Enhanced Passive Listening Compatibility

Setting: No Change (v) Copy to Table (↕)

Port	Setting
P0.1	<input type="checkbox"/>
P0.2	<input type="checkbox"/>
P0.3	<input type="checkbox"/>
P0.4	<input type="checkbox"/>

Set Values Refresh

Description of the displayed boxes

The page contains the following boxes:

- **Enhanced Passive Listening Compatibility**
Enable or disable this function for the entire device.
- **Setting**
 - Enabled
Enables the function for all ports of the device.
 - Disabled
Disables the function for all ports of the device.
 - No Change
No Change
- **Copy to Table**
Writes the setting made in "Setting" to the following table

Port-specific table:

If the function is enabled for the entire device, enable or disable this function on individual ports.

- **Port**
Displays the port of the device.
- **Setting**
Enable or disable the function for this port.

Configuration procedure

Enable the function for the entire device

1. Enable or disable "Enhanced Passive Listening Compatibility"
2. Click the "Set Values" button.

For all ports of the device:

1. From the drop-down list, select whether the function should be enabled or disabled or adopted unchanged.
2. Click the "Copy to Table" button.
3. Click the "Set Values" button.

For individual ports of the device:

1. Click the check box after the required port in the port table to enable or disable the function.
2. Click the "Set Values" button.

6.5.11 Loop Detection

With the "Loop Detection" function, you specify the ports for which loop detection will be activated. The ports involved send special test frames - the loop detection frames. If these frames are sent back to the device, there is a loop.

A "local loop" involving this device means that the frames are received again at a different port of the same device. If the sent frames are received again at the same port, there is a loop involving other network components "Remote Loop".

Note

A loop is an error in the network structure that needs to be eliminated. The loop detection can help to find the errors more quickly but does not eliminate them. The loop detection is not suitable for increasing network availability by deliberately including loops.

Note

Note that loop detection is not possible on the following ports:

- Ring ports
 - Standby ports
 - MRP Interconnection ports
-

Loop Detection

Loop Detection
 VLAN Loop Detection

	Interval[ms]	Threshold	Timeout[s]	Remote Reaction	Local Reaction	Copy to Table
All ports	No Change	No Change	No Change	No Change	▼ No Change	▼ Copy to Table

Port	Setting	Interval[ms]	Threshold	Timeout[s]	Remote Reaction	Local Reaction	Status	Source Port	Source VLAN	Reset
P0.1	forwarder ▼	1000	2	0	disable	▼ disable	▼ active	-	-	Reset
P0.2	forwarder ▼	1000	2	0	disable	▼ disable	▼ active	-	-	Reset
P0.3	forwarder ▼	1000	2	0	disable	▼ disable	▼ active	-	-	Reset
P0.4	forwarder ▼	1000	2	0	disable	▼ disable	▼ active	-	-	Reset

Description of the displayed boxes

The page contains the following boxes:

- **Loop Detection**
Enable or disable the loop detection.
If the option is enabled, the device sends untagged LLC frames.
- **VLAN Loop Detection**
Enable or disable the VLAN loop detection.
If the option is enabled, the device uses the VLAN information set at the corresponding port to send LLC frames.

Table 1 contains the following columns:

- **1st column**
Shows that the settings are valid for all ports of table 2.
- **Interval [ms] / Threshold value / Timeout [s] / Remote reaction / Local reaction**
Make the required settings.
- **Copy to Table**
If you click the button, the setting is adopted for all ports of table 2.

Table 2 contains the following columns:

- **Port**
Shows the available ports.
- **Setting**
Specify how the port handles loop detection frames. Select one of the following options from the drop-down list:

Note

Test frames create additional network load. We recommend that you only configure individual switches, for example at branch points of the ring, as "Sender" and the others as "Forwarder".

Spanning Tree ports cannot be configured as "Sender".

- Sender
Loop detection frames are sent out and forwarded.
- Forwarder
Loop detection frames from other devices are forwarded.
- blocked
The forwarding of loop detection frames is blocked.
- **Interval[ms]**
Specifies the send interval for loop detection frames in milliseconds.
- **Threshold**
By entering a number, specify the number of received loop detection frames as of which a loop is assumed.
- **Timeout[s]**
Specify the number of seconds after which the device automatically changes to the status in which it was before the loop. If the value "0" is set, you need to enable the port manually again following a loop with the "Reset" button. You can also reset the port by pulling the cable at the port and plugging it again.
- **Remote Reaction**
Specify how the port will react if a remote loop occurs. Select one of the two options from the drop-down list:
 - No action: A loop has no effect on the port.
 - Disable: The port is blocked.
- **Local reaction**
Specify how the port will react if a local loop occurs. Select one of the two options from the drop-down list:
 - No action: A loop has no effect on the port.
 - Disable: The port is blocked
- **Status**
This box shows whether loop detection is enabled or disabled for this port.
- **Source Port**
Shows the receiving port of the loop detection frame that triggered the last reaction.

- **Source VLAN**
This box shows the VLAN ID of the loop detection frame that triggered the last reaction. This requires that the "VLAN Loop Detection" check box is selected.
- **Reset**
After a loop in the network has been eliminated, click the "Reset" button to reset the port again.

Changing the configured port status with loop detection

The configuration of the port status can be changed with the "Loop Detection" function. If, for example, the administrator has disabled a port, the port can be enabled again after a device restart with "enabled". The port status "Link down" is not changed by "Loop Detection".

6.5.12 Link aggregation

6.5.12.1 General

Bundling network connections for redundancy and higher bandwidth

The link aggregation according to IEEE 802.3ad allows several connections between neighboring devices to be bundled to achieve higher bandwidths and additional protection against failure.

Ports on both partner devices are included in link aggregations and the devices are then connected via these ports. To assign ports (i.e. links) correctly to a partner device, the Link Aggregation Control Protocol (LACP) from the IEEE 802.3ad standard is used.

Note

When a port is assigned to a link aggregation but is not active (e.g. link down), the values displayed may differ from the values configured for the link aggregation.

If the port in the link aggregation becomes active, individual port configurations such as DCP forwarding are overwritten with the configured values of the link aggregation.

Display of the configured aggregation

The menu displays all the configured link aggregations.

Select	Port	Link Aggregation Name	MAC Address	Status	MTU	LACP	Frame Distribution	VLAN Mode	Unicast MAC Learning	P0.1	P0.2	P0.3	P0.4
<input type="checkbox"/>	AG1		00-5e-1d-d2-76-35	<input checked="" type="checkbox"/>	1514	on	Destination&Source MAC	Trunk	<input checked="" type="checkbox"/>	a	-	-	-
<input type="checkbox"/>	AG2		00-5e-1d-d2-76-36	<input checked="" type="checkbox"/>	1514	off	Destination&Source MAC	Hybrid	<input checked="" type="checkbox"/>	-	-	-	-
<input type="checkbox"/>	AG3		00-5e-1d-d2-76-37	<input checked="" type="checkbox"/>	1514	off	Destination&Source MAC	Hybrid	<input checked="" type="checkbox"/>	-	-	-	-
<input type="checkbox"/>	AG4		00-5e-1d-d2-76-38	<input checked="" type="checkbox"/>	1514	off	Destination&Source MAC	Hybrid	<input checked="" type="checkbox"/>	-	-	-	-

4 entries.

[Create](#) [Delete](#) [Set Values](#) [Refresh](#)

Description of the displayed boxes

The table has the following columns:

- **Select**
Select the row you want to delete.
- **Port**
Shows the virtual port number of this link aggregation. This identifier is assigned internally by the firmware.
- **Link Aggregation Name**
Shows the name of the link aggregation. This name can be specified by the user during configuration. The name is not absolutely necessary but can be useful to distinguish between the various link aggregations.
- **MAC Address**
Shows the MAC address of the link aggregation.
- **Status**
Enable or disable the link aggregation.
- **MTU**
Specify the packet size.
- **LACP**
 - On
Enables the sending of LACP frames.
 - Off
Disables the sending of LACP frames.

- **Frame Distribution**

Set the type of distribution of packets to the individual links of an aggregation.

- Destination&Source MAC
The distribution is based on a combination of the destination and source MAC address.
- Destination&Source IP
The distribution is based on a combination of the destination and source IP address.
- Destination&Source IP-MAC
The distribution is based on a combination of the destination and source IP address and MAC address.
- Destination&Source Port IP MAC
Distribution is based on a combination of the destination and source IP and MAC addresses and associated ports.

- **VLAN Mode**

Specify how the link aggregation is entered in a VLAN:

- Hybrid
The link aggregation sends tagged and untagged frames. It is not automatically a member of a VLAN.
- Trunk
The link aggregation only sends tagged frames and is automatically a member of all VLANs.
- Access
The port belongs to a provider switch that supports the function Q-in-Q VLAN Tunnel.

- **Unicast MAC Learning**
Enable or disable the learning of unicast addresses for a port. These unicast addresses are entered in the FDB as dynamically learned addresses.
- **List of ports**
Shows the ports that belong to this link aggregation. The following values can be selected from the drop-down list:
 - "-" (disabled)
Link aggregation is disabled.
 - "a" (active)
The port sends LACP frames and is only involved in the link aggregation when LACP frames are received.
 - "p" (passive)
The port is only involved in the link aggregation when LACP frames are received.
 - "o" (on)
The port is involved in the link aggregation and does not send any LACP frames.

Note

Within a "link aggregation", only ports with the following configuration are possible:

- all ports with "o"
 - all ports with "a" or "p".
-

Note

If you add a configured port to a link aggregation, the port adopts the configuration of the link aggregation. If you take the port out of the link aggregation, the settings of the port are reset to the factory settings.

Configuration procedure

Basics prior to configuration

1. First, identify the ports you want to put together to form a link aggregation between the devices.
2. Configure the link aggregation on the devices.
3. Adopt the configuration for all devices.
4. Perform the last step, the cabling.

Note

If you cable aggregated links prior to configuration, it is possible that you will create loops in the network! The network involved may deteriorate badly due to this or complete disruption may occur.

Creating a new link aggregation

1. Click the "Create" button to create a new link aggregation.
This creates a new row.
2. Select the ports that will belong to this link aggregation.
3. Click the "Set Values" button.

Deleting an aggregation

1. Using the check box at the beginning of a row, select the link aggregation you want to delete.
2. Click the "Delete" button.

Changing an aggregation

1. In the overview, click on the relevant table entry to change the configuration of a created link aggregation.
2. Make all the changes.
3. Click the "Set Values" button.

6.5.12.2 LACP timeout**Configuration of the LACP timeout**

In the IEEE 802.3ad standard, two possible values are defined for the length of the timeout, "Long" (90 seconds) and "Short" (3 seconds). This value defines the interval at which LACPDU's are sent. The timeout is always three times the send period. This means that the send period lasts 30 seconds with the "Long" setting and one second with the "Short" setting.

The value "Long" is configured by default for all ports. To enable a symmetric LACP configuration, the value "Short" can optionally be selected. For all ports of a link aggregation, select the same value for the timeout.

Link Aggregation Control Protocol (LACP) Timeout

General
LACP Timeout

Port	Setting	Copy to Table
All ports	No Change ▼	Copy to Table
P0.1	Long ▼	
P0.2	Long ▼	^
P0.3	Long ▼	■
P0.4	Long ▼	▼
P0.5	Long ▼	

Set Values
Refresh

Description of the displayed boxes

Table 1 has the following columns:

- **1st column**
Shows that the settings are valid for all ports of table 2.
- **Setting**
Select the setting from the drop-down list. You have the following setting options:
 - Short
The value for the LACP timeout is 3 seconds.
 - Long
The value for the LACP timeout is 90 seconds.
 - No Change
Table 2 remains unchanged.
- **Copy to Table**
When you click the button, the settings are adopted for all ports of table 2.

Table 2 has the following columns:

- **Port**
Shows all available ports. The port is made up of the module number and the port number, for example port 0.1 is module 0, port 1.
- **Setting**
Select the value "Short" or "Long" for this port.

6.5.13 DCP Forwarding

Applications

The DCP protocol is used by STEP 7 and SINEC PNI for configuration and diagnostics. When shipped, DCP is enabled on all ports; in other words, DCP frames are forwarded at all ports. With this option, you can disable the forwarding of the frames for individual ports, for example to exclude individual parts of the network from configuration with SINEC PNI or to divide the full network into smaller subnetworks for configuration and diagnostics.

Note

PROFINET configuration

Since DCP is a PROFINET protocol, the configuration created here is only effective in the VLAN associated with the TIA interface.

All the ports of the device are displayed on this page. After each displayed port, there is a drop-down list for function selection.

Discovery and Basic Configuration Protocol (DCP) Forwarding

	Setting		Copy to Table
All ports	No Change	▼	Copy to Table

Port	Setting		
P0.1	Forward	▼	▲ ▼
P0.2	Forward	▼	
P0.3	Forward	▼	
P0.4	Forward	▼	

Description of the displayed values

Table 1 has the following columns:

- **1st column**
Shows that the settings are valid for all ports of table 2.
- **Setting**
Select the setting from the drop-down list. If "No Change" is selected, the entry in table 2 remains unchanged.
- **Copy to Table**
If you click the button, the setting is adopted for all ports of table 2.

Table 2 has the following columns:

- **Port**
Shows the available ports. The port is made up of the module number and the port number, for example port 0.1 is module 0, port 1.
- **Setting**
From the drop-down list, select whether the port should block or forward outgoing DCP frames. You have the following options available:
 - Forward
DCP frames are forwarded via this port.
 - Block
No outgoing DCP frames are forwarded via this port. It is nevertheless still possible to receive via this port.

Configuration procedure

1. From the options in the drop-down list in the row, select which ports should support sending DCP frames.
2. Click the "Set Values" button.

6.5.14 LLDP

Identifying the network topology

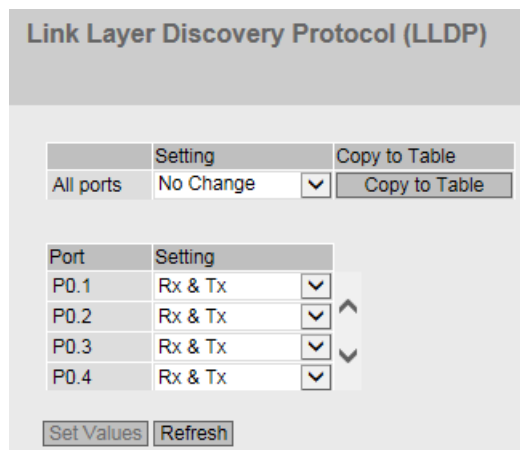
LLDP (Link Layer Discovery Protocol) is defined in the IEEE 802.1AB standard.

LLDP is a method used to discover the network topology. Network components exchange information with their neighbor devices using LLDP.

Network components that support LLDP have an LLDP agent. The LLDP agent sends information about itself and receives information from connected devices at periodic intervals. The received information is stored on the device.

Applications

PROFINET uses LLDP for topology diagnostics. In the default setting, LLDP is enabled for all ports; in other words, LLDP frames are sent and received on all ports. With this function, you have the option of enabling or disabling sending and/or receiving per port.



Description of the displayed boxes

Table 1 has the following columns:

- **1st column**
Shows that the settings are valid for all ports.
- **Setting**
Select the setting from the drop-down list. If "No Change" is selected, the entry in table 2 remains unchanged.
- **Copy to Table**
If you click the button, the setting is adopted for all ports of table 2.

Table 2 has the following columns:

- **Port**
Shows the available ports. The port is made up of the module number and the port number, for example, port 0.1 is module 0, port 1.
- **Setting**
From the drop-down list, select whether or not the port will send or receive LLDP frames. You have the following options available:
 - **Rx**
This port can only receive LLDP frames.
 - **Tx**
This port can only send LLDP frames.
 - **Rx & Tx**
This port can receive and send LLDP frames.
 - **"-" (disabled)**
This port can neither receive nor send LLDP frames.

Steps in configuration

1. Select the LLDP functionality of the port from the "Setting" drop-down list.
2. Click the "Set Values" button.

6.5.15 Fiber Monitoring Protocol

Requirements

- You can only use Fiber Monitoring with transceivers capable of diagnostics. Note the documentation of the devices.
- To be able to use the Fiber Monitoring function, enable LLDP. The Fiber Monitoring information is appended to the LLDP packets.

Monitoring optical links

With Fiber Monitoring, you can monitor the received power and the loss of power on optical links between two switches.

If you enable Fiber Monitoring on an optical port, the device sends the current transmit power of the port to its connection partner using LLDP packets. In addition to sending, the device also checks whether corresponding information is received from the connection partner.

Regardless of whether the IE switch receives diagnostics information from its connection partner, it monitors the received power measured at the optical port for the set limit values.

If Fiber Monitoring is enabled on the connection partner, the connection partner transfers the current value for the transmit power of the port to the device. The device compares the value it has received for the transmit power with the actually received power. The difference

between the receive power and the transmit power represents the power loss on the link. The calculated power loss is also monitored for the set limit values.

If the value of the received power or the power loss falls below or exceeds the set limit values, an event is triggered. You can set limit values in two stages for messages with the severity levels "Warning" and "Critical".

In "System > Events > Configuration", you can specify how the IE switch indicates the event.

Note

If you have enabled Fiber Monitoring and a pluggable transceiver with diagnostics capability is pulled, Fiber Monitoring is automatically disabled for this port and the set limit values and a possibly pending error status are deleted.

Fiber Monitoring Protocol (FMP)

Port	State	Rx Power [dBm] Maintenance Required (warning)	Rx Power [dBm] Maintenance Demanded (critical)	Power Loss [dB] Maintenance Required (warning)	Power Loss [dB] Maintenance Demanded (critical)
P0.1	<input checked="" type="checkbox"/>	-4	-6	-50	-55
P0.2	<input checked="" type="checkbox"/>	-25	-27	-50	-55
P0.4	<input checked="" type="checkbox"/>	-10	-12	-50	-55

Set Values Refresh

Description of the displayed boxes

In the table, you can specify the limit values for the measured received power to be monitored and the calculated power loss.

- Port**
Shows the optical ports that support Fiber Monitoring. This depends on the transceivers.
- Status**
Enable or disable Fiber Monitoring.
By default, the function is disabled.
- Rx Power [dBm] Maintenance Required (Warning)**
Specify the value at which you are informed of the deterioration of the received power by a message of the severity level "Warning".
If you enter the value "0", the received power is not monitored.
The default value depends on the respective transceiver.
- Rx Power [dBm] Maintenance Demanded (Critical)**
Specify the value at which you are informed of the deterioration of the received power by a message of the severity level "Critical".
If you enter the value "0", the received power is not monitored.
The default value depends on the respective transceiver.

- **Power Loss [dB] Maintenance Required (Warning)**
Specify the value at which you are informed of the power loss of the connection by a message of the severity level "Warning".
If you enter the value "0", the power loss is not monitored.
Default: -50 dB
- **Power Loss [dB] Maintenance Demanded (Critical)**
Specify the value at which you are informed of the power loss of the connection by a message of the severity level "Critical".
If you enter the value "0", the power loss is not monitored.
Default: -55 dB

Steps in configuration

Enabling Fiber Monitoring

Follow the steps below to enable the monitoring of a port:

1. Select the appropriate check box in the "Status" column.
2. For your setup, enter practical values at which you want to be informed of deterioration of the received power and the power loss of the connection.
3. Click the "Set Values" button.

Disabling Fiber Monitoring

Follow the steps below to disable the monitoring of a port:

1. Clear the appropriate check box in the "Status" column.
2. Click the "Set Values" button.

Follow the steps below to disable the monitoring of the Rx power or power loss:

1. Enter the value "0" in the appropriate box.
2. Click the "Set Values" button.

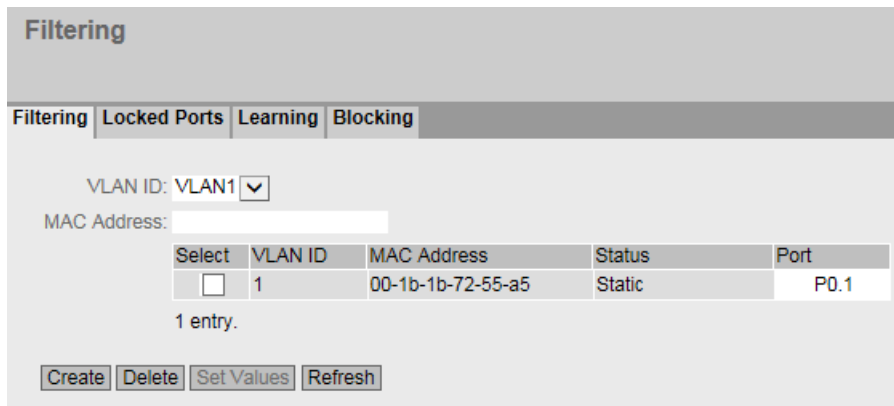
6.5.16 Unicast

6.5.16.1 Filtering

Address filtering

This table shows the unicast addresses entered statically by the user during parameter assignment.

On this page, you also define the static unicast filters.



Description of the displayed boxes

The page contains the following boxes:

- **VLAN ID**
Select the VLAN ID in which you configure a new static MAC address. If nothing is set, "VLAN1" is set as the basic setting.
- **MAC Address**
Enter the MAC address here.

This table contains the following columns:

- **Select**
Select the row you want to delete.
- **VLAN ID**
Shows the VLAN-ID assigned to this MAC address.
- **MAC Address**
Shows the MAC address of the node that the device has learned or the user has configured.
- **Status**
Shows the status of each address entry:
 - Static
Configured by the user. Static addresses are stored permanently; in other words, they are not deleted when the Aging TimeAging Time expires or when the switch is restarted.
 - Invalid
These values are not evaluated.
- **Port**
Shows the port via which the node with the specified address can be reached. Frames received by the device whose destination address matches this address will be forwarded to this port.

Note

You can only specify **one** port for unicast addresses.

Steps in configuration

To edit the entries, follow the steps below.

Creating a new entry

1. Select the relevant VLAN ID.
2. Enter the MAC address in the "MAC address" input box.
3. Click the "Create" button to create a new entry in the table.
4. Select the relevant port from the drop-down list.
5. Click the "Set Values" button.

Changing the entry

1. Select the relevant port.
2. Click the "Set Values" button.

Deleting an entry

1. Select the check box in the row to be deleted.
Repeat this for all entries you want to delete.
2. Click the "Delete" button to delete the selected entries from the filter table.
3. Click the "Refresh" button.

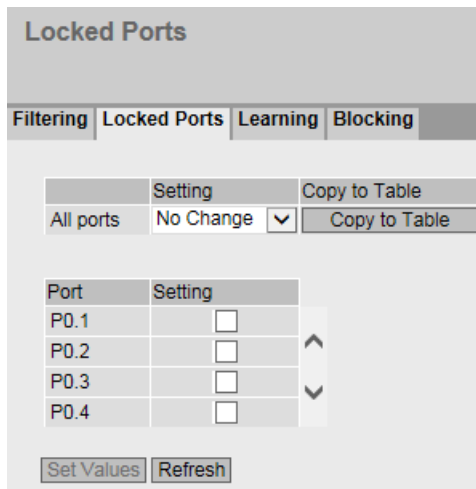
6.5.16.2 Locked Ports

Activating the access control

On this page, you can block individual ports for unknown nodes.

If the Port Lock function is enabled, packets arriving at this port from unknown MAC addresses are discarded immediately. Packets from known nodes are accepted by the port. The port accepts only static MAC addresses that were created previously either manually or with the "Start learning" function and the "Stop learning" function.

To enter all connected nodes automatically, there is a function for automatic learning (see "Layer 2 > Unicast > Learning").



Description of the displayed boxes

Table 1 has the following columns:

- **1st column**
Shows that the settings are valid for all ports of table 2.
- **Setting**
Select the setting from the drop-down list. You have the following setting options:
 - Enabled
Enables the port lock function.
 - Disabled
Disables the port lock function.
 - No Change
Table 2 remains unchanged.
- **Copy to Table**
If you click the button, the setting is adopted for all ports of table 2.

Table 2 has the following columns:

- **Port**
This column lists all the ports available on this device.
- **Setting**
Enable or disable access control for the port.

Configuration procedure

Enabling access control for an individual port

1. Select the check box in the relevant row in table 2.
2. To apply the changes, click the "Set Values" button.

Enabling access control for all ports

1. In the "Setting" drop-down list, select the "Enabled" entry.
2. Click the "Copy to table" button. The check box is enabled for all ports in table 2.
3. To apply the changes, click the "Set Values" button.

6.5.16.3 Learning

Starting/stopping learning

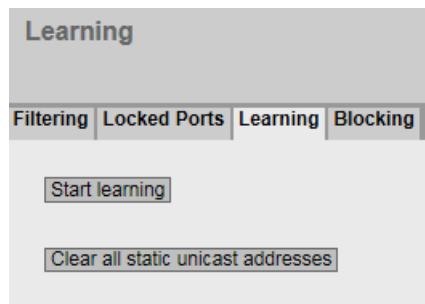
With the automatic learning function, all connected devices can be automatically entered statically in the unicast filter table.

The learning process is only ended by clicking on the "Stop learning" button. With this method, learning can take a few minutes or several hours in larger networks before all nodes have been found. Only nodes that send packets during the learning phase are found.

By subsequently enabling the Port Lock function, only packets from the nodes known after the end of the learning phase (static unicast entries) will be accepted at the relevant ports.

Note

If the Port Lock function was already active on individual ports prior to the automatic learning phase, no addresses will be learned on these ports. This makes it possible to restrict learning to certain ports. To do this, first enable the Port Lock function of the ports that are not intended to learn addresses.



Steps in configuration

Learning addresses

1. Click the "Start learning" button to start the learning phase.
After starting the learning phase, the "Start learning" button is replaced by the "Stop learning" button.
The device now enters the addresses of connected devices until you stop the function.
2. Click the "Stop learning" button to stop the learning function.
The button is once again replaced by the "Start learning" button. The learned entries are stored and are listed under "Layer 2 > Unicast > Filtering".

Note

With a very high data rate, it may occur that statically entered unicast addresses are shown in the unicast table as learned addresses. In this case, the following procedure is recommended:

1. Click the "Start learning" button to start the learning process.
2. Start data traffic.
3. Wait until the unicast table shows all MAC addresses as "Learnt" (menu "Information" > "Unicast").
4. Lock the ports (menu "Layer 2" > "Unicast" > "Locked Ports").
5. Click the "Stop learning" button to stop the learning process.

Deleting all static unicast addresses

1. Click the "Clear all static unicast addresses" button to delete all static entries.
In large networks with numerous nodes, automatic learning may lead to a lot of undesired static entries. To avoid having to delete these individually, this button can be used to delete all static entries. This function is disabled during automatic learning.

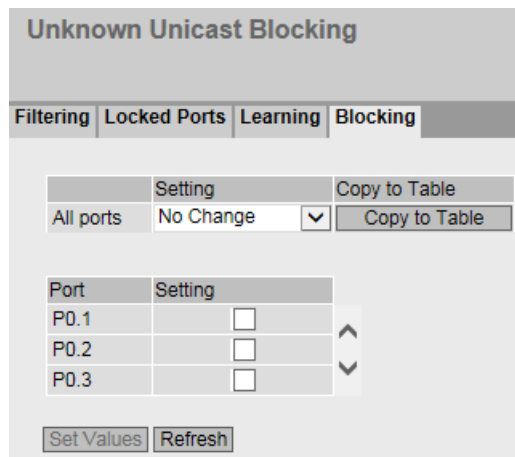
Note

Depending on the number of entries involved, deleting may take some time.

6.5.16.4 Blocking

Blocking forwarding of unknown unicast frames

On this page, you can block the forwarding of unknown unicast frames for individual ports.



Description of the displayed values

Table 1 has the following columns:

- **1st column**
Shows that the settings are valid for all ports of table 2.
- **Setting**
Select the setting from the drop-down list. You have the following setting options:
 - Enabled
Blocking of unicast frames is enabled.
 - Disabled
Blocking of unicast frames is disabled.
 - No change
Table 2 remains unchanged.
- **Copy to Table**
If you click the button, the setting is adopted for all ports of table 2.

Table 2 has the following columns:

- **Port**
Shows the available ports. The port is made up of the module number and the port number, for example port 0.1 is module 0, port 1.

Note

Ring redundancy/standby

If ring redundancy or standby is enabled, the ports configured for this are not included in the unicast blocking.

- **Setting**
Enable or disable the blocking of unicast frames.

Steps in configuration

Enabling blocking for an individual port

1. Select the check box in the relevant row in table 2.
2. To apply the changes, click the "Set Values" button.

Enabling blocking for all ports

1. In the "Setting" drop-down list, select the "Enabled" entry in table 1.
2. Click the "Copy to table" button. The check box is enabled for all ports in table 2.
3. To apply the changes, click the "Set Values" button.

6.5.17 Multicast

6.5.17.1 Groups

Multicast applications

In the majority of cases, a frame is sent with a unicast address to a particular recipient. If an application sends the same data to several recipients, the amount of data can be reduced by sending the data using one multicast address. For some applications, there are fixed multicast addresses (NTP, IETF1 Audio, IETF1 Video etc.).

Reducing network load

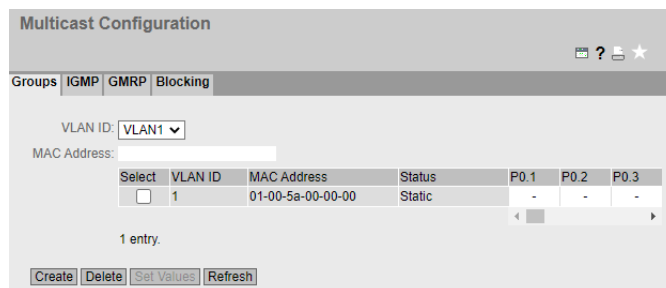
In contrast to unicast frames, multicast frames represent a higher load for the device. Generally, multicast frames are sent to all ports. There are three ways of reducing the load caused by multicast frames:

- Static entry of the addresses in the multicast filter table.
- Dynamic entry of the addresses by listening in on IGMP/MLD parameter assignment frames (IGMP/MLD configuration).
- Active dynamic assignment of addresses by GMRP frames.

The result of all these methods is that multicast frames are sent only to ports for which an appropriate address is entered.

The "Multicast Configuration" menu item shows the multicast frames currently entered in the filter table and their destination ports that the user set in the parameters (static).

Configuring multicast addresses



Description of the displayed boxes

The page contains the following boxes:

- **VLAN ID**
If you click on this text box, a drop-down list is displayed. Here you can select the VLAN ID of a new MAC address you want to configure.
- **MAC address**
Here you enter a new MAC multicast address you want to configure.

The table has the following columns:

- **Select**
Select the row you want to delete.
- **VLAN ID**
Here, the VLAN ID of the VLAN is displayed to which the MAC multicast address of this row is assigned.
- **MAC address**
Here, the multicast address is displayed that the device has learned or the user has configured.
- **Status - static**
Shows the status of each address entry. The address was entered statically by the user. Static addresses are stored permanently; in other words, they are not deleted when the aging time expires or when the device is restarted. These must be deleted by the user.
- **Port List**
There is a column for each slot. Within a column, the multicast group to which the port belongs is shown. The drop-down list provides the following options:
 - M
(Member) Multicast frames are sent via this port.
 - R
(Registered) Member of the multicast group, registration was by a GMRP frame.
 - F
(Forbidden) Not a member of the multicast group. Moreover, this address must not be an address learned dynamically with GMRP or IGMP/MLD.
 - –
Not a member of the multicast group. No multicast frames with the defined multicast MAC address are sent via this port.

Configuration procedure

Creating a new entry

Note

You cannot create any static multicast entries if GMRP is enabled.

1. Select the required VLAN ID from the ""drop-down list.
2. Enter the MAC address in the "MAC address" input box.
3. Click the "Create" button. A new entry is generated in the table.
4. Assign the relevant ports to the MAC address.
5. Click the "Set Values" button.

Creating layer 2 multicast addresses with a script and GMRP

6.5 The "Layer 2" menu

If you want to create several layer 2 multicast addresses using a script, GMRP must be disabled as long as the script is executing. Follow the steps outlined below:

1. If GMRP is enabled, disable it. You configure GMRP on the "Layer 2 > Multicast > GMRP" page.
2. Run the script.
3. Enable GMRP only after the script has completed and the layer 2 multicast addresses have been created.

Deleting an entry

1. Select the check box in the row to be deleted.
2. Click the "Delete" button.
The row is deleted from the display and from the memory of the device.

6.5.17.2 IGMP

Function

The device supports "IGMP Snooping" and the "IGMP Querier" function. If "IGMP Snooping" is enabled, IGMP frames (Internet Group Management Protocol) are evaluated and the multicast filter table is updated with this information. If "IGMP Querier" is also enabled, the device also sends IGMP queries that trigger responses from IGMP-compliant nodes.

IGMP Snooping Aging Time

In this menu, you can configure the aging time for IGMP Configuration. When the time elapses, entries created by IGMP are deleted from the address table if they are not updated by a new IGMP frame.

This applies to all ports and VLANS; a specific configuration is not possible.

IGMP Snooping Aging Time depending on the querier

The IE switch as IGMP querier

If the IE switch is used as an IGMP querier, the query interval is 125 seconds. For the "IGMP Snooping Aging Time", set at least 250 seconds.

Other IGMP queriers

If a different IGMP querier is used, the value of the "IGMP Snooping Aging Time" should be at least twice as long as the query interval.

Description of the displayed boxes

Internet Group Management Protocol (IGMP) Snooping & Querier

Groups | **IGMP** | GMRP | Blocking

IGMP Snooping

IGMP Snooping Aging Time[s]: 300

IGMP Querier

IGMP Snooping Switch IP Address: 0.0.0.0

IGMP Snooping Version: 3

Snooping Report Processing: Client Ports

Snooping Report Forward: Router Ports

Send Query on Topology Change

VLAN ID	IGMP Snooping	IGMP Querier
1	<input type="checkbox"/>	<input type="checkbox"/>

Set Values Refresh

The page contains the following boxes:

- IGMP Snooping**
 Enable or disable IGMP snooping. The function enables IGMP snooping on all interfaces and allows the assignment of IP addresses to multicast groups. If the function is enabled, the multicast addresses learned with IGMP snooping are entered in the multicast filter table and IGMP frames are forwarded.
- IGMP Snooping Aging Time[s]**
 Enter the value for the aging time in seconds in this box. As default, 300 seconds is set
 Range of values: 130 - 1225 seconds
- IGMP Querier**
 Enable or disable "IGMP Querier". The device sends IGMP queries cyclically.
- IGMP Snooping Switch IP Address**
 This IP address is used for sending the IGMP queries. If multiple IGMP Querier queries are sent in a network, the Querier with the smallest IP address takes on the Querier function. If the IP address 0.0.0.0 is set, the own IP address is used for sending the IGMP queries. You can enter any IP address as an alternative to specify the order of the active Queriers in the network.
- IGMP Snooping Version**
 Select the IGMP Snooping Version from the drop-down list.
- Snooping Report Processing**
 The following setting is possible:
 - Client Ports
The device processes IGMP joins only on client ports.
 - All Ports
The device processes IGMP joins on all ports.

- **Snooping Report Forward**
The following setting is possible:
 - All Ports
The device forwards IGMP joins to all ports.
 - Router Ports
The device forwards IGMP joins to router ports.
 - Non Edge Ports
The device forwards IGMP joins to all ports that are not Edge ports.
- **Send Query on Topology Change**
Enable or disable sending of additional IGMP queries on topology changes. In large Spanning Tree topologies, the sending of additional IGMP queries can lead to an undesired flood of queries.

The table has the following columns:

- **VLAN ID**
The VLAN ID for which IGMP Snooping or IGMP Querier should be activated.
- **IGMP Snooping**
Select the check box in this column for the VLANs for which IGMP Snooping should be activated. The specifications in this column only become valid when you enable IGMP Snooping for the device (first check box on this page).
- **IGMP Querier**
Select the check boxes in this column for the VLANs for which IGMP Querier should be activated.
If the IGMP Snooping check box for the device and the IGMP Snooping check box for a VLAN are selected, IGMP Querier is executed when the corresponding check box in the table is selected. This is true regardless of the status of the IGMP Querier check box for the device.

Configuration procedure

Switching on IGMP Snooping

1. Select the "IGMP Snooping" check box.
2. Enter the value for the aging time in seconds in the "IGMP Snooping Aging Time" box.
3. Select the IGMP Snooping Version from the drop-down list.
4. From the drop-down list, select whether the device should process IGMP joins only on client ports or on all ports.
5. In the "IGMP Snooping" table column, select the check boxes for the desired VLAN IDs.

Switching off IGMP Snooping

1. Clear the "IGMP Snooping" check box.

Switching on IGMP Querier

1. Select the "IGMP Snooping" check box.
2. Enter the value for the aging time in seconds in the "IGMP Snooping Aging Time" box.
3. Select the "IGMP Querier" check box.

- 4. In the "IGMP Snooping Switch IP Address" field, enter the IP address with which IGMP queries are to be sent.
- 5. In the "IGMP Querier" table column, select the check boxes for the desired VLAN IDs.

Switching off IGMP Querier

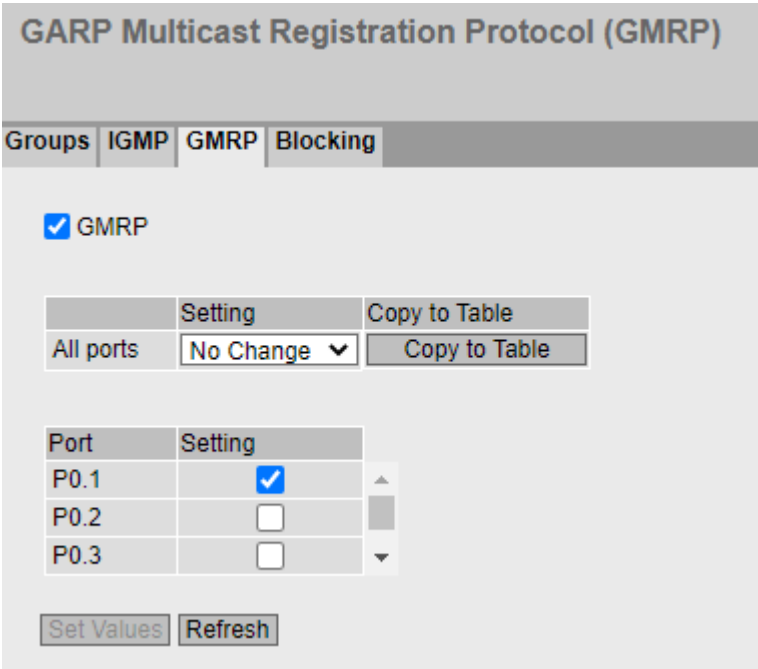
- 1. Clear the "IGMP Querier" check box.

6.5.17.3 GMRP

Activating GMRP

On this page, you specify whether or not GMRP is used for each individual port. If "GMRP" is disabled for a port, no registrations are made for it and it cannot send GMRP frames.

For GMRP to work, you need to enable the function globally and on the ports.



Timer

The following timers are set in the protocols mentioned above. The timer values are not configurable.

Timer	Description	Factory setting
Join-time	Time in milliseconds that passes between the transfer of two PDUs (Protocol Data Unit)	200 ms
Leave-time	Time period of the timer in milliseconds before the device changes its GARP status The timer starts and runs backwards with the defined time as soon as the device sends or receives a "Leave-all-time" message. The timer is stopped when the device receives a Join message.	600 ms
Leave-all-time	Time period of the timer in milliseconds before all devices change their GARP status	10000 ms

In devices connected via Layer 2, the same values must be set for the GARP/GMRP timers. If different values are set with the GARP/GMRP timers, GARP applications such as GMRP and GVRP cannot be executed successfully.

Description of the displayed boxes

The page contains the following box:

- **GMRP**
Enable or disable the GMRP function.

Table 1 has the following columns:

- **1st column**
Shows that the settings are valid for all ports of table 2.
- **Setting**
Select the setting from the drop-down list. You have the following setting options:
 - Enabled
Enables the sending of GMRP frames.
 - Disabled
Disables the sending of GMRP frames.
 - No Change
Table 2 remains unchanged.
- **Copy to Table**
When you click the button, the settings are adopted for all ports of table 2.

Table 2 has the following columns:

- **Port**
This column shows all the ports available on the device as well as the link aggregations.
- **Setting**
With this check box, you enable or disable GMRP for the port or link aggregation.

Configuration procedure

Enabling the sending of GMRP frames for an individual port

1. Select the "GMRP" check box.
2. Select the check box in the relevant row in table 2.
3. To apply the changes, click the "Set Values" button.

Enabling the sending of GMRP frames for all ports

1. Select the "GMRP" check box.
2. In the "Setting" drop-down list, select the "Enabled" entry.
3. Click the "Copy to Table" button. The check box is enabled for all ports in table 2.
4. To apply the changes, click the "Set Values" button.

6.5.17.4 Blocking

Disabling the forwarding of unknown multicast frames

On this page, you can block the forwarding of unknown multicast frames for individual ports.

Sperren unbekannter Multicast-Telegramme

Gruppen	IGMP	GMRP	Blocking
Alle Ports	Einstellung	Keine Änder	In Tabelle übernehmen

Port	Einstellung
P0.1	<input checked="" type="checkbox"/>
P0.2	<input type="checkbox"/>
P0.3	<input type="checkbox"/>
P0.4	<input type="checkbox"/>
P0.5	<input type="checkbox"/>

Description of the displayed values

Table 1 has the following columns:

- **1st column**
Shows that the settings are valid for all ports of table 2.
- **Setting**
Select the setting from the drop-down list. You have the following setting options:
 - Enabled
Blocking of multicast frames is enabled.
 - Disabled
Blocking of unknown multicast frames is disabled.
 - No Change
Table 2 remains unchanged.
- **Copy to Table**
If you click the button, the setting is adopted for all ports of table 2.

Table 2 has the following columns:

- **Port**
All available ports are listed in this column. Unavailable ports are not displayed.
- **Setting**
Enable or disable the blocking of multicast frames.

Steps in configuration

Enabling blocking for an individual port

1. Select the check box in the relevant row in table 2.
2. To apply the changes, click the "Set Values" button.

Enabling blocking for all ports

1. In the "Setting" drop-down list, select the "Enabled" entry.
2. Click the "Copy to Table" button. The check box is enabled for all ports in table 2.
3. To apply the changes, click the "Set Values" button.

6.5.18 Broadcast

Blocking the forwarding of broadcast frames

On this page, you can block the forwarding of broadcast frames for individual ports.

Note

Some communication protocols work only with the support of broadcast. In these cases, blocking can lead to loss of data communication. Block broadcast only when you are sure that you do not need it on the selected ports.

Broadcast Blocking		
	Setting	Copy to Table
All ports	No Change <input type="button" value="v"/>	<input type="button" value="Copy to Table"/>
Port	Setting	
P0.1	<input type="checkbox"/>	<input type="button" value="^"/> <input type="button" value="v"/>
P0.2	<input type="checkbox"/>	
P0.3	<input type="checkbox"/>	
P0.4	<input type="checkbox"/>	
<input type="button" value="Set Values"/>		<input type="button" value="Refresh"/>

Description of the displayed boxes

Table 1 has the following columns:

- **1st column**
Shows that the settings are valid for all ports of table 2.
- **Setting**
Select the setting from the drop-down list. You have the following setting options:
 - Enabled
The blocking of broadcast frames is enabled.
 - Disabled
The blocking of broadcast frames is disabled.
 - No change
Table 2 remains unchanged.
- **Copy to Table**
If you click the button, the setting is adopted for all ports of table 2.

Table 2 has the following columns:

- **Port**
All available ports are displayed.
- **Setting**
Enable or disable the blocking of broadcast frames.

Steps in configuration

Enabling the blocking of broadcast frames for an individual port

1. Select the check box in the relevant row in table 2.
2. To apply the changes, click the "Set Values" button.

Enabling the blocking of broadcast frames for all ports

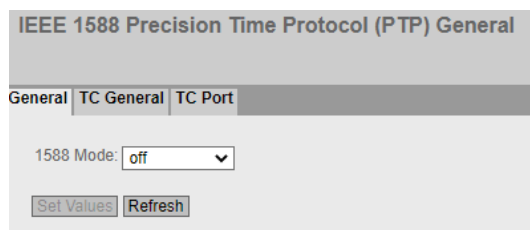
1. In the "Setting" drop-down list in table 1, select the "Enabled" entry.
2. Click the "Copy to Table" button. The check box is enabled for all ports in table 2.
3. To apply the changes, click the "Set Values" button.

6.5.19 PTP

6.5.19.1 General

IEEE 1588 with SCALANCE devices

The IEEE 1588v2 standard defines mechanisms with which highly precise time of day synchronization of devices in a network can be achieved. SCALANCE devices with suitable hardware support time synchronization according to IEEE 1588v2. The functionality is disabled on these devices when they are shipped and following a reset to factory settings. To be able to use PTP, enable this function and configure every port that is on the synchronization path as well as ports that are blocked due to redundancy mechanisms. PTP can also be used with redundancy mechanisms in the ring such as HRP, standby linking of rings, MRP and RSTP. The following sections describe the configuration options of Web Based Management.



IEEE 1588 Configuration

On this page, you specify how the device will process PTP messages.

Mode 1588

You can make the following settings:

- **off**
The device does not process any PTP messages. PTP messages are, however, forwarded according to the rules of the switch.
- **transparent**
The device adopts the function of a transparent clock and forwards PTP messages to other nodes while at the same time making entries in the correction field of the PTP message.

6.5.19.2 TC General**TC General**

On this tab, you will find the general settings for PTP.

The screenshot shows the configuration page for IEEE 1588 Precision Time Protocol (PTP) Transparent Clock (TC) General. The page has a title bar and three tabs: General, TC General, and TC Port. The TC General tab is active. The configuration fields are as follows:

IEEE 1588 Precision Time Protocol (PTP) Transparent Clock (TC) General	
General	TC General
Delay Mechanism:	peer to peer ▼
Domain Number:	0
VLAN ID:	- ▼
Set Values	Refresh

Configuration of the IEEE 1588 transparent clock

The page contains the following boxes:

- **Delay Mechanism**

Specify the delay mechanism the device will work with:

- end to end
The delay request response mechanism will be used.

Note

With end-to-end synchronization with more than 2 slaves, freak values > 100 ns can occur in the offset.

- peer to peer
The peer delay mechanism will be used.

- **Domain Number**

Enter the domain number for the device here. A SCALANCE device can only be assigned to one synchronization domain. The device ignores PTP messages with a different domain number.

- **VLAN ID**

Select the VLAN in which the device should synchronize itself.

6.5.19.3 TC port

Port settings

This tab contains the port settings for PTP.

IEEE 1588 Precision Time Protocol (PTP) Transparent Clock (TC) Port

General | **TC General** | TC Port

	Setting	Transport Mechanism	Copy to Table
All ports	No Change <input type="checkbox"/>	No Change <input type="checkbox"/>	Copy to Table <input type="button" value="↕"/>

Port	Setting	Faulty Flag	Transport Mechanism
P1.1	<input type="checkbox"/>	false	UDP IP v4 <input type="button" value="v"/>
P1.2	<input type="checkbox"/>	false	UDP IP v4 <input type="button" value="v"/>
P1.3	<input type="checkbox"/>	false	UDP IP v4 <input type="button" value="v"/>
P1.4	<input type="checkbox"/>	false	UDP IP v4 <input type="button" value="v"/>

Configuration of the IEEE 1588 transparent clock port parameters

Table 1 has the following columns:

- **1st column**
Shows that the settings are valid for all ports.
- **Setting**
Select the required setting. If "No Change" is selected, the entry in table 2 remains unchanged.
- **Transport Mechanism**
The following settings are possible:
 - Ethernet
 - UDP IPv4
 - No Change
If "No Change" is selected, the entry in table 2 remains unchanged.

Table 2 shows detailed information about the individual ports:

- **Port**
The port number. With modular devices, the slot number and port number are displayed separated by a dot.
- **Setting**
The port status. The following entries are possible:
 - Disabled
The port is not involved in PTP.
 - Enabled
The port processes PTP messages.
- **Faulty Flag**
The error status relating to PTP.
 - true
An error occurred.
 - false
No error has occurred on this port.
- **Transport mechanism**
Choose how this port will handle PTP message data traffic. You can make different settings for the ports of a device, however, the relevant communications partner must support the selected transport mechanism. The following settings are possible:
 - Ethernet
 - UDP IPv4

6.5.20 RMON

6.5.20.1 Statistics

Statistics

On this page you can specify the ports for which RMON statistics are displayed.

The RMON statistics are shown on the page "Information > Ethernet Statistics" in "Packet Size", "Frame Type" and "Packet Error" tabs.

Settings

- RMON**
 If you select this check box, Remote Monitoring (RMON) allows diagnostics data to be collected on the device, prepared and read out using SNMP by a network management station that also supports RMON. This diagnostic data, for example port-related load trends, allow problems in the network to be detected early and eliminated.

Note

If you disable RMON, these statistics are not deleted but retain their last status.

- Port**
 Select the ports for which statistics will be displayed.

The table has the following columns:

- Select**
 Select the row you want to delete.
- Port**
 Shows the ports for which statistics will be displayed.

Steps in configuration

Enabling the function

1. Select the "RMON" check box.
2. Click the "Set Values" button.
The "RMON" function is enabled.

Enabling RMON statistics for ports

Note

Requirement

To allow RMON statistics to be displayed for a port, the "RMON" function must be enabled.

1. Select the required port from the "Port" drop-down list or the entry "All Ports".
2. Click the "Create" button.
RMON statistics can be displayed for the selected port or for all ports.

Disabling RMON statistics for ports

1. Select the row you want to delete in the "Select" column.
2. Click the "Delete" button.
No RMON statistics are displayed for the selected port.

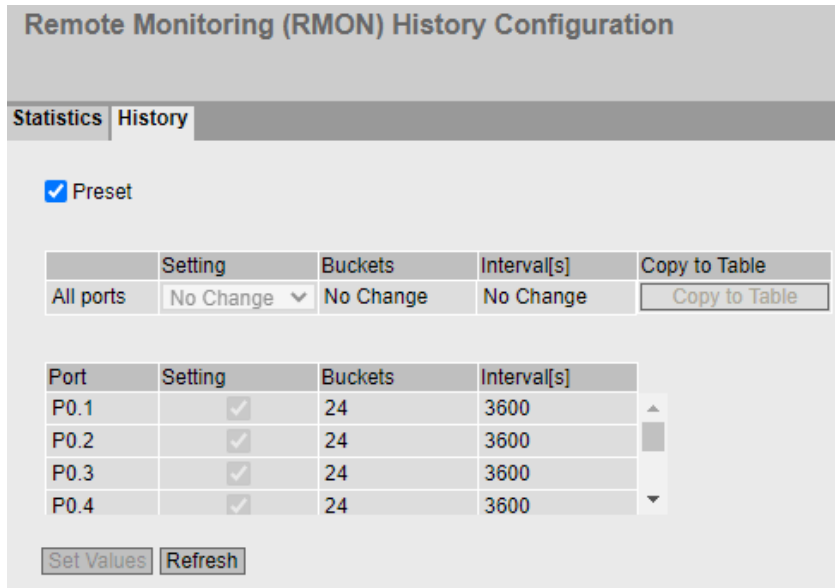
6.5.20.2 History

Samples of the statistics

On this page, you can specify whether or not samples of the statistics are saved for a port. You can specify how many entries should be saved and at which intervals samples should be taken.

Enabled RMON statistics are displayed on the WBM page "Information > Ethernet statistics > History".

Settings



The page contains the following boxes:

- **Default**
 If you enable the option, all custom RMON history settings are deleted and overwritten with the following settings for all ports:
 - Setting: Enabled
 - Entries: 24
 - Interval[s]: 3600
 The values for an individual configuration are locked as long as the default for the RMON history is enabled.
 If you disable the option, the settings are retained, but are individually configurable again.

Table 1 has the following columns:

- **1st column**
 Shows that the settings are valid for all ports.
- **Setting**
 Select the required setting. If "No Change" is selected, the entry in table 2 remains unchanged.
- **Buckets**
 Enter the maximum number of samples to be stored at the same time. If "No Change" is entered, the entry in table 2 remains unchanged

- **Interval [s]**
Enter the interval after which the current version of the statistics should be saved as sample. If "No Change" is entered, the entry in table 2 remains unchanged

Note

When defining the interval period, note that only multiples of 3 seconds are suitable as the interval period. The statistics are updated every 3 seconds. The value "0" is output in the periods in between.

- **Copy to Table**
If you click the button, the settings are adopted for all ports of table 2.

Table 2 has the following columns:

- **Port**
Shows the port to which the settings relate.
- **Setting**
Enable or disable the recording of the history on the relevant port.
- **Buckets**
Enter the maximum number of samples to be stored at the same time.
The maximum number of entries can be restricted by the capacity of the device.
Range of values: 1 - 65535
Factory setting: 24
- **Interval [s]**
Enter the interval after which the current version of the statistics should be saved as sample.
Range of values: 1 - 3600
Factory setting: 3600

Note

When defining the interval period, note that only multiples of 3 seconds are suitable as the interval period. The statistics are updated every 3 seconds. The value "0" is output in the periods in between.

Configuration procedure

Enabling RMON statistics for individual ports

1. Select the check box "Setting" in the relevant row in table 2.
The "Buckets" and "Interval[s]" boxes become active with the factory settings.
2. Enter the required values in the "Buckets" and "Interval[s]" boxes.
3. Click the "Set Values" button.

Enabling RMON statistics for all ports

1. In the "Setting" drop-down list, select the "Enabled" entry in table 1.
2. Enter the required values in the "Buckets" and "Interval[s]" boxes. If you do not change the entries in both boxes, the factory defaults will be used for all ports.

6.6 The "Layer 3" menu

3. Click the "Copy to Table" button.
The settings are adopted for all ports of table 2.
4. Click the "Set Values" button.

Activate **RMONdefault**

1. Select the "Default" check box.
2. Click the "Set Values" button.

6.6 The "Layer 3" menu

6.6.1 Layer 3 Configuration

6.6.1.1 General

Introduction

The page contains the overview of the layer 3 functions for IPv4 of the device. On this page, you enable or disable the required layer 3 function.

Die functions "Routing", "VRRP", "OSPF", "RIP" and "PIM" are available only on layer 3.

Layer 3 Configuration

General | ICMP

- Routing
- DHCP Relay Agent
- VRRP
- OSPF
- RIP
- PIM Routing
- ARP Keep Alive Status

ARP Keep Alive Interval: 30

Set Values Refresh

Description of the displayed boxes

The page contains the following boxes:

- **Routing** (only available with devices with a layer 3 license)
 - Enabled
IPv4 routing is enabled. You can only enable the routing function if DHCP is disabled on all configured interfaces.
 - Disabled
IPv4 routing is disabled.
- **DHCP Relay Agent**
Enable or disable the DHCP relay agent. You can configure other settings in "Layer 3 (IPv4)> DHCP Relay Agent".
- **VRRP** (only available with devices with a layer 3 license)
Enable or disable the VRRP function. IPv4 routing must be enabled beforehand. You can configure other settings in "Layer 3 (IPv4) > VRRP".
- **OSPF** (only available with devices with a layer 3 license)
Enable or disable routing using OSPF. To use OSPF, first enable the "Routing" function. You can configure other settings in "Layer 3 (IPv4) > OSPF".
- **RIP** (only available with devices with a layer 3 license)
Enable or disable routing using RIP. To use RIP, first enable the routing function. You can configure other settings in "Layer 3 (IPv4) > RIP".
- **PIM Routing** (only available with devices with a layer 3 license)
Enable or disable the PIM routing. You can configure other settings in "Layer 3 (IPv4) > PIM".

Note

If the "ARP Keep Alive Status" check box is grayed out, the ARP entries are changed from Next Hops to static ARP entries. You can only configure this operating behavior in the Command Line Interface with the `ipv4 nexthop arp_keep_alive` command.

- **ARP Keep Alive Status**
Enable or disable ARP Keep Alive. When ARP Keep Alive is enabled, the device checks all entries in the routing table to determine whether there is an entry for the specified gateway (Next Hop) in the ARP table. If there is no entry in the ARP table, the device sends an ARP query. If you clear this check box, the value in the ARP Keep Alive Interval input field is automatically set to the default value.
- **ARP Keep Alive Interval**
Interval in seconds at which the check is performed cyclically. If you enter a value here, the ARP Keep Alive Status check box is selected automatically.
Range of values: 30 ... 86400 seconds
Default: 30 seconds

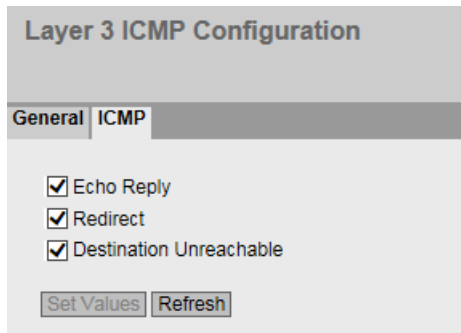
Configuration procedure

1. To use the required function, select the corresponding check box.
2. Click the "Set Values" button.

6.6.1.2 ICMP

Introduction

With ICMP (Internet Control Message Protocol), you check the availability of network nodes.



Description of the displayed boxes

The page contains the following boxes with which you enable or disable the corresponding protocol messages:

- **Echo Reply**
The device sends ping replies.
- **Redirect**
The device sends messages if the destination can be reached via another router.
- **Destination Unreachable**
The device sends messages if the destination cannot be reached.

Configuration procedure

1. To use the required function, select the corresponding check box.
2. Click the "Set Values" button.

6.6.2 Subnets

6.6.2.1 Overview

Creating subnets

The page shows the subnets for the selected interface. If more than one subnet is available on an interface, the first entry of this interface is of the address type "Primary".

All other subnets are created on this page. A subnet always relates to an interface. The interface is created on the "Configuration" tab.

Connected Subnets Overview

Overview
Configuration

Interface: VLAN1 ▼

Loopback

Select	Interface	TIA Interface	Status	Interface Name	MAC Address
<input type="checkbox"/>	vlan1	yes	enabled	vlan1	d4-f5-27-f7-2e-30
<input type="checkbox"/>	vlan7	-	enabled	vlan7	d4-f5-27-f7-2e-30

2 entries.

Create
Delete
Refresh

(Continuation of table)

IP Address	Subnet Mask	Address Type	IP Assgn. Method	Address Collision Detection Status	Loopback	MTU
192.168.16.30	255.255.255.0	Primary	Static	Active	-	1500
192.168.10.11	255.255.255.0	Primary	Static	Idle	-	1500

Description

The page contains the following boxes:

- **Interface**
Select the interface on which you want to configure another subnet.
- **Loopback**
Enable or disable the "loopback" property on the interface.
If the "Loopback" property is to be activated for an IP interface, the assigned VLAN must not contain member ports.
Since the IP interface is not linked to physical ports, the operating status of the IP interface is not dependent on the link status of the physical ports. The loopback interface can be reached as long as the device is connected to a suitable power supply.
You can access the device via the loopback interface.

Note

An interface configured as loopback must be located in its own subnet with a subnet mask of at least 30 bits.

The table has the following columns:

- **Select**
Select the row you want to delete.
- **Interface**
Shows the interface.
- **TIA Interface**
Shows whether or not the interface is used as TIA interface.
- **Status**
Shows the status of the interface.
- **Interface Name**
Shows the name of the interface.
- **MAC Address**
Shows the MAC address.
- **IP Address**
Shows the IPv4 address of the subnet.
- **Subnet Mask**
Shows the subnet mask.
- **Address Type**
Displays the address type. The following values are possible:
 - Primary
The first IPv4 address that was configured on an IPv4 interface.
 - Secondary
All other IPv4 addresses that were configured on an IPv4 interface.
- **IP Assgn Method**
Shows how the IPv4 address is assigned. The following values are possible:
 - Static
The IPv4 address is static. You enter the settings in "IP Address" and "Subnet Mask".
 - Dynamic (DHCP)
The device obtains a dynamic IPv4 address from a DHCPv4 server.

- **Address Collision Detection Status**

If new IPv4 addresses become active in the network, the "Address Collision Detection" function checks whether this can result in address collisions. The allows IPv4 addresses that would be assigned twice to be detected.

Note

The function does not run a cyclic check.

This column shows the current status of the function. The following values are possible:

- Idle
The interface is not enabled or does not have an IPv4 address.
 - Starting
This status indicates the start-up phase. In this phase, the device initially sends a query as to whether the planned IPv4 address already exists. If the address is not yet been assigned, the device sends the message that it is using this IP address as of now.
 - Conflict
The interface is not enabled. The interface is attempting to use an IPv4 address that has already been assigned.
 - Defending
The interface uses a unique IPv4 address. Another interface is attempting to use the same IPv4 address.
 - Active
The interface uses a unique IPv4 address. There are no collisions.
 - Not supported
If routing protocols are configured for the interface, the function for detection of address collisions is not supported.
 - Disabled
The function for detection of address collisions is disabled.
- **Loopback**
 - "-"
Shows that the "Loopback" property is disabled.
 - Yes
Shows that the "Loopback" property is enabled.
 - IP Source
Shows that the loopback interface is used as source IP address in specific protocols.
 - **MTU**
Shows the packet size.

Configuration procedure

1. Select the interface from the "Interface" drop-down list.
2. If appropriate select the "loopback" property.
3. Click the "Create" button. A new row is inserted in the table.
4. Click the "Set Values" button. Configure the subnet on the "Configuration" tab.

6.6.2.2 Configuration

On this page, you configure the IPv4 interface.

Connected Subnets Configuration

Overview **Configuration**

Interface (Name): ▾

Status: ▾

Interface Name:

MAC Address:

DHCP

IP Address:

Subnet Mask:

Address Type:

Loopback:

TIA Interface

MTU:

Description

The page contains the following boxes:

- **Interface (Name)**
Select the interface from the drop-down list.
- **Status**
Specify whether the interface is enabled or disabled.
 - Enabled
The interface is enabled. Data traffic is possible only over an enabled Interface.
 - Disabled
The interface is disabled.
- **Interface Name**
Enter the name of the interface.
- **MAC Address**
Displays the MAC address of the selected interface.
- **DHCP**
Enable or disable the DHCP client for this IPv4 interface.
- **IP Address**
Enter the IPv4 address of the interface. The IPv4 addresses must not be used more than once.

- **Subnet Mask**
Enter the subnet mask of the subnet you are creating. Subnets on different interfaces must not overlap.
- **Address Type**
Shows the type of the address. The following values are possible:
 - Primary
The first subnet of the interface.
- **Loopback**
Shows whether the "Loopback" property is enabled.
- **IP Source**

Note

This check box is only displayed when the "Loopback" property is enabled for the selected interface from the page "Layer 3 > Subnets > Overview".

When the option is enabled, the loopback interface is used as source IP address in the following protocols:

- RADIUS
- SNMPv1 Trap
- Syslog
- SNTP
- NTP
- SMTP
- TFTP
- SFTP

This option can be helpful, for example, when using a firewall or authentication over RADIUS. Because a router with multiple IP interfaces does not always specify the same IP interface as source, without this setting all IP interfaces of a router would have to be configured on a RADIUS server or in a firewall. This setting makes it possible for a router to use a loopback interface of the outgoing IP communication so that only this loopback interface must be known to the RADIUS server and the firewall.

When the option is disabled, the outgoing interface is specified as source in the protocols.

- **TIA Interface**
Select whether or not this interface should become the TIA interface.
- **MTU**
Size of the Maximum Transmission Unit (MTU) in bytes
Specify the packet size for the interface.
Range of values:
 - Default (Port or VLAN): 1500
 - Port: 64 ... 9194
 - IPv4 router port: 90 ... 9194
 - VLAN: 90 ... 1500

Configuration procedure

1. Select the interface from the "Interface (name)" drop-down list.
2. Enter a name for the Interface in "Interface Name".
3. Enter the IPv4 address of the subnet in the "IP Address" column.
4. Enter the subnet mask belonging to the IPv4 address in the "Subnet Mask" column
5. Click the "Set Values" button.

6.6.3 NAT

6.6.3.1 NAT

On this WBM page, you specify the basic settings for NAT.

Network Address Translation (NAT) Protocol

NAT | Static | Pool | NAPT

NAT

Idle Timeout[s]:

TCP Timeout[s]:

UDP Timeout[s]:

Interface Configuration

Interface: ▼

NAT

NAPT

Interface	NAT	NAPT
vlan1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

1 entry.

Description

The page contains the following boxes:

- **NAT**
Enable or disable NAT/NAPT for the entire device. When enabled, the device operates as a NAT router.
- **Idle Timeout[s]**
Enter the required time. The device checks cyclically after the set period has elapsed whether the aging time of TCP and UDP connections has elapsed. The connections whose aging time has elapsed since the last check are deleted from the table "NAT Translations".
- **TCP Timeout[s]**
Enter the required aging time for TCP connections. TCP connections are stored until no data exchange has taken place for the set period. Depending on the cyclic check when the Idle Timeout has elapsed, the connections are deleted from the table "NAT translations".
- **UDP Timeout[s]**
Enter the required aging time for UDP connections. UDP connections are stored until no data exchange has taken place for the set period. Depending on the cyclic check when the Idle Timeout has elapsed, the connections are deleted from the table "NAT translations".
- **Interface**
Select an IP interface from the drop-down list on which you want to configure NAT. As soon as you have configured an interface as a NAT interface, all other configurations are considered starting from this interface. This means for this interface that all networks reachable via the interface itself count as "Outside". All other networks are "Inside".

Note

If you have configured several NAT interfaces on a device, this means that a network is "Outside" from the perspective of one NAT interface and "Inside" from the perspective of another NAT interface.

- **NAT**
Enable or disable NAT for an IP interface.
An entry is created automatically in the "Pool" tab. The device can be reached from the external network using the IP address of the IP interface.
If you disable NAT for an IP interface and there are no configurations on the NAT interface, the entry is automatically deleted from the table.
- **NAPT**
Enable or disable NAPT for an IP interface.

6.6 The "Layer 3" menu

The table has the following columns:

- **Interface**
Interface on which there is a NAT configuration.
- **NAT**
Shows whether NAT is enabled or disabled for the selected IP interface.
NAT is only enabled when you have enabled NAT for the entire device.
- **NAPT**
Shows whether NAPT is enabled or disabled for the selected IP interface.
NAPT is only enabled when you have enabled NAT for the entire device.
If you do not create any further configurations for NAPT, the dynamic port translation is enabled automatically.
As default, a device in the internal network cannot be reached from an external network. If the internal device wants to communicate in an external network, the inside local address and the IP address of the IP interface have a port added and the internal device is assigned as inside local and inside global address. Using this inside global address, the internal device can be reached from the external network until the timer of the connection elapses.

Procedure

To configure NAT/NAPT, do the following:

1. Enter the required times.
2. Select the required IP interface.
3. Enable NAT/NAPT for the selected IP interface.
4. Click the "Set Values" button.
5. Make the settings you require for NAT/NAPT in the NAT/NAPT tabs.
6. Select the "NAT" check box in this tab.
7. Click the "Set Values" button.

6.6.3.2 Static

On this WBM page, you configure static 1:1 address translations.

You specify which inside global address the inside local address of a device will be converted to and vice versa. This variant allows connection establishment in both directions. The device in the internal network can be reached from the external network.

Network Address Translation (NAT) Static Configuration

NAT
Static
Pool
NAPT

Interface: vlan1 ▼

Inside Local Address:

Inside Global Address:

	Interface	Inside Local Address	Inside Global Address
<input type="checkbox"/>	vlan1	192.168.16.155	192.168.16.60

1 entry.

Create
Delete
Refresh

Description

The page contains the following boxes:

- **Interface**
Select the a NAT interface from the drop-down list for which you want to create further NAT configurations.
- **Inside Local Address**
Enter the actual address of the device that should be reachable from external.
- **Inside Global Address**
Enter the address at which the device can be reached from external.

The table has the following columns:

- **1st column**
Select the check box in the row to be deleted.
- **Interface**
NAT interface to which the setting relates.
- **Inside Local Address**
Shows the actual address of the device that should be reachable from external.
- **Inside Global Address**
Shows the address at which the device can be reached from external.

Procedure

To create a 1:1 address translation, proceed as follows:

1. Select the a NAT interface from the "Interface" drop-down list:
2. In "Inside Local Address" enter the actual address of the device that should be reachable from external.
3. In "Inside Global Address" enter the address at which the device can be reached from external.

6.6.3.3 Pool

On this WBM page, you configure dynamic address translations.

As default, a device in the internal network cannot be reached from an external network. If the internal device wants to communicate in an external network, an inside global address is assigned to it dynamically. Using this inside global address, the internal device can be reached from the external network until the timer of the connection elapses.

Network Address Translation (NAT) Pool Configuration

NAT Static Pool NAPT

Interface:

Inside Global Address:

Inside Global Address Mask:

	Interface	Inside Global Address	Inside Global Address Mask
<input type="checkbox"/>	vlan1	192.168.16.155	255.255.255.255

1 entry.

Description

The page contains the following boxes:

- **Interface**
Select the a NAT interface from the drop-down list for which you want to create further NAT configurations.
- **Inside Global Address**
Enter the start address for the dynamic assignment of addresses at which devices will be reachable from external.

Note

The address range for the dynamic address translation cannot contain any global IP address.

- **Inside Global Address Mask**
Enter the address mask of the external subnet.

The table has the following columns:

- **1st column**
Select the check box in the row to be deleted.
- **Interface**
NAT interface to which the setting relates.

- **Inside Global Address**
Shows the start address for the dynamic assignment of addresses at which devices will be reachable from external.
- **Inside Global Address Mask**
Shows the address mask of the external subnet.

Procedure

To create a dynamic address translation, proceed as follows:

1. Select the a NAT interface from the "Interface" drop-down list:
2. In "Inside Global Address" enter the start address for the dynamic assignment of addresses at which devices will be reachable from external.
3. In "Inside Global Address Mask" enter the address mask of the external subnet.

6.6.3.4 NATP

On this WBM page, you configure static port translations.

Network Address Port Translation (NAPT)

NAT Static Pool NAPT

Interface: vlan1

Inside Local Address:

Service: -

Start Port:

End Port:

Inside Global Port:

Protocol: TCP

Description:

	Interface	Inside Local Address	Start Port	End Port	Protocol	Inside Global Address	Inside Global Port	Description
<input type="checkbox"/>	vlan1	192.168.16.152	53	53	TCP	192.168.16.155	53	DNS

1 entry.

Create Delete Refresh

Description

The page contains the following boxes:

- **Interface**
Select the a NAT interface from the drop-down list for which you want to create further NAT configurations.
- **Inside Local Address**
Enter the actual address of the device that should be reachable from external.
- **Service**
Select the service for which the port translation is valid.
When you select a service, the same port is entered in the Start Port and End Port boxes. If you change the start port, the end port is changed accordingly.
if you select the entry "-", you can enter the start and end port freely.

- **Start Port**
Enter an inside local port.
- **End Port**
Depending on your selection in the "Service" drop down list, you can enter a inside local port or a port is displayed.
If you enter different ports in the Start Port and End Port boxes, the same port range is entered in the Inside Global Port box. A port range can only be translated to the same port range.
If you enter the same port in the Start Port and End Port boxes, you can enter any Inside Global Port.
- **Inside Global Port**
Depending on your selection in the "Service" drop down list, you can enter a port or a port is displayed.
- **Protocol**
Select the protocol for which the port translation is valid.
- **Description**
Enter a description for the port translation.

The table has the following columns:

- **1st column**
Select the check box in the row to be deleted.
- **Interface**
NAT interface to which the setting relates.
- **Inside Local Address**
Shows the actual address of the device that should be reachable from external.
- **Start Port**
Shows the start port that will be assigned to the inside local address.
- **End Port**
Shows the end port that will be assigned to the inside local address.
- **Protocol**
Shows the protocol for which the port translation is valid.
- **Inside Global Address**
Shows the address at which the device can be reached from external.
- **Inside Global Port**
Shows the port that will be assigned to the Inside Global Address.
- **Description**
Shows a description for the port translation.

Procedure

To create a static port translation, proceed as follows:

1. Select the a NAT interface from the "Interface" drop-down list:
2. In "Inside Local Address" enter the actual address of the device that should be reachable from external.
3. Select a service.

4. Depending on your selection in the "Service" drop-down list specify the start, end and inside global port.
5. Select a protocol.
6. Enter a description for the port translation.

6.6.4 Static Routes

Static route

On this page, you create the static IPv4 routes.

Static Routes

Destination Network:

Subnet Mask:

Gateway:

Gateway must be 0.0.0.0 for sink route configuration

Administrative Distance:

Select	Destination Network	Subnet Mask	Gateway	Interface	Administrative Distance	Status
<input type="checkbox"/>	100.10.0.0	255.255.0.0	sink		not used	active
<input type="checkbox"/>	192.168.177.0	255.255.255.0	192.168.200.254		255	inactive

2 entries.

Description

The page contains the following boxes:

- **Destination Network**
Enter the network address of the destination that can be reached via this route.
- **Subnet Mask**
Enter the corresponding subnet mask.
- **Gateway**
Enter the IPv4 address of the gateway via which this network address is reachable.
- **Administrative Distance**
Enter the administrative distance for the route. The administrative distance corresponds to the quality of a connection, based for example on speed or costs. If there are several equal routes, the route with the lowest value is used.
As default -1 is set. This setting means that the metric is not set.
Range of values: 1 - 255. Here, 1 is the value for the best possible route. The higher the value, the longer packets require to their destination.

The table has the following columns:

- **Select**
Select the row you want to delete.
- **Destination Network**
Shows the network address of the destination.
- **Subnet Mask**
Shows the corresponding subnet mask.
- **Gateway**
Shows the IPv4 address of the next gateway.
- **Interface**
Shows the interface of the route.
- **Administrative Distance**
Enter the administrative distance for the route. When creating the route, "not used" is entered automatically (value -1). The administrative distance corresponds to the quality of a connection, based for example on speed or costs. If there are several equal routes, the route with the lowest value is used.
Range of values: 1 - 255
- **Status**
Shows whether or not the route is active.

Configuration procedure

1. Enter the network address of the destination in the "Destination Network" input box.
2. Enter the corresponding subnet mask in the "Subnet Mask" input box.
3. Enter the gateway in the "Gateway" input box.
4. Enter the weighting of the route in "Administrative Distance".
5. Click the "Create" button. A new entry is generated in the table.
6. Click the "Set Values" button.

6.6.5 Route Maps

6.6.5.1 General

Route Maps

With route maps, you control how routing information is further processed. You can filter routing information and specify whether the information is further processed, modified or discarded.

Route maps operate according to the following principle:

- Routing information is compared with the filters of the route maps.
- The comparison is continued until the filters of a route map match the properties of an item of information.
- The information is then processed according to the route map settings:
 - The routing information is discarded.
 - The properties of the routing information are changed.

Settings

Route Maps General

General
Interface&Value Match
Source Match
Destination Match
Next Hop Match
Set

Name:

Sequence Number:

Select	Name	Sequence Number	Action
<input type="checkbox"/>	Map1	1	permit <input style="width: 20px;" type="text" value="v"/>
<input type="checkbox"/>	Map2	10	permit <input style="width: 20px;" type="text" value="v"/>

2 entries.

Create
Delete
Set Values
Refresh

Figure 6-1 Route maps general

- **Name**
Enter a name for the route map.
- **Sequence Number**
Enter a number for the route map.
You can create several route maps with the same name but with different sequence numbers. The sequence numbers then specify the order in which the route maps are processed.

The table has the following columns:

- **Select**
Select the row you want to delete.
- **Name**
Shows the name of the route map.

- **Sequence Number**
Shows the sequence number of the route map.
- **Action**
Specify what happens to the routing information that matches the settings of the route map:
 - permit
The routing information is further processed according to the settings you make in the "Set" tab.
 - deny
The routing information is discarded.

6.6.5.2 Interface & Value Match

On this page, you specify whether routing information for a route map is filtered according to interfaces, metric or tags.

Settings

Route Maps Interface&Value Match

General
Interface&Value Match
Source Match
Destination Match
Next Hop Match
Set

Route Map (Name/Seq.No.): ▼

Type: ▼

Interface: ▼

Metric:

Tag:

Route Type: ▼

Metric Type: ▼

Select	Type	Value
<input type="checkbox"/>	interface	vlan2

1 entry.

Figure 6-2 Filtering route maps interface and metric

- **Route Map (Name/Seq. No.)**
Select a route map.
The created route maps are available to you.
- **Type**
Select the basis for the filtering:
 - Interface
 - Metric
 - Tag
 - Route Type
 - metric type
- **Interface**
Select an interface.
This box is active only if you have selected the "Interface" entry in the "Type" drop-down list.
- **Metric**
Enter a value for the metric.
This box is active only if you have selected the "Metric" entry in the "Type" drop-down list.
- **Tag**
Enter a value for the tag.
This box is active only if you have selected the entry "Tag in the "Type" drop-down list.
- **Route Type**
Select the type of the route.
 - Local
The routing information for the route map is filtered according to directly connected routes (local interfaces).
 - Remote
The routing information for the route map is filtered according to learned or statically configured routes.

This box is active only if you have selected the entry "Route Type in the "Type" drop-down list.
- **metric type**
Select the type of the metric.
 - inter-area
The routing information for the route map is filtered according to routes learned from other areas.
 - intra-area
The routing information for the route map is filtered according to routes originating from the same area.
 - type-1-external
The routing information for the route map is filtered according to routes whose path costs (metric) are made up of the external path costs and the path costs to the ASBR.
 - type-2-external
The routing information for the route map is filtered according to routes with only external path costs (metric).

This box is active only if you have selected the entry "Metric Type" in the "Type" drop-down list.

The table has the following columns:

- **Select**
Select the row you want to delete.
- **Type**
Shows the selected type:
 - Interface
 - Metric
 - Tag
 - Route Type
 - metric type
- **Value**
Shows the selected interface or the value of the metric or of the tag.

6.6.5.3 Filtering the source

On this page, you specify whether or not the routing information for a route map is filtered based on the source IP address.

Settings

Figure 6-3 Route Maps Source Match

- **Route Map (Name/Seq. No.)**
Select a route map.
- **IP Address**
Enter the network address or the IP address of the source on which the filtering is based.
- **Subnet Mask**
Enter the subnet mask of the source on which the filtering is based.

The table has the following columns:

- **Select**
Select the row you want to delete.
- **IP Address**
Shows the IP address of the source.
- **Subnet Mask**
Shows the subnet mask of the source.

6.6.5.4 Destination Match

On this page, you specify whether the routing information for a route map is filtered based on the destination IPv4 address.

Settings

Figure 6-4 Route Maps Destination Match

- **Route Map (Name/Seq. No.)**
Select a route map.
- **IP Address**
Enter the network address of the destination on which the filtering is based.
- **Subnet Mask**
Enter the subnet mask of the destination on which the filtering is based.

The table has the following columns:

- **Select**
Select the row you want to delete.
- **IP Address**
Shows the IPv4 address of the destination.
- **Subnet Mask**
Shows the subnet mask of the destination.

6.6.5.5 Next Hop Match

On this page, you specify whether the filtering for a route map will be based on the router to which the routing information is sent next.

Settings

Figure 6-5 Route Maps Next Hop Match

- **Route Map (Name/Seq. No.)**
Select a route map.
- **IP Address**
Enter the IP address of the router to which the routing information will be sent next.

The table has the following columns:

- **Select**
Select the row you want to delete.
- **IP Address**
Shows the IP address of the next router.

6.6.5.6 Set

On this page, you specify whether or not the routing information will be changed by a route map.

You can only change the information of a "Permit" route map.

If, for example, you have filtered based on a certain metric, you can change the value of the metric here. The routing information is then forwarded with the new value.

Settings

Route Maps Set

General	Interface&Value Match	Source Match	Destination Match	Next Hop Match	Set
---------	-----------------------	--------------	-------------------	----------------	-----

Route Map (Name/Seq.No.):

Select	Name	Sequence Number	Metric	Tag
<input type="checkbox"/>	Map2	10	0	0

1 entry.

- **Route Map (Name/Seq. No.)**

Select a route map.

The table has the following columns:

- **Select**

Select the row you want to delete.

- **Name**

Shows the name of the route map.

- **Sequence Number**

Shows the sequence number of the route map.

- **Metric**

Enter the new value for the metric with which the routing information will be forwarded.

- **Tag**

Enter the new value for the tag with which the routing information will be forwarded.

6.6.6 DHCP Relay Agent

6.6.6.1 General

DHCP Relay Agent

If the DHCP server is in a different network from the DHCP client, the client cannot reach the server. The DHCP relay agent intercedes between the DHCP server and DHCP client.

If you configure option 82, the DHCP Relay Agent expands the packets to the DHCP server by a circuit ID and a remote ID.

You can specify up to 4 DHCP servers for the DHCP Relay Agent. If a DHCP server is unreachable, the device can switch to a different DHCP server.

Dynamic Host Configuration Protocol (DHCP) Relay Agent General

General | Option

DHCP Relay Agent

Send Option 82

Common Agent Address

Common Agent Interface: **vlan13** ▼

Server IP Address:

Select	Server IP Address
<input type="checkbox"/>	1.1.1.10

1 entry.

Description of the displayed values

The page contains the following boxes:

- **DHCP Relay Agent**
Enable or disable the DHCP Relay Agent.
- **Send Option 82**
Enable or disable option 82.
- **Common Agent Address**
Enable or disable the common agent address.
When the function is activated, in the DHCP request, the relay agent replaces the address of the receiving port with the address of the interface that you configure in "Common Agent Interface".
- **Common Agent Interface**
The relay agent uses the IP address of the interface selected here as the source address (giaddr) in DHCP requests.
- **Server IP address**
Enter the IPv4 address of the DHCP server.

The table has the following columns:

- **Select**
Select the row you want to delete.
- **Server IP Address**
Shows the IPv4 address of the DHCP server.

Steps in configuration

1. Enter the IPv4 address of the DHCP server in the "Server IP Address" input box.
2. Click the "Create" button. A new entry is generated in the table.

3. Select the "DHCP Relay Agent" check box.
4. Select the "Send Option 82" check box.
5. Click the "Set Values" button.

6.6.6.2 Option

Parameters of the DHCP Relay Agent

On this page, you can specify parameters for the DHCP server, for example the circuit ID. The circuit ID describes the origin of the DHCP query, for example, which port received the DHCP query.

You specify the DHCP server in the "General" tab.

Dynamic Host Configuration Protocol (DHCP) Relay Agent Option

General | **Option**

Global configuration

Circuit ID Router Index

Circuit ID Receive VLAN ID

Circuit ID Receive Port

Remote ID: 00-5e-1d-d2-76-00

Interface specific configuration

Interface: vlan2

Select	Interface	Remote ID Type	Remote ID	Circuit ID Type	Circuit ID	Status
<input type="checkbox"/>	vlan1	IP Address	192.168.16.155	Predefined	-	<input checked="" type="checkbox"/>

1 entry.

Create Delete Set Values Refresh

Description of the displayed values

The page contains the following boxes:

Global configuration

- **Circuit ID router index**
Enable or disable the check box. If you enable the check box, the router-Index is added to the generated circuit ID.
- **Circuit ID Receive VLAN ID**
Enable or disable the check box. If you enable the check box, the VLAN ID is added to the generated circuit ID.

- **Circuit ID Receive Port**
Enable or disable the check box. If you enable the check box, the receiving port is added to the generated circuit ID.

Note

You need to select a least one option.

You will find further information on the router index (Circuit ID Router Index) and port index (Circuit ID Receive Port) in the IfTable using SNMP.

You will find the VLAN ID on the WBM page "Layer 2 > VLAN > General".

- **Remote ID**
Shows the device ID.

Interface-specific configuration

- **Interface**
Select the interface from the drop-down list.

The table has the following columns:

- **Select**
Select the row you want to delete.
- **Interface**
Shows the interface.
- **Remote ID Type**
Select the type of device ID from the drop-down list. You have the following options:
 - IP Address
The IPv4 address of the device is used as the device ID.
 - MAC Address
The MAC address of the device is used as the device ID.
 - Free Text
If you use "Free Text", you can enter the device name as the device identifier in "Remote ID".
- **Remote ID**
Enter the device name. The box can only be edited if you select the entry "Free Text" for "Remote ID Type".
- **Circuit ID Type**
Select the type of circuit ID from the drop-down list. You have the following options:
 - Predefined
The circuit ID is created automatically based on the router index, VLAN ID or port.
 - Free Number
If you use "Free Number", you can enter the ID for "Circuit ID".

- **Circuit ID**
Enter the circuit ID. The box can only be edited if you select the "Free Number" entry for the "Circuit ID Type".
- **Status**
When the check box is selected, the DHCP Relay Agent for the corresponding interface is enabled. When a new row is created in the table, the DHCP Relay Agent is enabled by default.

Configuration procedure

Follow the steps below to specify the parameters manually:

1. Enable the required option in "Global configuration".
 - Circuit ID Router Index
 - Circuit ID Receive VLAN ID
 - Circuit ID Receive Port
2. Click the "Set Values" button.
3. Select the interface from the "Interface" drop-down list.
4. Click the "Create" button. A new row is inserted in the table.
5. Select the required entry from the "Remote ID Type" drop-down list.
 - IP Address
The IPv4 address is used as the device ID.
 - MAC Address
The MAC address is used as the device ID.
 - Free Text
Enter the device ID in "Remote ID".
6. Select the required entry from the "Circuit ID Type" drop-down list.
 - Predefined
The router index is added to the generated Circuit ID.
 - Free Number
Enter the ID in "Circuit ID".
7. Click the "Set Values" button.

6.6.7 VRRP

6.6.7.1 Router

Introduction

Using the "Create" button, you can create new virtual routers. A maximum of 52 Virtual routers can be configured. You can configure other parameters on the "Configuration" tab.

Note

- This function is available only with layer 3.
- Select the "VRRP" check box to configure VRRP.
- Simultaneous operation of VRRP and VRRPv3 is not possible.
- You can only use VRRP in conjunction with VLAN interfaces. Router ports are not supported.

Virtual Router Redundancy Protocol (VRRP) Router

Router | **Configuration** | Addresses Overview | Addresses Configuration | Interface Tracking | Address Tracking

VRRP
 Reply to pings on virtual interfaces
 ARP Sync
 VRID-Tracking

Interface: vlan1

VRID:

Select	Interface	VRID	Virtual MAC Address	Primary IP Address	Router State	Master IP Address	Priority	Advert. Interval	Preempt
<input type="checkbox"/>	vlan1	7	00-00-5e-00-01-07	0.0.0.0	Master	192.168.16.155	255	1	yes

1 entry.

Description of the displayed values

The page contains the following boxes:

- **VRRP**
Enable or disable the virtual redundant router protocol (VRRP).
- **Reply to pings on virtual interfaces**
When this is enabled, the router also responds to ping requests from virtual interfaces.
- **ARP Sync**
When this is enabled, the ARP table is synchronized with subordinate routers.

- **VRID-Tracking**
Enable or disable VRID tracking.

Note

You cannot select the "VRID-Tracking" check box when the "Master" check box is selected in the "Configuration" tab.

When enabled, all VRRP instances are monitored. If the status of a VRRP instance changes to "Initialize", the priority of all VRRP instances is reduced to the value "1". If the status of the VRRP instance changes, the original priority of all VRRP instances is restored.

- **Interface**
Select the VLAN Interface that functions as the virtual router from the drop-down list.
- **VRID**
Enter the ID of the virtual router in the input box. This ID defines the group of routers that form a virtual router (VR). In the group, this is the same. It can no longer be used for other groups.
Valid values are 1.. 255.

The table has the following columns:

- **Select**
Select the row you want to delete.
- **Interface**
Shows the interface that functions as the virtual router.
- **VRID**
Shows the ID of the virtual router.
- **Virtual MAC Address**
Shows the virtual MAC address of the virtual router.
- **Primary IP Address**
Shows the numerically lowest IPv4 address in this VLAN. The entry 0.0.0.0 means that the "Primary" address on this VLAN is used. Otherwise all IPv4 addresses configured on this VLAN in the "Layer 3 (IPv4) > Subnets" menu are valid values.
- **Router State**
Shows the current status of the virtual router. Possible values are:
 - Master
The router is the Master router and handles the routing functionality for all assigned IP addresses.
 - Backup
The router is the backup router. If the master router fails, the backup router takes over the tasks of the master router.
 - Initialize
The virtual router has just been turned on. It will soon change to the "Master" or "Backup" state.
- **Master IP Address**
Shows the IPv4 address of the master router.

- **Priority**
Shows the priority of the virtual router.
Valid values are 1-254.
If an IPv4 address is assigned to the VRRP router that is also actually configured on the local IPv4 interface, the value 255 is entered automatically. All other priorities can be distributed freely among the VRRP routers. The higher the priority, the earlier the VRRP router becomes "Master".
- **Advert. Interval**
Shows the interval at which the master router sends VRRP packets.
- **Preempt**
Shows the precedence of a router when changing roles between backup and master.
 - yes
This router has precedence when changing roles.
 - no
This router does not have precedence when changing roles.

VRRP and DHCP server

If you want to operate a DHCP server on the devices of a VRRP group, the DHCP server must be configured on the master router. Backup routers do not react to DHCP queries. Make sure that the master router is statically configured and that after a failure, becomes the master of the VRRP group again.

Steps in configuration

1. Select the "VRRP" check box.
2. Select the required interface.
3. Enter the ID of the virtual router in the "VRID" input box.
4. Click the "Create" button. A new row is inserted in the table.
5. Select the "Reply to pings on virtual interfaces" check box so that virtual addresses reply to pings as well.
6. Select the "VRID Tracking" check box to monitor the VRID.
7. Click the "Set Values" button. To configure the virtual router, click on the "Configuration" tab.

6.6.7.2 Configuration

Introduction

On this page, you configure the virtual router.

Note

This function is available only with layer 3.

Virtual Router Redundancy Protocol (VRRP) Configuration

Router	Configuration	Addresses Overview	Addresses Configuration	Interface Tracking	Address Tracking
--------	---------------	--------------------	-------------------------	--------------------	------------------

Interface / VRID:

Primary IP Address:

Master

Priority:

Advertisement Interval[s]:

Preempt lower priority Master

Track Id:

Decrement Priority:

Current Priority:

Description of the displayed values

The page contains the following boxes:

- **Interface / VRID**
Select the ID of the virtual router you are configuring from the drop-down list.
- **Primary IP Address**
Select the numerically lowest IPv4 address from the drop-down list: If the router becomes master router, the router uses this IPv4 address.

Note

If you only configure one subnet on this VLAN, no entry is necessary. The entry is then 0.0.0.0.

If you configure more than one subnet on the VLAN and you want a specific IPv4 address to be used as the source address for VRRP packets, select the IPv4 address from the drop-down list. Otherwise, the numerically lowest IPv4 address will be used.

- **Master**
If this option is enabled, the numerically lowest IPv4 address is entered for "Associated IP Address". This means that the highest priority IPv4 address of the VRRP router is used as the virtual IPv4 address of the virtual master router. The option must be disabled for the backup routers in this group and the IP address of the router in "Associated IP address" must be used.

Note

When you select the "Master" check box, the "Preempt lower priority Master" check box is also selected automatically. Furthermore, the "VRID Tracking" check box cannot be selected in the "Router" tab.

6.6 The "Layer 3" menu

- **Priority**
Enter the priority of this virtual router. Valid values are 1-254.
If an IPv4 address is assigned to the VRRP router that is also actually configured on the local IPv4 interface, the value 255 is entered automatically. All other priorities can be distributed freely among the VRRP routers. The higher the priority, the earlier the VRRP router becomes "Master".
- **Advertisement Interval**
Enter the interval in seconds after which a master router sends a VRRP packet again.
- **Preempt lower priority Master**
Allow the precedence when changing roles between backup and master based on the selection process.
- **Track ID**
Select a track ID.
- **Decrement Priority**
Enter the value by which the priority of the VRRP interface will be reduced.
- **Current Priority**
Shows the priority of the VRRP interface after the monitored interface has changed to the "down" status.

Steps in configuration

To configure a virtual router as the master router, follow the steps below:

1. Select the ID of the virtual router you want to configure from the "Interface / VRID" drop-down list.
2. Select the source address from the "Primary IP Address" drop-down list.
3. Select the "Master" check box.
4. From the "Priority" drop-down list, enter the priority of this virtual router.
5. Enter the interval in "Advertisement Interval".
6. Select the "Preempt lower priority Master" check box.
7. Select a track ID.
8. Value by which the priority of the VRRP interface will be reduced
9. Click the "Set Values" button.

6.6.7.3 Addresses Overview

Overview

This page shows which IPv4 addresses the virtual router monitors. Each virtual router can monitor a maximum of 10 IPv4 addresses.

Note

This function is available only with layer 3.

Virtual Router Redundancy Protocol (VRRP) Associated IP Addresses Overview							
Router	Configuration	Addresses Overview	Addresses Configuration	Interface Tracking	Address Tracking		
Interface	VRID	Number of Addresses	Associated IP Address (1)	Associated IP Address (2)	Associated IP Address (3)	Associated IP Address (4)	
vian1	7	1	192.168.16.155				

Description of the displayed boxes:

The table has the following columns:

- **Interface**
Shows the interface that functions as the virtual router.
- **VRID**
Shows the ID of this virtual router.
- **Number of addresses**
Shows the number of IPv4 addresses.
- **Assigned IP address (1) ... Assigned IP address (10)**
Shows the router IPv4 addresses monitored by this virtual router. If a router takes over the role of master, the routing function is taken over by this router for all these IPv4 addresses.

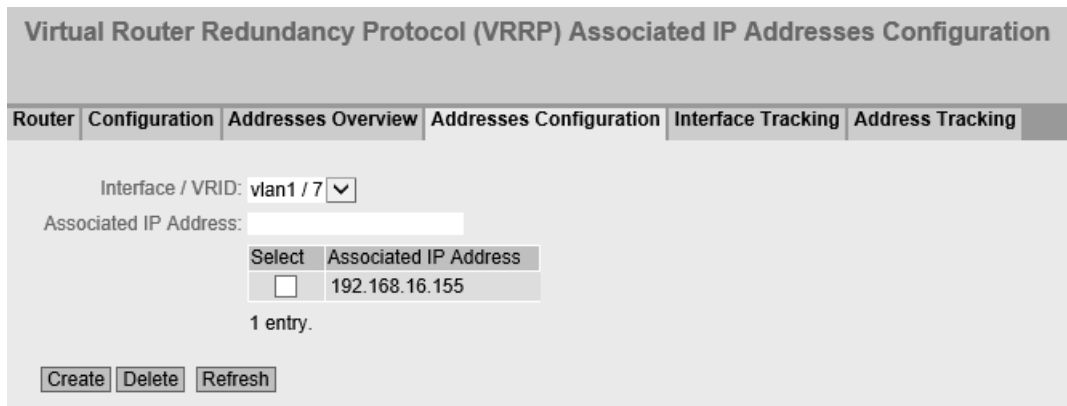
6.6.7.4 Address Configuration

Creating or changing the monitored IPv4 addresses

On this page, you can create, modify or delete the IPv4 addresses to be monitored. A maximum of 10 IPv4 addresses can be monitored by a virtual router.

Note

This function is available only with layer 3.



Description of the displayed values

The page contains the following boxes:

- **Interface / VRID**
Select the virtual router from the drop-down list.
- **Associated IP address**
Enter the IPv4 address that the virtual router will monitor.
A maximum of 10 IPv4 addresses are possible.

The table has the following columns:

- **Select**
Select the row you want to delete.
- **Associated IP Address**
Shows the IPv4 addresses that the virtual router monitors.

Steps in configuration

1. Select the ID of the virtual router from the "Interface / VRID" drop-down list.
2. Enter the IPv4 address that the virtual router will monitor.
3. Click the "Create" button. A new entry is generated in the table.

6.6.7.5 Interface Tracking

Introduction

On this page, you configure the monitoring of interfaces.

When the link of a monitored interface changes from "up" to "down", the priority of the assigned VRRP interface is reduced. You configure the value by which the priority is reduced on the page "Layer 3 > VRRP/VRRPv3 > Configuration".

When the link of the interface changes back from "down" to "up", the original priority of the VRRP interface is restored.

Note

This function is available only with layer 3.

Virtual Router Redundancy Protocol (VRRP) Interface Tracking

Router	Configuration	Addresses Overview	Addresses Configuration	Interface Tracking	Address Tracking
--------	---------------	--------------------	-------------------------	--------------------	------------------

Interface: P0.1 ▼

Track Id:

Track Id: All ▼

Track Interface Count: 0

Select	Track Id	Interface
<input type="checkbox"/>	5	P0.1
<input type="checkbox"/>	5	P1.1

2 entries.

Create
Delete
Refresh

Description of the displayed values

The page contains the following boxes:

- **Interface**
From the drop-down list, select the interface to be monitored.
- **Track ID**
Enter a track ID.
- **Track ID**
Select a track ID.
- **Track Interface Count**
Enter how many monitored interfaces need to change to the "down" status, before the priority is changed.

The table has the following columns:

- **Select**
Select the check box in the row to be deleted.
- **Track ID**
Shows the track ID.
- **Interface**
Shows the interface that is being monitored.

Steps in configuration

1. Select the required interface from the "Interface" drop-down list.
2. In the "Track ID" box, enter the required ID.
3. Click the "Create" button.
4. Select an ID from the "Track ID" drop-down list.
5. In the "Track Interface Count" enter the number of interfaces.
6. Click the "Set Values" button.
7. Link the monitoring to a VRRP interface in the "Configuration" tab.

6.6.7.6 Address Tracking

Tracking of IP addresses

You configure the tracking of IP addresses on this page. The router sends a ping request to each of the configured IP addresses within the specified time period. If no response is received within a specified time period, the VRRP priority of the corresponding interface is reduced.

Note

This function is available only with layer 3.

Virtual Router Redundancy Protocol (VRRP) Address Tracking

Router	Configuration	Addresses Overview	Addresses Configuration	Interface Tracking	Address Tracking
--------	---------------	--------------------	-------------------------	--------------------	------------------

Track Id:

IP Address:

Select	Track Id	IP Address	Ping Period[s]	Ping Timeout [s]
<input type="checkbox"/>	17	192.168.16.172	5	15
<input type="checkbox"/>	45	192.168.16.199	5	15

2 entries.

Create
Delete
Set Values
Refresh

Description

The page contains the following boxes:

- **Track ID**
Enter the track ID.
- **IP Address**
Enter the IP address to be tracked. You can enter a maximum of five IP addresses.

The table has the following columns:

- **Select**
Select the row you want to delete.
- **Track ID**
Shows the track ID.
- **IP Address**
Shows the IP address to be tracked.
- **Ping Period[s]**
Shows the cycle time in seconds between two ping requests.
- **Ping Timeout[s]**
Shows the time in seconds that the router waits for a ping response. The minimum duration is three times the ping period.

Configuration procedure

1. In the "Track ID" field, enter the required ID.
2. In the "IP Address" field, enter the IPv4 address that the virtual router is to track.
3. Click the "Create" button. A new entry is generated in the table.

6.6.8 VRRPv3

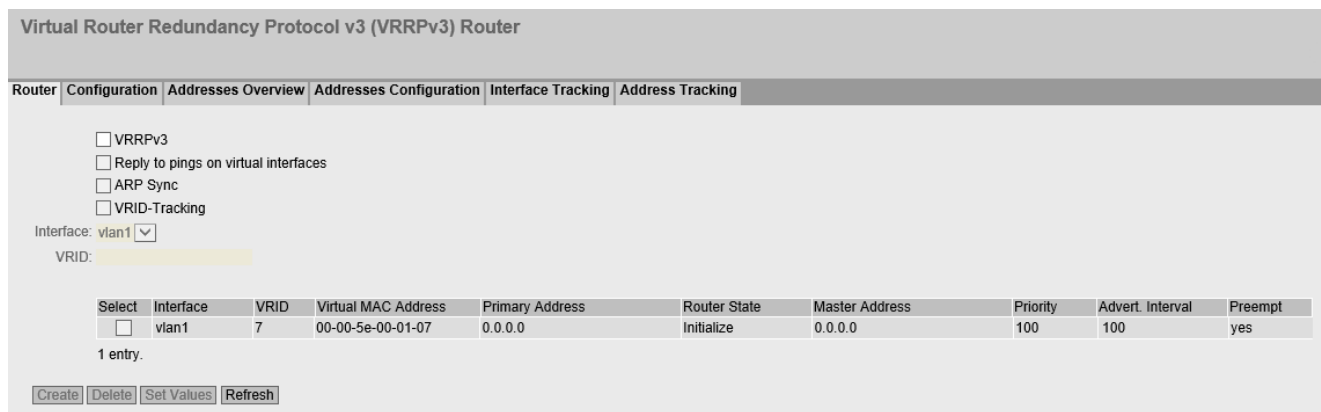
6.6.8.1 Router

Introduction

Using the "Create" button, you can create new virtual routers. A maximum of 52 Virtual routers can be configured. You can configure other parameters on the "Configuration" tab.

Note

- This function is available only with layer 3.
 - Simultaneous operation of VRRP and VRRPv3 is not possible.
 - Select the "VRRPv3" check box to configure VRRPv3.
 - You can use VRRPv3 on VLAN interfaces. Router ports are not supported.
-



Description

The page contains the following:

- **VRRPv3**
Enable or disable the virtual redundant router protocol (VRRPv3).
- **Reply to pings on virtual interfaces**
When this is enabled, the router also responds to ping requests from virtual interfaces.
- **ARP Sync**
When this is enabled, the ARP table is synchronized with subordinate routers.
- **VRID-Tracking**
Enable or disable VRID tracking.
When enabled, all VRRP instances are monitored. If the status of a VRRP instance changes to "Initialize", the priority of all VRRP instances is reduced to the value "1".
If the status of the VRRP instance changes, the original priority of all VRRP instances is restored.
- **Interface**
Select the required VLAN interface operating as virtual router.
- **VRID**
Enter the ID of the virtual router. This ID defines the group of routers that form a virtual router (VR). In the group, this is the same. It can no longer be used for other groups.
Valid values are 1.. 255.

The table has the following columns:

- **Select**
Select the check box in the row to be deleted.
- **Interface**
Shows the Interface that functions as the virtual router.
- **VRID**
Shows the ID of the virtual router.
- **Virtual MAC Address**
Shows the virtual MAC address of the virtual router.

- **Primary IP Address**
Shows the numerically lowest IPv4 address in this VLAN. The entry 0.0.0.0 means that the "Primary" address on this VLAN is used. Otherwise all IPv4 addresses configured on this VLAN in the "Layer 3 (IPv4) > Subnets" menu are valid values.
- **Router State**
Shows the current status of the virtual router. Possible values are:
 - Master
The router is the master router and handles the routing functionality for all assigned IPv4 addresses.
 - Backup
The router is the backup router. If the master router fails, the backup router takes over the tasks of the master router.
 - Initialize
The virtual router has just been turned on. It will soon change to the "Master" or "Backup" state.
- **Master IP Address**
Shows the IPv4 address of the master router.
- **Priority**
Shows the priority of the virtual router.
Valid values are 1-254.
If an IPv4 address is assigned to the VRRP router that is also actually configured on the local IPv4 interface, the value 255 is entered automatically. All other priorities can be distributed freely among the VRRP routers. The higher the priority, the earlier the VRRP router becomes "Master".
- **Advertisement Interval**
Shows the interval at which the master router sends VRRPv3 packets.
- **Preempt**
Shows the precedence of a router when changing roles between backup and master.
 - yes
This router has precedence when changing roles.
 - no
This router does not have precedence when changing roles.

VRRP and DHCP server

If you want to operate a DHCP server on the devices of a VRRP group, the DHCP server must be configured on the master router. Backup routers do not react to DHCP queries. Make sure that the master router is statically configured and that after a failure, becomes the master of the VRRP group again.

Steps in configuration

1. Select the "VRRPv3" check box.
2. Select the required interface.
3. Enter the ID of the virtual router in the "VRID" input box.

6.6 The "Layer 3" menu

4. Click the "Create" button. A new row is inserted in the table.
5. Select the "Reply to pings on virtual interfaces" check box so that virtual IPv4 addresses reply to pings as well.
6. Select the "VRID Tracking" check box to monitor the VRID.
7. Click the "Set Values" button. To configure the virtual router, click on the "Configuration" tab.

6.6.8.2 Configuration

Introduction

On this page, you configure the virtual router.

Note

This function is available only with layer 3.

Virtual Router Redundancy Protocol v3 (VRRPv3) Configuration

Router | **Configuration** | **Addresses Overview** | **Addresses Configuration** | **Interface Tracking** | **Address Tracking**

Interface / VRID:

Primary Address:

Master

Priority:

Advertisement Interval[cs]:

Preempt lower priority Master

VRRP Compatible Mode

Track Id:

Decrement Priority:

Current Priority:

Description

The page contains the following:

- **Interface / VRID**
Select the ID of the virtual router to be configured.
- **Primary Address**
Select the primary IPv4 address. If the router becomes master router, the router uses this IPv4 address.

Note

If you only configure one subnet on this VLAN, no entry is necessary. The entry is then 0.0.0.0.

If you configure more than one subnet on the VLAN and you want a specific IPv4 address to be used as the source address for VRRP packets, select the IPv4 address. Otherwise, the numerically lowest IPv4 address will be used.

- **Master**
If enabled, the numerically lowest IPv4 address is entered for "Associated IP Address". This means that the numerically lowest IPv4 address of the VRRPv3 router is used as the virtual IP address of the virtual master router. The backup routers in this group must disable the option and use the IPv4 address of the router in "Associated IP address".
- **Priority**
Enter the priority of this virtual router. Valid values are 1-254.
If an IPv4 address is assigned to the VRRPv3 router that is also actually configured on the local IPv4 interface, the value 255 is entered automatically. All other priorities can be distributed freely among the VRRPv3 routers. The higher the priority, the earlier the VRRPv3 router becomes "Master".
- **Advertisement interval**
Enter the interval in seconds after which a master router sends a VRRPv3 packet again.
- **Preempt lower priority Master.**
Allow precedence when changing roles between backup and master based on the selection process.
- **VRRP Compatible Mode**
When enabled, the VRRPv3 router sends and receives VRRPv2 packets in addition to VRRPv3 packets for configured IPv4 addresses. Only necessary when not all VRRP routers support VRRPv3.
- **Track ID**
Select a track ID.
- **Decrement Priority**
Enter the value by which the priority of the VRRPv3 interface will be reduced.
- **Current Priority**
Shows the priority of the VRRPv3 interface after the monitored interface has changed to the "down" status.

Steps in configuration

To configure a virtual router as the master router, follow the steps below:

1. Select the ID of the virtual router you want to configure from the "Interface / VRID" drop-down list.
2. Select the "Status" check box.
3. Select the source address from the "Primary Address" drop-down list.
4. From the "Priority" drop-down list, enter the priority of this virtual router.
5. Select the "Master" check box.
6. Enter the interval in "Advertisement Interval".
7. Select the "Preempt lower priority Master" check box.
8. Select the "VRRP Compatible Mode" check box.
9. Select a track ID.
10. Enter the value by which the priority of the VRRPv3 interface will be reduced
11. Click the "Set Values" button.

6.6.8.3 Addresses Overview

Overview

This page shows which IPv4 addresses the virtual router monitors. Each virtual router can monitor a maximum of 10 IPv4 addresses.

Note

This function is available only with layer 3.

Virtual Router Redundancy Protocol v3 (VRRPv3) Associated IP Addresses Overview							
Router	Configuration	Addresses Overview	Addresses Configuration	Interface Tracking	Address Tracking		
Interface	VRID	Number of Addresses	Associated IP Address (1)	Associated IP Address (2)	Associated IP Address (3)	Associated IP Address (4)	
vlan1	7	0	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	
<input type="button" value="Refresh"/>							

Description of the displayed values

The table has the following columns:

- **Interface**
Shows the Interface that functions as the virtual router.
- **VRID**
Shows the ID of this virtual router.

- **Number of Addresses**
Shows the number of IPv4 addresses.
- **Associated IP Address (1) ...Associated IP Address (10)**
Shows the router IPv4 addresses monitored by this virtual router. If a router takes over the role of master, the routing function is taken over by this router for all these IPv4 addresses.

6.6.8.4 Address Configuration

Creating or changing the monitored IP addresses

On this page, you can create, modify or delete the IPv4 addresses to be monitored. A maximum of 10 IPv4 addresses can be monitored by a virtual router.

Note

This function is available only with layer 3.

Virtual Router Redundancy Protocol v3 (VRRPv3) Associated IP Addresses Configuration

Router	Configuration	Addresses Overview	Addresses Configuration	Interface Tracking	Address Tracking
--------	---------------	--------------------	-------------------------	--------------------	------------------

Interface / VRID: ▼

Associated IP Address:

Select	Associated IP Address
<input type="checkbox"/>	192.168.16.140

1 entry.

Description

The page contains the following:

- **Interface / VRID**
Select the ID of the virtual router.
- **Associated IP Address**
Enter the IPv4 address that the virtual router will monitor.
A maximum of 10 IPv4 addresses are possible.

The table has the following columns:

- **Select**
Select the check box in the row to be deleted
- **Associated IP Address**
Shows the IPv4 addresses that the virtual router monitors.

Steps in configuration

1. Select the ID of the virtual router.
2. Enter the IPv4 address that the virtual router will monitor.
3. Click the "Create" button. A new entry is generated in the table.

6.6.8.5 Interface Tracking

Introduction

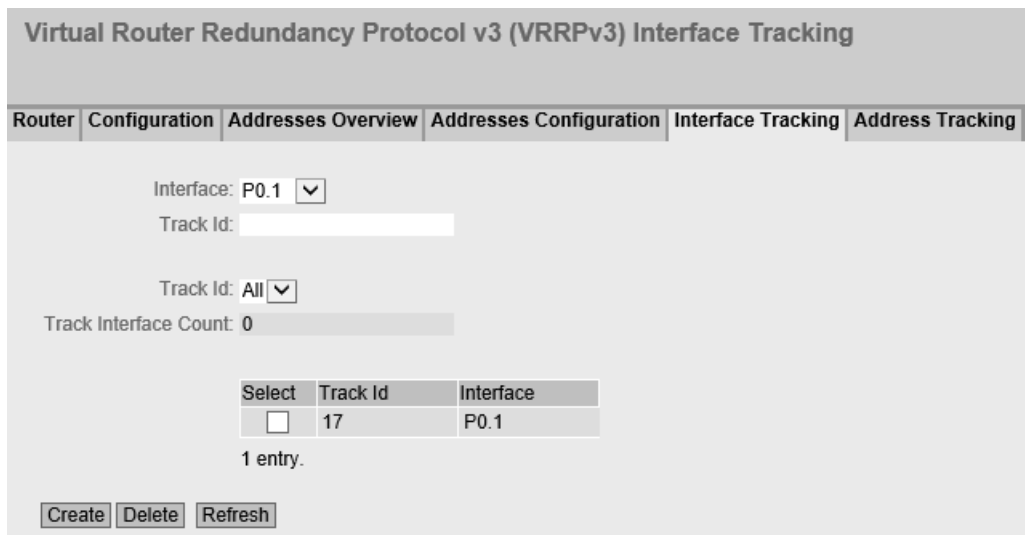
On this page, you configure the monitoring of interfaces.

When the link of a monitored interface changes from "up" to "down", the priority of the assigned VRRP interface is reduced. You configure the value by which the priority is reduced on the page "Layer 3 > VRRP/VRRPv3 > Configuration".

When the link of the interface changes back from "down" to "up", the original priority of the VRRP interface is restored.

Note

This function is available only with layer 3.



Description of the displayed values

The page contains the following boxes:

- **Interface**
From the drop-down list, select the interface to be monitored.
- **Track ID**
Enter a track ID.

- **Track ID**
Select a track ID.
- **Track Interface Count**
Enter how many monitored interfaces need to change to the "down" status, before the priority is changed.

The table has the following columns:

- **Select**
Select the check box in the row to be deleted.
- **Track ID**
Shows the track ID.
- **Interface**
Shows the interface that is being monitored.

Steps in configuration

1. Select the required interface from the "Interface" drop-down list.
2. In the "Track ID" box, enter the required ID.
3. Click the "Create" button.
4. Select an ID from the "Track ID" drop-down list.
5. In the "Track Interface Count" enter the number of interfaces.
6. Click the "Set Values" button.
7. Link the monitoring to a VRRP interface in the "Configuration" tab.

6.6.8.6 Address Tracking

Introduction

You configure the tracking of IP addresses on this page. The router sends a ping request to each of the configured IP addresses within the specified time period. If no response is received within a specified time period, the VRRP priority of the corresponding interface is reduced.

Note

This function is available only with layer 3.

Virtual Router Redundancy Protocol v3 (VRRPv3) Address Tracking

Router	Configuration	Addresses Overview	Addresses Configuration	Interface Tracking	Address Tracking
---------------	----------------------	---------------------------	--------------------------------	---------------------------	-------------------------

Track Id:

IP Address:

Select	Track Id	IP Address	Ping Period[s]	Ping Timeout [s]
<input type="checkbox"/>	17	192.168.16.172	5	15
<input type="checkbox"/>	45	192.168.16.199	5	15

2 entries.

Create
Delete
Set Values
Refresh

Description

The page contains the following boxes:

- **Track ID**
Enter the track ID.
- **IP Address**
Enter the IP address to be tracked. You can enter a maximum of five IP addresses.

The table has the following columns:

- **Select**
Select the row you want to delete.
- **Track ID**
Shows the track ID.
- **IP Address**
Shows the IP address to be tracked.
- **Ping Period[s]**
Shows the cycle time in seconds between two ping requests.
- **Ping Timeout[s]**
Shows the time in seconds that the router waits for a ping response. The minimum duration is three times the ping period.

Configuration procedure

1. In the "Track ID" field, enter the required ID.
2. In the "IP Address" field, enter the IPv4 address that the virtual router is to track.
3. Click the "Create" button. A new entry is generated in the table.

6.6.9 OSPFv2

6.6.9.1 Configuration

Introduction

On this page, you configure the routing using OSPFv2.

Note

This function is available only with layer 3.

Open Shortest Path First v2 (OSPFv2) Configuration

Configuration	Redistribution	Summary Address	Areas	Area Range	Interfaces	Interface Authentication	Virtual Links
Virtual Link Authentication							
<input checked="" type="checkbox"/> OSPFv2							
Router ID: <input type="text" value="192.168.16.100"/>				<input checked="" type="checkbox"/> OSPFv2 RFC1583 Compatibility			
Border Router: <input type="text" value="Not Area Border Router"/>							
New LSA Received: <input type="text" value="0"/>				New LSA Configured: <input type="text" value="46"/>			
External LSA Maximum: <input type="text" value="-"/>							
Exit Interval[s]: <input type="text" value="-"/>							
Inbound Filter: <input type="text" value="-"/> <input type="button" value="v"/>							
Protocol Preference							
Default Distance: <input type="text" value="119"/>							
Route Map Preference							
Distance Route Map: <input type="text" value="-"/> <input type="button" value="v"/>							
Distance: <input type="text" value=""/>							
<input type="button" value="Set Values"/> <input type="button" value="Refresh"/>							

Description of the displayed values

The page contains the following boxes:

- **OSPFv2**
Enable or disable routing using OSPFv2.
- **Router ID**
Enter the name of one of the OSPFv2 interfaces. The name is entered in the IP address format and does not need to match the local IP address. The router ID must be unique in the network.

- **OSPFv2 RFC1583 Compatibility**
In newer RFCs, the calculation of the shortest route to the destination is defined differently. If the option is enabled, the shortest path is also calculated via the backbone with the lowest path costs (metric). This ensures compatibility with older systems.
If the option is disabled, paths within an area are preferred, even if the metric is higher. The paths do not necessarily lead via the backbone.
- **Border Router**
Displays the status of the OSPFv2 router. If the local system is an active member in at least 2 areas, this is an area border router.
- **New LSA Received**
Shows the number of received LSAs.
Updates and its own LSAs are not counted.
- **New LSA Configured**
Shows the number of different LSAs sent by this local system.
- **External LSA Maximum**
To limit the number of entries of external LSAs in the database, enter the maximum number of external LSAs.
- **Exit Interval [s]**
Enter the interval after which the OSPFv2 router once again attempts to leave the overflow status. A 0 means that the OSPF router attempts to exit the overflow status only following a restart.
- **Inbound Filter**
Select a route map that filters inbound routes.
- **Protocol Preferences**
 - **Default Distance**
Set the administrative distance for the OSPFv2 protocol.
- **Route Map Preferences**
 - **Distance Route Map**
Select a route map from the drop-down list for which you want to specify the administrative distance.
 - **Distance**
Configure the administrative distance for the previously selected route map.

Configuration procedure

1. Select the "OSPFv2" check box.
2. Enter the ID of the router in the "Router ID" input box.
3. Select the "AS Border Router" check box.
4. Click the "Set Values" button.

6.6.9.2 Redistribution

Redistribute Routes

On this page, you configure the redistribution of routing information.

Note

This function is available only with layer 3.

Redistribution

Configuration | **Redistribution** | Summary Address | Areas | Area Range | Interfaces | Interface Authentication | Virtual Links

Virtual Link Authentication

AS Border Router

Redistribute Routes

Default

Connected

Static

RIP

Route Map:

Default Information Originate

Metric:

Metric Type:

Metric Configuration

Subnet Address:

Subnet Mask:

Select	Subnet Address	Subnet Mask	Metric	Metric Type
<input type="checkbox"/>	192.168.16.89	255.255.0.0	1	External type 1

1 entry.

Description

The page contains the following boxes:

- **AS Border Router**

Specify whether the router is an AS border router. An AS border router intercedes between multiple autonomous systems, for example if you have an additional RIP network. An AS border router is also necessary to add and to distribute static routes.

- **Redistribute Routes**

Specify which known routes are distributed using OSPFv2. The following settings are possible:

- Default

Note

The "Default" setting and the "Default Information Originate" check box cannot be activated at the same time.

- Connected
- Static
- RIP

Note

The options can only be enabled on an AS border router. Enabling the Default and Static options, in particular, can cause problems if they are enabled at too many points in the network, for example, forwarding loops.

- **Route Map**

Select a route map that filters which routes are forwarded using OSPFv2.

- **Default Information Originate**

Enables the "Metric" and "Metric type" fields.

Define whether a standard route is generated for external routes into the OSPF routing domain.

Note

The "Default Information Originate" check box cannot be selected if the "Default" setting is selected for "Redistribute Routes".

- **Metric**

If you enter metric information in this text box, the device becomes the default gateway for external routes in the OSPF routing domain.

Range of values: 1 ... 16777215

- **Metric Type**

This drop-down list is only active when a value is entered in the "Metric" text box. Select how the metric is calculated. You have the following options:

 - External type 1**

The sum of internal and external path costs.
 - External type 2**

Only external costs; the internal path costs are ignored.
- **Metric Configuration**

Configure the metric for forwarding routes of a subnet.

 - **Subnet Address**

The IPv4 address of the network whose routing information is to be forwarded.
 - **Subnet Mask**

The subnet mask of the network whose routing information is to be forwarded.

The table contains the following columns:

- **Select**

Select the row you want to delete.
- **Subnet Address**

Shows the IP address of the network whose routing information will be forwarded.
- **Subnet Mask**

Shows the subnet mask of the network whose routing information will be forwarded.
- **Metric**

The Metric for the subnet.
- **Metric Type**

Select how the metric is calculated. The following options are possible:

 - **External type 1**

The sum of internal and external path costs.
 - **External type 2**

Only external costs; the internal path costs are ignored.

Configuration procedure

1. Enter the IP address of the network whose routing information will be forwarded.
2. Enter the subnet mask of the network whose routing information will be forwarded.
3. Click the "Create" button. A new entry is generated in the table.
4. In the "Metric" column, enter the Metric for the subnet.
5. Select the suitable entry in the "Metric Type" column.
6. Click the "Set Values" button.

6.6.9.3 Summary Address

Subnets for routing information

On this page, you configure subnets for grouping routing information.

Note

This function is available only with layer 3.

Summary Address

Configuration | Redistribution | **Summary Address** | Areas | Area Range | Interfaces | Interface Authentication | Virtual Links

Virtual Link Authentication

Subnet Address:

Subnet Mask:

Area ID:

Select	Subnet Address	Subnet Mask	Area ID	Action	Translation
<input type="checkbox"/>	192.0.0.0	255.0.0.0	0.0.0.0	Allow All	<input checked="" type="checkbox"/>
<input type="checkbox"/>	192.0.0.1	255.0.0.0	2.2.2.2	Advertise	<input checked="" type="checkbox"/>

2 entries.

Description of the displayed boxes

- **Subnet Address**
The IPv4 address of the network whose routing information is to be forwarded.
- **Subnet Mask**
The subnet mask of the network whose routing information is to be forwarded.
- **Area ID**
The ID of the area to which the subnet is assigned.

The table contains the following columns:

- **Select**
Select the row you want to delete.
- **Subnet Address**
Shows the IP address of the network whose routing information will be forwarded.
- **Subnet Mask**
Shows the subnet mask of the network whose routing information will be forwarded.
- **Area ID**
The ID of the area to which the subnet is assigned.

- **Action**
The following settings are possible:
 - **Allow All**
This setting is only possible for the area ID 0.0.0.0. The backbone area generates an LSA message of type 5 for the address range and LSA messages of type 7 in the connected NSSAs.
 - **Deny All**
This setting is only possible for the area ID 0.0.0.0. No LSAs of type 5 or type 7 are generated for the address range.
 - **Advertise**
The address range is advertised outside the areas. If the area ID is 0.0.0.0, the router generates LSA messages of Type 5. If the area ID is not 0.0.0.0, the router generates LSA messages of Type 7.
 - **No Advertise**
If the area ID is 0.0.0.0, no LSA messages of type 5 will be generated. The NSSAs connected to the backbone area generate LSA messages of Type 7. If the area ID is not 0.0.0.0, no LSA messages of type 7 will be generated.
- **Translation**
If the check box is selected, LSAs (Link State Advertisement) at the NSSA border router will be translated.

6.6.9.4 Areas

Overview

An Autonomous System can be divided into smaller areas.

On this page, you can view, create, modify or delete the areas of the router.

Note

This function is available only with layer 3.

Open Shortest Path First v2 (OSPF v2) Areas

Configuration	Redistribution	Summary Address	Areas	Area Range	Interfaces	Interface Authentication	Virtual Links	Virtual Link Authentication
---------------	----------------	-----------------	-------	------------	------------	--------------------------	---------------	-----------------------------

Area ID:

Select	Area ID	Area Type	Summary	Metric	Updates	LSA Count	Area BR	AS BR
<input type="checkbox"/>	0.0.0.0	Backbone	No Summary	0	3	1	0	0
<input type="checkbox"/>	1.1.1.1	Normal	No Summary	0	3	0	0	0

2 entries.

Description of the displayed values

The page contains the following boxes:

- **Area ID**
Enter the identifier of the area. The database is synchronized for all routers of an area. The area identifier must be unique in the network.
The area identifier is a 32-bit number with the following format: x.x.x.x where x = 0 ... 255
The area identifier 0.0.0.0 is reserved for the backbone area and cannot be deleted.

This table contains the following columns:

- **Select**
Select the row you want to delete.
- **Area ID**
Shows the identifier of the area.
- **Area Type**
Select the area type in the drop-down list.
 - Standard
 - Stub
 - NSSA
- **Summary**
Specify whether summary LSAs are generated for this area.
 - Summary: Summary LSAs are generated and sent to the area.
 - No Summary: Summary LSAs are not generated and sent to the area.
- **Metric**
Displays the costs for the OSPFv2 interface.
- **Updates**
Shows the number of recalculations of the routing tables.
- **LSA Count**
Shows the number of LSAs in the database.
- **Area BR**
Shows the number of reachable area border routers (ABR) within this area.
- **AS BR**
Shows the number of reachable autonomous system border routers (ASBR) in this area.

Steps in configuration

1. Enter the ID for the area in the "Area ID" input box.
2. Click the "Create" button. A new entry is generated in the table.
3. Select the type of area, for example Stub in the "Area Type" drop-down list.
4. Select the "Summary LSA" entry in the "Summary" drop-down list.
5. Click the "Set Values" button.

6.6.9.5 Area Range

Creating a new OSPFv2 area range

Using the "Create" button in the "OSPFv2 Area Range" menu, up to four networks can be grouped together under one area ID. The method is used only with area border routers. This means that an area border router only advertises one route for grouped areas to the outside.

Note

This function is available only with layer 3.

Open Shortest Path First v2 (OSPF v2) Area Range

Configuration	Redistribution	Summary Address	Areas	Area Range	Interfaces	Interface Authentication	Virtual Links																		
Virtual Link Authentication																									
<div style="margin-bottom: 5px;">Area ID: <input type="text" value="0.0.0.0"/></div> <div style="margin-bottom: 5px;">Subnet Address: <input type="text"/></div> <div style="margin-bottom: 5px;">Subnet Mask: <input type="text"/></div> <div style="margin-bottom: 5px;">Link State Type: <input type="text" value="Summary"/></div> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="background-color: #d0d0d0;">Select</th> <th style="background-color: #d0d0d0;">Area ID</th> <th style="background-color: #d0d0d0;">Subnet Address</th> <th style="background-color: #d0d0d0;">Subnet Mask</th> <th style="background-color: #d0d0d0;">Link State Type</th> <th style="background-color: #d0d0d0;">Advertise</th> </tr> </thead> <tbody> <tr> <td style="text-align: center;"><input type="checkbox"/></td> <td>0.0.0.0</td> <td>10.0.0.0</td> <td>255.0.0.0</td> <td>Summary</td> <td style="text-align: center;"><input checked="" type="checkbox"/></td> </tr> <tr> <td style="text-align: center;"><input type="checkbox"/></td> <td>0.0.0.0</td> <td>172.0.0.0</td> <td>255.0.0.0</td> <td>Summary</td> <td style="text-align: center;"><input checked="" type="checkbox"/></td> </tr> </tbody> </table> <p style="margin-top: 5px;">2 entries.</p> <div style="margin-top: 5px;"> <input type="button" value="Create"/> <input type="button" value="Delete"/> <input type="button" value="Set Values"/> <input type="button" value="Refresh"/> </div>								Select	Area ID	Subnet Address	Subnet Mask	Link State Type	Advertise	<input type="checkbox"/>	0.0.0.0	10.0.0.0	255.0.0.0	Summary	<input checked="" type="checkbox"/>	<input type="checkbox"/>	0.0.0.0	172.0.0.0	255.0.0.0	Summary	<input checked="" type="checkbox"/>
Select	Area ID	Subnet Address	Subnet Mask	Link State Type	Advertise																				
<input type="checkbox"/>	0.0.0.0	10.0.0.0	255.0.0.0	Summary	<input checked="" type="checkbox"/>																				
<input type="checkbox"/>	0.0.0.0	172.0.0.0	255.0.0.0	Summary	<input checked="" type="checkbox"/>																				

Description of the displayed boxes

The page contains the following boxes:

- **Area ID**
Select the ID of the area from the drop-down list. You specify the ID on the "Areas" tab.
- **Subnet Address**
Enter the IPv4 address of the network that will be grouped.
- **Subnet mask**
Enter the subnet mask of the network that will be grouped.
- **Link State Type**
 - **Summary**
Summary of routes within the areas in which OSPF is enabled.
 - **NSSA external**
Inclusion of routes from a **Not So Stubby Area** (LSA type 7) and conversion into LSA type 5.

6.6 The "Layer 3" menu

The table contains the following columns:

- **Select**
Select the row you want to delete.
- **Area ID**
Shows the ID of the area.
- **Subnet Address**
Shows the IP address of the network that will be grouped.
- **Subnet Mask**
Shows the subnet mask of the network that will be grouped.
- **Link State Type**
Shows which types of routes are summarized.
- **Advertise**
Enable this option to advertise the grouped network.

Configuration procedure

1. Select the ID of the area from the drop-down list.
2. Enter the IP address of the network that will be grouped.
3. Enter the subnet mask of the network that will be grouped.
4. From the drop-down list, select which types of routes should be summarized.
5. Click the "Create" button. A new entry is generated in the table.
6. Enable the "Advertise" option to advertise the grouped network.
7. Click the "Set Values" button.

6.6.9.6 Interfaces

Overview

On this page, you can configure OSPFv2 interfaces.

Note

This function is available only with layer 3.

Open Shortest Path First v2 (OSPFv2) Interfaces

Configuration | Redistribution | Summary Address | Areas | Area Range | Interfaces | Interface Authentication | Virtual Links | Virtual Link Authentication

Default Passive Interface

IP Address: 0.0.0.0
 Area ID: 0.0.0.0

Select	IP Address	Address Type	Area ID	Passive Interface	Metric	Priority	Trans. Delay	Retrans. Delay	Hello Interval	Dead Interval
<input type="checkbox"/>	192.168.16.155	Primary	0.0.0.0 <input type="button" value="v"/>	<input type="checkbox"/>	1	1	1	5	10	40

1 entry.

Description

The page contains the following boxes:

- **Default: Passive Interface**
If this check box is selected, all newly created interfaces are created as passive interfaces.
- **IP Address**
Select the IPv4 address of the OSPFv2 interface from the drop-down list.
- **Area ID**
Select the ID of the area that is connected to the OSPFv2 interface from the drop-down list.

Note

For the secondary interface select the same Area ID as for the corresponding primary interface.

The information whether an address type is primary or secondary can be found in the "Address Type" column on the "Layer 3 (IPv4) > Subnets > Overview" page.

Select the ID of the area that is connected to the OSPFv2 interface from the drop-down list. The table has the following columns:

- **Select**
Select the row you want to delete.
- **IP Address**
Shows the IPv4 address of the OSPFv2 interface.
- **Address Type**
There are two address types:
 - Primary
 - Secondary
 Cells for secondary addresses are grayed out and show the values of the associated primary address.
- **Area ID**
Select the ID of the area that is connected to the OSPFv2 interface from the drop-down list.

- **Passive Interface**
Specify the behavior of the interface:
 - Enabled
No OSPFv2 information (e.g. Hello packets and LSDB updates) is sent via this interface and learned.
All information that an interface learned before the option was enabled are retained in the LSDB. The information is deleted when the option is disabled or the interface is removed from the OSPF configuration.
 - Disabled
OSPFv2 information is sent via this interface and learned.
- **Metric**
Enter the costs for the OSPFv2 interface.
- **Priority**
Enter the router priority. The priority is only relevant for selecting the designated router or designated border router. This parameter can be selected differently on routers within the same subnet.
Range of values: 0 to 255
Default setting: 1
- **Trans. Delay**
Enter the required delay when sending a connection update.
Range of values: 1 s to 3600 s
Default setting: 1 s
- **Retrans. Delay**
Enter the time after which an OSPFv2 packet is transferred again if no confirmation was received.
Range of values: 1 s to 3600 s
Default setting: 5 s
- **Hello Interval**
Enter the interval between two Hello packets.
Range of values: 1 s to 65,535 s
Default setting: 10 s
- **Dead Interval**
Enter the interval after which the neighbor router is marked as "failed" if no more Hello packets are received from it during this time.
Default setting: 40 s

Configuration procedure

1. Select the IPv4 address of the OSPFv2 interface from the "IP Address" drop-down list.
2. Select the ID of the area with which the OSPFv2 interface is connected from the "Area ID" drop-down list.
3. Click the "Create" button. A new entry is generated in the table.
4. Make the required settings or use the factory defaults.
5. Click the "Set Values" button.

6.6.9.7 Interface Authentication

Configuring the interface authentication

On this page, you define the authentication of the interface.

Open Shortest Path First v2 (OSPFv2) Interface Authentication

Configuration	Redistribution	Summary Address	Areas	Area Range	Interfaces	Interface Authentication	Virtual Links	Virtual Link Authentication
---------------	----------------	-----------------	-------	------------	------------	---------------------------------	---------------	-----------------------------

OSPF Interface: 192.168.16.155

Authentication Type: none

Simple Authentication

Password:

Confirmation:

MD5 Authentication

Authentication Key ID:

Select	Authentication Key ID	MD5 Key	MD5 Key Confirmation	Youngest Key ID
<input type="checkbox"/>	45			yes

1 entry.

Description of the displayed boxes

The page contains the following boxes:

- **OSPF interface**
Select the OSPFv2 interface for which you want to configure authentication.
- **Authentication Type**
Select the authentication method. You have the following options:
 - None
No authentication
 - Simple
Authentication using an unencrypted password
 - MD5
Authentication using MD5

Section "Simple Authentication"

- **Password**
Enter a password.
- **Confirmation**
Confirm the entered password.

Section "MD5 Authentication"

- **Authentication Key ID**
Enter the identifier of the MD5 authentication key.
Enter the ID for MD5 authentication with which the password will be used as a key.
Since the key ID is transferred with the protocol, the same key must be stored under the same key ID on all neighboring routers.

The table has the following columns:

- **Select**
Select the row you want to delete.
- **Authentication Key ID**
Can only be edited if you set the MD5 authentication method. It is only possible to use several keys there.
- **MD5 Key**
Enter the MD5 key.
- **MD5 Key Confirmation**
Confirm the entered key.
- **Youngest Key ID**
Shows whether or not the MD5 key is the latest key ID.

Configuration procedure

1. Select the OSPFv2 interface and the authentication method from the drop-down lists.
2. Enter the following data in the relevant input box:
 - Password and confirmation for simple authentication
 - Authentication key ID for MD5 authentication
3. Click the "Create" button.
4. Enter the MD5 key and the confirmation of the MD5 key.
5. Click the "Set Values" button.

6.6.9.8 Virtual Links

Overview

Due to the protocol, each area border router must have access to the backbone area for protocol reasons. If a router is not connected directly to the backbone area, a virtual link to it is created.

Note

This function is available only with layer 3.

Note

Note that when creating a virtual link both the transit area and the backbone area must already be configured.

A virtual link must be configured identically at both ends.

Open Shortest Path First v2 (OSPFv2) Virtual Links

Configuration | Redistribution | Summary Address | Areas | Area Range | Interfaces | Interface Authentication | **Virtual Links**

Virtual Link Authentication

Since the device is not an ABR, Virtual Links are not functional

Neighbor Router ID:

Transit Area ID: 1.1.1.1

Select	Transit Area ID	Neighbor Router ID	Virt. Link Status	Trans. Delay	Retrans. Delay	Hello Interval	Dead Interval
<input type="checkbox"/>	1.1.1.1	5.5.5.5	down	1	5	10	40

1 entry.

Description of the displayed boxes

The page contains the following note:

- **Since the device is not an ABR, Virtual Links are not functional**
This note is displayed when at least one virtual link is configured and the device is not an area border router.

The page contains the following boxes:

- **Neighbor Router ID**
Enter the ID of the neighbor router at the other end of the virtual connection.
- **Transit Area ID**
Select the ID of the area that connects both routers from the drop-down list.

The table contains the following columns:

- **Select**
Select the row you want to delete.
- **Transit Area ID**
Shows the ID via which the two routers are connected.
- **Neighbor Router ID**
Shows the ID of the neighbor router at the other end of the virtual connection.
- **Virt. Link Status**
Specify the status of the virtual link. The following states are possible:
 - down: The virtual link is inactive.
 - point-to-point: The virtual link is active.

6.6 The "Layer 3" menu

- **Trans. Delay**
Enter the expected delay when sending a link update packet.
Range of values: 1 s to 3600 s
Default: 1 s
- **Retrans. Delay**
Enter the time after which a packet is transferred again if no confirmation was received.
Range of values: 1 s to 3600 s
Default: 5 s
- **Hello Interval**
Enter the interval between two Hello packets.
Range of values: 1 s to 65,535 s
Default: 10 s
- **Dead Interval**
Enter the interval after which the neighbor router counts as "failed" if no more Hello packets are received from it during this time.
Default setting: 40 s

Configuration procedure

1. Enter the ID of the neighbor router at the other end of the virtual link in "Neighbor Router ID".
2. Select the area ID that connects the two routers from the "Transit Area ID" drop-down list.
3. Click the "Create" button. A new entry is generated in the table.
4. Enter the suitable values in "Transit Delay", "Retrans. Delay" and "Dead Interval".
5. Click the "Set Values" button.

6.6.9.9 Virtual Link Authentication

Configuring the interface login

On this page, you define the authentication of the interface.

Open Shortest Path First v2 (OSPFv2) Virtual Link Authentication

Configuration	Redistribution	Summary Address	Areas	Area Range	Interfaces	Interface Authentication	Virtual Links	Virtual Link Authentication
---------------	----------------	-----------------	-------	------------	------------	--------------------------	---------------	-----------------------------

Virtual Link (Area/Neighbor): ▾

Authentication Type: ▾

Simple Authentication

Password:

Confirmation:

MD5 Authentication

Authentication Key ID:

Select	Authentication Key ID	MD5 Key	MD5 Key Confirmation	Youngest Key ID
<input type="checkbox"/>	45			yes

1 entry.

Description of the displayed boxes

The page contains the following boxes:

- **Virtual Link (Area/Neighbor)**
Select the virtual link for which you want to configure authentication.
- **Authentication Type**
Select the authentication method. You have the following options:
 - None
No authentication
 - Simple
Authentication using an unencrypted password
 - MD5
Authentication using MD5

Section "Simple Authentication"

- **Password**
Enter a password.
- **Confirmation**
Confirm the entered password.

Section "MD5 Authentication"

- **Authentication Key ID**
Enter the identifier of the MD5 authentication key.
Enter the ID for MD5 authentication with which the password will be used as a key.
Since the key ID is transferred with the protocol, the same key must be stored under the same key ID on all neighboring routers.

The table has the following columns:

- **Select**
Select the row you want to delete.
- **Authentication Key ID**
Can only be edited if you set the MD5 authentication method. It is only possible to use several keys there.
- **MD5 Key**
Enter the MD5 key.
- **MD5 Key Confirmation**
Confirm the entered key.
- **Youngest Key ID**
Shows whether or not the MD5 key is the latest key ID.

Configuration procedure

1. Select the virtual connection and the authentication method from the drop-down lists.
2. Enter the following data in the relevant input box:
 - Password and confirmation for simple authentication
 - Authentication key ID for MD5 authentication
3. Click the "Create" button.
4. Enter the MD5 key and the confirmation of the MD5 key.
5. Click the "Set Values" button.

6.6.10 RIPv2

6.6.10.1 Configuration

The Routing Information Protocol (RIP) creates routing tables automatically. As compared to the previous version, version RIPv2 provides Classless Inter-Domain Routing (CIDR) and modified sending of RIP packets (multicast instead of broadcast), among other features.

On this page, you configure the routing using RIPv2.

Note

RIPv2 is available only on layer 3.

Settings

Routing Information Protocol v2 (RIPv2) Configuration

Configuration | Interfaces

RIPv2

Inbound Filter: -

Redistribute Routes

Static Default

Connected

Static

OSPF

Route Map: -

Protocol Preference

Default Distance: 121

Route Map Preference

Distance Route Map: -

Distance:

Set Values Refresh

- **RIPv2**
Enable or disable routing using RIPv2.
- **Inbound Filter**
Select a route map that filters inbound routes.
- **Redistribute Routes**
Specify which known routes are distributed using RIPv2.
The following types of route exist:
 - Static Default
 - Connected
 - Static
 - OSPF
- **Route Map**
Select a route map that filters which routes are forwarded using RIPv2.

- **Protocol Preferences**
 - **Default Distance**
Set the administrative distance for the RIPv2 protocol.
- **Route Map Preferences**
 - **Route Map Distance**
Select a route map from the drop-down list for which you want to specify the administrative distance.
 - **Distance**
Configure the administrative distance for the previously selected route map.

6.6.10.2 Interfaces

Overview

On this page, you can configure RIPv2 interfaces.

Note

RIPv2 is available only with layer 3.

Settings

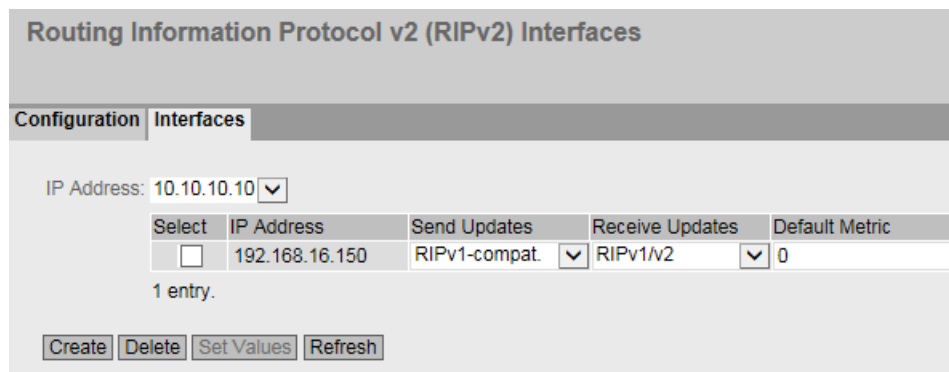


Figure 6-6 RIPv2 interfaces

- **IP Address**
Select the IPv4 address of the RIPv2 interface.

The table contains the following columns:

- **Select**
Select the row you want to delete.
- **IP Address**
Shows the IPv4 address of the RIPv2 interface

- **Send Updates**
Select the way in which updates are sent:
 - **no send**
No updates are sent.
 - **RIPv1**
Updates for RIPv1 are sent.
 - **RIPv1-compatible.**
RIPv2 updates are sent as broadcasts according to the rules of RIPv1.
 - **RIPv2**
Updates for RIPv2 are sent as multicasts.
 - **RIPv1 demand**
RIPv1 packets are sent only as a response to an explicit query.
 - **RIPv2 demand**
RIPv2 packets are sent only as a response to an explicit query.
- **Receive Updates**
Select the form in which received updates are accepted:
 - **no receive**
No updates are received.
 - **RIPv1**
Only updates of RIPv1 are received.
 - **RIPv2**
Only updates of RIPv2 are received.
 - **RIPv1/v2**
Updates of RIPv1 and RIPv2 are received.
- **Default Metric**
Enter the costs for the RIPv2 interface.

6.6.11 IGMP

6.6.11.1 IGMP

IGMP

On this page, you configure IGMP (Internet Group Management Protocol).

IGMP is a network protocol used for IP multicast. When IP multicasting IP packets with one IP address are distributed to multiple clients at the same time. IGMP can manage dynamic and static multicast groups.

Description of the displayed boxes

Internet Group Management Protocol (IGMP)

IGMP | Static Groups | Multicast Sources

IGMP

Interface: vlan1

Select	Interface	Version	Query Interval[s]	Max. Response Time[1/10 s]	Last Member Query Interval[1/10 s]
<input type="checkbox"/>	vlan1	3 <input type="button" value="v"/>	125	100	10

1 entry.

Robustness	Immediate Leave	Explicit Tracking	Admin State	Operational State
2 <input type="button" value="v"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Up

The page contains the following boxes:

- **IGMP**
Enable or disable (Internet Group Management Protocol) for the entire device.
- **Interface**
Select the required interface on which you want to configure IGMP.

The table has the following columns:

- **Select**
Select the row you want to delete.
- **Interface**
Shows the interface.
- **Version**
Select the version of IGMP.
- **Query Interval [s]**
Define the interval at which the multicast router sends IGMP queries.
Specified in seconds
- **Max. Response Time [1/10 s]**
Specify the duration in an IGMP query that is available to the client to respond to a query. This value is specified in tenths of a second.

- **Last Member Query Interval [1/10 s]**

The period of time in tenths of a second after the last Leave message in which the multicast router searches for further clients that want to receive a multicast.
- **Robustness**

With this value, you take into account the packet loss rate of a network. You can select a value between "1" and "3" from the drop-down list. Select the setting "1" for networks with a low packet loss rate. Select the setting "3" for networks with a high packet loss rate. The default value is "2".
- **Immediate Leave**

With this check box, you enable the "Immediate Leave (IGMPv2)" function. In this case, the multicast router then a multicast group as soon as it receives a Leave message from a registered client. The multicast router does not query whether a further client wants to receive the multicast.
- **Explicit Tracking**

Enable or disable the "Explicit Tracking" function for the interface (IGMPv3).
If the "Explicit Tracking" function is enabled, the multicast router tracks precisely which clients log on to a multicast group (Join) and log off (Leave). As soon as the last client has logged off from a multicast group, the multicast router deletes the multicast group. Since the multicast router has precise information about the logged on and logged off clients, the multicast router does not need to query whether a further client wants to receive the multicast.
- **Admin Status**

Enable or disable IGMP on the interface.
- **Operating Status**

Shows the operating status of the interface, see also "System > Ports > Overview".

 - Up
 - Down

Configuration procedure

1. Select the "IGMP" check box.
2. Select an interface.
3. Click the "Create" button.
4. Select the required settings in the table.
5. Click the "Set Values" button.

6.6.11.2 Static Groups

Multicast groups for IGMP

On this page, you create the static multicast group for IGMP.

Internet Group Management Protocol (IGMP) Static Groups

IGMP | **Static Groups** | Multicast Sources

IGMP Interface:

Multicast Group:

Select	Interface	Multicast Group
<input type="checkbox"/>	vlan1	224.7.7.7

1 entry.

Description of the displayed boxes

The page contains the following boxes:

- **IGMP Interface**
Select the interface for which you want to create a multicast group.
- **Multicast Group**
Enter the multicast address of the group.

The table has the following columns:

- **Select**
Select the row you want to delete.
- **Interface**
Shows the interface.
- **Multicast group**
Shows the IP address of the multicast group.

Configuration procedure

1. Select the required interface
2. Enter the IP address of the multicast group.
3. Click the "Create" button.
4. Click the "Set Values" button.

6.6.11.3 Multicast Sources

Configuration of source addresses

On this page, you specify that multicast packages are only received from defined IP addresses. If you specify a multicast group that has not yet been created as static group, a new table entry is automatically created on the "Static Group" page.

Internet Group Management Protocol (IGMP) Multicast Sources

IGMP
Static Groups
Multicast Sources

IGMP Interface:

Multicast Group:

Source Address:

Select	Interface	Multicast Group	Source Address
<input type="checkbox"/>	vlan1	224.7.7.7	192.168.16.45

1 entry.

Create
Delete
Refresh

Description of the displayed boxes

The page contains the following boxes:

- **IGMP Interface**
Select the interface for which you want to create a multicast group.
- **Multicast Group**
Enter the multicast address of the group.
- **Source Address**
Enter the IP address of the device from which multicast packages are to be received. You can restrict the receipt of multicast packages to specific sources.

The table has the following columns:

- **Select**
Select the row you want to delete.
- **Interface**
Shows the interface.
- **Multicast Group**
The IP address of the multicast group.
- **Source Address**
The IP address from which the group is to receive multicast packages.

Configuration procedure

1. Select the required interface
2. Enter the IP address of the multicast group.
3. Enter the source address.
4. Click the "Create" button.
5. Click the "Set Values" button.

6.6.12 PIM

6.6.12.1 PIM

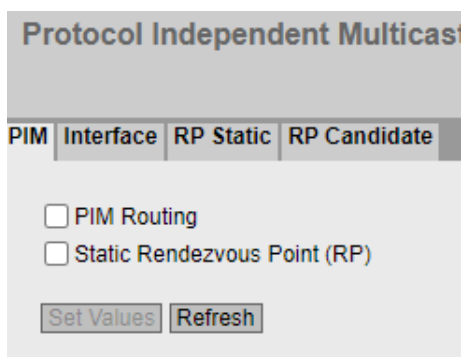
PIM stands for Protocol Independent Multicast and enables the dynamic routing of multicast packets. Sparse mode is available for PIM. In Sparse Mode, a Rendezvous Point is defined at which other routers can query multicast information.

On this page, you configure PIM.

Note

PIM is available only on layer 3.

Settings



- **PIM Routing**
Enable or disable PIM globally on the device.
- **Static Rendezvous Point (RP)**
Enable or disable that the device uses static configured rendezvous points.

6.6.12.2 Interface

Overview

On this page, you configure PIM interfaces.

Note

PIM is available only on layer 3.

Settings

The page contains the following boxes:

- **Interface**
Select a VLAN IP interface.
- **PIM**
If you select this check box, The selected interface is assigned PIM.
- **Bootstrap Router (BSR) Candidate**
If you enable this check box, you specify that the interface will become a candidate for the bootstrap router. A BSR coordinates the rendezvous points in a PIM network.
- **BSR Candidate Value**
Enter the priority of the interface as BSR candidate.
Which candidate becomes the BSR is decided based on the priority. The candidate with the highest priority becomes the BSR.
If the same priority is set for two candidates, when necessary the decision is made based on the IP address. The interface with the higher IP address becomes BSR.
A BSR coordinates the rendezvous points in a PIM network.

6.6 The "Layer 3" menu

- Designated Router (DR) Priority**
 Enter the DR priority of the interface.
 Which candidate becomes the DR is decided based on the DR priority. The candidate with the highest priority becomes the DR.
 If the same priority is set for two candidates, when necessary the decision is made based on the IP address. The interface with the higher IP address becomes DR.
 The DR forwards the IGMP Joins to the rendezvous point.
- BSR Border**
 When enabled there is no BSR communication via this interface. As a result a PIM network is divided into PIM domains.

6.6.12.3 RP Static

Overview

On this page you specify which interfaces will become static rendezvous points.
 Configure the static RP on all devices of the PIM component.

Note

PIM is available only on layer 3.

Settings

Protocol Independent Multicast (PIM) Rendezvous Point (RP) Static Configuration

PIM	Interface	RP Static	RP Candidate
-----	-----------	-----------	--------------

Group Address:

Group Mask:

RP Address:

Select	Group Address	Group Mask	RP Address
<input type="checkbox"/>	224.0.0.5	255.255.255.255	192.168.16.9
<input type="checkbox"/>	224.0.0.6	255.255.255.255	10.0.1.1

2 entries.

The page contains the following boxes:

- **Group Address**
Enter the address of the multicast group for which the interface will become RP.
- **Group Mask**
Enter the subnet mask that restricts the multicast band.
- **RP Address**
Enter the IP address of the interface that will become RP.
- **Select**
Select the row you want to delete.
- **Group Address**
Shows the address of the multicast group.
- **Group Mask**
Shows the subnet mask.
- **RP Address**
Shows the IP address of the RP.

6.6.12.4 RP Candidate

Overview

On this page you specify which interfaces will be candidates for the rendezvous point (RP).

Within a PIM network you can configure several candidates for the RP. The BSR coordinates the candidates and decides on the RP.

Note

PIM is available only on layer 3.

Settings

Protocol Independent Multicast (PIM) Rendezvous Point (RP) Candidate Configuration

PIM	Interface	RP Static	RP Candidate											
				Group Address: <input type="text"/> Group Mask: <input type="text"/> RP Interface: <input type="text" value="vlan1 (192.168.16.155)"/>										
				<table border="1" style="width: 100%; border-collapse: collapse; text-align: center;"> <thead> <tr> <th style="width: 5%;">Select</th> <th style="width: 20%;">Group Address</th> <th style="width: 20%;">Group Mask</th> <th style="width: 20%;">RP Candidate</th> <th style="width: 15%;">RP Priority</th> </tr> </thead> <tbody> <tr> <td><input type="checkbox"/></td> <td>224.0.0.5</td> <td>255.255.255.255</td> <td>10.0.0.2</td> <td>192</td> </tr> </tbody> </table> <p>1 entry.</p>	Select	Group Address	Group Mask	RP Candidate	RP Priority	<input type="checkbox"/>	224.0.0.5	255.255.255.255	10.0.0.2	192
Select	Group Address	Group Mask	RP Candidate	RP Priority										
<input type="checkbox"/>	224.0.0.5	255.255.255.255	10.0.0.2	192										
<input type="button" value="Create"/> <input type="button" value="Delete"/> <input type="button" value="Set Values"/> <input type="button" value="Refresh"/>														

The page contains the following boxes:

- **Group Address**
Enter the address of the multicast group.
- **Group Mask**
Enter the subnet mask that restricts the multicast band.
- **RP Interface**
Select the interface that will become the RP candidate.
- **Select**
Select the row you want to delete.
- **Group Address**
Shows the address of the multicast group.
- **Group Mask**
Shows the subnet mask.
- **RP Candidate**
Shows the IP address of the RP.
- **RP Priority**
Enter the priority of the interface.
Which candidate becomes the rendezvous point is decided based on the RP priority. The candidate with the highest priority becomes the RP. The lower the value, the higher the priority.
If the same priority is set for two candidates, when necessary the decision is made based on the IP address. The interface with the lowest IP address becomes RP.

6.6.13 MSDP

6.6.13.1 MSDP

Overview

On this page, you configure MSDP.

MSDP (Multicast Source Discovery Protocol) is supported within one or multiple PIM-SM domains in combination with anycast RPs. Anycast RPs involve a redundancy concept for RPs. The RPs involved all receive the same IP address and are made known in the network. The RPs are linked together via MSDP sessions. The RPs synchronize their multicast sources via source active messages.

Configure MSDP on the rendezvous points.

Note

MSDP is available only on layer 3.

Settings

Multicast Source Discovery Protocol (MSDP)

MSDP | Peer

MSDP

Originator ID: 0.0.0.0

Cache Life Time: 0

Listener Port: 639

Peer In Route Map:

Source-Active (SA) Out Route Map:

Set Values Refresh

The page contains the following boxes:

- **MSDP**
Enable or disable MSDP.
- **Originator ID**
Select an interface for identification of the MSDP node. The Originator ID must be unique in the network.

6.6 The "Layer 3" menu

- Cache Life Time**
 Enter the time after which an entry with information of another RP is deleted from the SA cache if no SA cache updates are received. After an entry is created or updated, a timer starts and runs backwards with the defined time. SA cache updates are received cyclically and reset the timer of the entry. When the timer expires without an SA cache update being received in this time. the corresponding entry is deleted.
 If the value "0" is set, no SA cache entries are saved.
- Listener Port**
 TCP port via which the device communicates with other MSDP nodes. If you change the listener port, only new MSDP connections are affected that are created after this change. Existing MSDP connections continue to use the previous listener port.
- Peer In Route Map**
 You have the option of entering the name of a route map for filtering protocol information here.
- Source-Active (SA) Out Route Map**
 You have the option of entering the name of a route map for filtering outgoing source-active messages here.

6.6.13.2 Peer

Overview

On this page, you configure MSDP partners.

Note

MSDP is available only on layer 3.

Settings

Select	Peer Address	Local Address	Admin Status	Connection Status	Keepalive Interval[s]	Peer Hold Time Interval[s]	Connect Retry Interval[s]	TTL Threshold
<input type="checkbox"/>	100.1.1.1	192.168.16.155	<input checked="" type="checkbox"/>	Listening	60	75	30	1

The page contains the following boxes:

- Peer Address**
 Enter the IP address of the MSDP partner to which the device will establish a connection.
- Connected Interface**
 Select the interface via which the device communicates with the MSDP partner.

The table contains the following columns:

- **Select**
Select the row you want to delete.
- **Peer Address**
Shows the address of the MSDP partner.
- **Local Address**
Shows the IP address of the interface via which the device communicates with the MSDP partner.
- **Admin Status**
Enable or disable the connection.
- **Connection Status**
Shows the status of the connection.
 - Listening
The device is waiting for the connection.
 - Connecting
Connection establishment
 - Established
The connection is established.
 - Inactive
The connection is not active.
 - Disabled
The connection is disabled.
- **Keepalive Interval[s]**
Define the interval at which the device sends keepalive messages to the MSDP partners.
- **Peer Hold Time Interval[s]**
Define the time after which an MSDP connection is terminated if no keepalive messages are received from the MSDP partner.
- **Connect Retry Interval[s]**
Define the interval after which an attempt is made to establish a connection. If there is no MSDP connection to a partner, when the Connect Retry Interval elapses, an attempt is made to establish a connection.
- **TTL Threshold**
Define the maximum number of routers that may be passed through on the way to the MSDP partner (hop count). If the specified value used is exceeded, the frame is discarded.

6.7 The "Security" menu

6.7.1 User management

Overview of user management

Access to the device is managed by configurable user settings. Set up users with a password for authentication. Assign a role with suitable rights to the users.

The authentication of users can either be performed locally by the device or by an external RADIUS server. You configure how the authentication is handled on the "Security > AAA > General" page.

Compatibility with predecessor versions

With firmware version 5.1, user management was expanded by the RADIUS authorization mode "Vendor Specific". To ensure compatibility with firmware versions ≤ 5.0 , the default setting was selected so that following a firmware update the earlier authentication mode "conventional" continues to be used.

Local logon

The local logging on of users by the device runs as follows:

1. The user logs on with user name and password on the device.
2. The device checks whether an entry exists for the user.
 - If an entry exists, the user is logged in with the rights of the associated role.
 - If no corresponding entry exists, the user is denied access.

Login via an external RADIUS server

RADIUS (Remote Authentication Dial-In User Service) is a protocol for authentication authorization o users by servers on which user data can be stored centrally.

Depending on the RADIUS authorization mode you have selected on the "Security > AAA > RADIUS Client" page, the device evaluates different information of the RADIUS server.

RADIUS authorization mode "Standard"

If you have set the authorization mode "conventional", the authentication of users via a RADIUS server runs as follows:

1. The user logs on with user name and password on the device.
2. The device sends an authentication request with the login data to the RADIUS server.
3. The RADIUS server runs a check and signals the result back to the device.
 - The RADIUS server reports a successful authentication and for the "Service Type" attribute returns the value "Administrative User" to the device
→ The user is logged in with read/write rights.
 - The RADIUS server reports a successful authentication and returns a different or even no value to the device for the attribute "Service Type".
→ The user is logged in with read rights.
 - The RADIUS server reports a failed authentication to the device:
→ The user is denied access.

RADIUS authorization mode "Vendor Specific"**Requirement**

For the RADIUS authorization mode "Vendor Specific" the following needs to be set on the RADIUS server:

- Manufacturer code: 4196
- Attribute number: 1
- Attribute format: Character string (group name)

Procedure

If you have set the authorization mode "Vendor Specific", the authentication of users via a RADIUS server runs as follows:

1. The user logs on with user name and password on the device.
2. The device sends an authentication request with the login data to the RADIUS server.
3. The RADIUS server runs a check and signals the result back to the device.

Case A: The RADIUS server reports a successful authentication and returns the group assigned to the user to the device.

- The group is known on the device and the user is not entered in the table "External User Accounts"
→ The user is logged in with the rights of the assigned group.
- The group is known on the device and the user is entered in the table "External User Accounts"
→ The user is assigned the role with the higher rights and logged in with these rights.
- The group is not known on the device and the user is entered in the table "External User Accounts"
→ The user is logged in with the rights of the role linked to the user account.
- The group is not known on the device and the user is not entered in the table "External User Accounts"
→ The user is logged in with the rights of the role "Default".

Case B: The RADIUS server reports a successful authentication but does not return a group to the device.

- The user is entered in the table "External User Accounts":
→ The user is logged in with the rights of the linked role "".
- The user is not entered in the table "External User Accounts":
→ The user is logged in with the rights of the role "Default".

Case C: The RADIUS server reports a failed authentication to the device:

- The user is denied access.

Assignment of a VLAN via RADIUS or guest VLAN

Authentication with a change to the VLAN configuration

If during authentication a port is assigned to a VLAN dynamically using the function "RADIUS VLAN Assignment Allowed" or "Guest VLAN" the options are as follows:

- If the VLAN that is to be assigned has not been created on the device, the authentication is rejected.
- If the VLAN that is to be assigned has been created on the device:
 - The port becomes an untagged member in the assigned VLAN if it was not already.
→ This makes it possible for the static configuration of the port in this VLAN to be overwritten and not restored if the authentication is retracted.
 - The port VID of the port is changed to the ID of the assigned VLAN.

Note

If the port is only to be assigned to one VLAN, you need to adapt the VLAN configuration manually. As default, all ports are untagged members in "VLAN 1".

If the authentication is canceled, e.g. by link down, the dynamic changes are canceled.

- The port is no longer a member in the assigned VLAN.
- The port VID of the port is reset to the value it had prior to authentication.

Note

If the port VID corresponds to the assigned port VID prior to authentication, the port remains an untagged member in this VLAN.

Authentication without a change to the VLAN configuration

If during authentication no VLAN is assigned either by the function "RADIUS VLAN Assignment Allowed" or by "Guest VLAN", the existing VLAN configuration of the port remains unchanged.

6.7.2 Users

6.7.2.1 Local Users

Local Users

On this page, you create local users with the corresponding rights.

Note

The values displayed depend on the rights of the logged-in user.

Local Users

Local Users
Roles
Groups

Case Sensitive User Accounts

User Account:

Password Policy: high

Password:

Password Confirmation:

Role: user

Select	User Account	Role	Description
<input type="checkbox"/>	admin	admin	System defined local user

1 entry.

Create
Delete
Set Values
Refresh

Description

The page contains the following boxes:

- **Case Sensitive User Accounts**
 When this check box is selected, a distinction is made between uppercase and lowercase in the user name. If user names have been created that differ only in case, you can no longer clear this check box.
- **User Account**
 Enter the name for the user. The name must meet the following conditions:
 - It must be unique.
 - It must be between 1 and 32 characters long.
 - The following characters must not be included: | ? " ; : § °
 The characters for Space and Delete also cannot be included.

Note

User name cannot be changed

After a user is created, the user name can no longer be changed.

If a user name needs to be changed, the user must be deleted and a new user created.

- **Password Policy**
Shows which password policy is being used on the device:
 - **High**
Password length: at least 8 characters, maximum 32 characters
At least 1 uppercase letter
At least 1 special character
At least 1 number
 - **Low**
Password length: at least 6 characters, maximum 32 characters
 - **User defined**
The user specifies the details of the password policy.

You configure the password policy of the device on the page "Security > Passwords > Options".

- **Password**
Specify the password. The strength of the password depends on the set password policy.
- **Password Confirmation**
Enter the password again to confirm it.
- **Role**
Select a role:
 - user
Read rights: Users with this role can read device parameters but cannot change them.
Users with this role can change their own password.
 - admin
Read/write rights: Users with this role can both read and change device parameters. Users can change the passwords for all user accounts.

The table contains the following columns:

- **Select**
Select the check box in the row to be deleted.

Note

The users preset in the factory as well as logged in users cannot be deleted or changed.

- **User Account**
Shows the user name.
- **Role**
Shows the role of the user.

Procedure

Note**Changes in "Trial" mode**

Even if the device is in "Trial" mode, changes that you carry out on this page are saved immediately.

Creating users

1. Enter the name for the user.
2. Enter the password for the user.
3. Enter the password again to confirm it.
4. Select the role of the user.
5. Click the "Create" button.

Deleting users

1. Select the check box in the row to be deleted.
2. Click the "Delete" button. The entries are deleted and the page is updated.

6.7.2.2 Roles

Roles

On this page, you create roles that are valid locally on the device.

Note

The values displayed depend on the rights of the logged-in user.

User Roles

Local Users | **Roles** | Groups

Role Name:

Select	Role	Function Right	Description
<input type="checkbox"/>	user	1	System defined role, with readonly access to configuration data of this component.
<input type="checkbox"/>	admin	15	System defined role, with read/write access to configuration data of this component.
<input type="checkbox"/>	default	1	Internal role, for authenticated users without group/role mapping in this component.
<input type="checkbox"/>	everybody	0	Internal role, assigned to users when authentication failes. Access will be denied.
<input type="checkbox"/>	Maintenance	15	User defined role, with read/write access

5 entries.

Description

The page contains the following:

- **Role Name**
Enter the name for the role. The name must meet the following conditions:
 - It must be unique.
 - It must be between 1 and 64 characters long.

Note

Role name cannot be changed

After creating a role, the name of the role can no longer be changed.

If a name of a role needs to be changed, the role must be deleted and a new role created.

The table contains the following columns:

- **Select**
Select the check box in the row to be deleted.

Note

Predefined roles and assigned roles cannot be deleted or modified.

- **Role**
Shows the name of the role.
- **Function Right**
Select the function rights of the role:
 - **0**
If authentication fails, the user is assigned the role. Access to the device is not possible.
 - **1**
Users with this role can read device parameters but cannot change them. Users with this role can change their own password.
 - **15**
Users with this role can both read and change device parameters.

Note

Function right cannot be changed

If you have assigned a role, you can no longer change the function right of the role.

If you want to change the function right of a role, follow the steps outlined below:

1. Delete all assigned users.
 2. Change the function right of the role:
 3. Assign the role again.
-

- **Description**
Enter a description for the role. With predefined roles a description is displayed. The description text can be up to 100 characters long.

Procedure

Creating a role

1. Enter the name for the role.
2. Click the "Create" button.
3. Select the function rights of the role.
4. Enter a description for the role.
5. Click the "Set Values" button.

Deleting a role

1. Select the check box in the row to be deleted.
2. Click the "Delete" button. The entries are deleted and the page is updated.

6.7.2.3 Groups

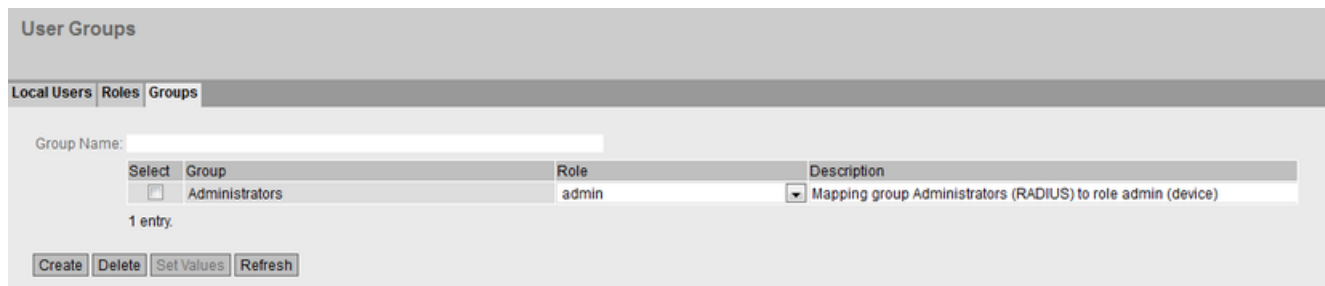
User groups

On this page you link a group with a role.

In this example the group "Administrators" is linked to the "admin" role: The group is defined on a RADIUS server. The role is defined locally on the device. When a RADIUS server authenticates a user and assigns the user to the "Administrators" group, this user is given rights of the "admin" role.

Note

The values displayed depend on the rights of the logged-in user.



Description

The page contains the following:

- **Group Name**

Enter the name of the group. The name must match the group on the RADIUS server.

The name must meet the following conditions:

- It must be unique.
- It must be between 1 and 64 characters long.
- The following are not permitted: § ? " ; :

The table contains the following columns:

- **Select**

Select the check box in the row to be deleted.

- **Group**

Shows the name of the group.

- **Role**

Select a role. Users who are authenticated with the linked group on the RADIUS server receive the rights of this role locally on the device.

You can choose between system-defined and self-defined roles, refer to the page "Security > Users > Roles."

- **Description**

Enter a description for the link of the group.to a role. The description text can be up to 100 characters long.

Procedure

Linking a group to a role.

1. Enter the name of a group.
2. Click the "Create" button.
3. Select a role.
4. Enter a description for the link of a group.to a role.
5. Click the "Set Values" button.

Deleting the link between a group and a role

1. Select the check box in the row to be deleted.
2. Click the "Delete" button. The entries are deleted and the page is updated.

6.7.3 Passwords

6.7.3.1 Passwords

Configuration of the device passwords

Note

If you are logged in via a RADIUS server, you cannot change any local device passwords.

On this page, you can change passwords. If you are logged on with read/write rights, you can change the passwords for all user accounts. If you are logged in with read rights, you can only change your own password.

Account Passwords

Passwords | **Options**

Current User: admin

Current User Password:

User Account: admin

Password Policy: high

New Password:

Password Confirmation:

Description of the displayed values

The page contains the following boxes:

- **Current User**
Shows the user that is currently logged in.
- **Current User Password**
Enter the password for the currently logged in user.
- **User Account**
Select the user whose password you want to change.

- **Password Policy**
Shows which password policy is being used when assigning new passwords.
 - **High**
Password length: at least 8 characters, maximum 32 characters
At least 1 uppercase letter
At least 1 special character
At least 1 number
 - **Low**
Password length: at least 6 characters, maximum 32 characters
 - **User defined**
Custom password policy

You configure the password policy on the page "Security > Passwords > Options".

- **New Password**
Enter the new password for the selected user.
It cannot contain the following characters:
 - § ? " ; :
 - The character for Delete and blanks also cannot be included.
- **Password Confirmation**
Enter the new password again to confirm it.

Procedure

Note

When you log in for the first time or following a "Restore Factory Defaults and Restart" with the preset user "admin" you will be prompted to change the password. You can also rename the user preset in the factory "admin" once.

The user name and the password are set as follows in the factory:

- admin: admin
-

Note

Changing the password in "Trial" mode

Even if you change the password in "Trial" mode, this change is saved immediately.

1. Enter the password for the currently logged in user in the "Current User Password" input box.
2. In the "User Account" drop-down list select the user whose password you want to change.
3. Enter the new password for the selected user in the "New Password" input box.
4. Repeat the new password in the "Password Confirmation" input box.
5. Click the "Set Values" button.

6.7.3.2 Options

On this page, you specify which password policy will be used when assigning new passwords.

The screenshot shows a web-based configuration interface for password options. At the top, there is a header "Password Options" and a sub-header "Options". Below this, there are two main sections: "Password Policy" and "Password Policy Details".

Password Policy: The current policy is set to "high". The "New Password Policy" is also set to "high" via a dropdown menu.

Password Policy Details:

- Minimum Password Length: 8
- Minimum Number of Numeric Characters: 1
- Minimum Number of Special Characters: 1
- Minimum Number of Uppercase Letters: 1
- Minimum Number of Lowercase Letters: 0

At the bottom of the form, there are two buttons: "Set Values" and "Refresh".

Description

- **Password Policy**
Shows which password policy is currently being used.
- **New Password Policy**
Select the required setting from the drop-down list.
 - High
Password length: at least 8 characters, maximum 128 characters
At least 1 number
At least 1 special character
At least 1 uppercase letter
 - Low
Password length: at least 6 characters, maximum 128 characters
 - User-defined
Configure the desired password requirements under "Password Policy Details".
- **Password Policy Details**
When you have selected the "High" or "Low" password policy, the relevant password requirements are displayed.
When you have selected the "User-defined" password policy, you can configure the relevant password requirements.
 - Minimum Password Length
Specifies the minimum length of a password.
 - Minimum Number of Numeric Characters
Specifies the minimum number of numeric characters in a password.
 - Minimum Number of Special Characters
Specifies the minimum number of special characters in a password.
 - Minimum Number of Uppercase Letters
Specifies the minimum number of uppercase characters in a password.
 - Minimum Number of Lowercase Letters
Specifies the minimum number of lowercase characters in a password.

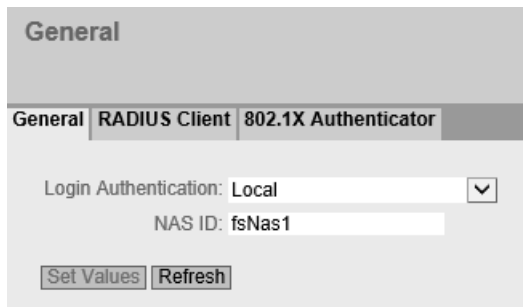
6.7.4 AAA

6.7.4.1 General

Login of network nodes

The designation used "AAA" stands for "Authentication, Authorization, Accounting". This feature is used to identify and allow network nodes and to make the corresponding services available to them.

On this page, you configure the login.



Description of the displayed boxes

The page contains the following boxes:

Note

To be able to use the login authentication "RADIUS", a RADIUS server must be stored and configured for user authentication.

- **Login Authentication**
Specify how the login is made:
 - Local
The authentication must be made locally on the device.
 - RADIUS
The authentication must be handled via a RADIUS server.
 - Local and RADIUS
The authentication is possible both with the users that exist on the device (user name and password) and via a RADIUS server. The user is first searched for in the local database. If the user does not exist there, a RADIUS request is sent.
 - RADIUS and fallback Local
The authentication must be handled via a RADIUS server. A local authentication is performed only when the RADIUS server cannot be reached in the network.
- **NAS ID**
Enter the NAS ID (Network Access Server Identifier) in this text box. The NAS ID identifies the device that sends a request to a RADIUS server.

6.7.4.2 RADIUS Client

Authentication over an external server

The concept of RADIUS is based on an external authentication server.

Each row of the table contains access data for one server. In the search order, the primary server is queried first. If the primary server cannot be reached, secondary servers are queried in the order in which they are entered.

If no server responds, there is no authentication.

Remote Authentication Dial In User Service (RADIUS) Client

General | RADIUS Client | 802.1X Authenticator

RADIUS Authorization Mode: Standard
 Disconnect Packet

Select	Auth. Server Type	RADIUS Server Address	Server Port	Shared Secret
<input type="checkbox"/>	Login & 802.1X <input type="button" value="v"/>	0.0.0.0	1812	••••••
<input type="checkbox"/>	Login & 802.1X <input type="button" value="v"/>	10.0.0.1	1812	••••••

2 entries.

Continuation of table:

Shared Secret Conf.	Max. Retrans.	Timeout[s]	Primary Server	Test	Test Result
	3	5	no <input type="button" value="v"/>	<input type="button" value="Test"/>	

Description of the displayed boxes

The page contains the following boxes:

- **RADIUS Authorization Mode**

For the login authentication, the RADIUS authorization mode specifies how the rights are assigned to the user with a successful authentication (Page 460).

- Standard

In this mode, the user is logged in with administrator rights if the server returns the value "Administrative User" to the device for the attribute "Service Type". In all other cases the user is logged in with read rights.

- Vendor Specific

In this mode, the assignment of rights depends on whether and which group the server returns for the user and whether or not there is an entry for the user in the table "External User Accounts".

- **Disconnect Packet**

If you select this check box, the device evaluates the Disconnect messages of the RADIUS server.

The table has the following columns:

- **Select**
Select the row you want to delete.
- **Auth. Server Type**
Select the which authentication method the server will be used for.
 - Login
The server is used only for the login authentication.
 - 802.1X
The server is used only for the 802.1X authentication.
 - Login & 802.1X
The server is used for both authentication procedures.
- **RADIUS Server Address**
Enter the IP address or the FQDN of the RADIUS server.
- **Server Port**
Here, enter the input port on the RADIUS server. As default, input port 1812 is set. The range of values is 1 to 65535.
- **Shared Secret**
Enter your access ID here. The range of values is 1...128 characters.
- **Shared Secret Conf.**
Enter your access ID again as confirmation.
- **Max. Retrans.**
Here, enter the maximum number of retries for an attempted request.
The initial connection attempt is repeated the number of times specified here before another configured RADIUS server is queried or the login counts as having failed. As default 3 retries are set, this means 4 connection attempts. The range of values is 1 to 5.
- **Timeout [s]**
Enter the time for which the client waits from a response from the RADIUS server here.
- **Primary Server**
Using the options in the drop-down list, specify whether or not this server is the primary server. You can select one of the options "yes" or "no".
- **Test**
With this button, you can test whether or not the specified RADIUS server is available. The test is performed once and not repeated cyclically.
- **Test Result**
Shows whether or not the RADIUS server is available:
 - Not reachable
The IP address is not reachable.
The IP address is reachable, the RADIUS server is, however, not running.
The IP address is reachable, the RADIUS server does not, however accept the specified shared secret.
 - Reachable, key accepted
The IP address is reachable, the RADIUS server accepts the specified shared secret.

The test result is not automatically updated. To delete the test result click the "Refresh" button.

Configuration procedure

Entering a new server

1. Click the "Create" button. A new entry is generated in the table.
The following default values are entered in the table:
 - Auth. Server Type: Login & 802.1X
 - RADIUS Server Address: 0.0.0.0
 - Server Port: 1812
 - Max. Retrans.: 3
 - Primary server: No
 2. In the relevant row, enter the following data in the input boxes:
 - Required Auth. Server Type
 - RADIUS Server Address
 - Server Port
 - Shared Secret
 - Confirm Shared Secret
 - Max. Retrans.: 3
 - Primary server: Yes/No
 3. Click the "Set Values" button.
 4. If necessary, test the reachability of the RADIUS server.
- Repeat this procedure for every server you want to enter.

Modifying servers

1. In the relevant row, enter the following data in the input boxes:
 - RADIUS Server Address
 - Server Port
 - Shared Secret
 - Confirm Shared Secret
 - Max. Retrans.
 - Primary Server
 2. Click the "Set Values" button.
 3. If necessary, test the reachability of the RADIUS server.
- Repeat this procedure for every server whose entry you want to modify

6.7 The "Security" menu

Deleting servers

1. Click the check box in the first column before the row you want to delete to select the entry for deletion.
Repeat this for all entries you want to delete.
2. Click the "Delete" button. The data is deleted from the memory of the device and the page is updated.

6.7.4.3 802.1X Authenticator

Setting up network access

An end device can only access the network after the device has verified the login data of the device with the authentication server. The authentication can be via 802.1X or the MAC address.

When authenticating using 802.1X both the end device and the authentication server must support the EAP protocol (Extensive Authentication Protocol).

Enabling authentication for individual ports

By enabling the relevant options, you specify for each port whether or not network access protection according to IEEE 802.1X is enabled on this port.

802.1X Authenticator ? 📄 ★

General | RADIUS Client | **802.1X Authenticator**

MAC Authentication
 Guest VLAN

802.1X Fallback Timeout[s]:
 802.1X Fallback Retry Count:

	802.1X Auth. Control	802.1X Re-Authentication	Re-Authentication Timeout[s]	Tx Timeout[s]	MAC Authentication	MAC Auth. only on Timeout
All ports	No Change ▼	No Change ▼	No Change	No Change	No Change ▼	No Change ▼

Port	802.1X Auth. Control	802.1X Re-Authentication	Re-Authentication Timeout[s]	Tx Timeout[s]	MAC Authentication	MAC Auth. only on Timeout
P0.1	Force Authorized ▼	<input type="checkbox"/>	3600	5	Disabled ▼	<input type="checkbox"/>
P0.2	Force Authorized ▼	<input type="checkbox"/>	3600	5	Disabled ▼	<input type="checkbox"/>
P0.3	Force Authorized ▼	<input type="checkbox"/>	3600	5	Disabled ▼	<input type="checkbox"/>

Continuation of table:

RADIUS VLAN Assignment Allowed	Default VLAN ID	MAC Auth. Max Allowed Addresses	Guest VLAN	Guest VLAN ID	Guest VLAN Max Allowed Addresses	Copy to Table
No Change ▼	No Change	No Change	No Change ▼	No Change	No Change	Copy to Table

RADIUS VLAN Assignment Allowed	Default VLAN ID	MAC Auth. Max Allowed Addresses	Guest VLAN	Guest VLAN ID	Guest VLAN Max Allowed Addresses
<input type="checkbox"/>	0	1	<input type="checkbox"/>	1	1
<input type="checkbox"/>	0	1	<input type="checkbox"/>	1	1

Description

The page contains the following boxes:

- **MAC Authentication**
Enable or disable MAC Authentication for the device.
- **Guest VLAN**
Enable or disable the "Guest VLAN" function for the device.
- **802.1X Fallback Timeout [s]**
Specify the time interval in seconds after which the device is reinitialized for 802.1X authentication at the relevant port if MAC authentication was not successful. The default value is 0 seconds, i.e. there is no fallback timeout and no reinitialization for the 802.1X authentication.
- **802.1X Fallback Retry Count**
Specify how often the port is reinitialized for 802.1X authentication if MAC authentication was not successful.

Table 1 has the following columns:

- **1st column**
Shows that the settings are valid for all ports of table 2.
- **802.1X Auth. Control**
Select the required setting.
If "No Change" is selected, the entry in table 2 remains unchanged.
- **802.1X Re-Authentication**
Select the required setting.
If "No Change" is selected, the entry in table 2 remains unchanged.
- **Re-Authentication Timeout[s]**
Specify the time interval in seconds after which the device is reauthenticated at the relevant port. The default value is 3600 seconds.
If "No Change" is selected, the entry in table 2 remains unchanged.
- **Tx Timeout[s]**
Select the required setting.
If "No Change" is selected, the entry in table 2 remains unchanged.

- **MAC Authentication**

Configure MAC authentication for a port:

- Disabled
MAC authentication is disabled for the port.
- Enabled
Select this option for the port if end devices are to be authenticated using the "MAC Authentication" method.
If "Auto" is configured for "802.1x Auth. Control" and the "MAC Authentication" is enabled, the timeout for the "802.1X" procedure is 5 seconds. If manual input is necessary at a port for the authentication with the "802.1X" procedure, the 5 seconds may not be adequate. To be able to run authentication using "802.1X", disable the MAC authentication on this port.
- Sticky
If this parameter is configured, new MAC addresses are automatically authenticated or rejected depending on the number of currently authenticated MAC addresses on a port (MAC Auth. Max Allowed Addresses).
If a new MAC address requests on a port and the number of currently authenticated MAC addresses on the port is < the number of maximum permitted MAC addresses, the request is automatically successful.
If a new MAC address requests on a port and the number of currently authenticated MAC addresses on the port is \geq the number of maximum permitted MAC addresses, the request automatically fails.
MAC addresses authenticated through this mechanism are stored as static MAC addresses. The authentication status is retained during link change events and restart of the device. You must delete the MAC addresses manually.

Note

Requirements:

- The parameter is only active if MAC Authentication is globally enabled for the device.
- The "802.1X Auth. Control" is configured to "Force Authorized".
- A value ≥ 1 and ≤ 5 is configured for "MAC Auth. Max Allowed Addresses".
- The number of statically configured MAC addresses on a port is \leq the maximum number of permitted addresses.

Note

No RADIUS server configuration is required for this parameter.

If the parameter is configured, the following applies to the corresponding port:

- Only values ≤ 5 can be configured for "MAC Auth. Max Allowed Addresses".
 - New static MAC addresses can only be configured on the port as long as their number is < the number of maximum permitted MAC addresses ("MAC Auth. Max Allowed Addresses").
-

- **MAC Auth only on Timeout**

Select the required setting.

If "No Change" is selected, the entry in table 2 remains unchanged.

- **RADIUS VLAN Assignment Allowed**

Select the required setting.

If "No Change" is selected, the entry in table 2 remains unchanged.

Note

The VLAN assignment of RADIUS is only applied if the port has not already been configured for this VLAN. If the port VLAN ID matches the VLAN ID assigned by RADIUS, the type of membership in this VLAN must be preconfigured.

Note**Private VLAN functionality and RADIUS authentication**

When VLAN assignment is enabled via RADIUS authentication for one or more ports of a VLAN, you should not configure this VLAN additionally as private VLAN.

The private VLAN functionality in connection with VLAN assignment via RADIUS authentication can result in an inconsistent system state.

- **Default VLAN ID**

Specify the desired VLAN ID.

If "No Change" is selected, the entry in table 2 remains unchanged.

- **MAC Auth. Max Allowed Addresses**

Specify how many MAC addresses can communicate on the port at the same time.

If "No Change" is entered, the entry in table 2 remains unchanged.

- **Guest VLAN**

Select the required setting.

If "No Change" is selected, the entry in table 2 remains unchanged.

- **Guest VLAN ID**

Specify the VLAN ID of the port.

If "No Change" is entered, the entry in table 2 remains unchanged.

- **Guest VLAN Max Allowed Addresses**

Specify how many end devices are allowed on this port in the "Guest VLAN" at the same time.

If "No Change" is entered, the entry in table 2 remains unchanged.

- **Copy to Table**

If you click the button, the settings are adopted for all ports of table 2.

Table 2 has the following columns:

- **Port**
This column lists all the ports available on this device.
- **802.1X Auth. Control**
Specify the authentication of the port:
 - Force Unauthorized
Data traffic via the port is blocked.
 - Force Authorized
Data traffic via the port is allowed without any restrictions.
Factory setting
 - Auto
End devices are authenticated on the port with the "802.1X" method.
The data traffic via the port is permitted or blocked depending on the authentication result.
- **802.1X Re-Authentication**
Enable this option if you want reauthentication of an already authenticated end device to be repeated cyclically.
- **Re-Authentication Timeout[s]**
Specify the time interval in seconds after which the device is reauthenticated at the relevant port. The default value is 3600 seconds.
- **Tx Timeout[s]**
The value specifies the period of time in seconds after which an EAP request packet is sent if no client responds. If MAC authentication is enabled, a switch is made from 802.1X authentication to MAC authentication after the third EAP request packet.
The default value is 5 seconds.
- **MAC Authentication**
Enable this option if you want end devices to be authenticated with the "MAC Authentication" method.
If "Auto" is configured for "802.1x Auth. Control" and the "MAC Authentication" is enabled, the timeout for the "802.1X" procedure is 5 seconds. If manual input is necessary at a port for the authentication with the "802.1X" procedure, the 5 seconds may not be adequate. To be able to run authentication using "802.1X", disable the MAC authentication on this port.
- **MAC Auth only on Timeout**
If this check box is selected, MAC authentication is only possible after a 802.1X timeout, but not after a failed 802.1X authentication. When the check box is not selected, MAC authentication is possible both after an 802.1X timeout and after a failed 802.1X authentication.
- **Adopt RADIUS VLAN Assignment**
The RADIUS server informs the IE switch of the VLAN to which the port will belong. Enable this option if you want the information of the server to be taken into account.
The port can only be assigned to the VLAN, if the VLAN has been created on the device.
Otherwise, authentication (Page 460) is rejected.

- **Default VLAN ID**

If a VLAN ID is transmitted to the RADIUS server during a successful authentication and the "RADIUS VLAN Assignment Allowed" check box is selected, the current PVID of the port is changed to the value transmitted by the RADIUS server. Otherwise, an "Untagged membership" of the port may be set up in the relevant VLAN to enable communication in the respective VLAN.

The Default VLAN ID determines the assignment of the VLAN ID when the "RADIUS VLAN Assignment Allowed" check box is selected, but the RADIUS server does not send a VLAN ID after successful authentication. You have two options:

- **The value "0" is configured for the default VLAN ID**

The PVID currently configured for the port continues to be used.

- **A value in the range from "1 ... 4094" is configured for the Default VLAN ID**

The PVID of the port is changed to the "Default VLAN ID" configured in this column as if it had been transmitted by the RADIUS server.

In all cases, a changed PVID is reset to the originally configured value after the device logs out. Any "Port membership" that has been set up is deleted again. This applies to both 802.1X authentication and MAC authentication.

- **MAC Auth. Max Allowed Addresses**

- 1 - 200

Specify how many MAC addresses can communicate on the port at the same time.

Note

If a device uses several MAC addresses, all MAC addresses must be authenticated. Store all the MAC addresses to be authenticated on the RADIUS server. Enter the number in the "MAC Auth. Max Permitted Addresses" box.

- 0

You can set the value "0". This setting has the effect that after the first successful authentication of a MAC address, the port is released for all MAC addresses.

Use case

If you configure the value "0" for a port, connect this port to a WLAN access point. After the AP has authenticated itself successfully, all MAC addresses are released on this port. All WLAN clients connected to the AP can communicate on the port without their own authentication. Make sure that the clients are authenticated by the AP.

- **Guest VLAN**

Enable this option if you want the end device to be permitted in the guest VLAN if authentication fails.

The port can only be assigned to the VLAN, if the VLAN has been created on the device. Otherwise Authentication (Page 460) is rejected.

This function is also known as "Authentication failed VLAN".

- **Guest VLAN ID**

Enter the VLAN ID of the guest VLAN.

- **Guest VLAN Max Allowed Addresses**

Specify how many end devices are allowed on this port in the "Guest VLAN" at the same time. Range of values: 1 - 100

Configuration procedure

Enable authentication for an individual port

1. Select the required options in the relevant row in table 2.
2. To apply the changes, click the "Set Values" button.

Enable authentication for all ports

1. Select the required options in table 1.
2. Click the "Copy to Table" button. The relevant settings are adopted for all ports in table 2.
3. To apply the changes, click the "Set Values" button.

6.7.5 MAC ACL

6.7.5.1 Rules Configuration

On this page, you specify the access rules for the MAC-based Access Control List (MAC ACL). MAC ACLs can be used with physical ports. Using the MAC-based ACL, you can specify whether frames of certain MAC addresses are forwarded or discarded. The maximum number of ACL rules can be found in the WBM section "Configuration limits (Page 22)".

MAC Access Control List Configuration

Rules Configuration | **Ingress Rules** | Egress Rules

Priority:

Select	Rule Number	Priority	Source MAC	Dest. MAC	Action	Ingress Interfaces	Egress Interfaces
<input type="checkbox"/>	1	5	00-00-00-00-00-00	00-00-00-00-00-00	Forward ▼	P0.1,P0.5	P0.1
<input type="checkbox"/>	2	3	00-00-00-00-00-00	00-00-00-00-00-00	Forward ▼	P0.1	

2 entries.

Description

The page contains the following boxes:

- **Priority**
Assign a priority for the ACL rule.
Range of values: 1 ... 255.
The greater the value, the higher the priority. Rules with the priority 255 therefore have the highest priority and are processed first.

Note

Processing order of the lists

However, multiple ACL rules with the same priority can be assigned to the same port. In this case, note that the rule order is not clearly defined. Rules with the same port can only be assigned to the same port if the order of processing is not important.

The table has the following columns:

- **Select**
Select the row you want to delete. If this entry is used, this is grayed out and you cannot delete it.
- **Rule Number**
Shows the number of the ACL rule. If you create a new entry, a new line with a unique number is created.
- **Priority**
Contains the previously specified priority.
- **Source MAC Address**
Enter the MAC address of the source. Only a unicast MAC address can be set as source MAC address.
- **Dest. MAC Address**
Enter the MAC address of the destination.
- **Action**
Select whether the frame is forwarded or rejected when it corresponds to the ACL rule.
 - Forward
If the frame complies with the ACL rule, the frame is forwarded.
 - Discard
If the frame complies with the ACL rule, the frame is not forwarded.
- **Ingress Interfaces**
Shows a list of all ingress interfaces to which this rule applies.
- **Egress Interfaces**
Shows a list of all egress interfaces to which this rule applies.

Note**Entering the MAC addresses**

You can configure access rules for MAC addresses.

The rule created in this way only applies to all source or destination MAC addresses if you enter the address "00-00-00-00-00-00" for the source and/or destination MAC address.

Note**Loop detection**

Activating loop detection can prevent rules for Multicast MAC addresses from being applied.

Note

No ACL rules for locally supported protocols

ACL rules are not applied to packets from locally supported protocols. This restriction applies to the following protocols:

- HRP
- Standby
- DCP
- LLDP
- RSTP
- MRP

Make the specifications for receiving and sending packets for these protocols directly on the configuration page of the respective protocol.

Creating rules

1. In the "Priority" field, specify a numerical value as the priority for the ACL rule.
2. Click the "Create" button. A new row with a unique number (rule number) is created in the table.
3. Enter the MAC address of the source in "Source MAC Address".
4. Enter the MAC address of the destination in "Dest. MAC Address".
5. In the "Action" drop-down list select whether the frame is forwarded or rejected when it corresponds to the ACL rule.
6. Click the "Set Values" button.

Deleting rules

1. Enable "Select" in the row to be deleted.
2. Click the "Delete" button. The entry is deleted.

6.7.5.2 Ingress Rules

Introduction

On this page, you specify the ACL rule according to which incoming frames are filtered at interfaces. You specify the ACL rules in the "Rules Configuration" tab.

MAC ACL Ingress Rules

Rules Configuration |
 Ingress Rules |
 Egress Rules

Interface:

Add Rule:

Remove Rule:

Priority▲	Rule Number	Source MAC	Dest. MAC	Action
3	2	00-00-00-00-00-00	00-00-00-00-00-00	Forward ▼
5	1	00-00-00-00-00-00	00-00-00-00-00-00	Forward ▼

2 entries.

Description

The page contains the following boxes:

- **Interface**
Select the required interface from the drop-down list. The available interfaces depend on your device.
- **Add Rule**
In the drop-down list, select the ACL rule to be assigned to the interface.
- **Add**
To assign the ACL rule to the interface, click the "Add" button. The configuration is shown in the table.
- **Remove Rule**
From the "Remove Rule" drop-down list, select the ACL rule to be deleted.
- **Remove**
To remove the ACL rule from the interface, click the "Remove" button.

The table has the following columns:

- **Priority**
Shows the order of the ACL rules.
- **Rule Number**
Shows the number of the ACL rule.

6.7 The "Security" menu

- **Source MAC address**
Shows the MAC address of the source.
- **Destination MAC Address**
Shows the MAC address of the destination.
- **Action**
Shows the action.
 - Forward
If the frame complies with the ACL rule, the frame is forwarded.
 - Discard
If the frame complies with the ACL rule, the frame is not forwarded.

Configuration procedure

Follow the steps below to assign an ACL rule to an interface:

1. Select the interface from the "Interface" drop-down list.
2. Select the ACL rule in the "Add Rule" drop-down list.
3. Click the "Add" button. A new entry is generated in the table.

Follow the steps below to remove an ACL rule from an interface:

1. Select the interface from the "Interface" drop-down list.
2. Select the ACL rule in the "Remove Rule" drop-down list.
3. Click the "Remove" button. The corresponding entry is removed in the table.

6.7.5.3 Egress Rules

Introduction

On this page, you specify the ACL rules according to which outgoing frames are filtered at interfaces. You specify the ACL rule in the "Rules Configuration" tab.

MAC ACL Egress Rules

Rules Configuration |
 Ingress Rules |
 Egress Rules

Interface: P0.1 ▼

Add Rule: Rule 2 ▼

Add

Remove Rule: Rule 1 ▼

Remove

Priority	Rule Number	Source MAC	Dest. MAC	Action
5	1	00-00-00-00-00-00	00-00-00-00-00-00	Forward ▼

1 entry.

Refresh

Description of the displayed boxes

The page contains the following boxes:

- **Interface**
Select the required interface from the drop-down list. The available interfaces depend on your device.
- **Add Rule**
In the drop-down list, select the ACL rule to be assigned to the interface.
- **Add**
To assign the ACL rule to the interface, click the "Add" button. The configuration is shown in the table.
- **Remove Rule**
From the "Remove Rule" drop-down list, select the ACL rule to be deleted.
- **Remove**
To remove the ACL rule from the interface, click the "Remove" button.

The table has the following columns:

- **Priority**
Shows the order of the ACL rules.
- **Rule Number**
Shows the number of the ACL rule.
- **Source MAC address**
Shows the MAC address of the source.

6.7 The "Security" menu

- **Destination MAC Address**
Shows the MAC address of the destination.
- **Action**
Shows the action.
 - Forward
If the frame complies with the ACL rule, the frame is forwarded.
 - Discard
If the frame complies with the ACL rule, the frame is not forwarded.

Configuration procedure

Follow the steps below to assign an ACL rule to an interface:

1. Select the interface from the "Interface" drop-down list.
2. Select the ACL rule in the "Add Rule" drop-down list.
3. Click the "Add" button. A new entry is generated in the table.

Follow the steps below to remove an ACL rule from an interface:

1. Select the interface from the "Interface" drop-down list.
2. Select the ACL rule in the "Remove Rule" drop-down list.
3. Click the "Remove" button. The corresponding entry is removed in the table.

6.7.6 IP ACL

6.7.6.1 Rules Configuration

On this page, you specify the rules for the IP-based Access Control List (IP ACL). IP ACLs can be used with physical ports and IP interfaces. Using the IP-based ACL, you can specify whether packets of certain IPv4 addresses are forwarded or discarded. The maximum number of ACL rules can be found in the WBM section "Configuration limits (Page 22)".

IP Access Control List Configuration

Rules Configuration | Protocol Configuration | Ingress Rules | Egress Rules

Priority:

Select	Rule Number	Priority	Source IP	Source Subnet Mask	Dest. IP	Dest. Subnet Mask	Action	Ingress Interfaces	Egress Interfaces
<input type="checkbox"/>	1	7	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	Forward	P0.1	P0.1
<input type="checkbox"/>	2	2	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	Forward	P0.1	

2 entries.

[Create](#) [Delete](#) [Set Values](#) [Refresh](#)

Description

The page contains the following boxes:

- **Priority**
Assign a priority for the ACL rule.
Range of values: 1 ... 255.
The greater the value, the higher the priority. Rules with the priority 255 therefore have the highest priority and are processed first.

Note

Processing order of the lists

However, multiple ACL rules with the same priority can be assigned to the same port. In this case, note that the rule order is not clearly defined. Rules with the same port can only be assigned to the same port if the order of processing is not important.

The table has the following columns:

- **Select**
Select the row you want to delete. If this entry is used, this is grayed out and you cannot delete it.
- **Rule Number**
Shows the number of the ACL rule. If you create a new entry, a new line with a unique number is created.
- **Priority**
Contains the previously specified priority.
- **Source IP**
Enter the IPv4 address of the source.
- **Source Subnet Mask**
Enter the subnet mask of the source.
- **Dest. IP**
Enter the IPv4 address of the destination.
- **Dest. Subnet Mask**
Enter the subnet mask of the destination.
- **Action**
Select whether the frame is forwarded or rejected when it corresponds to the ACL rule.
 - Forward
If the frame complies with the ACL rule, the frame is forwarded.
 - Discard
If the frame complies with the ACL rule, the frame is not forwarded.
- **Ingress Interfaces**
Shows a list of all ingress interfaces to which this rule applies.
- **Egress Interfaces**
Shows a list of all egress interfaces to which this rule applies.

Note

Subnet mask for individual hosts

If you create the rule for a single system (one IPv4 address), specify the subnet mask "255.255.255.255".

If the rule is to apply to all IP addresses, enter the IP address "0.0.0.0" and the subnet mask "0.0.0.0".

Creating rules

1. In the "Priority" field, specify a numerical value as the priority for the ACL rule.
2. Click the "Create" button. A new row with a unique number (rule number) is created in the table.
3. Enter the data of the source in "Source IP" and in "Source Subnet Mask".
4. Enter the data of the destination in "Dest. IP" and in "Dest. Subnet Mask".
5. In the "Action" drop-down list select whether the frame is forwarded or rejected when the frame corresponds to the ACL rule.
6. Click the "Set Values" button.

Deleting rules

1. Enable "Select" in the row to be deleted.
2. Click the "Delete" button. The entry is deleted.

6.7.6.2 Protocol Configuration

On this page, you specify the rules for protocols.

IP ACL Protocol Configuration

Rules Configuration Protocol Configuration Ingress Rules Egress Rules									
Rule Number	Protocol	Protocol Number	Source Port Min.	Source Port Max.	Dest. Port Min.	Dest. Port Max.	Message Type	Message Code	DSCP
1	Any	255	0	65535	0	65535	255	255	
1 entry.									
<input type="button" value="Refresh"/>									

Description

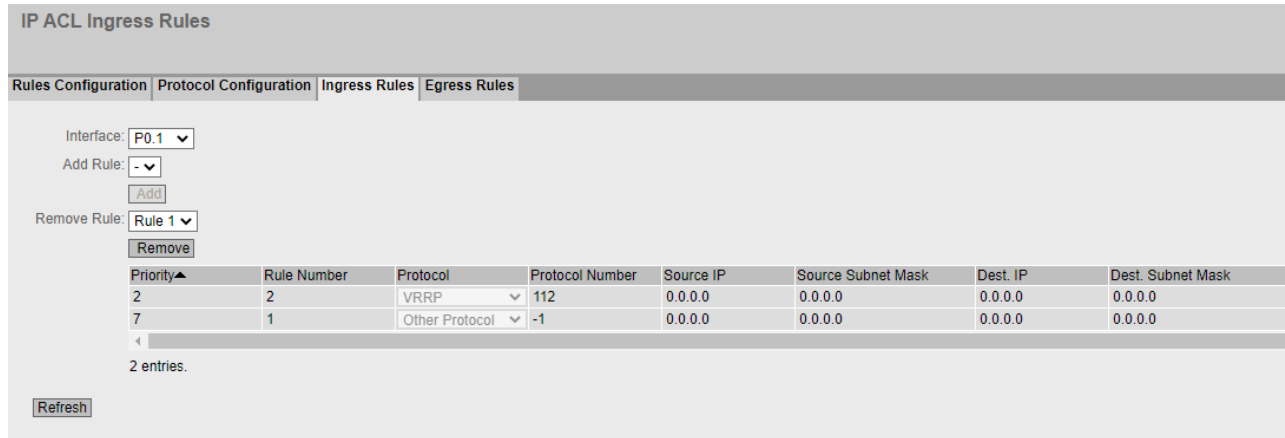
The table has the following columns:

- **Rule Number**
Shows the number of the protocol rule. When you create a rule, a new row with a unique number is created.
- **Protocol**
Select the protocol for which this rule is valid.
 - IP
 - OSPF
 - VRRP
 - ICMP
 - TCP
 - UDP
 - Any
 - Other Protocol
- **Protocol Number**
Enter a protocol number to define further protocols.
This box can only be edited if you have set "Other Protocol" for the protocol.
- **Source Port Min.**
Enter the lowest possible port number of the source port.
This box can only be edited if you have set "TCP" or "UDP" for the protocol.
- **Source Port Max.**
Enter the highest possible port number of the source port.
This box can only be edited if you have set "TCP" or "UDP" for the protocol.
- **Dest. Port Min.**
Enter the lowest possible port number of the destination port.
This box can only be edited if you have set "TCP" or "UDP" for the protocol.
- **Dest. Port Max.**
Enter the highest possible port number of the destination port.
This box can only be edited if you have set "TCP" or "UDP" for the protocol.
- **Message Type**
Enter a message type to decide the format of the message.
This box can only be edited if you have set "ICMP" for the protocol.
- **Message Code**
Enter a message code to specify the function of the message.
This box can only be edited if you have set "ICMP" for the protocol.
- **DSCP**
Enter a value for classifying the priority.
This box cannot be edited if you have set "ICMP" for the protocol.

6.7.6.3 Ingress Rules

Introduction

On this page, you specify the ACL rules according to which incoming packets are handled by interfaces. You specify the ACL rules in the "Rules Configuration" tab.



Continuation of table:

Action	Source Port Min.	Source Port Max.	Dest. Port Min.	Dest. Port Max.	Message Type	Message Code	DSCP
Forward	0	65535	0	65535	-1	-1	
Forward	0	65535	0	65535	-1	-1	

Description

The page contains the following boxes:

- Interface**
 Select the required interface from the drop-down list. The available interfaces depend on your device.
 To select a VLAN interface, an IP interface must be configured.

Note

If you use a VLAN interface, the ACL rule applies to all ports that belong to the VLAN.

- Add Rule**
 In the drop-down list select the ACL rule to be assigned to the interface.
- Add**
 To permanently assign the ACL rule to the interface, click the "Add" button. The configuration is shown in the table.
- Remove Rule**
 From the "Remove rule" drop-down list, select the ACL rule to be deleted.
- Remove**
 To remove the ACL rule from the interface, click the "Remove" button.

The table has the following columns:

- **Priority**
Shows the priority of the ACL rules.
- **Rule Order**
Shows the order of the ACL rules.
- **Rule Number**
Shows the number of the ACL rule.
- **Protocol**
Shows the protocol for which this rule is valid.
- **Protocol Number**
Shows the protocol number.
- **Source IP**
Shows the IPv4 address of the source.
- **Source Subnet Mask**
Shows the subnet mask of the source.
- **Dest IP**
Shows the IP address of the destination.
- **Dest. Subnet Mask**
Shows the subnet mask of the destination.
- **Action**
Select whether the frame is forwarded or rejected when it corresponds to the ACL rule.
 - Forward
If the frame complies with the ACL rule, the frame is forwarded.
 - Discard
If the frame complies with the ACL rule, the frame is not forwarded.
- **Source Port Min.**
Shows the lowest possible port number of the source port.
- **Source Port Max.**
Shows the highest possible port number of the source port.
- **Dest. Port Min.**
Shows the lowest possible port number of the destination port.
- **Dest. Port Max.**
Shows the highest possible port number of the destination port.
- **Message Type**
Shows a message type to decide the format of the message.
- **Message Code**
Shows a message code to specify the function of the message.
- **DSCP**
Shows a value for classifying the priority.

Configuration procedure

Follow the steps below to assign an ACL rule to an interface:

1. Select the interface from the "Interface" drop-down list.
2. Select the ACL rule in the "Add Rule" drop-down list.
3. Click the "Add" button. A new entry is generated in the table.

Follow the steps below to assign an ACL rule to an interface:

1. Select the interface from the "Interface" drop-down list.
2. Select the ACL rule in the "Remove Rule" drop-down list.
3. Click the "Remove" button. The corresponding entry is deleted.

6.7.6.4 Egress Rules

Introduction

On this page, you specify the ACL rules according to which outgoing packets are handled by interfaces. You specify the ACL rules in the "Rules Configuration" tab.

IP ACL Egress Rules

Rules Configuration | Protocol Configuration | Ingress Rules | **Egress Rules**

Interface: P0.1

Add Rule: Rule 2

Remove Rule: Rule 1

Priority	Rule Number	Protocol	Protocol Number	Source IP	Source Subnet Mask	Dest. IP	Dest. Subnet Mask
7	1	Other Protocol <input type="button" value="v"/>	-1	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0

1 entry.

Continuation of table:

Action	Source Port Min.	Source Port Max.	Dest. Port Min.	Dest. Port Max.	Message Type	Message Code	DSCP
Forward <input type="button" value="v"/>	0	65535	0	65535	-1	-1	

Description

The page contains the following boxes:

- **Interface**
Select the required interface from the drop-down list. The available interfaces depend on the device.
To select a VLAN interface, an IP interface must be configured.

Note

If you use a VLAN interface, the ACL rule applies to all ports that belong to the VLAN.

- **Add Rule**
In the drop-down list select the ACL rule to be assigned to the interface.
- **Add**
To assign the ACL rule to the interface, click the "Add" button. The configuration is shown in the table.

Note

An ACL rule with the content "deny any" must not be applied to outgoing packets.

- **Remove Rule**
From the "Remove rule" drop-down list, select the ACL rule to be deleted.
- **Remove**
To remove the ACL rule from the interface, click the "Remove" button.

The table has the following columns:

- **Priority**
Shows the priority of the ACL rules.
- **Rule Order**
Shows the order of the ACL rules.
- **Rule Number**
Shows the number of the ACL rule.
- **Protocol**
Shows the protocol for which this rule is valid.
- **Protocol Number**
Shows the protocol number.
- **Source IP**
Shows the IPv4 address of the source.
- **Source Subnet Mask**
Shows the subnet mask of the source.
- **Dest IP**
Shows the IP address of the destination.
- **Dest. Subnet Mask**
Shows the subnet mask of the destination.

- **Action**
Select whether the frame is forwarded or rejected when it corresponds to the ACL rule.
 - Forward
If the frame complies with the ACL rule, the frame is forwarded.
 - Discard
If the frame complies with the ACL rule, the frame is not forwarded.
- **Source Port Min.**
Shows the lowest possible port number of the source port.
- **Source Port Max.**
Shows the highest possible port number of the source port.
- **Dest. Port Min.**
Shows the lowest possible port number of the destination port.
- **Dest. Port Max.**
Shows the highest possible port number of the destination port.
- **Message Type**
Shows a message type to decide the format of the message.
- **Message Code**
Shows a message code to specify the function of the message.
- **DSCP**
Shows a value for classifying the priority.

Configuration procedure

Follow the steps below to assign an ACL rule to an interface:

1. Select the interface from the "Interface" drop-down list.
2. Select the ACL rule in the "Add Rule" drop-down list.
3. Click the "Add" button. A new entry is generated in the table.

Follow the steps below to remove an ACL rule from an interface:

1. Select the interface from the "Interface" drop-down list.
2. Select the ACL rule in the "Remove Rule" drop-down list.
3. Click the "Remove" button. The corresponding entry is removed in the table.

6.7.7 Management ACL

Description of configuration

On this page, you can increase the security of your device. To specify which station with which IP address is allowed to access your device, configure the IP address or an entire address range.

You can select the protocols and the ports of the station with which it is allowed to access the device.

Management Access Control List

Management ACL

IP Address:

Subnet Mask:

Select	Rule Order	IP Address	Subnet Mask	VLANs Allowed	SNMP	TELNET	HTTP	HTTPS	SSH	P0.1	P0.2
<input type="checkbox"/>	1	192.168.16.254	255.255.255.255	1-4094	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

1 entry.

Description of the displayed boxes

Note

Before you enable this function, note the following

A bad configuration may mean that you can no longer access the device. You can then only remedy this by resetting the device to the factory defaults and then reconfiguring. You should therefore configure an access rule that allows access to the management before you enable the function.

The page contains the following boxes:

- **Management ACL**
Enable or disable access control to the management of the IE switch. As default, the function is disabled.

Note

If the function is disabled, there is unrestricted access to the management of the IE switch. The configured access rules are only taken into account when the function is enabled.

- **IP Address**
Enter the IPv4 address or the network address for which the rule will apply. If you use the IPv4 address 0.0.0.0, the settings apply to all IPv4 addresses.
- **Subnet Mask**
Enter the subnet mask. The subnet mask 255.255.255.255 is for a specific IPv4 address. If you want to allow a subnet, for example a class C subnet, enter 255.255.255.0. The subnet mask 0.0.0.0 applies to all subnets.

The table has the following columns:

- **Select**
Select the row you want to delete.
- **Rule Order**
Shows the order in which the ACL rules are checked. As soon as a rule matches, it is used. The following rules are ignored.
- **IP Address**
Shows the IPv4 address.

- **Subnet Mask**
Shows the subnet mask.
- **VLANs Allowed**
Enter the number of the VLAN in which the device is located. The station can only access the device if it is located in this configured VLAN. If this input box remains empty, there is no restriction relating to the VLANs.
- **SNMP**
Specify whether the station (or the IPv4 address) can access the device using the SNMP protocol.
- **TELNET**
Specify whether the station (or the IPv4 address) can access the device using the TELNET protocol.
- **HTTP**
Specify whether the station (or the IPv4 address) can access the device using the HTTP protocol.
- **HTTPS**
Specify whether the station (or the IPv4 address) can access the device using the HTTPS protocol.
- **SSH**
Specify whether the station (or the IPv4 address) can access the device using the SSH protocol.
- **Px.y**
Specify whether the station (or the IPv4 address) can access the device via this port. The port is made up of the module number and the port number, for example port 0.1 is module 0, port 1.

Steps in configuration

Note

Before you enable this function, note the following

A bad configuration may mean that you can no longer access the device. You can then only remedy this by resetting the device to the factory defaults and then reconfiguring. You should therefore configure an access rule that allows access to the management before you enable the function.

Note

Keep to the order

The order in which you create the ACL rules corresponds to the order in which the rules are checked. As soon as a rule matches, it is used. The following rules are ignored.

Create new rule

1. Enter the IP address in the "IP Address" input box.
2. Enter the subnet mask in the "Subnet Mask" input box.
3. Click the "Create" button to create a new row in the table.

4. Configure the entries of the new row.
5. Click the "Set Values" button to transfer the new entry to the device.

Enabling function

1. Select the "Management ACL" check box.
2. Click the "Set Values" button to enable the configured access rules.

Change rule

1. Configure the data of the rule you want to change.
2. Click the "Set Values" button to transfer the changes to the device.

Delete rule

1. Select the check box in the row to be deleted.
2. Repeat this procedure for every entry you want to delete.
3. Click the "Delete" button. The rules are deleted and the page is updated.

6.7.8 Brute Force Prevention

Description of configuration

Brute Force Prevention refers to the protection of the device from unauthorized access by trying a sufficiently large number of passwords. The number of incorrect login attempts within a specific time period is limited for this purpose.

Brute Force Prevention ?

User Specific BFP is Enabled

Acceptable Invalid Login Attempts Per User:

IP Specific BFP is Enabled

Acceptable Invalid IP Login Attempts Per IP:

Global Parameters

BFP Trigger Interval[min]:

BFP Automatic Reset Timer[min]:

User Specific BFP:

User	Failed Logins	Last Failed[s]	Blocked[s]	Clear
Unknown User	0	0	not blocked	<input type="button" value="Clear"/>
admin	0	0	not blocked	<input type="button" value="Clear"/>
Service	7	28	692	<input type="button" value="Clear"/>

3 entries.

IP Specific BFP:

IP	Failed Logins	Last Failed[s]	Blocked[s]	Clear
192.168.178.2	0	0	not blocked	<input type="button" value="Clear"/>

Description of the displayed boxes

The page contains the following boxes:

- **User Specific BFP is Enabled / User Specific BFP is Disabled**
Shows whether the user-specific Brute Force Prevention is enabled.
The login authentication determines whether you can enable user-specific Brute Force Prevention. You configure login authentication in the menu "Security > AAA > General" in the "Login Authentication" drop-down list. User-specific Brute Force Prevention is available for the "Local" and "Local and RADIUS" modes, and not available for the "RADIUS" and "RADIUS and Fallback Local" modes.
- **Acceptable Invalid Login Attempts Per User**
The maximum number of invalid login attempts for a user after which login is blocked. All users that are not configured as local users for the device are summarized under the user name "UnknownUser".
If you configure the value "0", user-specific Brute Force Prevention is disabled.
The default value is "12".
- **IP Specific BFP is Enabled.**
Shows whether the IP-specific Brute Force Prevention is enabled.
- **Acceptable Invalid IP Login Attempts Per IP**
The maximum number of invalid login attempts for an IP address after which login is blocked.
If you configure the value "0", IP-specific Brute Force Prevention is disabled.
The default value is "10".
- **BFP Trigger Interval [min]**
The time in minutes that is relevant for counting invalid login attempts. If the number of permitted invalid login attempts is reached during this time (per user or per IP address), the device blocks login for a specific period of time. Invalid login attempts per user and per IP address are handled independently of one another. You can enter a value between 5 and 255 minutes. The default value is 5 minutes.
- **BFP Automatic Reset Timer[min]**
Time in minutes for which the device blocks login because the maximum number of invalid login attempts was exceeded. You can enter a value between 0 and 255 minutes.
If you configure the value "0", login is blocked indefinitely after the maximum number of invalid login attempts is reached.
The default value is 12 minutes.

The **User Specific BFP** table has the following columns:

- **User**
The user who attempted to log in.
- **Failed Logins**
The number of failed login attempts.
- **Last Failed[s]**
Time in seconds since the last failed login attempt. To display the current value, click the "Refresh" button.

- **Blocked[s]**
Shows the status of the user:
 - Not blocked
Login with this user name is possible.
 - Duration
Time in seconds for which login with this user name is blocked. To display the current value, click the "Refresh" button.
If blocking has been lifted due to expiry of the time configured in the "BFP Automatic Reset Timer" box, the status of the user changes to "Not blocked".
 - Indefinitely blocked
Login with this user name is blocked until you manually delete the blocking or restart the device.
- **Delete**
Ends blocking for the user and resets the following displays:
 - The value in the "Last Failed" box is set to "0".
 - The status of the user in the "Blocked" box is set to "Not blocked".

The **IP Specific BFP** table has the following columns:

- **IP**
The IP address of the device for the login attempt.
- **Failed Logins**
The number of failed login attempts.
- **Last Failed**
Time in seconds since the last failed login attempt. To display the current value, click the "Refresh" button.
- **Blocked[s]**
Shows the status of the IP address:
 - Not blocked
Login with this IP address is possible.
 - Duration
Time in seconds for which login with this IP address is blocked. To display the current value, click the "Refresh" button.
If blocking has been lifted due to expiry of the time configured in the "BFP Automatic Reset Timer" box, the status of the IP address changes to "Not blocked".
 - Indefinitely blocked
Login with this IP address is blocked until you manually delete the blocking or restart the device.
- **Delete**
Ends blocking for the IP address and resets the following displays:
 - The value in the "Last Failed" box is set to "0".
 - The status of the IP address in the "Blocked" box is set to "Not blocked".

Troubleshooting/FAQ

7.1 Downloading new firmware using TFTP without WBM and CLI

Firmware

The firmware is signed and encrypted. This ensures that only firmware created by Siemens can be downloaded to the device.

Procedure with Microsoft Windows

You can download new firmware to the device using TFTP. To do this, the device does not need to be reachable either using Web Based Management (WBM) or using the Command Line Interface (CLI). This can be the case if there was a power failure during a firmware update.

When pressing the button, observe the information in the section "Configuration of the SELECT/SET button (Page 247)".

Follow the steps below to load new firmware using TFTP:

1. Turn off the power to the device.
2. Press the SELECT/SET button and reconnect the device to the power supply with the button pressed.
3. Hold down the button until the red fault LED "F" starts to flash.
4. Release the button as long as the red error LED is still flashing..
This time only lasts a few seconds.
The bootloader of the device waits in this status for a new firmware file that you can download by TFTP.
5. Connect a PC to an Ethernet port of the device with an Ethernet cable.
6. Assign an IP address to the device using DHCP or SINEC PNI.
7. In a Windows command prompt, go to the directory where the file with the new firmware is located and use the following command:

```
tftp -i <IP address> put <firmware file>.
```

Note

You can enable TFTP in Microsoft Windows as follows:

"Control Panel" > "Programs and Features" > "Turn Windows features on or off" > "TFTP Client".

Once the firmware has been transferred completely to the device and validated, the device restarts. This may take a few minutes.

7.2 Message: SINEMA configuration not yet accepted

When the following message is displayed in the display area an error has occurred transferring the configuration from STEP 7 Basic / Professional as of V13 to the device:

"SINEMA Configuration not accepted yet. With restart of device, all configuration changes will be lost."

One possible cause is, for example, that during transfer the device was not reachable.

If you now change a parameter directly on the device (WBM/CLI/SNMP) these changes are lost when the device restarts.

Solution

1. Open the relevant STEP 7 project in STEP 7 Basic / Professional
2. Open the project view.
3. Select the device in the project tree.
4. Select the "Go to network view" command in the shortcut menu.
5. Select the device in the network view.
6. In the shortcut menu of the selected device select the command "SCALANCE configuration > Save as start configuration".

Result

The configuration is saved on the device. The message is no longer visible in the display area. A configuration change directly on the device is no longer lost due to a restart of the device.

7.3 Exchange of configuration data with STEP 7 Basic/Professional using a file

You use the two file types "RunningSINEMAConfig" and "SINEMAConfig" ("System > Load&Save > HTTP/TFTP/SFTP") to exchange configuration data between a device (WBM) and STEP7 Basic/Professional using a file. The export/import of a file via STEP 7 Basic/Professional is described below.

Exporting configuration data via STEP 7 Basic/Professional

To export configuration data via STEP 7 Basic/Professional, follow these steps:

1. Open the relevant STEP 7 project in STEP 7 Basic/Professional.
2. Open the project view.
3. Open the network view or the topology view.
4. Open the Hardware catalog.
5. In the hardware catalog, navigate to the device with the relevant article number.
6. Select the desired device with a mouse click.

7.3 Exchange of configuration data with STEP 7 Basic/Professional using a file

7. Set the matching firmware version via the drop-down list of the hardware catalog.
8. Drag-and-drop the device to the network view or to the topology view.
9. Select the device in the network view or in the topology view.
10. Configure the device in the Inspector window under "Properties > General".
11. In the Inspector window, navigate to the "Management" parameter under "Properties > General".
12. In the parameter group "Load / save file", click the "Save to file" button.
13. Select a storage location for the file.
14. Assign a name for the file.
15. Click the "Save" button.
The "Save configuration file" dialog opens.
16. Assign a password for the encryption of the file.

Note

You need this password when you load the file to a device via the WBM.

17. Click the "OK" button.

Importing configuration data via STEP 7 Basic/Professional

To import configuration data via STEP 7 Basic/Professional, follow these steps:

1. Open the relevant STEP 7 project in STEP 7 Basic/Professional.
2. Open the project view.
3. Open the network view or the topology view.
4. Open the Hardware catalog.
5. In the hardware catalog, navigate to the device with the relevant article number.
6. Select the desired device with a mouse click.
7. Set the matching firmware version via the drop-down list of the hardware catalog.
8. Drag-and-drop the device to the network view or to the topology view.
9. Select the device in the network view or in the topology view.
10. In the Inspector window, navigate to the "Management" parameter under "Properties > General".
11. In the parameter group "Load / save file", click the "Load from file" button.
12. Select the desired file.
13. Click the "Open" button.
The "Load configuration file" dialog opens.

14. Enter the password for the decryption of the file.

Note

You assign this password in the WBM under "System > Load&Save > Passwords".

15. Click the "OK" button.

Appendix A "Syslog messages"

The Syslog messages can contain the following parameters:

Parameter	Description	Possible values or example
ip address	IPv4 or IPv6 address	IP address according to RFC1035 or RFC4291 Section 2.2
src port dest port	Port that is shown as decimal number. Format: %d	0 ... 65535
dest mac src mac	MAC address Format: %02x:%02x:%02x;%02x:%02x:%02x	00:0C:29:2F:09:B3
protocol	Name of the service that has generated this event or of the Layer 4 protocol used. Format: %s	Possible entries of: UDP TCP WBM Telnet SSH TFTP SFTP
group	String that identifies the group based on its name Format: %s	it-service
user name	String that identifies the authenticated user based on his/her name without spaces Format: %s	maier
action user name	Identifies the user based on his/her name This is not the authenticated user. Format: %s	Peter.Maier
role	Symbolic name for the group role Format: %s	Administrator
time minute timeout	Number of minutes Format: %d	44
failed login count	Number of failed logins Format: %d	10
max sessions	Number of sessions Format: %d	10
trigger pin	String for an IO pin that triggers the event without spaces Format: %s	D11
firewall rule	String for a firewall rule with spaces Format: %s	Rule1
subject	String for the subject in the certificate. Used as part of the certificate-based authentication with spaces and must also include Unicode characters Format: (% S) or (% S% S) for UTF8 code.	(Peter Maier)

Parameter	Description	Possible values or example
config detail	String for the configuration with spaces Format: %s	OpenVPN
connection name	Name of the VPN connection	to_Baugruppe1
firewall accept	Firewall action executed (accepted package)	ACCEPT
firewall action reject	Firewall action executed (rejected package)	REJECT DROP
length	Length of the network packet (in bytes) Format: %d	52
network interface	Symbolic name of a network interface Format: %s	vlan1

Human user identification and authentication

{Local interface}: User {User name} logged in.

Example	Console: User admin logged in.
Explanation	A user has successfully logged in to the device via a local interface. In the example, the "admin" user successfully logged in via the console interface.
Severity	Info
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 1.1

{Local interface}: User {User name} failed to log in.

Example	Console: User admin failed to log in.
Explanation	Incorrect user name or password specified during login.
Severity	Warning
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 1.1

{Protocol}: User {User name} logged in from {IP address}.

Example	WBM / UDP / TCP / Telnet / SSH / Console / PNIO / PB / OPC: User admin logged in from 192.168.0.1.
Explanation	Valid login information that was specified during login.
Severity	Info
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 1.1

{Protocol}: User {User name} failed to log in from {IP address}.

Example	WBM / UDP / TCP / Telnet / SSH / Console / PNIO / PB / OPC: User admin failed to log in from 192.168.0.1.
Explanation	Incorrect user name or password specified during login.
Severity	Warning

Facility	local0
Standard	IEC 62443-3-3 Reference: SR 1.1

{Local interface}: User {User name} logged out.

Example	Console: User admin logged out.
Explanation	A user has logged out via a local interface of the device. In the example, the "admin" user logged out manually via the console interface.
Severity	Info
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 1.1

{Protocol}: User {User name} logged out from {IP address}.

Example	WBM / UDP / TCP / Telnet / SSH / Console / PNIO / PB / OPC: User admin logged out from 192.168.0.1.
Explanation	Session ended with user logout.
Severity	Info
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 1.1

{Local interface}: Default user {User name} logged in.

Example	Console: Default user admin logged in.
Explanation	A user has successfully logged in to the device via a local device interface with a default user profile and password. In the example, the default user "admin" successfully logged in via the console interface.
Severity	Info
Facility	local0
Standard	IEC 62443-3-3 Reference: n/a (NERC-CIP 007-R5)

{Protocol}: Default user {User name} logged in from {IP address}.

Example	WBM / UDP / TCP / Telnet / SSH / Console / PNIO / PB / OPC: Default user <user name> logged in from 192.168.0.1.
Explanation	Default user has logged in via the IP address.
Severity	Info
Facility	local0
Standard	IEC 62443-3-3 Reference: n/a (NERC-CIP 007-R5)

{Protocol}: {IP address} - No response from the RADIUS server.

Example	WBM / UDP / TCP / Telnet / SSH / Console / PNIO / PB / OPC: 192.168.1.105 - No response from the RADIUS server.
Explanation	No access to the server or the server is not responding.
Severity	Warning

Facility	local0
Standard	IEC 62443-3-3 Reference: SR 1.1

{Protocol}: {IP address} - No response from the IdP server.

Example	WBM / UDP / TCP / Telnet / SSH / Console / PNIO / PB / OPC: 192.168.1.105 - No response from the IdP server.
Explanation	No access to the server or the server is not responding.
Severity	Warning
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 1.1

Account management

{Protocol}: Password protection was enabled for resource {Resource}.

Example	WBM: Password protection was enabled for resource FullReadAccess.
Explanation	Password protection was enabled for this resource.
Severity	Info
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 1.3

{Protocol}: Authentication was enabled.

Example	WBM: Authentication was enabled.
Explanation	Authentication was enabled.
Severity	Info
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 1.3

{Protocol}: Password protection was disabled for resource {Resource}.

Example	WBM: Password protection was disabled for resource FullReadAccess.
Explanation	Password protection was disabled for this resource.
Severity	Info
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 1.3

{Protocol}: Authentication was disabled.

Example	WBM: Authentication was disabled.
Explanation	Authentication was disabled.
Severity	Info
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 1.3

{Protocol}: User {User name} changed own password.

Example	WBM: User admin changed own password.
Explanation	User has changed own password.
Severity	Info
Facility	local0
Standard	IEC 62443-3-3 Reference: SR1.3

{Protocol}: User {User name} changed password of user {Action user name}.

Example	Telnet: User admin changed password of user test.
Explanation	User has changed the password of another user.
Severity	Info
Facility	local0
Standard	IEC 62443-3-3 Reference: SR1.3

{Protocol}: User {User name} disabled user-account {Destination user name}.

Example	WBM / UDP / TCP / Telnet / SSH / Console / PNIO / PB / OPC: User <User name> disabled user-account {Destination user name}.
Explanation	An authenticated user blocks the user account of another user.
Severity	Info
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 2.4

{Protocol}: User {User name} enabled user-account {Destination user name}.

Example	WBM / UDP / TCP / Telnet / SSH / Console / PNIO / PB / OPC: User <User name> enabled user-account {Destination user name}.
Explanation	An authenticated user blocks the user account of another user.
Severity	Info
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 2.4

{Protocol}: Default admin account was changed to {User name}.

Example	WBM / UDP / TCP / Telnet / SSH / Console / PNIO / PB / OPC: Default admin account was changed to maier.
Explanation	The default administrator account was changed.
Severity	Info
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 1.3

{Protocol}: Default user account was changed to {User name}.

Example	WBM / UDP / TCP / Telnet / SSH / Console / PNIO / PB / OPC: Default user account was changed to <new user>.
Explanation	The default account was changed.
Severity	Info

Facility	local0
Standard	IEC 62443-3-3 Reference: SR 1.3

{Protocol}: User {User name} created user-account {Action user name}.

Example	WBM: User admin created user-account service.
Explanation	The user has created an account.
Severity	Info
Facility	local0
Standard	IEC 62443-3-3 Reference: SR1.3

{Protocol}: User {User name} changed user-account {Destination user name} with role {Role}.

Example	WBM / UDP / TCP / Telnet / SSH / Console / PNIO / PB / OPC: User admin changed user-account admin2 with role Administrator.
Explanation	The administrator has changed an existing account.
Severity	Info
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 1.3

{Protocol}: User {User name} deleted user-account {Action user name}.

Example	WBM: User admin deleted user-account service.
Explanation	The administrator deleted an existing account.
Severity	Info
Facility	local0
Standard	IEC 62443-3-3 Reference: SR1.3

Authorization enforcement

{Protocol}: The firewall {Firewall rule} for User {User name} was granted. Timeout is {Timeout} min.

Example	WBM / UDP / TCP / Telnet / SSH / Console / PNIO / PB / OPC: The firewall Rule 1 for User admin was granted. Timeout is 44 min.
Explanation	Access to important resources was granted.
Severity	Info
Facility	local0
Standard	IEC 62443-3-3 Reference: n/a (NERC-CIP 005-R2)

{Protocol}: The firewall {Firewall rule} for {Trigger pin} was granted. Timeout is {Timeout} min.

Example	WBM / UDP / TCP / Telnet / SSH / Console / PNIO / PB / OPC: The firewall Rule 1 for DI1 was granted. Timeout is 44 min.
Explanation	Access to important resources was granted.
Severity	Info

Facility	local0
Standard	IEC 62443-3-3 Reference: n/a (NERC-CIP 005-R2)

{Protocol}: The firewall {Firewall rule} for User {User name} was denied.

Example	WBM / UDP / TCP / Telnet / SSH / Console / PNIO / PB / OPC: The firewall Rule 1 for User admin was denied.
Explanation	Access to important resources was denied.
Severity	Warning
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 2.1

{Protocol}: The firewall {Firewall rule} for {Trigger pin} was denied.

Example	WBM / UDP / TCP / Telnet / SSH / Console / PNIO / PB / OPC: The firewall Rule 1 for D11 was denied.
Explanation	Access to important resources was denied.
Severity	Warning
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 2.1

{Protocol}: The firewall {Firewall rule} for User {User name} was denied by administrator.

Example	WBM / UDP / TCP / Telnet / SSH / Console / PNIO / PB / OPC: The firewall Rule 1 for User maier was denied by administrator.
Explanation	Access to important resources was denied.
Severity	Warning
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 2.1

Identifier management

{Protocol}: User {User name} created group {Group} and assigned to role {Role}.

Example	WBM: User admin created group it-service and assigned to role service.
Explanation	The administrator has created a group and assigned it to a role.
Severity	Info
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 1.4

{Protocol}: User {User name} deleted group {Group} and the role {Role} assignment.

Example	WBM: User maier deleted group it-service and the role service assignment.
Explanation	The administrator has deleted an existing group and the role assignment.
Severity	Info
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 1.4

{Protocol}: User {User name} created role {Role}.

Example	WBM / UDP / TCP / Telnet / SSH / Console / PNIO / PB / OPC: User <User name> created role <Role>.
Explanation	Role was created.
Severity	Info
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 4.7

{Protocol}: User {User name} deleted role {Role}.

Example	WBM / UDP / TCP / Telnet / SSH / Console / PNIO / PB / OPC: User <User name> deleted role <Role>.
Explanation	Role was deleted.
Severity	Info
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 4.8

{Protocol}: User {User name} changed role {Role}.

Example	WBM / UDP / TCP / Telnet / SSH / Console / PNIO / PB / OPC: User <User name> changed role <Role>.
Explanation	Role was changed.
Severity	Info
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 4.9

Unsuccessful login attempts**{User name} account is locked for {Time minute} minutes after {Failed login count} unsuccessful login attempts.**

Example	User service account is locked for 44 minutes after 10 unsuccessful login attempts.
Explanation	If there are too many failed logins, the corresponding user account was locked for a specific period of time.
Severity	Warning
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 1.11

{Protocol}: {IP address} is blocked for {Time second} seconds after {Failed login count} unsuccessful login attempts.

Example	WBM: 192.168.1.105 is blocked for 600 seconds after 11 unsuccessful login attempts.
Explanation	If there were too many failed logins, the corresponding IP address was locked for a specific period of time.
Severity	Warning
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 1.11

Session lock

The session of user {User name} was closed after {Time} seconds of inactivity.

Example	The session of user admin was closed after 60 seconds of inactivity.
Explanation	The current session was locked due to inactivity.
Severity	Warning
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 2.5

Remote session termination

{Protocol}: Remote session {Config detail} was closed after {Time second} seconds of inactivity.

Example	WBM / UDP / TCP / Telnet / SSH / Console / PNIO / PB / OPC: Remote session OpenVPN was closed after 44 seconds of inactivity.
Explanation	The remote session was ended after a period of inactivity.
Severity	Info
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 2.6

Access via untrusted networks

{Protocol}: Remote access enabled via {Trigger condition}.

Example	WBM / UDP / TCP / Telnet / SSH / Console / PNIO / PB / OPC: Remote access enabled via E/A-Pin.
Explanation	Remote access is permitted.
Severity	Info
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 1.13

{Protocol}: Remote access disabled via {Trigger condition}.

Example	WBM / UDP / TCP / Telnet / SSH / Console / PNIO / PB / OPC: Remote access disabled via E/A-Pin.
Explanation	Remote access is denied.
Severity	Info
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 1.13

{Protocol}: User {User name} logged in from {IP address}.

Example	WBM / UDP / TCP / Telnet / SSH / Console / PNIO / PB / OPC: User admin logged in from 192.168.1.105.
Explanation	The user has successfully logged in to the remote device.
Severity	Info
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 1.13

{Protocol}: User {User name} failed to login from {IP address}.

Example	WBM / UDP / TCP / Telnet / SSH / Console / PNIO / PB / OPC: User admin failed to login from 192.168.1.105.
Explanation	The user cannot log in to the remote device.
Severity	Warning
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 1.13

{Protocol}: User {User name} has logged out.

Example	WBM / UDP / TCP / Telnet / SSH / Console / PNIO / PB / OPC: User admin has logged out.
Explanation	User has logged out.
Severity	Info
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 1.13

{Protocol}: Connection from {IP address} established.

Example	WBM / UDP / TCP / Telnet / SSH / Console / PNIO / PB / OPC: Connection from 192.168.1.105 established.
Explanation	VPN connection is established.
Severity	Info
Facility	local0
Standard	IEC 62443-3-3 Reference: n/a (NERC-CIP 005-R1)

{Protocol}: Connection from {IP address} closed.

Example	WBM / UDP / TCP / Telnet / SSH / Console / PNIO / PB / OPC: Connection from 192.168.1.105 closed.
Explanation	VPN connection is closed.
Severity	Info
Facility	local0
Standard	IEC 62443-3-3 Reference: n/a (NERC-CIP 005-R1)

{Protocol}: Connection from {IP address} failed. Reason: {Reason}.

Example	WBM / UDP / TCP / Telnet / SSH / Console / PNIO / PB / OPC: Connection from 192.168.1.105 failed. Reason: unsuccessful authentication.
Explanation	The connection could not be established due to invalid authentication.
Severity	Warning
Facility	local0
Standard	IEC 62443-3-3 Reference: n/a (NERC-CIP 005-R3)

Identification and authentication of devices**{Protocol}: Device {Src mac} access granted.**

Example	WBM: Device 00:0C:29:2F:09:B3 access granted.
Explanation	Device access is granted due to successful port authentication. In the example, access of the device with the source MAC address "00:0C:29:2F:09:B3" is granted.
Severity	Info
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 1.2

{Protocol}: {IP address} access granted.

Example	WBM / UDP / TCP / Telnet / SSH / Console / PNIO / PB / OPC: 192.168.1.105 access granted.
Explanation	Access is granted by the passed firewall rule or ACL.
Severity	Info
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 1.2

{Protocol}: {IP address} access granted.

Example	WBM / UDP / TCP / Telnet / SSH / Console / PNIO / PB / OPC: 192.168.1.105 access granted.
Explanation	Access granted via Cloud Connector.
Severity	Info
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 1.2

{Protocol}: Device {Src mac} access denied.

Example	WBM: Device 00:0C:29:2F:09:B3 access denied.
Explanation	Device access is denied due to unsuccessful port authentication. In the example, access of the device with the source MAC address "00:0C:29:2F:09:B3" is denied.
Severity	Warning
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 1.2

{Protocol}: {IP address} access blocked.

Example	WBM / UDP / TCP / Telnet / SSH / Console / PNIO / PB / OPC: 192.168.1.105 access blocked.
Explanation	Access blocked by firewall rule or Access Control List.
Severity	Warning
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 1.2

{Protocol}: {IP address} access blocked.

Example	WBM / UDP / TCP / Telnet / SSH / Console / PNIO / PB / OPC: 192.168.1.105 access blocked.
Explanation	Access via Cloud Connector is blocked.
Severity	Warning
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 1.2

{Protocol}: Connection from device {IP address} subject {Subject} successfully established.

Example	WBM: Connection from device 192.168.1.105 subject (Peter Maier) successfully established.
Explanation	The device authentication was successful. In the example, a connection from a device with the IP address "192.168.1.105" to the SINEC OS device was set up successfully.
Severity	Info
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 1.2

{Protocol}: Connection from device {IP address} subject {Subject} failed.

Example	WBM: Connection from device 192.168.1.105 subject (Peter Maier) failed.
Explanation	The device authentication has failed.
Severity	Warning
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 1.2

Limiting the number of simultaneous sessions**{Protocol}: The maximum number of {Max sessions} concurrent login session exceeded.**

Example	SSH: The maximum number of 8 concurrent login sessions exceeded.
Explanation	The maximum number of parallel sessions has been exceeded. In the example, the maximum number of 8 simultaneous sessions via SSH was exceeded.
Severity	Warning
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 2.7

Protection of check information**{Protocol}: User {User name} has cleared the logging buffer.**

Example	SSH: User admin has cleared the logging buffer.
Explanation	A user has deleted the local logbook. In the example, the user "admin" has deleted the local logbook.
Severity	Info

Facility	local0
Standard	IEC 62443-3-3 Reference: SR 3.9

Nonrepudiation**{Protocol}: User {User name} has changed the configuration.**

Example	SSH: User admin has changed the configuration.
Explanation	A user has changed the configuration. In the example, the user "admin" has changed the configuration.
Severity	Info
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 2.12

{Protocol}: User {User name} has deactivated {Config detail} configuration.

Example	WBM / UDP / TCP / Telnet / SSH / Console / PNIO / PB / OPC: User admin has deactivated OpenVPN configuration.
Explanation	User has disabled specific configuration data.
Severity	Info
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 2.12

{Protocol}: User {User name} has initiated a reset to factory defaults.

Example	SSH: User admin has initiated a reset to factory defaults.
Explanation	A user has initiated a reset to default settings. In the example, the user "admin" has initiated a reset to default settings.
Severity	Info
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 2.12

Device configuration changed.

Example	Device configuration changed.
Explanation	The device configuration has been changed permanently.
Severity	Info
Facility	local0
Standard	IEC 62443-3-3 Reference: SR2.12

Communication integrity**{Protocol}: Integrity verification failed.**

Example	Console: Integrity verification failed.
Explanation	An integrity fault was detected while the communication integrity of a message was being checked. Only certificate-based communication is possible.
Severity	Warning

Facility	local0
Standard	IEC 62443-3-3 Reference: SR 3.1

Software and information integrity

Firmware integrity verification failed. Backup firmware started.

Example	Firmware integrity verification failed. Backup firmware started.
Explanation	An integrity fault was detected while the firmware integrity was being checked. The backup firmware was loaded.
Severity	Warning
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 3.4

{Protocol}: Software integrity verification failed.

Example	WBM: Software integrity verification failed.
Explanation	An integrity fault was detected while the software integrity was being checked.
Severity	Warning
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 3.4

Integrity violations in configuration data detected

Example	Integrity violations in configuration data detected
Explanation	An integrity fault was detected while the configuration integrity was being checked.
Severity	Warning
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 3.4

Session integrity

{Protocol}: Session ID verification failed.

Example	WBM: Session ID verification failed.
Explanation	The session ID is invalid.
Severity	Warning
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 3.8

Protection against DoS events

{Protocol}: Dos attack detected.

Example	WBM: Dos attack detected.
Explanation	Denial of service attack is detected.
Severity	Warning
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 3.8

Data backup in automation system**{Protocol}: User {User name} created backup file.**

Example	WBM / UDP / TCP / Telnet / SSH / Console / PNIO / PB / OPC: User maier created backup file.
Explanation	User has created a backup file.
Severity	Info
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 7.3

{Protocol}: User {User name} failed to create backup file.

Example	WBM / UDP / TCP / Telnet / SSH / Console / PNIO / PB / OPC: User <user name> failed to create backup file.
Explanation	Creation of backup file by user failed.
Severity	Warning
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 7.3

Restoration of the automation system**{Protocol}: User {User name} failed to apply backup file.**

Example	WBM / UDP / TCP / Telnet / SSH / Console / PNIO / PB / OPC: User <user name> failed to apply backup file.
Explanation	Use of backup file by user failed.
Severity	Warning
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 7.4

{Protocol}: User {User name} loaded file type ConfigPack (restart required).

Example	WBM: User admin loaded file type ConfigPack (restart required).
Explanation	The configuration is applied.
Severity	Info
Facility	local0
Standard	IEC 62443-3-3 Reference: SR7.4

{Protocol}: Failed to load file type Firmware.

Example	WBM: Failed to load file type Firmware.
Explanation	Firmware upload has failed.
Severity	Warning
Facility	local0
Standard	IEC 62443-3-3 Reference: SR7.4

{Protocol}: Loaded file type Firmware {Version} (restart required).

Example	TFTP: Loaded file type Firmware V02.00.00 (restart required).
Explanation	The firmware was successfully loaded.
Severity	Info
Facility	local0
Standard	IEC 62443-3-3 Reference: SR7.4

{Protocol}: User {User name} loaded file type Firmware {Version} (restart required).

Example	WBM: User admin loaded file type Firmware V02.00.00 (restart required).
Explanation	The user has successfully loaded the firmware.
Severity	Info
Facility	local0
Standard	IEC 62443-3-3 Reference: SR7.4

{Protocol}: Software {Version} was activated.

Example	WBM: Software V02.00.00 was activated.
Explanation	The software was successfully activated.
Severity	Info
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 7.4

{Protocol}: User {User name} activated the Software {Version}.

Example	WBM: User <User name> activated the Software V02.00.00.
Explanation	The user has successfully activated the software.
Severity	Info
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 7.4

{Protocol}: Software activation failed.

Example	WBM: Software activation failed.
Explanation	The software activation has failed.
Severity	Warning
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 7.4

{Protocol}: User {User name} failed to activate Software {Version}.

Example	WBM: User <User name> failed to activate Software V02.00.00.
Explanation	The software activation by the user has failed.
Severity	Warning
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 7.4

Index

1

1588, 372

A

Access control, 357, 359
 Automatic learning, 359
ACL, 359, 498
 IP ACL, 490
 MAC ACL, 484
Aging
 Dynamic MAC Aging, 317
Aging time, 364
Article number, 100
Authentication, 219, 478
Available system functions, 19

B

Backup, 279
BFP, 501
Bidirectional Multicast, 452
Bridge, 330
 Bridge priority, 330
 Root bridge, 330
Bridge Max Age, 331
Bridge Max Hop Count, 331
Broadcast, 371
Brute Force Prevention, 501
Button, 247

C

Cable test, 276
Class of Service, 285
CLP
 Formatting, 272
 Saving the configuration, 272
Command Line Interface (CLI), 505
Configuration limits, 22
Configuration mode, 160
CoS, 285
 Traffic queue, 286
CoS (Class of Service), 76
CRC, 121

D

DCP Discovery, 274
DCP Forwarding, 350
DCP server, 350
DCP Server, 159
Default VLAN ID, 478
Dense mode, 452
DHCP
 Client, 197
 Host Options, 213
 Relay Agent, 210
 Server, 202
DNS Client, 164
DNS domain, 166
Documentation on the Internet, 13
DSCP, 287
DST
 Daylight saving time, 230, 232

E

Error status, 103
Error type
 Collisions, 121
 CRC, 121
 Fragments, 121
 Jabbers, 121
 Oversize, 121
 Undersize, 121
Ethernet Statistics
 History, 122
 Interface statistics, 117
 Packet Error, 120
 Packet Size, 118
 Packet Type, 119
EtherNet/IP, 266
 DLR ports, 266
 DLR Status, 268
 Ring port status, 268
 Supervisor, 268
Event log table, 101
Events
 Log Table, 101

F

- Fault monitoring
 - Connection status change, 260
- Fault Monitoring
 - Power supply, 259
 - Redundancy, 263
- Filter
 - Filter configuration, 357
- Forward Delay, 331

G

- Geographic coordinates, 162
- GMRP, 367
- Groups, 468
- Guest VLAN, 478
- GVRP, 298

H

- Hardware version, 100
- Hello time, 331
- HRP, 322
- HTTP
 - Load/save, 173
 - Port, 158
 - Server, 158
- HTTPS
 - Port, 158
 - Server, 158

I

- IEEE 1588, 372
- IEEE 802.1X, 478
- IGMP, 364
- Information
 - 802.1X port status, 152
 - ARP table, 101
 - Groups, 152
 - LLDP, 127
 - Log Table, 101
 - MAC Auth. Address table, 154
 - Ring redundancy, 111, 113
 - Role, 151
 - Security, 148, 150
 - SNMP, 147
 - Spanning Tree, 104

- Start page, 92
- Versions, 98
- IPv4 address, 163
- IPv4 routing
 - MSDP Cache, 143
 - NAT Translations, 137
 - OSPFv2 interfaces, 130
 - OSPFv2 LSDB (information), 135
 - OSPFv2 neighbors, 132
 - OSPFv2 Virtual Neighbors, 133
 - PIM BSRs, 142
 - PIM interfaces, 138
 - PIM Neighbors, 139
 - PIM Routes, 140
 - PIM RPs, 141
 - RIPv2 Statistics, 136
 - Routing table, 129

L

- LACP, 345
- LACP timeout, 349
- Layer 2, 281
- Layer 3 (IPv4), 380
 - Configuration, 380
- LLDP, 127, 352
- Local Users, 463
- Location, 162
- Logging in, 88
- Login, 501
- Logout
 - Automatic, 246
- Loop, 342
- Loop detection, 342

M

- MAC ACL, 487
 - Configuration, 487, 489
- Maintenance data, 99
- Management ACL, 498
- Manufacturer, 99
- Mirroring, 81
 - Destination, 311
 - General, 308
 - IP Flow, 315
 - MAC Flow, 314
 - Port, 312
 - VLAN, 313
- MRP Interconnection, 115, 325
 - Configuration, 64

- Operating principle, 62
- Topology, 61
- MSDP, 457
 - Peer, 458
- MSDP Cache, 143
- MSTP, 329, 337
 - Port, 332
 - Port parameters, 338
- MSTP instance, 338, 339
- Multicast, 124, 362
- Multicast Sources, 451
- Multiple Spanning Tree, 332, 337

N

- NAPT
 - Configuring, 393
- NAT
 - Configuring, 389, 391, 392
- NAT Translations, 137
- Negotiation, 252
- NTP, 362
 - Client, 238
 - Server, 245

O

- OSPF (IPv4)
 - Area range, 435
 - Areas, 433
 - Configuration, 427
 - Interface Authentication, 439
 - Interfaces, 436
 - OSPFv2 interfaces, 130
 - OSPFv2 LSDB (information), 135
 - OSPFv2 neighbors, 132
 - OSPFv2 Virtual Neighbors, 133
 - Virtual Link Authentication, 443
 - Virtual Links, 440

P

- Packet Error
 - Collisions, 121
 - CRC, 121
 - Fragments, 121
 - Jabbers, 121
 - Oversize, 121
 - Undersize, 121
- Packet error statistics, 120

- Password, 470
 - Options, 473
- PIM
 - Interfaces, 453
 - Protocol, 452
 - RP Candidate, 455
 - RP Static, 454
- PIM BSRs, 142
- PIM interfaces, 138
- PIM Neighbors, 139
- Ping, 273
- PLUG, 269
- point-to-point, 41
- Port, 254
 - Port configuration, 259
- Port configuration, 254, 259
- Port diagnostics
 - Cable test, 276
 - SFP Diagnostics, 277
- Port Overview, 250
- Prioritization, 289
- Priority, 289, 331
- PROFINET, 39, 265
- PROFINET IO, 39
- PTP, 372, 373, 374
 - General, 373
 - Port, 374
 - Transparent clock, 373

Q

- QoS, 289
- QoS Trust, 76

R

- RADIUS, 474
- Rate control, 291
- Re-authentication, 478
- Recurring, 484, 487
 - Configuration, 484, 490
 - Egress, 489
 - Ingress, 487
 - IP ACL, 490
 - MAC ACL, 484
- Redundancy, 318, 322
- Redundancy procedure
 - HRP, 51
- Redundant networks, 330
- Rendezvous point, 452
- Reset, 167

- Reset timer BFP, 501
- Restart, 167
- Ring redundancy, 318
 - HRP, 283, 319
 - MRP, 283, 319
 - Ring ports, 320
 - Standby, 322
- RIP (IPv4)
 - RIPv2 Statistics, 136
- RIPv2
 - Configuration, 445
 - Interfaces, 446
- RMON
 - History, 377
 - Statistics, 376
- Roles, 466
- Root Max Age, 331
- Route Map, 396
- Route Maps, 396
- Routing, 395
 - IPv4 routing table, 129
 - Static IPv4 routes, 395
- RSTP, 329
- RSTP+
 - Configuration, 46
 - Properties, 42
 - Topology, 43

S

- Scope of the manual, 11
- Security settings, 222
- SELECT/SET button, 247, 505
- Serial number, 100
- SFP Diagnostics, 277
- SFTP
 - Load/save, 181
- SHA algorithm, 222
- SINEC PNI, 350
- SMTP
 - Client, 158
- SNMP, 82, 159, 216, 222
 - Groups, 221
 - Overview, 147
 - SNMPv1, 82
 - SNMPv2c, 82
 - SNMPv3, 82
 - Trap, 226
- SNMPv3
 - Access, 222
 - Groups, 221
 - Notifications, 226

- Users, 219
- Views, 224
- Software version, 100
- Spanning Tree, 328
 - Information, 104
 - MSTP, 329
 - Passive listening, 341
 - Rapid Spanning Tree, 41
 - RSTP, 329
- SSH
 - Port, 157
 - Server, 157
- Standby, 322
- Standby redundancy, 73
- Start page, 92
- STEP 7, 350
- STP, 329
- Subnet mask, 35
- Subnets
 - Configuration (IPv4), 386
 - Overview (IPv4), 382
- Syslog, 248
 - Client, 158
- System
 - Configuration, 156
 - General information, 161
- System event log
 - Agent, 248
- System events
 - Configuration, 188
 - Severity filter, 192
 - Severity Filters, 192
- System manual, 13
- System Time, 228

T

- Telnet
 - Port, 157
 - Server, 157
- TFTP
 - Load/save, 177
- Time, 159
- Time of day
 - Manual setting, 228
 - Precision Time Protocol, 243
 - PTP Client, 243
 - SIMATIC Time Client, 242
 - SNTP (Simple Network Time Protocol), 235
 - System time, 228
 - Time zone, 237, 241

- Time-of-day synchronization, 235
- UTC time, 237, 241
- Trigger interval BFP, 501
- Trust Mode, 289

U

- Unicast, 123
- User groups, 468

V

- Vendor ID, 100
- VLAN, 75
 - Port VID, 301
 - Priority, 301
 - Tag, 301
 - VLAN ID, 77
 - VLAN tag, 76
- VRRP
 - Interface Tracking, 414
 - VRRP address configuration (IPv4), 413
 - VRRP address overview (IPv4), 413
 - VRRP addresses overview (IPv4), 422
 - VRRP configuration (IPv4), 410
 - VRRP routers (IPv4), 408
 - VRRP Statistics, 108
 - VRRPv3 Addresses Configuration (IPv4), 423
 - VRRPv3 Configuration (IPv4), 420
 - VRRPv3 Router (IPv4), 417
- VRRPv3
 - Interface Tracking, 424
 - VRRPv3 Statistics, 110

W

- Web Based Management
 - Requirement, 87
- Web Based Management (WBM), 505

