SIEMENS

SIMATIC NET

Industrial Ethernet Switches SCALANCE Layer 2 Switches Web Based Management (WBM) V4.5

Programming Manual

SCALANCE XB-200
SCALANCE XC-200
SCALANCE XF-200BA
SCALANCE XF-200G
SCALANCE XP-200 / XP-200G
SCALANCE XR-300WG

10/2023
C79000-G8976-C360-15

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.

Siemens AG
Digital Industries
Postfach 48 48
90026 NÜRNBERG
GERMANY

C79000-G8976-C360-15
Ⓟ 10/2023 Subject to change

Table of contents

Introduction 1

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

Validity of this configuration manual

This Configuration Manual covers the following products:

- SCALANCE XB-200
- SCALANCE XC-200
- SCALANCE XF-200BA
- SCALANCE XF-200G
- SCALANCE XP-200
- SCALANCE XP-200G
- SCALANCE XR-300WG

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 XB-200 firmware as of version 4.5
- SCALANCE XC-200 firmware as of version 4.5
- SCALANCE XF-200BA firmware as of version 4.5
- SCALANCE XF-200G firmware as of version 4.5
- SCALANCE XP-200 firmware as of version 4.5
- SCALANCE XP-200G firmware as of version 4.5
- SCALANCE XR-300WG firmware as of version 4.5

1.3 Designations used

Classification	Description	Terms used
Product group	If information applies to all devices and variants of a product group, the product group is named.	e.g. SCALANCE XC-200
Device	If information relates to a specific device, the device name is used.	e.g. SCALANCE XC206-2SFP
Device group	If information applies to a specific group of devices, a corresponding abbreviation is used.	-
	If information applies to all gigabit variants of SCALANCE XC-200, the following term is used.	SCALANCE XC-200G

1.4 Predefined defaults

PROFINET variants

- Ring Redundancy: On
- Ring Redundancy Mode: ARD Mode
- Spanning Tree Protocol (STP): Off
- Passive Listening: On
- VLAN Awareness: Off
- PROFINET Device Diagnostics: On
- IGMP Snooping: Off
- IGMP Querier: Off
- IPv4 Address Collision Detection - defense method: Never give up
- EtherNet/IP Device Diagnostics: Off
- QoS Trust Mode: Trust

EtherNet/IP variants

- Ring Redundancy: Off
- Ring Redundancy Mode: Off
- Spanning Tree Protocol (STP): On
- Passive Listening: Off
- VLAN Awareness: On
- PROFINET Device Diagnostics: Off
- IGMP Snooping: On
- IGMP Querier: On
- IPv4 Address Collision Detection - defense method: Attempt to defend

- EtherNet/IP Device Diagnostics: On
- QoS Trust Mode: Trust CoS-DSCP

Industrial Ethernet profile

- Ring Redundancy: Off
- Ring Redundancy Mode: Off
- Spanning Tree Protocol (STP): On
- Passive Listening: Off
- VLAN Awareness: On
- PROFINET Device Diagnostics: On
- IGMP Snooping: Off
- IGMP Querier: Off
- IPv4 Address Collision Detection - defense method: Never give up
- EtherNet/IP Device Diagnostics: Off
- QoS Trust Mode: Trust CoS-DSCP

1.5 Supplementary documentation

Documentation on the Internet

You can find the current version of the documents on the Internet at (https://support.industry.siemens.com/cs/de/en/ps/15273/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 Layer 2 Switches Command Line Interface (CLI)" for SCALANCE XB-200/XC-200/XF-200BA/XF-200G/XP-200/XP-200G/XR-300WG
  This document contains the CLI commands that are supported by the IE switches.
- Operating Instructions "SCALANCE XB-200", "SCALANCE XC-200", "SCALANCE XF-200BA", "SCALANCE XF-200G", "SCALANCE XP-200", "SCALANCE XP-200G" and "SCALANCE XR-300WG"
  These documents contain information on installing, connecting up and approvals for the products.
  - SCALANCE XB-200 (https://support.industry.siemens.com/cs/ww/en/ps/15291/man)
  - SCALANCE XC-200 (https://support.industry.siemens.com/cs/ww/en/ps/24185/man)
  - SCALANCE XF-200BA (https://support.industry.siemens.com/cs/ww/en/ps/15287/man)
  - SCALANCE XF-200G (https://support.industry.siemens.com/cs/ww/en/ps/15285/man)
  - SCALANCE XP-200 (https://support.industry.siemens.com/cs/ww/en/ps/21869/man)
  - SCALANCE XP-200G (https://support.industry.siemens.com/cs/ww/en/ps/21869/man)
  - SCALANCE XR-300WG (https://support.industry.siemens.com/cs/ww/en/ps/15296/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

The following WBM pages have been extended to include new system functions or parameters:

- Information > Dashboard (Page 110)
- System > Port > Configuration: Fast startup support of devices with gigabit ports (Page 256)

- System > Port > Configuration: Action when the number of monitored nodes is exceeded (Page 256)
- System > DHCP > DHCP Snooping (Page 215)
- System > EtherNet/IP: Support of DLR VLAN ID "0" (Page 271)

Existing system functions have been released as of V4.5 for the following devices or interfaces:

- SCALANCE XR300WG: Link Aggregation
- SCALANCE XR300WG: Multiple Spanning Tree Protocol (MSTP)

See also

Load & Save (Page 171)

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 Cybersecurity information

Siemens provides products and solutions with industrial cybersecurity 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 cybersecurity 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 cybersecurity measures that may be implemented, please visit
https://www.siemens.com/global/en/products/automation/topic-areas/industrial-cybersecurity.html (https://www.siemens.com/global/en/products/automation/topic-areas/industrial-cybersecurity.html).

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 Cybersecurity RSS Feed under https://new.siemens.com/global/en/products/services/cert.html (https://new.siemens.com/global/en/products/services/cert.html).

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

License conditions

Note

Open source software

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

You will find license conditions in the following documents on the supplied data medium:

- OSS_Siemens_86.pdf
- OSS_SCALANCE-XB-200-XC-200-XF-200BA-XP-200-XR-300WG_86.pdf

You will find these documents on the product DVD.

1.12 Marken

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

SCALANCE, C-PLUG, OLM

Description

2

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 full duplex, available with the following devices:
    SCALANCE XC206-2SFP with the appropriate pluggable transceivers
    SCALANCE XC-200G
    SCALANCE XF-200G
    SCALANCE XP-208 with the article numbers 6GK5208-0HA10-2AS6, 6GK5208-0HA10-2ES6 and 6GK5208-0UA10-5ES6
    SCALANCE XP216
    SCALANCE XP-200G
    SCALANCE XR-300WG
  - 10 Gbps full duplex, available with the following devices:
    SCALANCE XC-200G PoE
    SCALANCE XC-200G PoE EEC with the appropriate pluggable transceivers
    SCALANCE XR326-2C PoE WG
  - 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.
- Power over Ethernet (PoE)
  Devices with the "PoE" identification in the type designation support 'Power over Ethernet'.
- 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.
- 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 (not with SCALANCE XB-200)
- H-Sync support
  You will find more information in the section "Ring (Page 324)"
- 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 XB-200	SCALANCE XR-300WG	SCALANCE XC-200	SCALANCE XF-200G	SCALANCE XP-200	SCALANCE XP-200G	SCALANCE XF-200BA
Information	ARP table	✓	✓	✓	✓	✓	✓	✓
	Log table	✓	✓	✓	✓	✓	✓	✓
	Ethernet Statistics	✓	✓	✓	✓	✓	✓	✓
	Diagnostics (temperature)	-	✓	✓	✓	✓	✓	✓
System	SMTP client	✓	✓	✓	✓	✓	✓	✓
	DHCP client	✓	✓	✓	✓	✓	✓	✓
	DHCP server	✓ 1)	✓ 1)	✓	✓	✓	✓	✓
	SNMP	✓	✓	✓	✓	✓	✓	✓
	Manual time setting	✓	✓	✓	✓	✓	✓	✓
	DST	✓	✓	✓	✓	✓	✓	✓
	SNTP	✓	✓	✓	✓	✓	✓	✓
	NTP	✓	✓	✓	✓	✓	✓	✓
	SIMATIC Time Client	✓	✓	✓	✓	✓	✓	✓
	Auto logout	✓	✓	✓	✓	✓	✓	✓
	Syslog Client	✓	✓	✓	✓	✓	✓	✓
	NOA switch functionality	-	-	✓ 4)	-	-	-	-
	Fault monitoring	✓	✓	✓	✓	✓	✓	✓
	PROFINET	✓	✓	✓	✓	✓	✓	✓
	EtherNet/IP	✓	✓	✓	✓	✓	✓	✓ 2)
	Cable tester	✓	✓	✓	✓	✓	✓	✓
	SFP Diagnostics	-	✓	✓	-	-	-	-

Menu item in the WBM	System functions	SCALANCE XB-200	SCALANCE XR-300WG	SCALANCE XC-200	SCALANCE XF-200G	SCALANCE XP-200	SCALANCE XP-200G	SCALANCE XF-200BA
Layer 2	Sending priorities	-	-	✓	✓	✓	✓	✓
	CoS Map	✓	✓	✓	✓	✓	✓	✓
	DSCP Mapping	✓	✓	✓	✓	✓	✓	✓
	QoS prioritization	✓	✓	✓	✓	✓	✓	✓
	CoS port reassignment	-	-	✓	✓	✓	✓	✓
	Load control	✓	✓	✓	✓	✓	✓	✓
	GVRP	-	-	✓	✓	✓	✓	✓
	Port-based VLAN	✓	✓	✓	✓	✓	✓	✓ 2)
	Private VLAN	-	-	✓	✓	✓	✓	-
	Provider bridge	-	-	✓	✓	✓	✓	-
	Switch-Port VLAN Trunk	-	✓	✓	✓	✓	✓	✓ 2)
	Port-based mirroring	✓	✓	✓	✓	✓	✓	✓
	Dynamic MAC aging	✓	✓	✓	✓	✓	✓	✓
	Ring redundancy	✓	✓	✓	✓	✓	✓	✓
	H-Sync support	-	-	✓	✓	✓	✓	✓
	S2 devices	-	-	✓	✓	✓	✓	✓
	CiR/H-CiR support	-	-	✓	✓	✓	✓	✓
	Ring with RSTP	✓	✓	✓	✓	✓	✓	✓
	Standby (HRP)	✓	✓	✓	✓	✓	✓	✓
	Observer (HRP)	-	-	✓	✓	✓	✓	✓
	Link Check	✓	✓	✓	-	-	-	✓
	MRP multiple rings	✓	✓	✓	-	✓	✓	-
	MRP Interconnection	✓	✓	✓	✓	✓	✓	✓
	Spanning Tree	✓	✓	✓	✓	✓	✓	✓
	RSTP	✓	✓	✓	✓	✓	✓	✓
	RSTP+	✓	✓	✓	✓	✓	✓	✓
	MSTP	-	✓	✓	✓	✓	✓	-
	Enhanced Passive Listening Compatibility	✓	✓	✓	✓	✓	✓	✓
	Loop detection	✓	✓	✓	✓	✓	✓	✓
	Link Aggregation / LACP	-	✓	✓	✓	✓	✓	✓
	DCP forwarding	✓	✓	✓	✓	✓	✓	✓

Menu item in the WBM	System functions	SCALANCE XB-200	SCALANCE XR-300WG	SCALANCE XC-200	SCALANCE XF-200G	SCALANCE XP-200	SCALANCE XP-200G	SCALANCE XF-200BA
	LLDP	✓	✓	✓	✓	✓	✓	✓
	Fiber monitoring	-	✓	✓	-	-	-	-
	Unicast filter	✓	✓	✓	✓	✓	✓	✓
	Locked ports	✓	✓	✓	✓	✓	✓	✓
	Unicast learning	✓	✓	✓	✓	✓	✓	✓
	Unicast blocking	✓	✓	✓	✓	✓	✓	✓
	Multicast groups	✓	✓	✓	✓	✓	✓	✓
	IGMP	✓	✓	✓	✓	✓	✓	✓
	GMRP	-	-	✓	✓	✓	✓	✓
	Multicast blocking	✓	✓	✓	✓	✓	✓	✓
	Broadcast blocking	✓	✓	✓	✓	✓	✓	✓
	PTP	-	-	✓ [3]	✓	-	✓	-
	RMON	✓	✓	✓	✓	✓	✓	✓
	RMON history	✓	✓	✓	✓	✓	✓	✓
Layer 3	Single-Hop Inter-VLAN-Routing	-	-	✓	✓	✓	✓	-
	DHCP relay agent	✓	✓	✓	✓	✓	✓	✓
	Common agent address	-	-	✓	✓	✓	✓	-
	NAT/NAPT	-	-	✓	✓	✓	✓	-
Security	Users	✓	✓	✓	✓	✓	✓	✓
	Passwords	✓	✓	✓	✓	✓	✓	✓
	RADIUS authentication	✓	✓	✓	✓	✓	✓	✓
	MAC authentication	✓	✓	✓	✓	✓	✓	✓
	Guest VLAN	-	-	✓	✓	✓	✓	✓
	802.1X Re-Authentication	✓	✓	✓	✓	✓	✓	✓
	Management ACL	✓	✓	✓	✓	✓	✓	✓
	Brute Force Prevention	✓	✓	✓	✓	✓	✓	✓

1) Restricted

2) Not with DNA devices

3) Only SCALANCE XC-200G

4) Only SCALANCE XC-200G EEC

Availability of hardware

The following table shows the hardware of the IE switches.

We reserve the right to make technical changes.

	SCALANCE XB-200	SCALANCE XR-300WG	SCALANCE XC-200	SCALANCE XF-200G	SCALANCE XP-200	SCALANCE XP-200G	SCALANCE XF-200BA
C-PLUG support	-	-	✓	✓	✓	✓	✓
SELECT/SET button	-	-	✓ 2) 3)	-	✓ 3)	✓ 3) 4)	-
RESET button	✓ 2)	✓ 2)	-	✓	✓ 2)	✓ 2)	-
SET button	-	-	-	-	-	-	✓ 2)
Signaling contact	-	-	✓	-	✓	✓	✓
Serial interface	✓	✓	✓	✓	✓	✓ 4)	-
Display modes	-	-	✓	-	✓	✓ 4)	-
Pluggable transceiver slots	-	-	✓	-	-	-	-
Combo ports	-	✓	✓	-	-	-	-
Bus adapter slots	-	-	-	-	-	-	✓
Power over Ethernet	-	✓ 1)	✓ 1)	-	✓ 1)	✓ 1)	-

1) "PoE" identifier in device name

2) Function of the buttons: Restore Factory Defaults

3) Function of the buttons: Set Fault Mask

4) Not with the SCALANCE XP200G PP

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.

	Configurable function	Maximum number						
		SCALANCE XB-200	**SCALANCE XR-300WG**	**SCALANCE XC-200**	**SCALANCE XF-200G**	**SCALANCE XP-200**	**SCALANCE XP-200G**	**SCALANCE XF-200BA**
System	Maximum frame size (ingress)	1632 bytes	10 KB	1632 bytes / 2048 bytes / 10 KB [7)]	10 KB	1632 bytes / 10 KB [8)]	10 KB	1632 bytes
	Syslog server	3						
	E-mail server	3						
	DHCP pools	16 [1)]	28 [1)]	24				
	IPv4 addresses per DHCP pool	1		24				
	IPv4 addresses managed by the DHCP server (dynamic + static)	16 [1)]	28 [1)]	576				
	DHCP static assignments per DHCP pool	-		24				
	SNMPv1 trap recipient	10						
	SNMPv3 Users	48						
	SNMPv3 Groups	41						
	SNMPv3 Views (incl. 2 default views)	46						
	SNTP server	1 [9)]						
	NTP server	1		4 [9)]				1
	Agent/TIA interfaces [2)]	1						
	Devices displayed via DCP Discovery	100						

	Configurable function	Maximum number						
		SCALANCE XB-200	**SCALANCE XR-300WG**	**SCALANCE XC-200**	**SCALANCE XF-200G**	**SCALANCE XP-200**	**SCALANCE XP-200G**	**SCALANCE XF-200BA**
Layer 2	QoS priority queues	4		4/8 [6]	8	4/8 [10]	8	4
	Virtual LANs (port-based, including VLAN 1)	257 [3]						
	Private VLAN	-		1				-
	Primary PVLANs	-		1				-
	Secondary isolated PVLANs	-		24				-
	Secondary community PVLANs	-		256				-
	Mirroring sessions	1						
	Standby ports	1						
	MRP rings	4			1	4		1
	Configured MRP Interconnection connections	64						
	Enabled MRP Interconnection connections	1		2				
	Maximum number of devices with enabled MRP Interconnection in a ring	10						
	Multiple Spanning Tree instances	-	4					-
	Link aggregations	-	2/4/8 [5]					
	Ports in a link aggregation	-		8	4	8		4
	Static unicast addresses	128						
	Static multicast addresses without activated GMRP	256						
	Static multicast addresses with activated GMRP	-		50				
	Addresses learned using IGMP snooping	512						

	Configurable function	Maximum number						
		SCALANCE XB-200	**SCALANCE XR-300WG**	**SCALANCE XC-200**	**SCALANCE XF-200G**	**SCALANCE XP-200**	**SCALANCE XP-200G**	**SCALANCE XF-200BA**
Layer 3	VLAN IP interfaces	24						
	DHCP Relay Agent interfaces	1		24				1
	DHCP Relay Agent server	4						
	NAT interfaces	-		1				-
	Dynamic NAT configurations (pools)	-		100				-
	Static NAT configurations	-		100				-
Security	Users	30 (incl. user preset in the factory "admin")						
	Roles	29						
	Groups	32						
	IP addresses of RADIUS servers	6						
	Simultaneous MAC authentications (authenticated and blocked) per device [4]	2000	-	2000				
	Simultaneous MAC authentications (authenticated and blocked) per port (configurable) [4]	200						
	Management ACLs (access rules for management)	10						

[1] With the SCALANCE XB-200 and SCALANCE XR-300WG, the number of DHCP pools and manageable IPv4 addresses depends on the number of ports. The number of ports corresponds to the maximum number of DHCP pools and manageable IPv4 addresses.

[2] This is an IP interface.

[3] Devices with Y functionality do not support VLANs.

[4] 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 MAC authentications of the port are reset.

[5] Since a link aggregation consists of at least 2 ports, the maximum number of link aggregations is dependent on the number of ports.
- For devices with up to 4 ports, a maximum of 2 link aggregations is possible.

- For devices with up to 8 ports, a maximum of 4 link aggregations is possible.
- For devices with more than 8 ports, a maximum of 8 link aggregations is possible.

6) The devices of the SCALANCE XC-200G product group support 8 queues. All other XC-200 devices support 4 queues.

7) With the following devices, the maximum frame size (ingress) is 2048 bytes:
- Devices with combo ports (suffix "C" in type designation)
- PoE variants (suffix "PoE" in type designation)

The following devices support 10 KB jumbo frames:
- All gigabit variants (suffix "G" in type designation), also those with combo ports.
- All devices that support Power over Ethernet (suffix "PoE" in type designation)
- SCALANCE XC216-4C

With all other XC-200 devices, the maximum frame size (ingress) is 1632 bytes.

8) The gigabit ports of a SCALANCE XP-200 support 10 KB jumbo frames. With all other ports, the maximum frame size is 1632 bytes.

9) Maximum number of NTP/SNTP servers that can be configured for a device.

10) The following devices of the SCALANCE XP-200 product group support 8 queues:

- 6GK5 208-0HA10-2AS6
- 6GK5 208-0HA10-2ES6
- 6GK5 208-0UA10-5ES6

All other XP-200 devices support 4 queues.

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 C-PLUG

NOTICE
Do not remove or insert a C-PLUG during operation A C-PLUG may only be removed or inserted when the device is turned off.

A C-PLUG is an exchangeable storage medium for storing the configuration data of the device. This allows fast and uncomplicated replacement of a device. The C-PLUG is taken from the previous device and inserted in the new device. The first time it is started up, the replacement device has the same configuration as the previous device except for the device-specific MAC address set by the vendor. A C-PLUG stores the current information about the configuration of a device.

A C-PLUG can be used to save the firmware. You will find more information under "System > PLUG".

Note

The device can also be operated without a C-PLUG.

How it works

Operating mode

In terms of the C-PLUG, there are three modes for the device:

- Without C-PLUG
  The device stores the configuration in internal memory.
  This mode is active if no C-PLUG is inserted.
- With unwritten C-PLUG
  If an unwritten C-PLUG (factory status or deleted with Clean function) is used, the local configuration already existing on the device is automatically stored on the inserted C-PLUG during startup.
  This mode is active as soon as an unwritten C-PLUG is inserted.
- With written C-PLUG
  A device with a written and accepted C-PLUG uses the configuration data of the C-PLUG automatically when it starts up. The requirement for acceptance is that the data was written by a compatible device type.
  If there is configuration data in the internal memory of the device this is overwritten.
  This mode is active as soon as a written C-PLUG is inserted.

Operation with C-PLUG

The configuration stored on the C-PLUG is displayed over the user interfaces.

If changes are made to the configuration, the device stores the configuration directly on the C-PLUG, if this is in the "ACCEPTED" status and in internal memory.

Response to errors

Inserting a C-PLUG that does not contain the configuration of a compatible device type and inadvertently removing the C-PLUG, or general malfunctions of the C-PLUG are indicated by the diagnostic mechanisms of the device.

- Fault LED
- Web Based Management (WBM)
- SNMP
- Command Line Interface (CLI)
- PROFINET diagnostics

The user then has the choice of either removing the C-PLUG again or selecting the option to reformat the C-PLUG.

See also

PLUG (Page 275)

Security recommendations 3

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.

- 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

- The devices SCALANCE XF204G, SCALANCE XB206-2 as of firmware version V4.4 or SCALANCE XP-200G as of firmware version V4.5 use certificates for elliptic curve cryptography ("ECDSA certificates"). Only use ECDSA certificates in PEM format that were generated with the following curves:
  - secp256r1 (NIST P-256)
  - secp384r1 (NIST P-384)
  - secp521r1 (NIST P-521)

  RSA certificates are no longer supported as of this firmware version. The existing RSA certificates on the device are automatically replaced with self-signed ECDSA certificates. On the device there is a preset SSL certificate with the key length 256 bits for the elliptic-curves cryptography. Replace this certificate with a self-made certificate with key. We recommend that you use a certificate signed either by a reliable external or by an internal certification authority.
- There is a preset SSL/TLS (RSA) certificate with 2048 bit key length in other devices. 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 a certification authority including key revocation and management to sign certificates.
- Make sure that user-defined private keys are protected and inaccessible to unauthorized persons.
- Verify certificates and fingerprints on the server and client to prevent "man in the middle" attacks.
- Change certificates and keys immediately if there is a suspicion of compromise.

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

Note

Packet filtering

Packets are processed according to their importance for the operation of the network. Some packets directed to the CPUs of the switch may be discarded due to various security-relevant packet filters. Therefore, it can occur that not all ICMP packets are delivered to the CPUs, for example, and are thus not responded to.

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.

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

Service	Protocol / Port number	Default port status	Configurable		Authentication	Encryption [5]
			Port	Service		
DHCPv4 Server	UDP/67	Closed	-	✓	-	-
DHCPv4 Client	UDP/68	Open	-	✓	-	-
EtherNet/IP	TCP/44818 UDP/2222 UDP/44818	Closed (Open with EtherNetIP variants)	-	✓	-	-
HTTP Server/Client [3]	TCP/80	Closed	✓	✓	✓	-
HTTPS WBM Server/ Client	TCP/443	Open	✓	✓	✓	✓
NTP Client	UDP/123	Closed	✓	✓	-	-
NTP (secure)	UDP/123	Closed	✓	✓	✓	-

Service	Protocol / Port number	Default port status	Configurable		Authentication	Encryption [5]
			Port	Service		
PROFINET	UDP/34964 UDP/49151 ... 49159 [1]	Open	-	✓	-	-
RADIUS Client	UPD/1812 [4] UPD/1813 [4]	Outbound only	✓	✓	-	-
	UDP/3799	Open	✓	✓	-	-
SFTP Server	UDP/22	Outbound only	✓	✓	✓	✓
SMTP Client	TCP/25	Closed	✓	✓	-	-
SMTP Client (secure)	TCP/465	Closed	✓	✓	✓	✓
SNMPv1/v2c [2] [3]	UDP/161	Open	✓	✓	-	-
SNMPv3	UDP/161	Open	✓	✓	Optional	Optional
SNMP Traps	UDP/162	Outbound only	-	✓	-	-
SNTP Client	UDP/123	Closed	✓	✓	-	-
SSH CLI Server	TCP/22	Open	✓	✓	✓	✓
Syslog Client	UDP/514	Closed	✓	✓	-	-
Syslog (secure) Client	TCP/6514	Closed	✓	✓	-	✓
Telnet [3]	TCP/23	Closed	✓	✓	✓	-
TFTP Client	UDP/69	Outbound only	✓	✓	-	-

1) Port number can be configured via the WBM.

2) Read-only access only.

3) Protocol according to Security by Default.

4) The port is closed by default and is displayed when a RADIUS server is configured. Port number can be configured via the WBM.

5) You can find additional information on the encryption methods used in the WBM appendix "Ciphers used".

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 port status	Service configurable
DCP	Setup mode [1]	✓
LLDP	Open	✓

Layer 2 service	Default port status	Service configurable
RSTP	Closed	✓
MSTP	Open	✓

1) Setting according to Security by Default.

Assignment of an IP address

4

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 save 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 XB-200: V5.5.4 and higher
    SCALANCE XP-200: As of V5.5.4 HF9
    SCALANCE XC-200: V5.5.4 HF11 and higher
    SCALANCE XR-300WG: As of V5.6
    SCALANCE XF-200BA: As of V5.6 HF3
    SCALANCE XC-200G: As of V5.6 as HSP11
    SCALANCE XF-200G: As of V5.7 as HSP1121
    SCALANCE XP-200G: As of V5.7 SP2 as HSP1124
    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 XB-200: V13 SP1 and higher
    SCALANCE XC-200: V14 and higher
    SCALANCE XP-200: V14 and higher
    SCALANCE XR-300WG: As of V15
    SCALANCE XF-200BA: As of V15
    SCALANCE XC-200G, devices with 8 ports: As of V15
    SCALANCE XC-200G, devices with more than 8 ports: As of V16
    SCALANCE XF-200G: As of V19
    SCALANCE XP-200G: As of V17 as HSP0395
    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 interface
  For more information on assigning the IP address using the CLI, refer to the documentation "SCALANCE Layer 2 Switches Command Line Interface (CLI)"
- **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 15: DNS domain name
- 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.

- 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

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 270)".

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 271)".

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 171)".

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. Fur 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.

- 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+

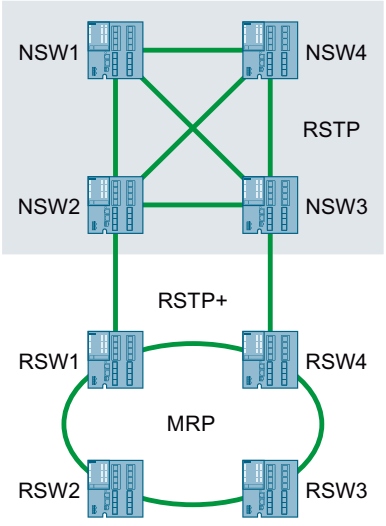
In principle, all devices at the connection points between RSTP network and MRP ring must support the RSTP+ method. All other devices in the MRP ring must forward BPDUs (Bridge Protocol Data Unit).

5.3.2.2 Topology for RSTP+

RSTP network and MRP ring

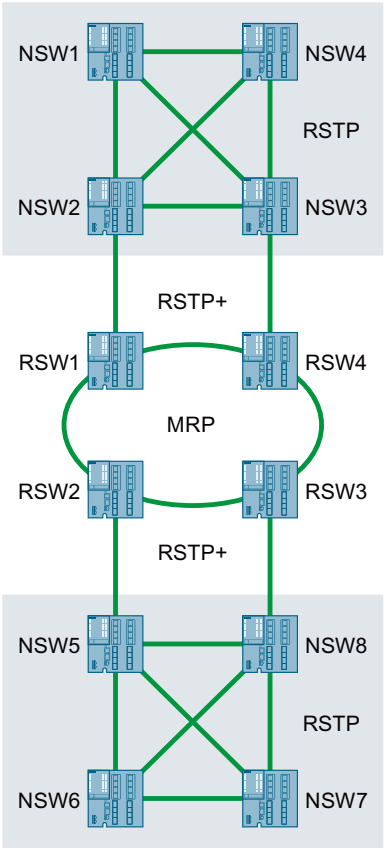
The redundant integration of MRP rings into an RSTP network is not possible without RSTP+ because parallel operation of RSTP and MRP on one port is not permitted. Only the devices of the MRP ring that are connected to the RSTP network must support RSTP+. In the example topology shown, these are the two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



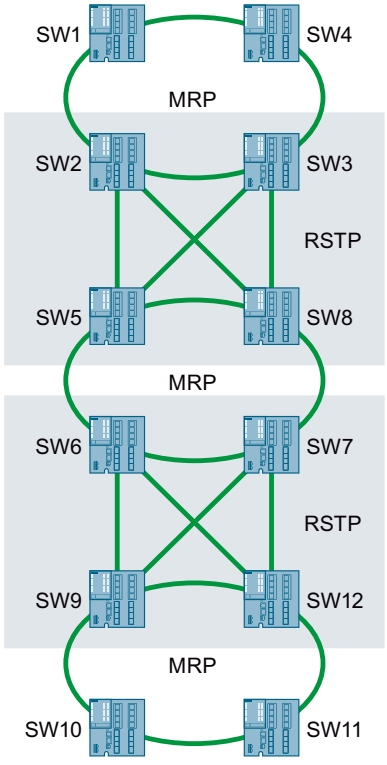
Multiple RSTP network areas and MRP ring

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.

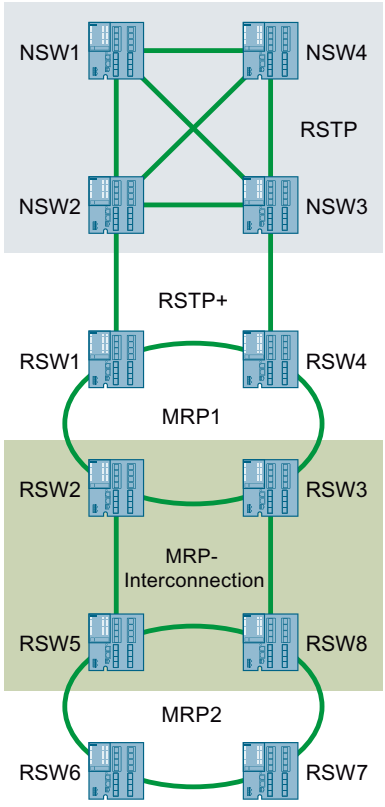


RSTP network and two MRP rings with MRP Interconnection

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 10)".

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+.

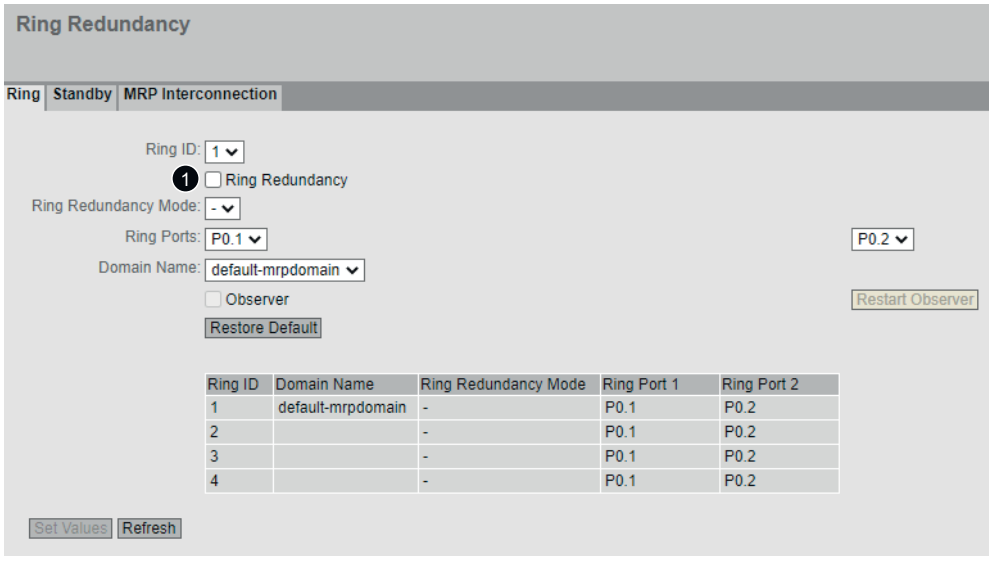
The required port settings are made automatically during this process.

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".

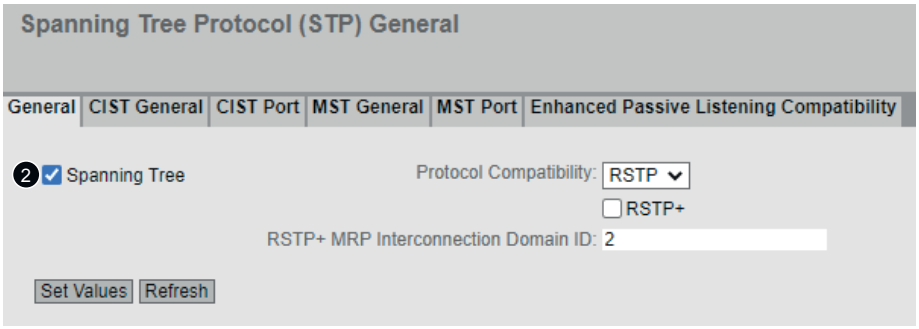


Step 2: Enable Spanning Tree

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.

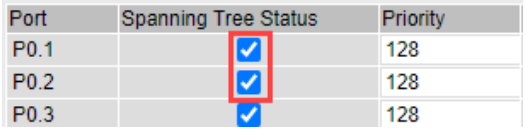


Check the ring port settings in the menu "Layer 2 > Spanning Tree" on the page "CIST Port" or "ST Port".

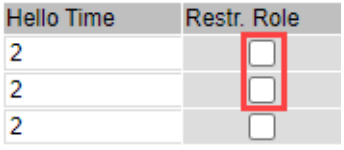
The table on this page lets you configure Spanning Tree for individual ports.

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.

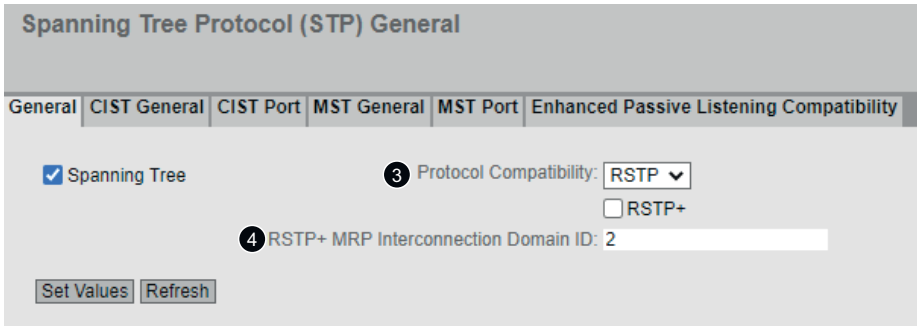


- The check box for the two ring ports in the table column "Restr. Role" must be cleared. This is necessary so that the behavior of the ring ports is exclusively controlled by MRP, the redundancy manager. The function of MRP is not affected by RSTP+.



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.

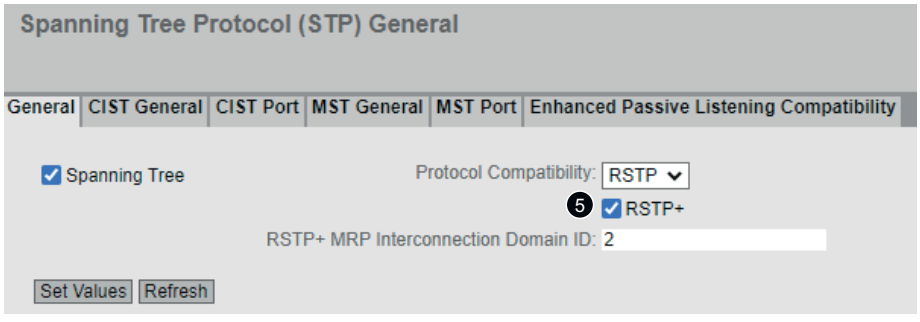
The RSTP+ MRP Interconnection Domain ID must be unique throughout the network and must differ from any MRP Interconnection Domain ID that may need to be configured. Different IDs are necessary to distinguish TCNs (Topology Change Notifications) of the RSTP network from TCNs of the MRP ring. This assignment 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+

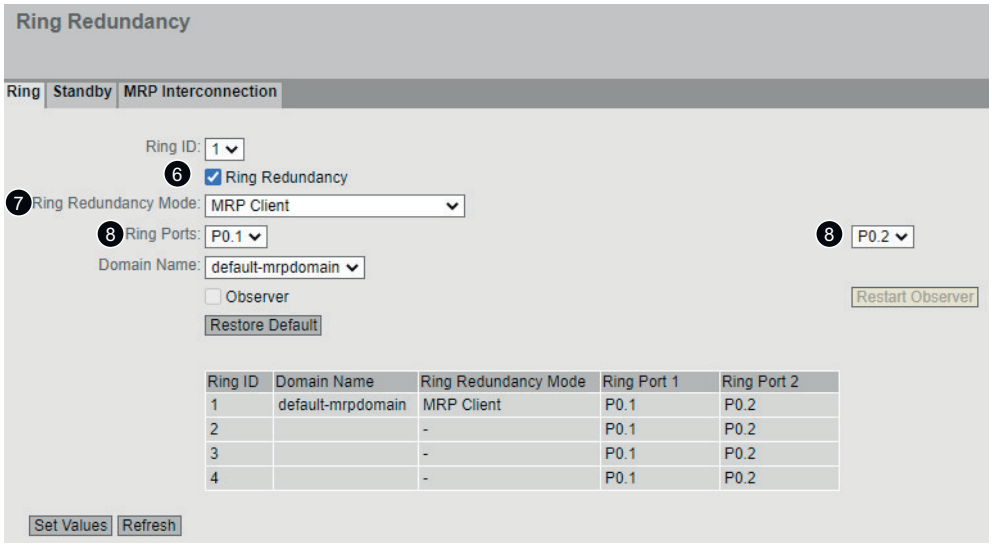
In the "Layer 2 > Spanning Tree > General" menu, select the "RSTP+" check box and then click the "Set Values" button to save the configuration.



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+.



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.

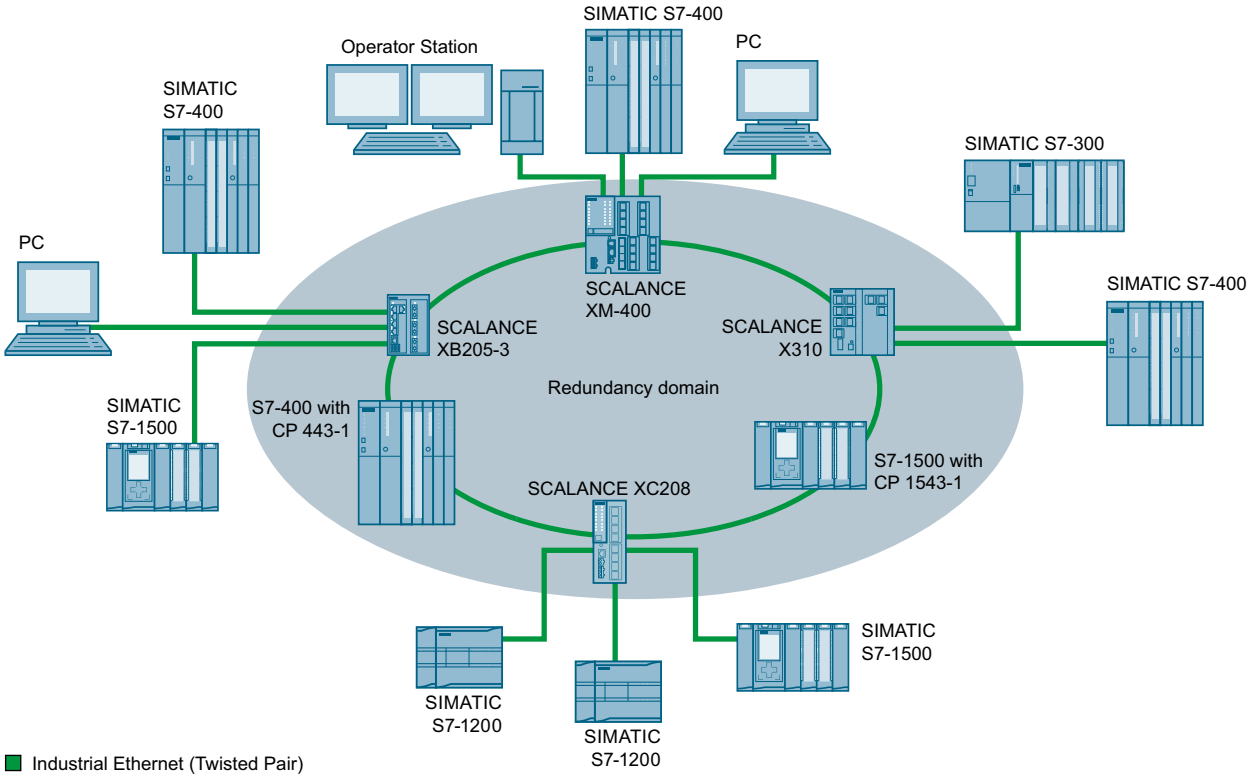


Figure 5-1 Example of a ring topology with the MRP media redundancy protocol

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.

Note

Number of devices

Except in PROFINET IO systems, MRP ring topologies with up to 120 SCALANCE X switches Firmware Version 4.3.1 and higher have been tested successfully.

Requirement:

- The connection settings (transmission medium / duplex) have been set to full duplex and at least 1 Gbps for all ring ports.

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 291)
- Ring (Page 324)

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.

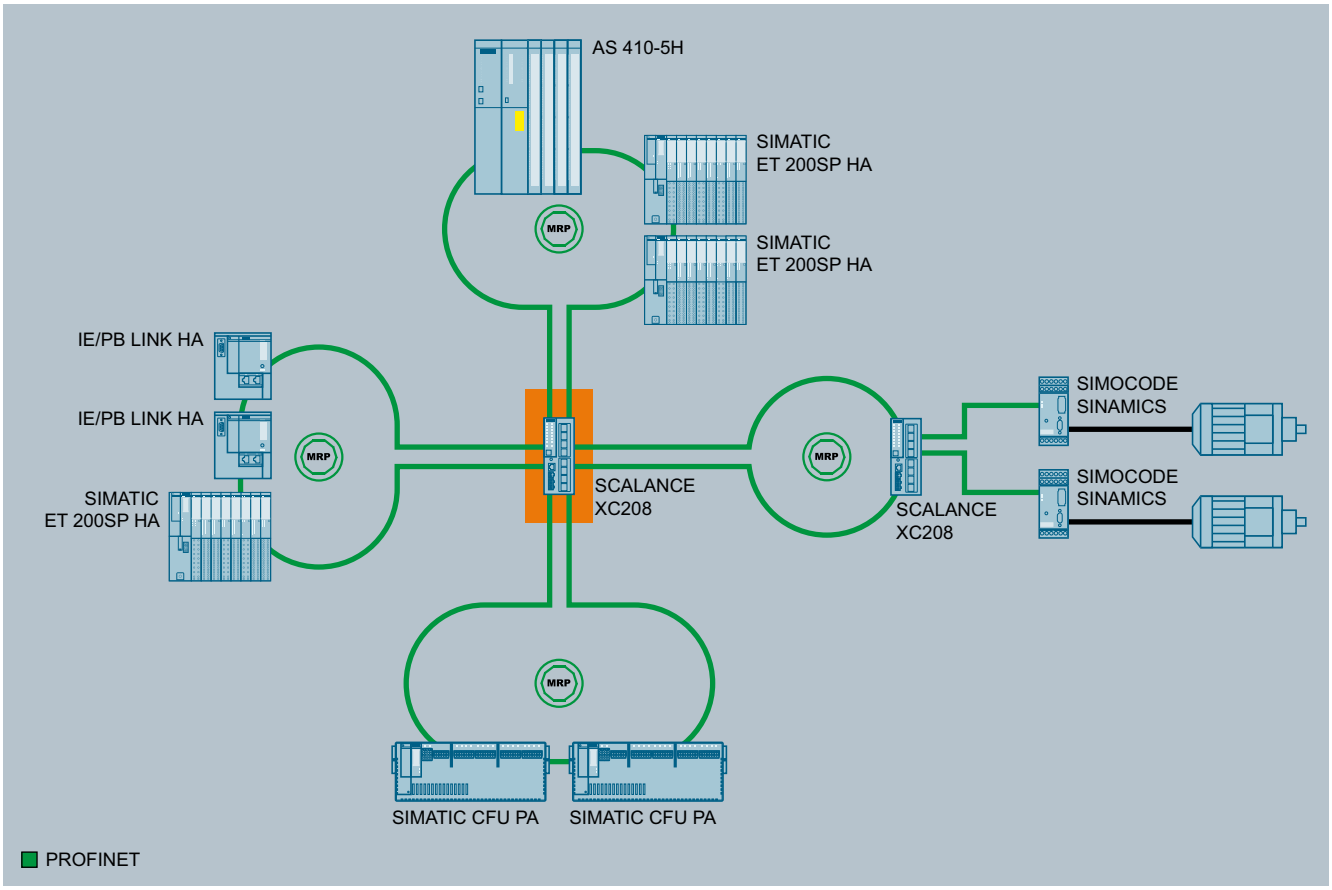


Figure 5-2 MRP multiple ring topology

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 XP-200G as of firmware version V4.5
- 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 XP-200G as of firmware version V4.5
- 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.

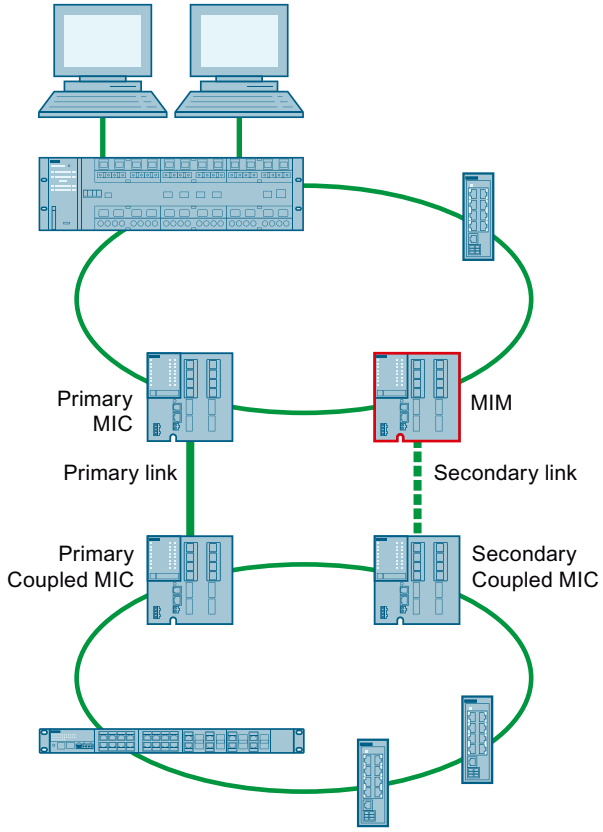


Figure 5-3 Redundant connection of two MRP rings with MRP Interconnection

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 XP-200G as of firmware version V4.5
- 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 XP-200G devices have firmware as of version V4.5
- 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 V4.5 for SCALANCE XP-200G

As of firmware version V4.5, MRP Interconnection is released for the SCALANCE XP-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.

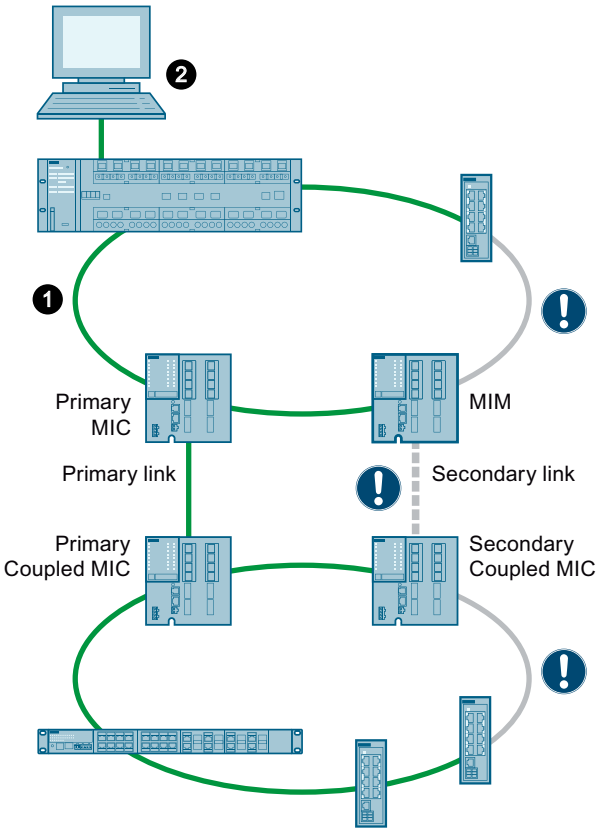
5.3.5.3 Configuring an MRP Interconnection connection

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)

5.3.5.4 Connecting the devices and basic configuration



Step 1: Plug cables

Connect the devices according to the planned topology except for one connection distance in each ring. The two devices intended for the secondary link (MIM and Secondary Coupled MIC) must not be connected yet.

Step 2: Assign IP addresses

Use a PC connected to the network to access the devices. Assign one IP address to each device, for example with SINEC PNI. Then configure the devices with the WBM or the CLI.

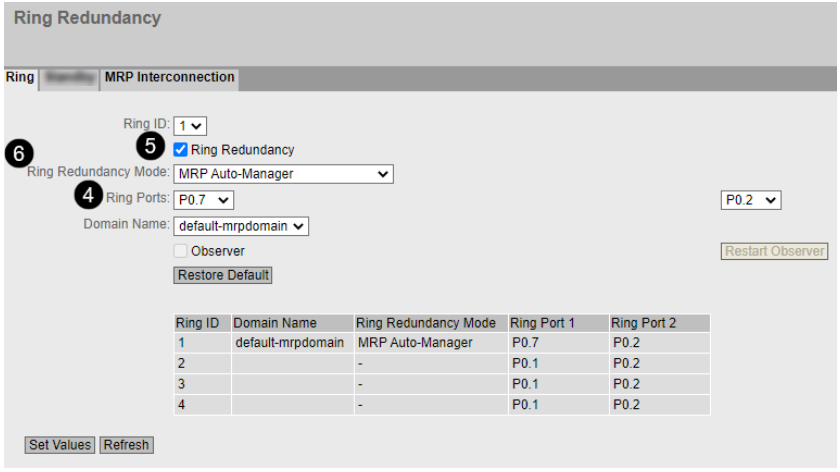
Step 3: Configure Spanning Tree

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.

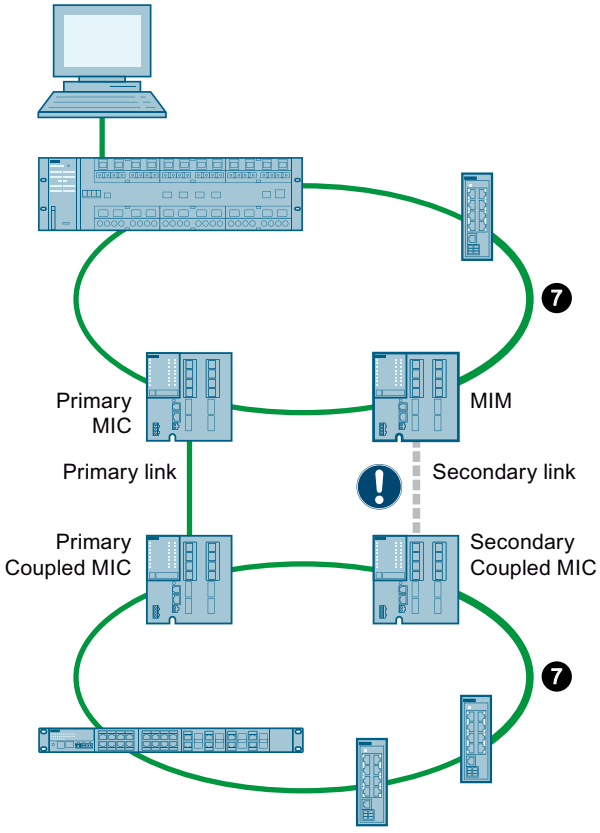
Note

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

Note

Configuring the MRP Interconnection via STEP 7

As of version 4.5, you can configure the MRP Interconnection with STEP 7 V5.7 SP2 and GSDML or HSP1124.

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:

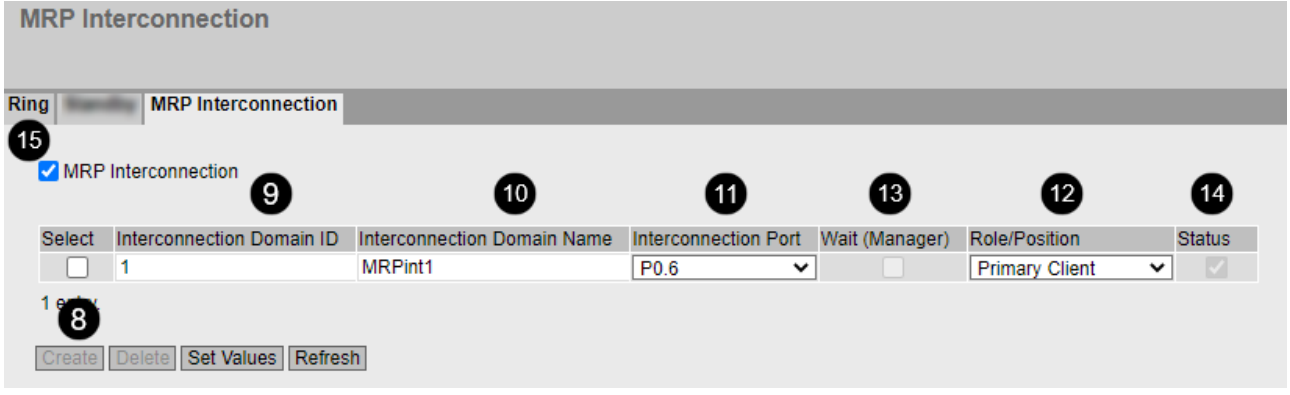
1. Secondary Coupled MIC
2. Primary Coupled MIC
3. Primary MIC
4. MIM

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 XP-200G as of firmware version V4.5
    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

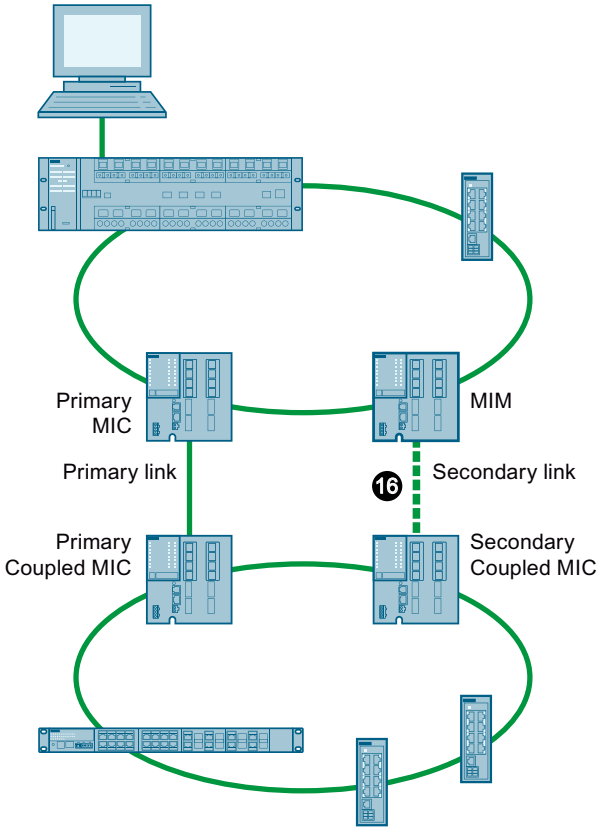
Click the "Set Values" button.

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

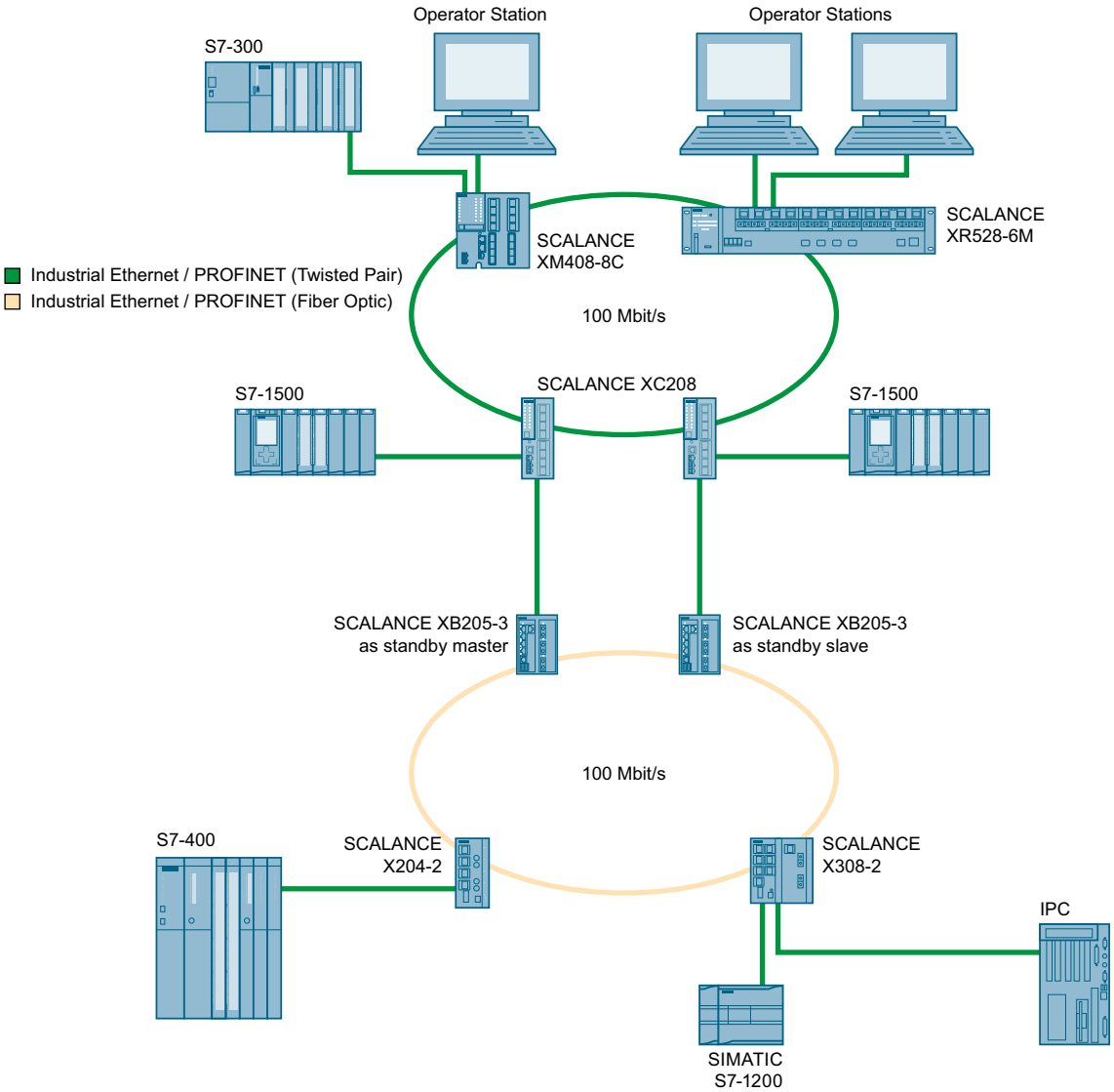


Figure 5-4 Example of a redundant link between rings

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.

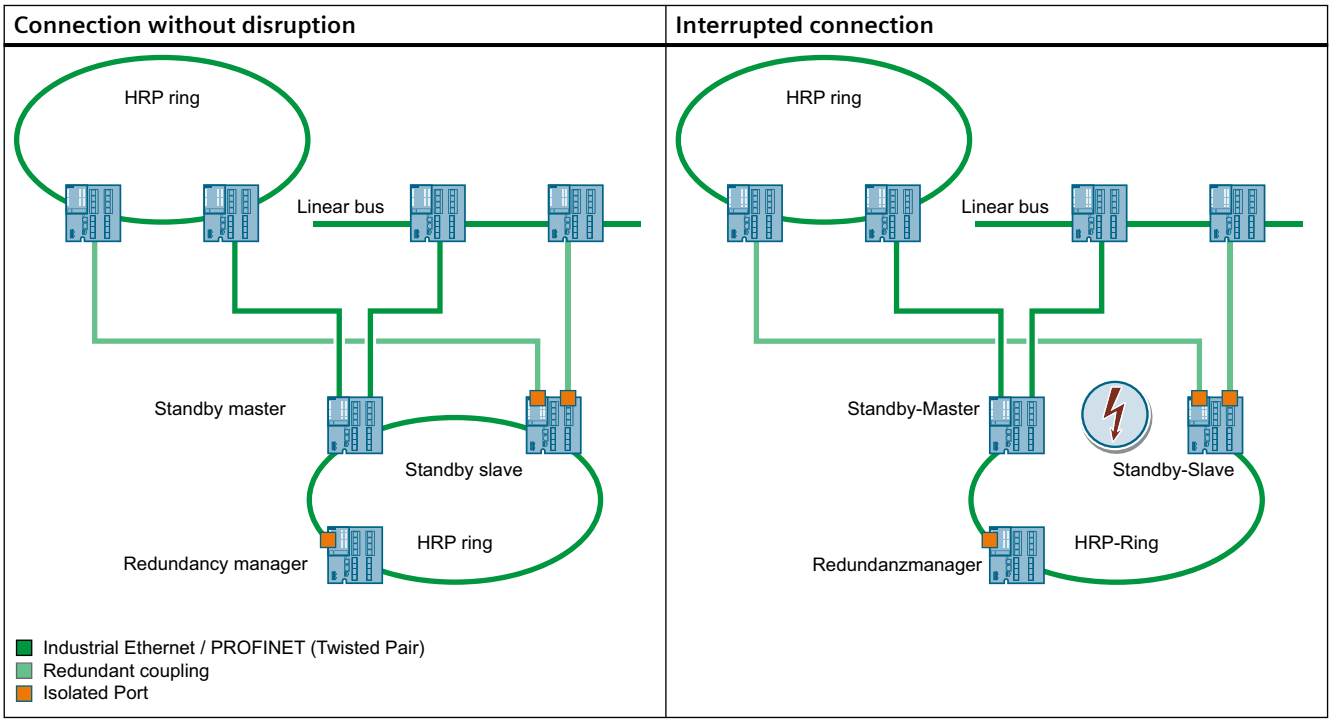
The two standby redundancy switches connected in the configuration exchange data frames with each other to synchronize their operating statuses (one device is master and the other slave). If there are no problems, only the link from the master to the other network segment is active. If this link fails (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.

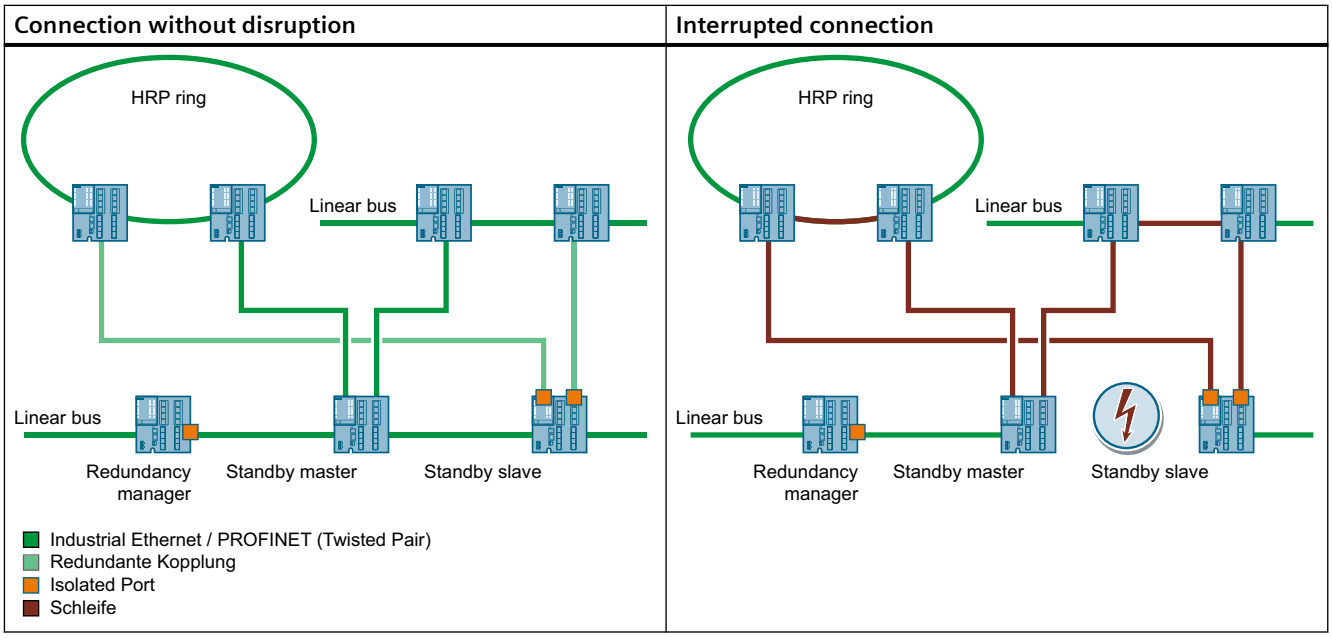
Standby master and slave in a closed network segment

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.



5.3.7 Link Check

Monitoring optical connections in the ring

On optical connections disturbances are possible in which the optical connection is not completely interrupted, but frames are lost sporadically. Such problems can, for example, be caused by defective optical cables, dirty connectors or device defects.

The redundancy manager of an HRP or MRP ring with optical connections detects a "non-recoverable ring error" with such a disturbance. The redundancy manager cannot eliminate the disturbance by closing the ring. Closing the ring in this case, would lead to circulating frames.

With the Link Check function, you can monitor the transmission quality of optical sections within an HRP or MRP ring, identify disturbed connections and under certain conditions turn them off. When the disturbed section is turned off, the redundancy manager can close the ring and restore communication.

How Link Check works

Behavior with an undisturbed connection

If you enable Link Check on two connected ring ports, the two connection partners exchange Link Check frames cyclically on these ports. The frames received by one connection partner are sent back to the other.

When the devices receive back the frames they sent from the connection partner, the connection is prepared for Link Check. The connection partners then increase the send frequency of the Link Check test frames and the actual connection monitoring is active.

Behavior with a disturbance

When connection monitoring is enabled, you can see the number of sent and received Link Check test frames on the "Information > Redundancy > Link Check" page. Based on these statistics you can recognize smaller disturbances for which the disturbance does not yet cause the transmission line to be closed down by Link Check.

Link Check recognizes a connection as being disturbed and closes it down when too many test frames are lost within a given period. Link Check uses several intervals to be able to recognize sudden occurrences of errors as well as a continuous low error rate.

A port that was turned off by Link Check must be reset to be able to communicate again. To do this you have 2 options:

- Pull out the connecting cable and plug it in again.
- Reset the function on both connection partners using the "Reset" button. This must be done on both devices within 30 s.

Note

When you use the "Reset" button, loops can form temporarily resulting in a loss of data traffic. The loop is automatically cleared again.

If this is not acceptable for your application, reset Link Check by pulling the cable and plugging it in again.

After resetting Link Check, the function is restarted on the port and the statistics are reset.

Configuring via a PROFINET IO controller

If MRP is configured via a PROFINET IO controller, you can start the Link Check function for the optical ring ports of the 1st MRP ring instance using WBM or CLI.

When a new configuration is transferred, Link Check is automatically disabled on all ports that were not configured as ring ports of the 1st MRP ring instance.

Note

Events relating to the Link Check function are reported only indirectly by PROFINET IO. If the MRP diagnostic interrupts are enabled and a ring port is disabled by Link Check, PROFINET IO generates an error message that the connection no longer exists.

5.3.8 Parallel Redundancy Protocol

Parallel Redundancy Protocol

The "Parallel Redundancy Protocol" (PRP) is a redundancy protocol for Ethernet networks. It is defined in Part 3 of the IEC 62439 standard. This redundancy method allows data communication to be maintained without interruption/reconfiguration time if there are interruptions in the network.

The PRP method is supported, for example, by the devices of the SCALANCE X-200RNA product line.

Overlong frames

When sending PRP frames, the IE switch expands the frame with a PRP trailer. With frames with the maximum length, appending the PRP trailer results in an overlong frame that exceeds the maximum permitted frame length (according to the IEEE 802.3 standard).

To prevent data loss with overlong frames, all network components located in a PRP network must support a frame length of at least 1528 bytes.

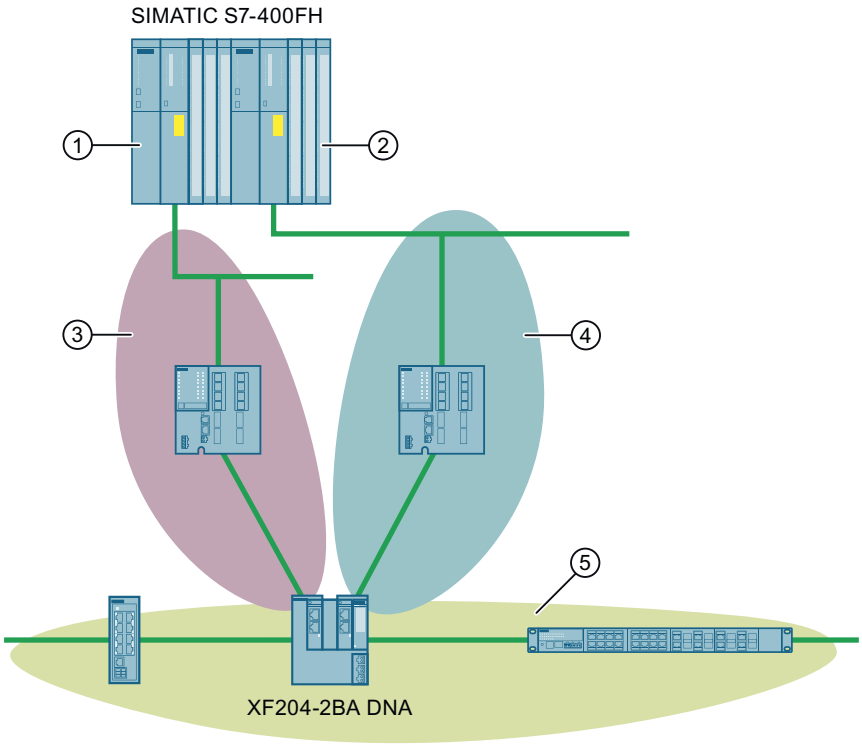
The devices described in this manual can be used in PRP networks, see also section "Configuration limits (Page 20)".

5.3.9 Dual Network Access (DNA)

Operating principle and topology

Dual Network Access (DNA) is a technology for connecting a network with two networks decoupled from one another. A switch that makes this functionality available is also known as a "Y switch". This refers to the connection of the switch to the two other networks. The ports of the Y-switch for connection to the two decoupled networks are the DNA ports.

A usual usage case is the connection of a redundant controller to an MRP ring. Connection of a line topology, as illustrated in the following figure, is also possible, however:



① First controller of the redundant control system
② Second controller of the redundant control system
③ Network of the first controller
④ Network of the second controller
⑤ Shared network (in this example: line topology), both controllers have access to this network.

The first DNA port of the Y-switch is connected to the network ③, the second DNA port to the network ④. The Y-switch ensures that the two networks ③ and ④ are decoupled from one another. No access is possible to the devices in network ④ from the devices in network ③ and vice versa.

The other ports of the Y-switch that are not DNA ports connect the two networks ③ and ④ with the network ⑤. The devices in network ⑤ can be reached from both network ③ and network ④. In network ⑤, devices are used that function as S2 devices and establish a connection to both controllers as S2 devices.

Note

You can use the following devices as Y-switch:

- SCALANCE XF204-2BA DNA

5.3.10 Dual Network Access-Redundanz (DNA-Redundanz)

Operating principle and topology

DNA redundancy means the use of redundant Dual Network Access for connecting a network with two networks decoupled from one another. For this purpose, two Y-switches are used: a DNA manager and a DNA client. DNA redundancy is only possible with an MRP ring. One Y-switch takes on the roles of MRP manager and DNA manager and a second Y-switch takes on the roles of MRP client and DNA client. There is a connection to the two decoupled networks when at least one Y-switch is in operation.

In regular operation, the DNA ports of the DNA client are blocked and the DNA ports of the DNA manager are in "Forwarding" state. If the DNA client no longer receives MRP frames from the manager because it was switched off, for example, it switches its two DNA ports to the "Forwarding" state.

Note

You can use the following devices as DNA manager or DNA client:

- SCALANCE XF204-2BA DNA

Configuring DNA redundancy

The following section describes in detail the procedure for configuring DNA redundancy. Execute the configuration steps in the order listed here to prevent network loops.

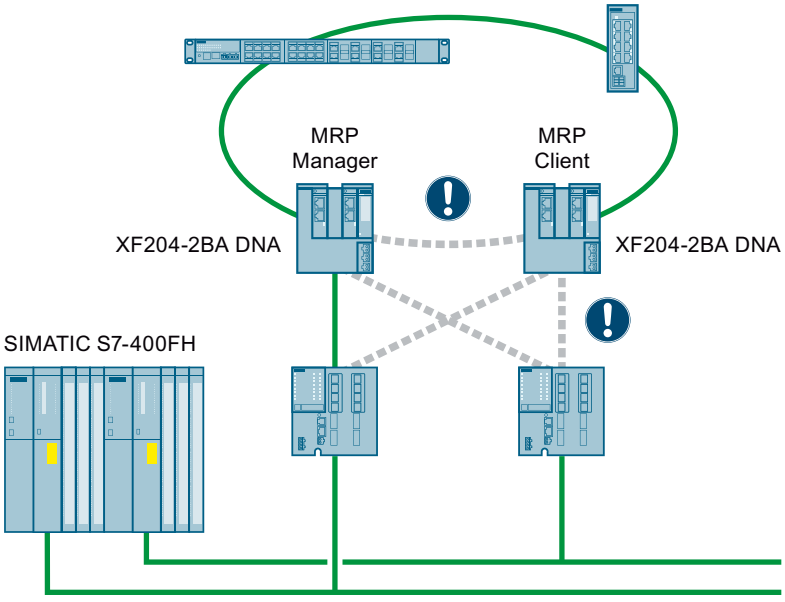
Note

Changing the ring ports later

To change the preconfigured ring ports, disable DNA redundancy first.

Step 1: Connect devices

Connect all devices of the MRP ring except the connection between the MRP manager and the MRP client. Connect only one DNA port of the MRP Manager with one of the controllers or with the switch to which the controller is connected.



Step 2: Configuration

If the devices are not to use PROFINET functionality, you can set up DNA redundancy without STEP 7 Classic. Configure MRP and DNA redundancy by accessing the devices directly with the WBM or the CLI. Both devices can be reached via the MRP ring. Because the MRP ring is still open, circulating frames are excluded, even if no MRP configuration is active yet.

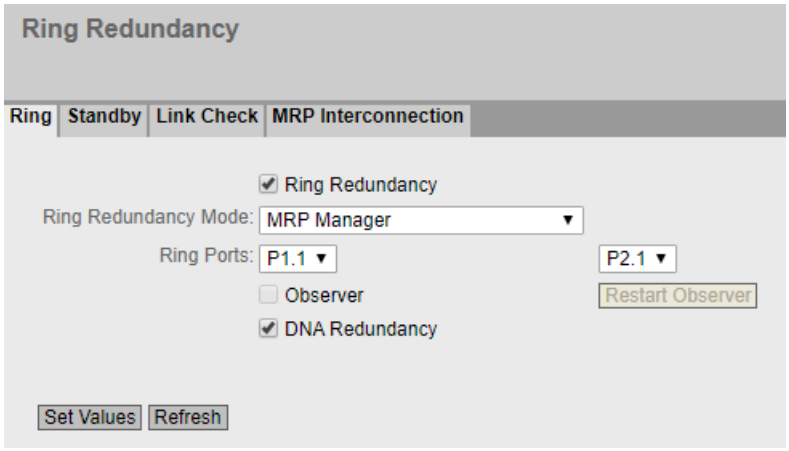
Note

Changing the ring ports

To change the preconfigured ring ports, disable DNA redundancy first.

Step 2 without PROFINET functionality in Web Based Management

1. Open the WBM of the Y-switch that is to take on the role of DNA manager.
2. Open the WBM page "Layer 2 > Ring Redundancy > Ring":



3. Select the "Ring Redundancy" check box.
4. Select the "MRP Manager" entry in the "Ring Redundancy Mode" drop-down list.
5. Select the ring ports of the MRP manager in the two "Ring Ports" drop-down lists.
6. Select the "DNA Redundancy" check box. The two ports that are not ring ports are DNA ports.
7. Click the "Set Values" button.
8. Open the WBM of the Y-switch that is to take on the role of DNA client.
9. Open the WBM page "Layer 2 > Ring Redundancy > Ring".
10. Select the "Ring Redundancy" check box.
11. Select the "MRP Client" entry in the "Ring Redundancy Mode" drop-down list.
12. Select the ring ports of the MRP client in the two "Ring Ports" drop-down lists.
13. Select the "DNA Redundancy" check box. The two ports that are not ring ports are DNA ports.
14. Click the "Set Values" button.
15. Configure the remaining devices in the ring as MRP clients.

Step 2 without PROFINET functionality with the Command Line Interface

1. Open the CLI of the Y-switch that is to take on the role of DNA manager in a Windows console.
2. Execute the following command in global configuration mode:
   `ring-redundancy mode mrpmanager`

3. Configure the ring ports in redundancy configuration mode with the following command:
   `ring ports <interface-type> <interface-id> <interface-type> <interface-id>`
   The parameters are the interface type and the interface name for the two ring ports.
   Example:
   To configure the same ring ports as in the previous screenshot, the following command is necessary:
   `ring ports fa 1/1 fa 2/1`
   The two ports that are not ring ports are DNA ports. In the example, these are the ports 1/2 and 2/2.
4. Enable DNA redundancy in global configuration mode with the following command:
   `ring-redundancy dna-redundancy`
5. Open the CLI of the Y-switch that is to take on the role of DNA client in a Windows console.
6. Execute the following command in global configuration mode:
   `ring-redundancy mode mrpclient`
7. Configure the ring ports in redundancy configuration mode with the following command:
   `ring ports <interface-type> <interface-id> <interface-type> <interface-id>`
   The parameters are the interface type and the interface name for the two ring ports. The two ports that are not ring ports are DNA ports.
8. Enable DNA redundancy in global configuration mode with the following command:
   `ring-redundancy dna-redundancy`
9. Configure the remaining devices in the ring as MRP clients.

Note

You disable DNA redundancy in global configuration mode with the following command:

`no ring-redundancy dna-redundancy`

Step 2 with PROFINET functionality

If the devices are to use PROFINET functionality, you need to configure DNA redundancy in STEP 7 Classic. Follow the steps outlined below:

Note

Loading the GSDML file into STEP 7 Classic

DNA redundancy is available as of firmware version V4.2. You may need to load the GSDML file of the Y-switch into STEP 7 Classic first before you can configure DNA redundancy with PROFINET functionality in STEP 7 Classic. You will find the GSDML file of the device in the following WBM menu: System > Load&Save > GSDML.

1. Open the HW Config program.
2. Select the Y-switch that is to take on the role of the DNA manager and open the "PNIO Properties" dialog box.

3. Click on the "Media redundancy" tab and configure the following parameters:
   - Role
     Select the "Manager" setting.
   - Ring ports
     The ring ports of the MRP manager.
   - Domain
     Both Y-switches must be in the same domain.
4. Click on the "Parameters" tab and select the "DNA Redundancy" check box. The MRP manager will also be the DNA manager.
5. Click "OK" to finish configuration of the DNA manager.
6. Select the Y-switch that is to take on the role of the DNA client and open the "PNIO Properties" dialog box.
7. Click on the "Media redundancy" tab and configure the following parameters:
   - Role
     Select the "Client" setting.
   - Ring ports
     The ring ports of the MRP client.
   - Domain
     Both Y-switches must be in the same domain.
8. Click on the "Parameters" tab and select the "DNA Redundancy" check box. The MRP client will also be the DNA client.
9. Click "OK" to finish configuration of the DNA client.
10. Configure the remaining devices in the ring as MRP clients. All MRP clients must belong to the domain of the MRP manager.
11. Load the configuration into the controller.

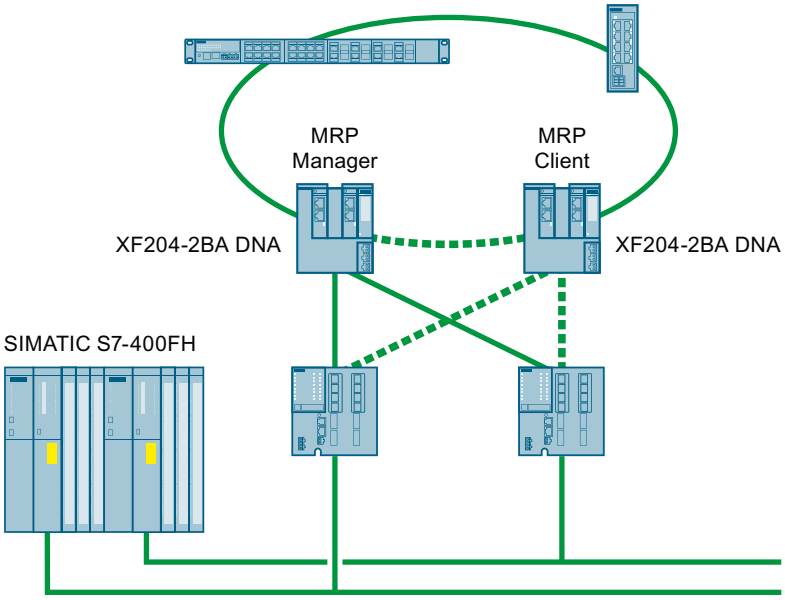
Note

Configure the topology in STEP 7 Classic.

The status of the DNA port cannot be monitored with the "MRP diagnostic alarm" function of the controller. To monitor the connections between Y-switch and controller, you need to configure this topology in STEP 7 Classic.

Step 3: Make connections

Close the MRP ring. Connect the remaining DNA ports with the controllers or with the switches to which the controllers are connected.



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 86)). 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 311)".

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:

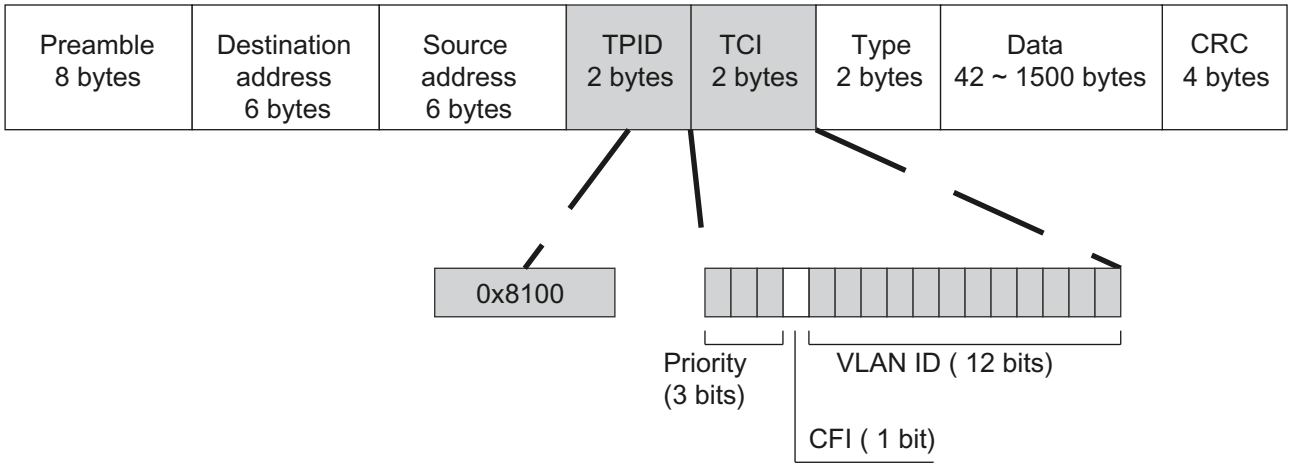


Figure 5-5 Structure of the expanded Ethernet frame

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

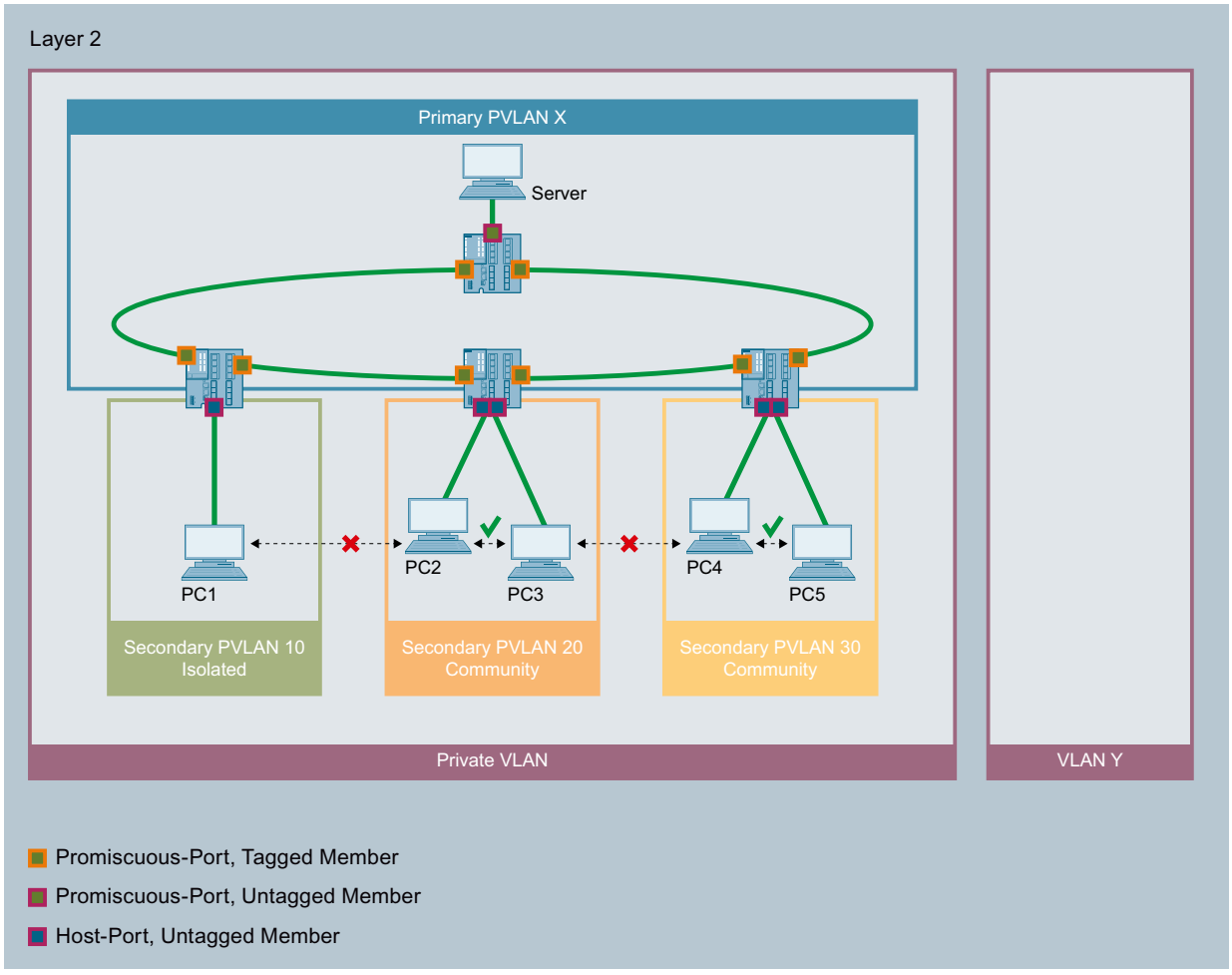
If you use the same VLAN ID for secondary PVLANs on different IE switches, the end devices in these secondary PVLANs can communicate with other via layer 2 across the different switches. The ports that connect different IE switches cannot be configured as trunk ports.

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 ports 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.

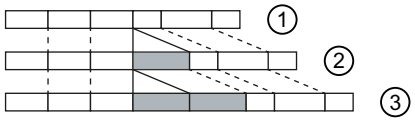
In this example all PCs can communicate with the server. The server can communicate with all PCs. PC1 cannot communicate with any other PC. The PCs within a community secondary PVLAN can communicate with each other but not with the PCs in another secondary PVLAN.

5.4.4 VLAN tunnel

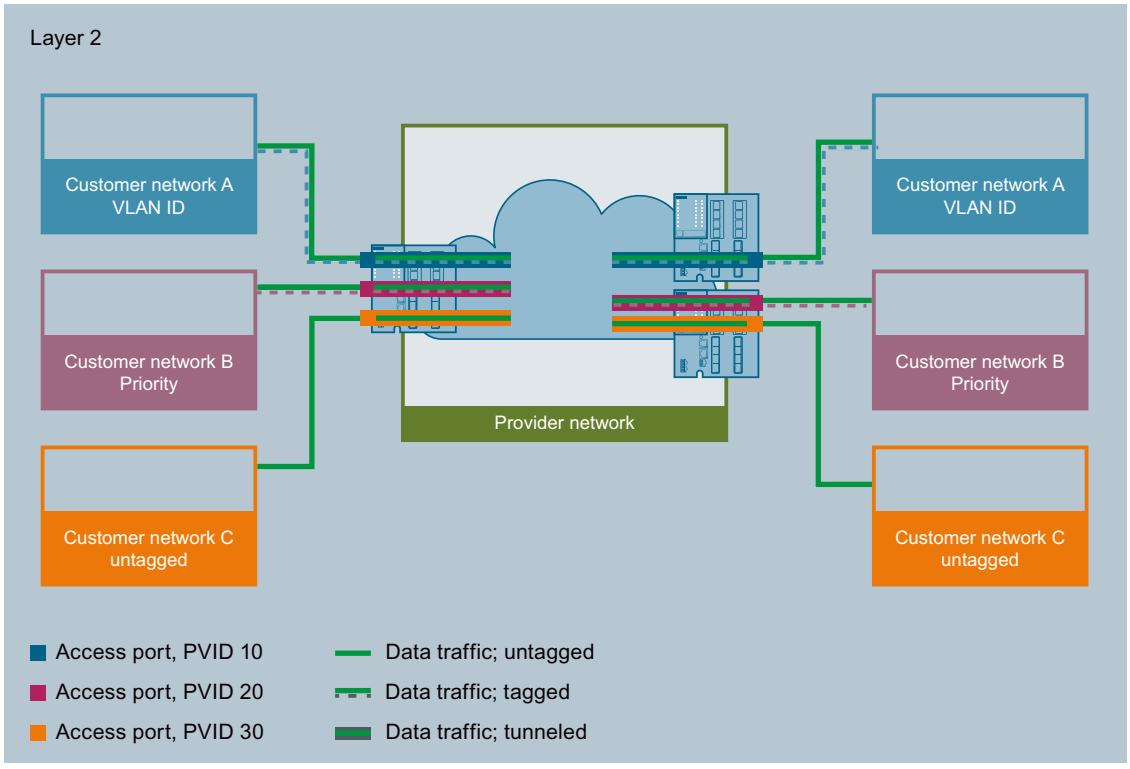
With the Q-in-Q VLAN Tunnel function it is possible to forward the data traffic from different customer networks using a VLAN tunnel via a provider network. Every customer network has the full number of possible VLANs available.

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

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 incoming frame is a broadcast or agent frame.
   → When the first condition is met, the switch takes into account the priority set on the "General (Page 295)" page.
   The switch sorts the frame into a queue according to the assignment on page "CoS Map (Page 297)".
2. If the first condition is not met the switch checks whether the frame contains a VLAN tag.
   → If the second condition is met the switch checks the settings for the priority on the "General (Page 295)" 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 Map (Page 297)".
3. If the second 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 300)".

See also

General (Page 305)

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.

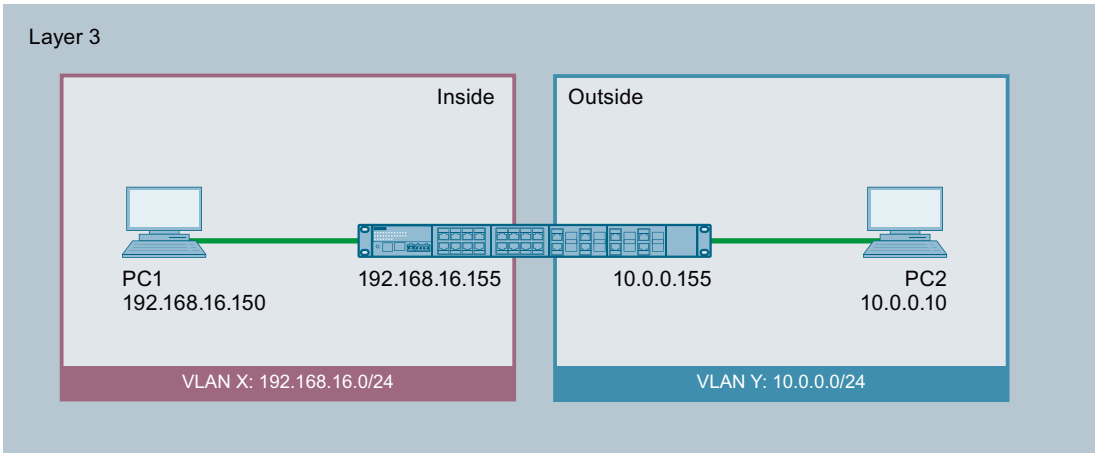
With Network Address Translation (NAT), IP subnets are divided into "Inside" and "Outside". The division is from the perspective of a NAT interface. All networks that can be reached via the NAT interface itself count as "Outside" for this interface. All networks that can be reached via other IP interfaces 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 398)".

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 403)".

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.

5.9 Single-Hop Inter-VLAN-Routing

Introduction

A physical network is divided into broadcast domains and subnets by VLANs.

Devices (hosts) within a VLAN can communicate with each other directly via layer 2. The frames are forwarded to the relevant device based on the MAC address.

Devices from different VLANs cannot communicate with each other directly via layer 2. The data traffic must be routed based on the IP address.

With the Single-Hop Inter-VLAN-Routing function it is possible that devices from different VLANs communicate with each other without a router being necessary.

Requirements

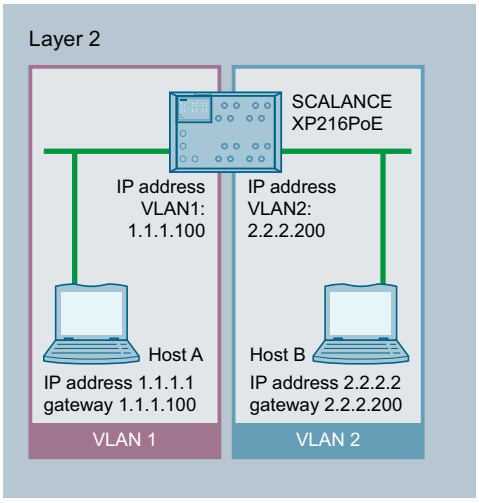
- The IE switch can manage several IP interfaces.
- The switch is a member in the VLANs to be routed.
- With the hosts, the IP address of the VLAN is entered as default gateway.

Single-Hop Inter-VLAN-Routing

The IE switch receives a frame and recognizes that it is addressed to a device in another VLAN. It forwards the frame to the corresponding port in the VLAN.

The IE switch only knows VLANs with which it is directly connected (Connected). With Single-Hop Inter-VLAN-Routing it is therefore only possible to route between two local IP interfaces.

Example



In this example, the host A is connected to the IE switch via VLAN1. Host A is connected to the IE switch via VLAN2. With host A, the IP address of VLAN 1 is entered as the default gateway. With host B the IP address of VLAN 2 is entered as the default gateway.

If the Single-Hop Inter-VLAN-Routing function is enabled on the SCALANCE XP216PoE, host A and host B can communicate with each other.

Configuring with Web Based Management 6

6.1 Web Based Management

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

Requirements

- The device has an IP address.

  Note

  Assign an IP address for 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 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:

- Mozilla Firefox
- Google Chrome
- Microsoft Edge

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

Display of the WBM on mobile devices

For mobile devices, the following minimum requirements must be met:

Resolution	Operating system	Internet browser
960 x 640 pixels	Android as of version 4.2.1 iOS as of version 6.0.2	Chrome as of version 18 on Android Safari as of version 6 on iOS

Tested with the following Internet browsers for mobile devices:

- Apple Safari as of version 8 on iOS as of version 8.1.3 (iPad Mini Model A1432)
- Google Chrome as of version 40 on Android as of version 5.0.2 (Nexus 7C Asus)
- Mozilla Firefox as of version 35 on Android as of version 5.0.2 (Nexus 7C Asus)

Note

Display of the WBM and working with it on mobile devices

The display and operation of the WBM pages on mobile devices may differ compared with the same pages on desktop devices. Some pages also have an optimized display for mobile devices.

6.2 Login

Establishing a connection to a device

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

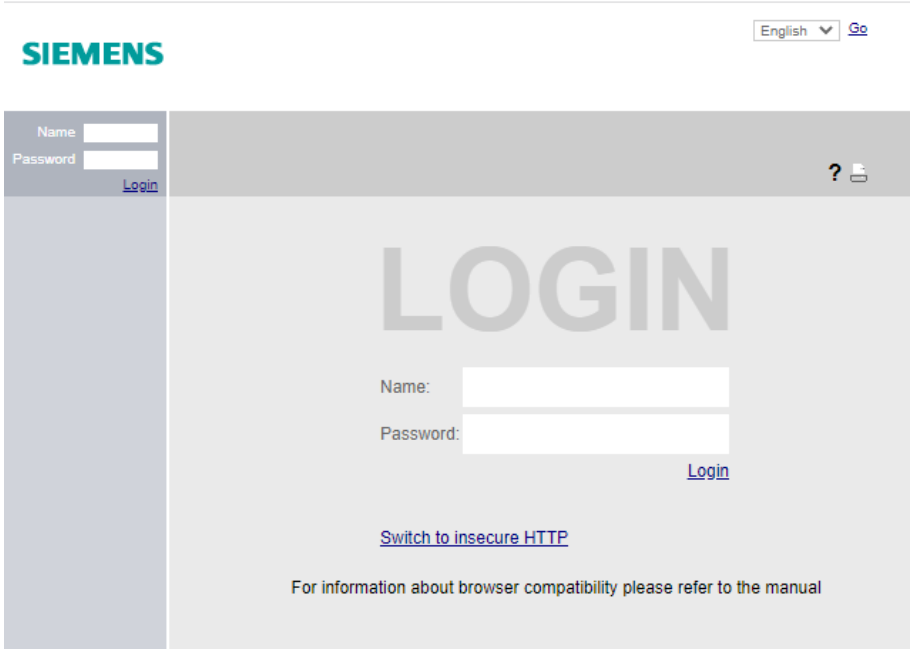
1. There is a connection between the device and the Admin PC. With the ping command, you can check whether or not a device can be reached.
2. In the address field of the web browser, enter "https://" followed by the IP address of the device to be configured or its URL, e.g. https://192.168.16.178.
 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

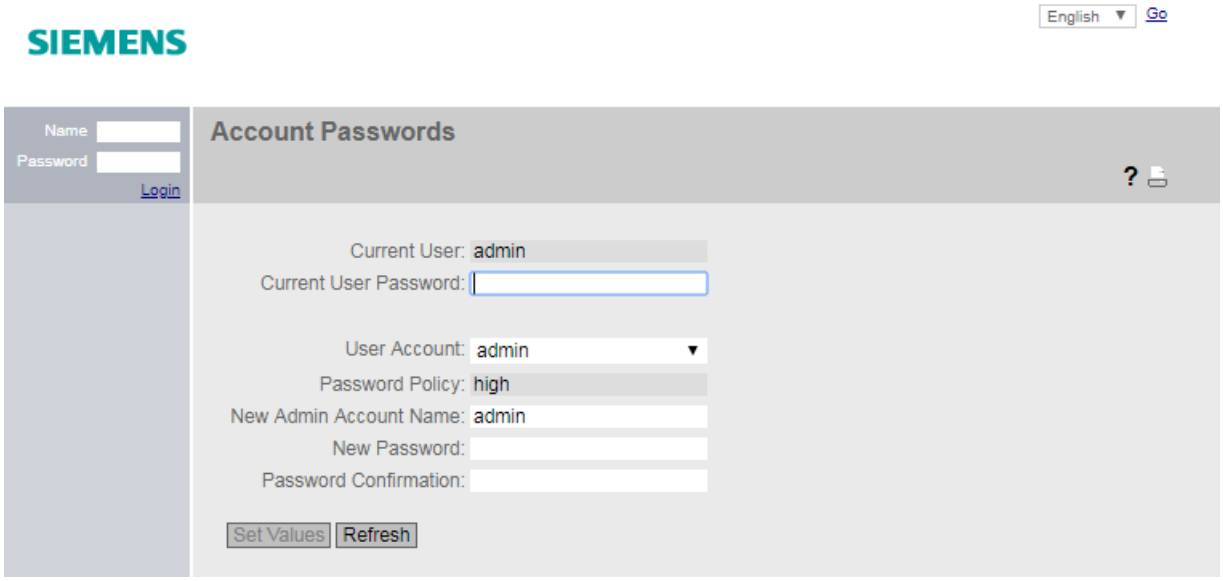
1. "Name" input box:
   - When you log in for the first time or following a "Restore Factory Defaults and Restart", enter the user preset in the factory "admin".
     With this user account, you can change the settings of the device (read and write access to the configuration data).
   - Enter the user 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.

3. 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.

4. 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 431)".

6.3 The "Information" menu

6.3.1 Start page

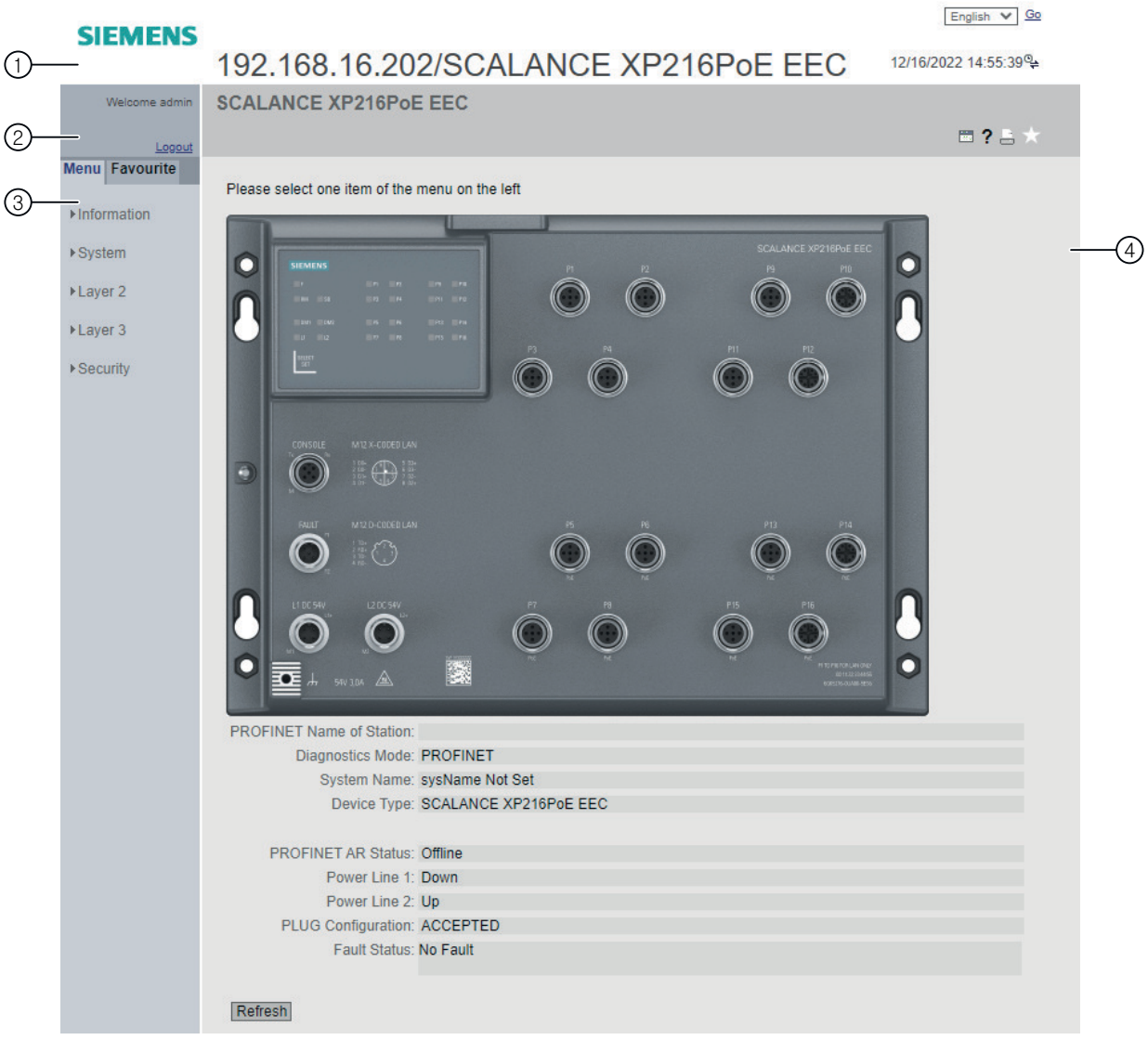
View of the Start page

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.
- **Device name**
  Shows the name of the device.
- **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. This window is displayed for every menu item/submenu after opening and can be moved as desired. 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 submenus. 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 "Back" 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 very 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 immediately."

Note

Interrupting the save

Saving starts only after the timer in the message has elapsed. In this case the following message appears "Saving configuration data in progress. Please do not switch off the device". How long saving takes depends on the device.

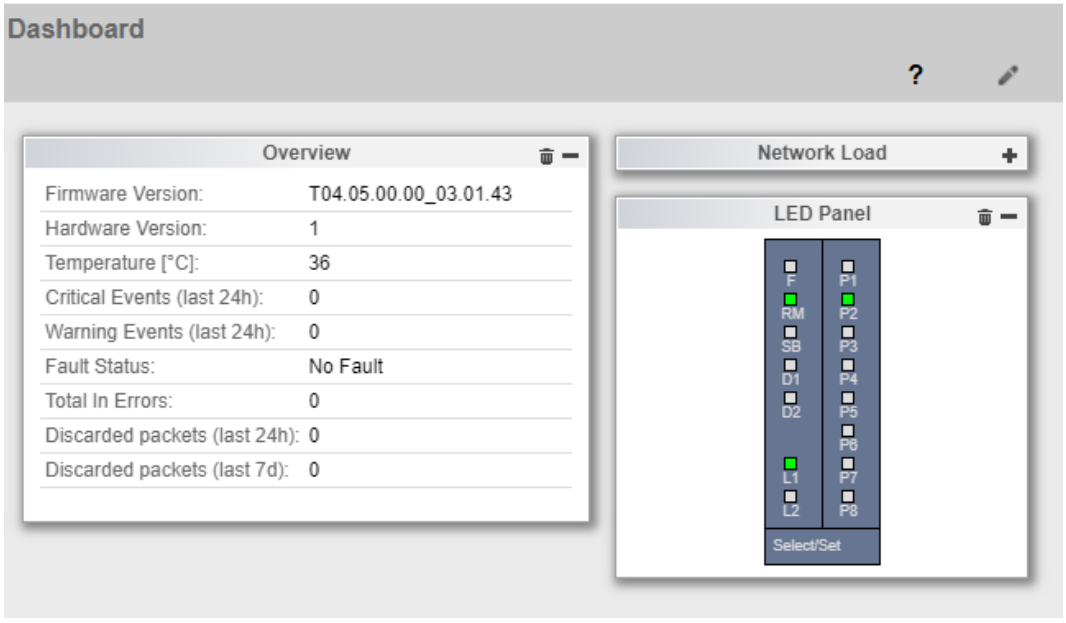
- Do not switch off the device immediately after the timer has elapsed.

6.3.2 Dashboard

This page provides a quick overview of the most important device settings and status. You can compile your own dashboard from available dashboard contents. These contents can be shown or hidden, expanded and collapsed and placed at a desired position on the page. When you click on an individual information field or block, you are forwarded to the WBM page of the respective setting or statistic. This makes it easy to find related configuration pages.

The dashboard is updated every 60 seconds.

To manage the dashboard contents, you require a user role with the function right 15.



Working with the dashboard

To show dashboard contents on the dashboard, click in the upper right portion of the work area. Select the desired contents. These are shown as dashboard blocks on the dashboard.

You have the following options:

- Add new dashboard contents to the dashboard
- Delete dashboard contents
- Expand and collapse dashboard contents
- Arrange dashboard contents with drag-and-drop

The following dashboard contents are available for selection:

- System overview
- LED display
- Network load

Buttons

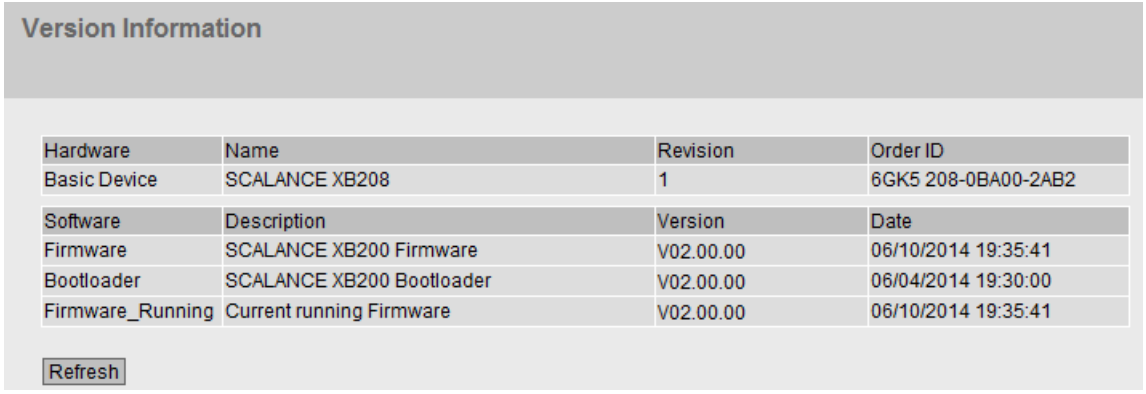
The availability of the buttons depends on the selected dashboard contents.

Icon	Meaning
	Opens the dialog with the selection of available dashboard contents
	Expands the dashboard contents.
	Collapses the dashboard contents.
	Deletes the dashboard contents

6.3.3 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.



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.

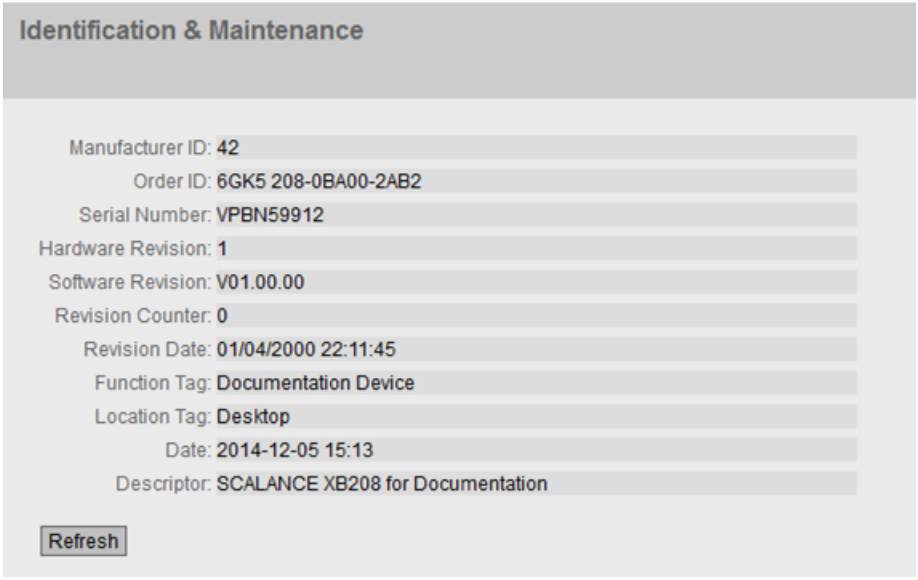
Table 2 has the following columns:

- **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.

6.3.4 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.



Description of the displayed values

The table has the following rows:

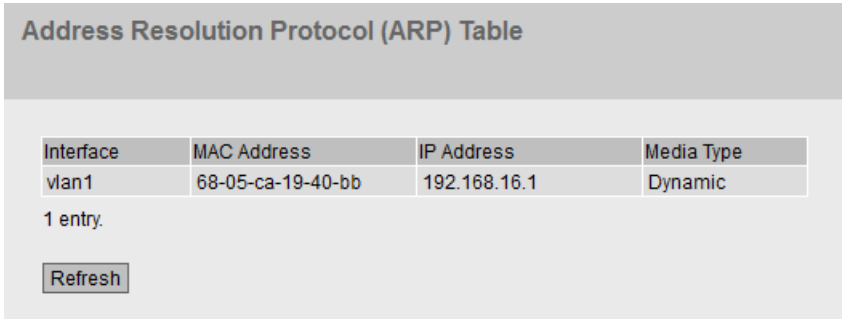
- **Manufacturer ID**
  Shows the manufacturer ID.
- **Order ID**
  Shows the order number.
- **Serial Number**
  Shows the serial number.
- **Hardware Revision**
  Shows the hardware version.
- **Software version**
  Shows the software version.
- **Revision Counter**
  Regardless of a version change, 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.

6.3.5 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.



Description of the displayed values

The table has the following columns:

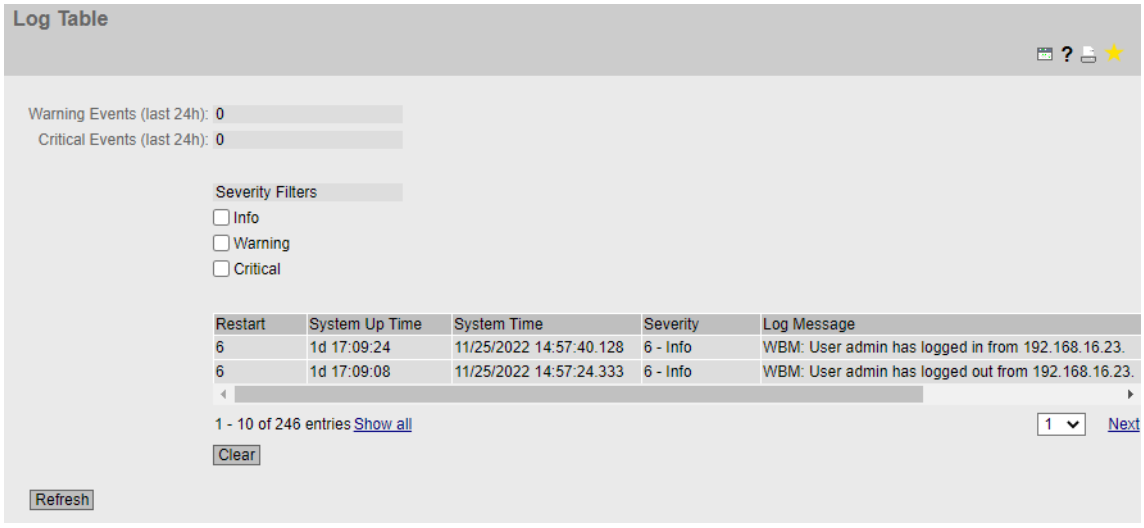
- **Interface**
  Shows the interface via which the row entry was learnt.
- **MAC Address**
  Shows the MAC address of the destination or source device.
- **IP Address**
  Shows the IPv4 address of the destination device.
- **Media Type**
  Shows the type of connection.
  - Dynamic
    The device recognized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

6.3.6 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.

6.3.7 Faults

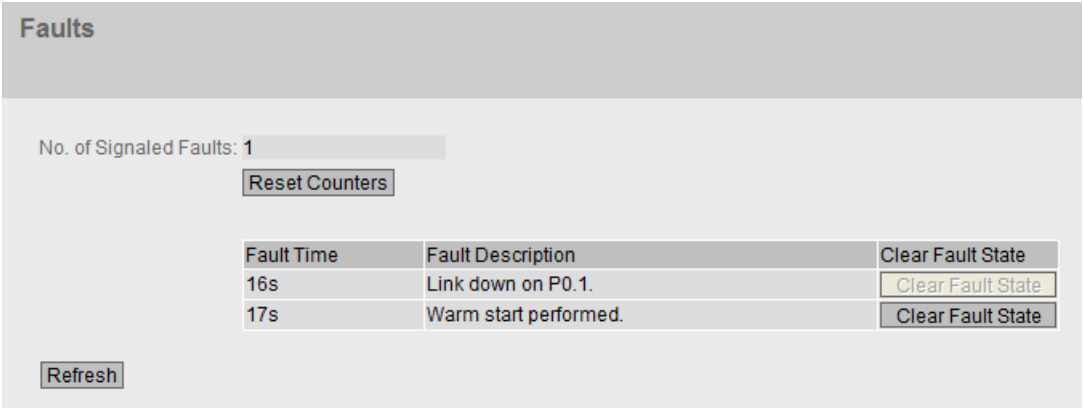
Error status

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.



Description

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

The table contains the following columns:

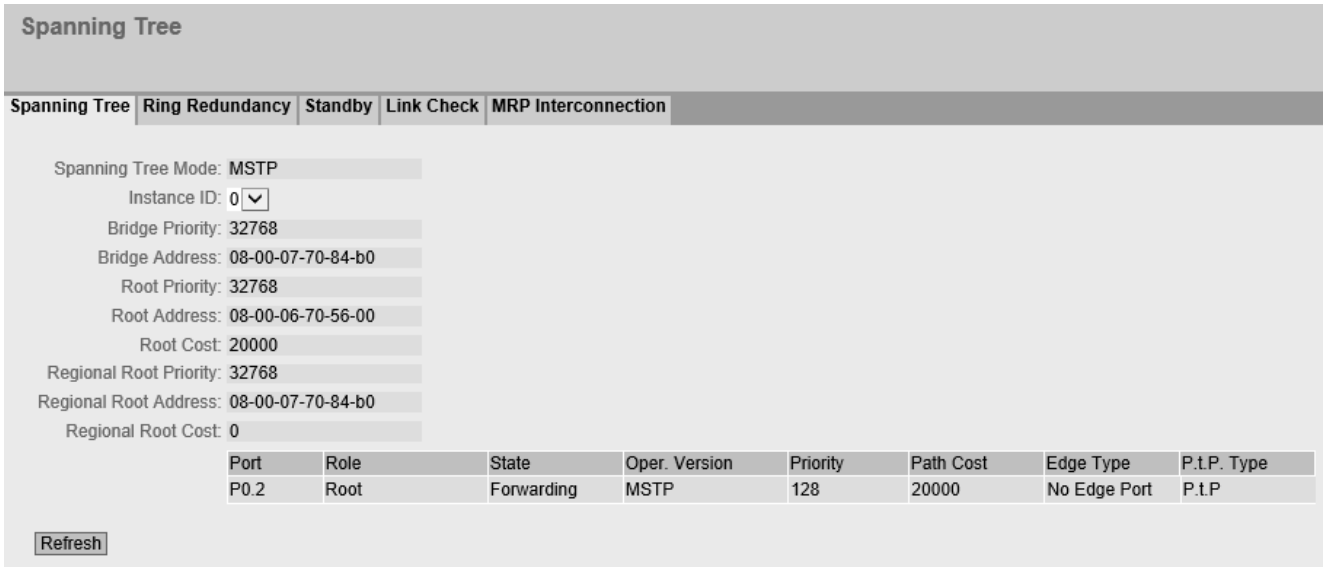
- **Fault Time**
  Shows the time the device has been running since the last system restart when the described error/fault occurred.
- **Fault Description**
  Displays a brief description of the fault/error that has occurred.
- **Clear Fault State**
  Some faults can be acknowledged and thus removed 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.

6.3.8 Redundancy

6.3.8.1 Spanning Tree

Introduction

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



Description of the displayed values

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. Both 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
    If a switch has several ports to the same network segment, the "poorer" port becomes the backup port.
  - 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

    An end device is connected to 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.

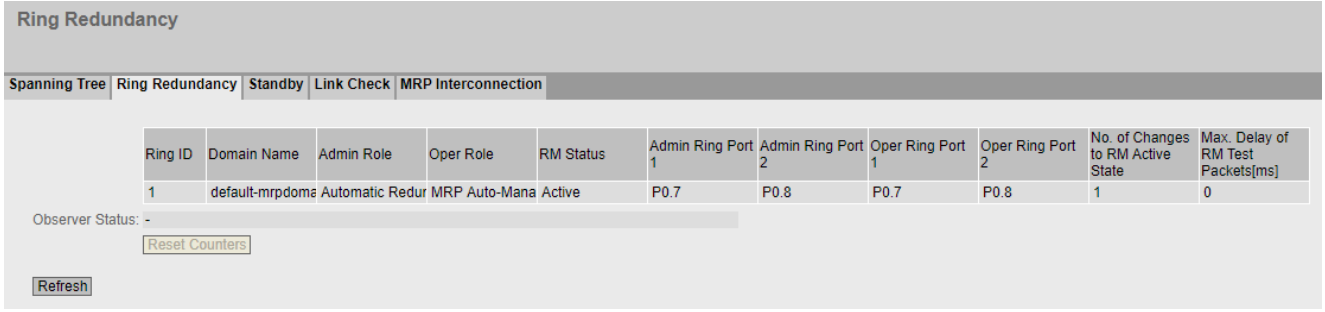
    Note

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

6.3.8.2 Ring Redundancy

Information on ring redundancy

On this page, you obtain information about the status of the device in terms of ring redundancy. The text boxes on this page are read-only. When ring redundancy is disabled, the table is empty.



Description of the displayed values

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.
- **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 boxes are displayed:

- **Observer Status**
  Shows the current status of the observer.
- **"Reset Counters" button**

  Note

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

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

6.3.8.3 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.

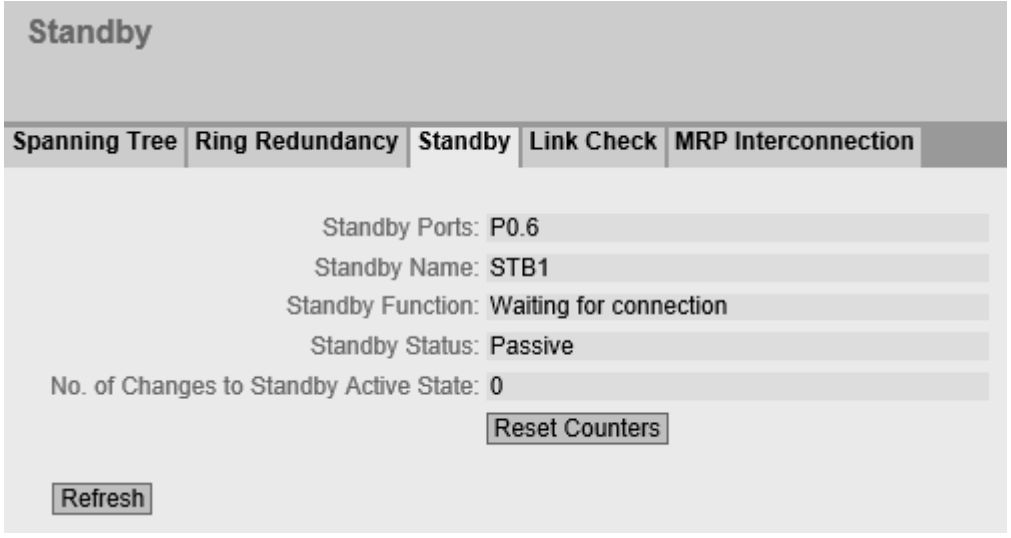
Note

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**
  The "Standby Status" display box 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.

Description of the button

"Reset Counters" button

Click "Reset Counters" to reset all counters. The counter is reset when there is a restart.

6.3.8.4 Link Check

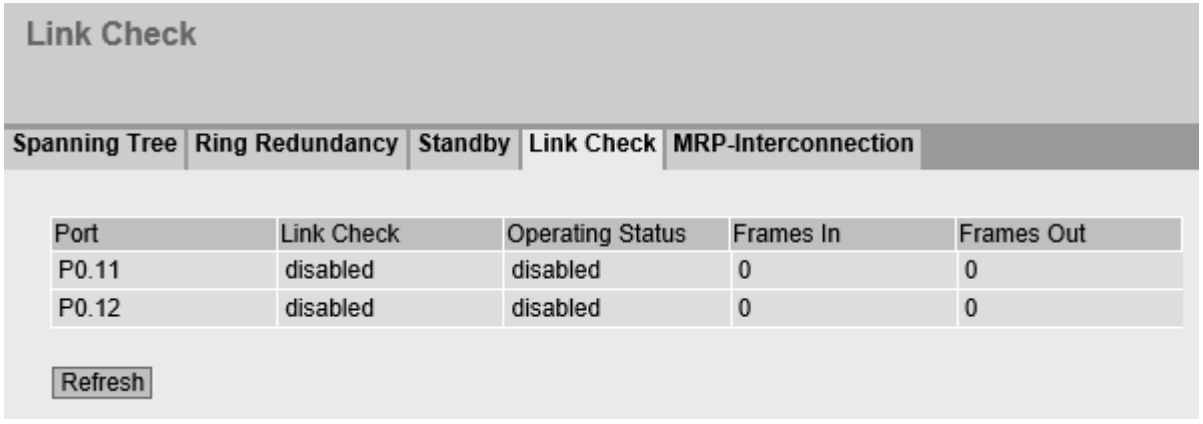
Monitoring optical connections in the ring

The page shows the following information on the link check:

- The ring ports
- The current status (activated or not activated)
- The statistics of sent and received Link Check frames of the monitored connections.

Note

If you use Link Check together with a redundancy protocol (e.g. HRP), the values for the sent and received Link Check frames can be different.



Description of the displayed values

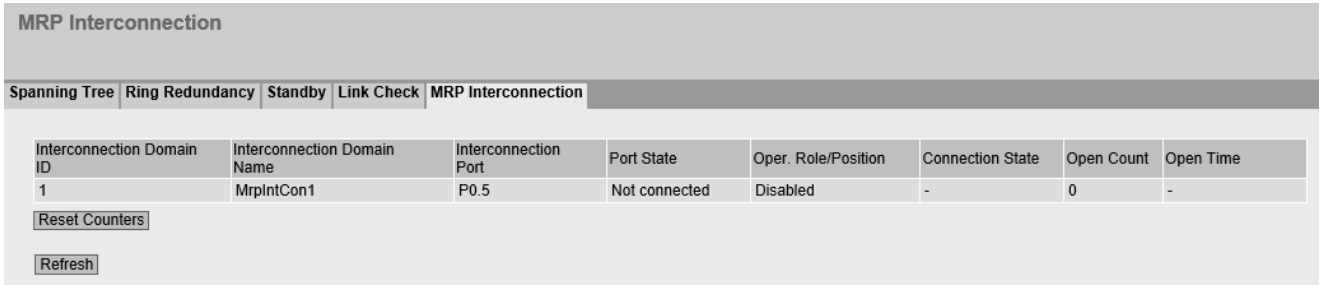
The following fields are displayed:

- **Port**
  Shows the port to which the following information relates. The port is made up of the module number and the port number, for example port 0.1 is module 0, port 1.
- **Link Check**
  Shows whether the Link Check function is enabled or disabled. Link Check can only be enabled for optical ports.

- **OperState**
  Shows the status of the Link Check function. The following statuses are possible:
  - Disabled
    The function is disabled.
  - Enabled
    The function is enabled. The connection partner has not yet confirmed the monitoring.
  - Running
    The function is enabled. The connection monitoring is enabled. The outgoing and incoming test frames are counted and matched up.
  - Faults
    The function is enabled. Link Check has detected a fault on the monitored section and turned off the port.
- **Frames in**
  Shows how many Link Check test frames were received.
- **Frames out**
  Shows how many Link Check test frames were sent

6.3.8.5 MRP Interconnection

Redundant linking of rings



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 following options are available:
  - 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 following options are available:
  - Disabled
  - Manager
  - Primary Client
  - Secondary Client
- **Connection Status**
  The status of the MRP Interconnection domain. The following options are available:
  - 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.
- **Reset Counter**
  Click "Reset Counter" to reset the counter. The counter is reset when there is a restart.

6.3.9 Ethernet Statistics

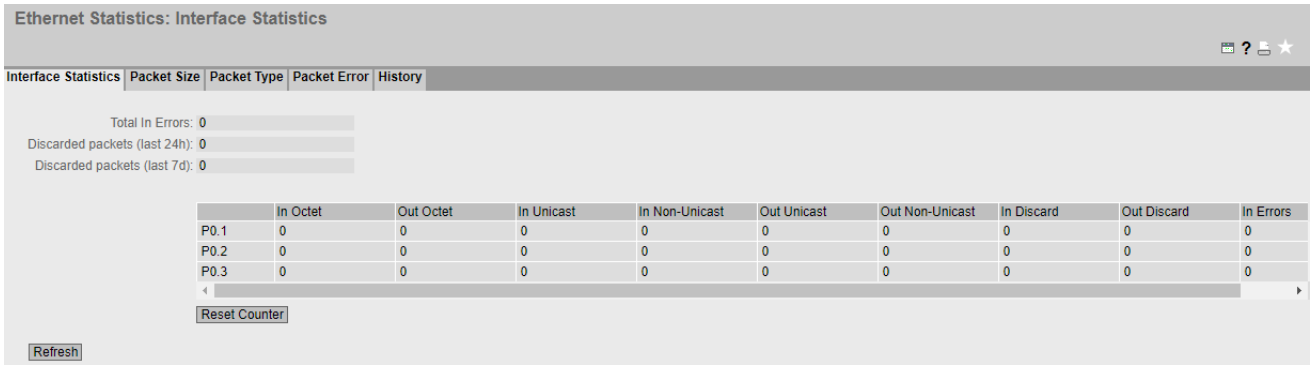
6.3.9.1 Interface Statistics

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.



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.

- **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".

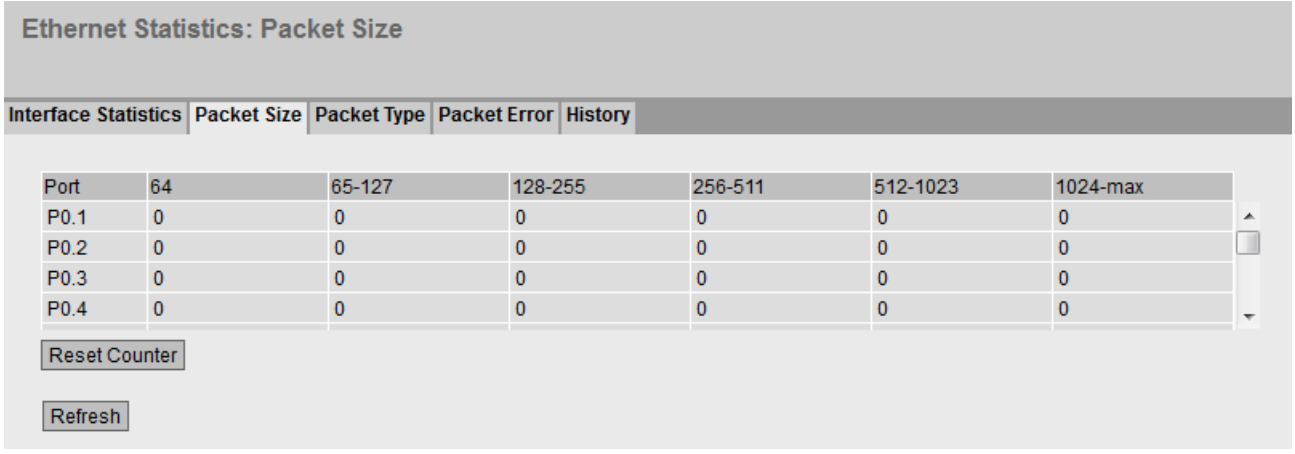
6.3.9.2 Packet Size

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.



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.

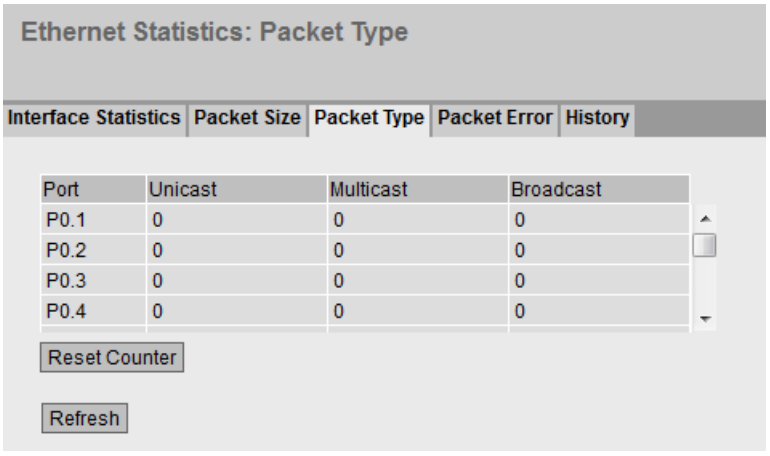
6.3.9.3 Packet Type

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.



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".

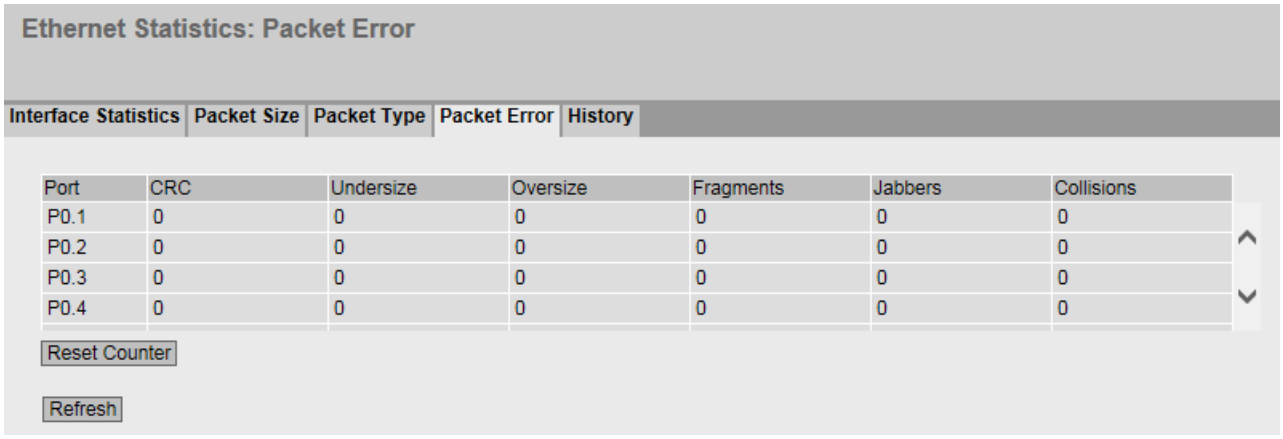
6.3.9.4 Packet Error

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.



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

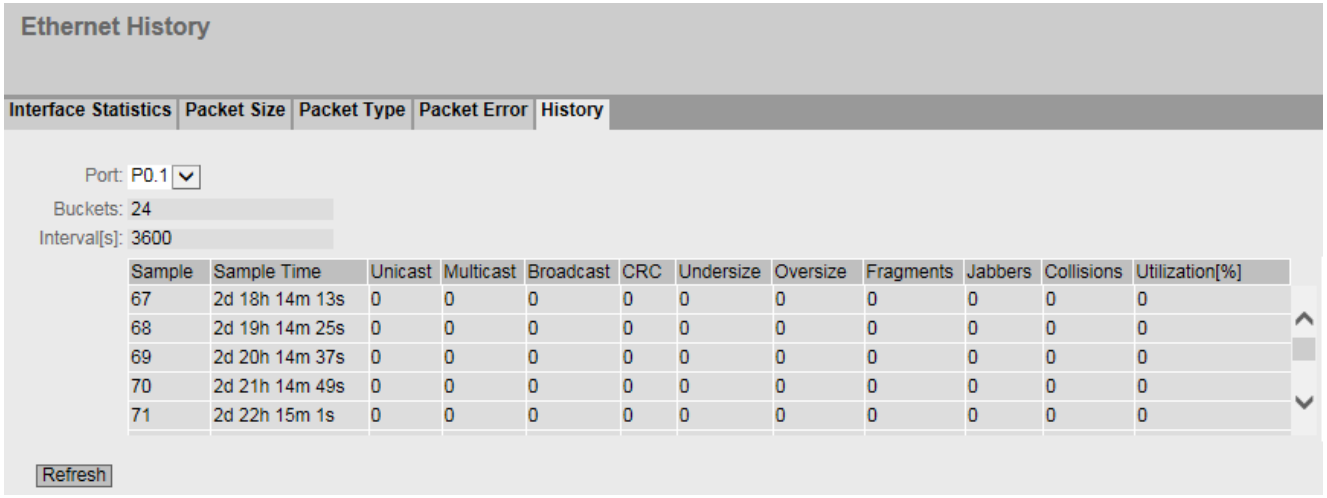
    Packets with a length less than 64 bytes and a bad CRC checksum.
  - Jabbers
    VLAN-tagged packets with an incorrect CRC checksum that were discarded because they were too long.
  - Collisions
    Collisions that were detected.

6.3.9.5 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.



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

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.

6.3.10 Unicast

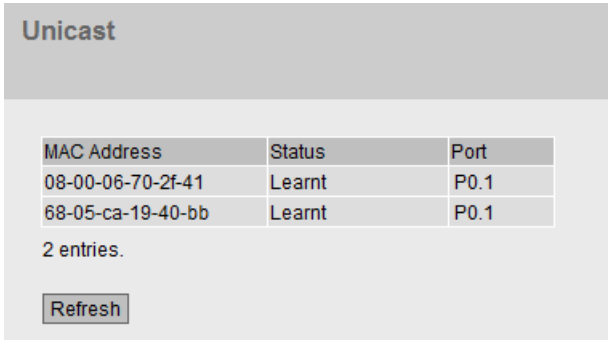
Status of the unicast filter table

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.

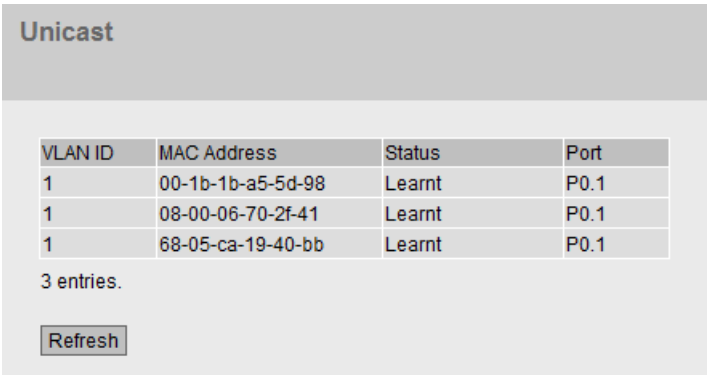
Dependency on the "Base bridge mode"

The displayed columns depend on which "Base bridge mode" is set. If you change the "Base bridge mode", the existing entries are lost.

WBM page for the base bridge mode "802.1D Transparent Bridge":



WBM page for the Base bridge mode "802.1Q VLAN Bridge":



Description

This table can contain 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.
- **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 learned 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 are being forwarded to this port.

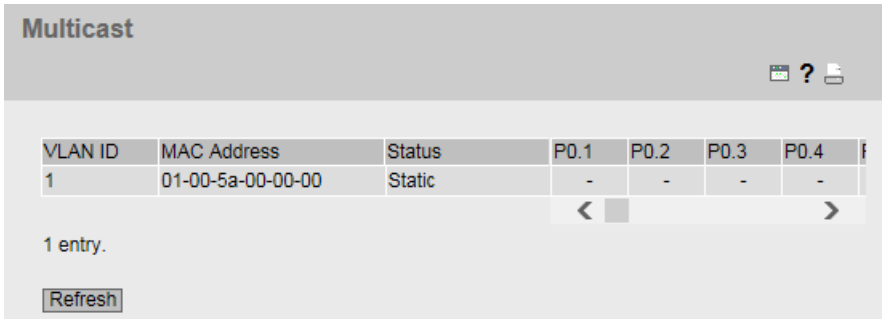
6.3.11 Multicast

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).

Dependency on the "Base bridge mode"

If you change the "Base bridge mode", the existing entries are lost.



Description

This table can contain 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.

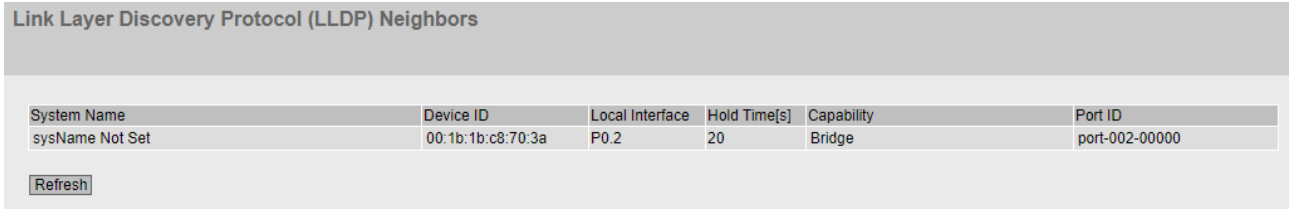
- **Status**
  Shows the status of each address entry. The following information is possible:
  - Static
    The address was entered statically by the user. Static addresses are stored permanently; in other words, they are not deleted when the aging time expires or when the device is restarted. These can be deleted by the user.
  - IGMP
    The destination port for this address was obtained using IGMP.
  - 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 an IGMP 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. Moreover, learning dynamically via IGMP is not permitted at this port.

6.3.12 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".



Description

The table contains the following columns:

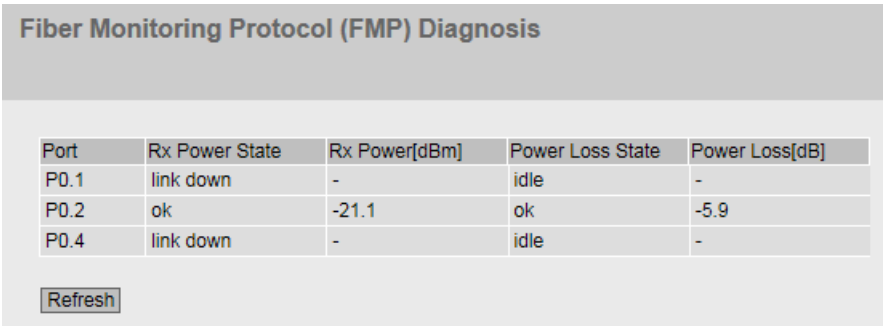
- **System Name**
  System name of the connected device
- **Device ID**
  Device ID of the connected device. The device ID corresponds to the device name, which is assigned via SINEC PNI, for example. If no device name is assigned, the MAC address of the device is displayed.
- **Local Interface**
  Port 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.

6.3.13 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".



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.

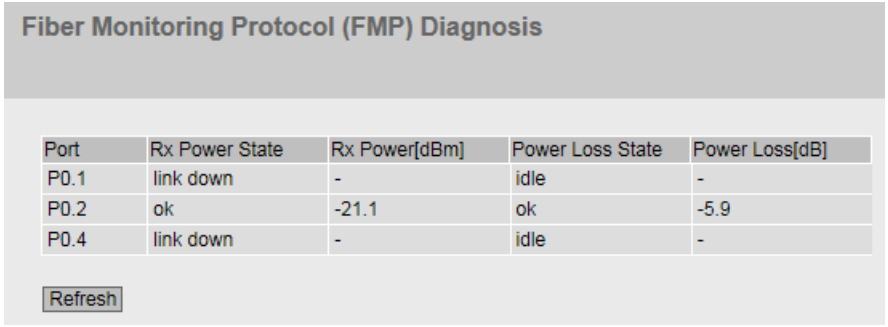
6.3.14 Plastic Optical Fiber

Monitoring of POF ports

This page shows the diagnostics data for interfaces with plastic optical fiber (POF).

The currently available link power margin is shown as a numerical value for each POF port.

The link power margin indicates the attenuation on the connection between sender and receiver that can be overcome. The higher the link power margin, the higher the attenuation can be while maintaining a functioning link. If the link power margin sinks, the attenuation has increased, for example due to aging or a defect. The longer the cable being used, the lower the link power margin available.



Description of the displayed values

The table contains the following columns:

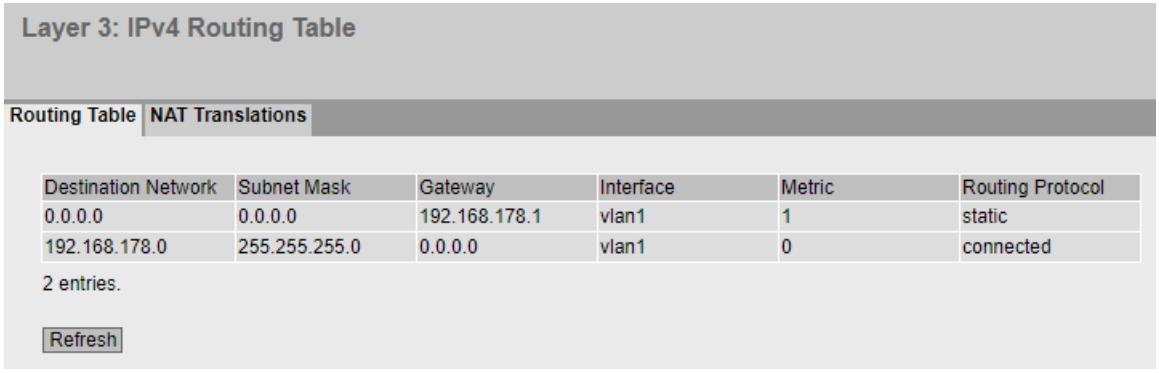
- **Port**
  Shows all POF ports.
- **Power State**
  Shows the current status of the port.
  - **disabled**
    The monitoring is disabled.
  - **ok**
    There is an adequate link power margin for problem-free operation.
  - **maint. req.**
    Check the link.
    A warning is signaled.
  - **maint. 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.
- **Power**
  Shows the current value of the link power margin.
  If there is no connection (Link down) or the monitoring is disabled, "-" is displayed. If the monitoring is not enabled on the partner port, the value 0.0 is displayed.
- **Power [dBm] Maintenance Required (warning)**
  Shows the value at which you are informed of a deterioration of the link power margin by a message of the severity level "Warning".
- **Power [dBm] Maintenance Demanded (critical)**
  Shows the value at which you are informed of a deterioration of the link power margin by a message of the severity level "Critical".

6.3.15 Routing

6.3.15.1 Routing Table

Introduction

This page shows the routes currently being used.



Description of the displayed values

The table has the following columns:

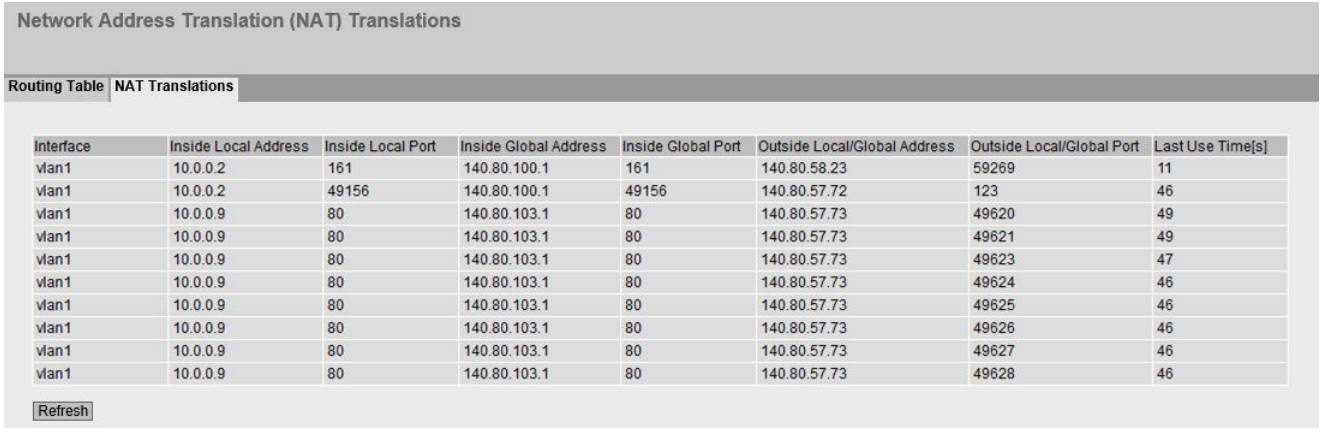
- **Destination Network**
  Shows the destination address of this route.
- **Subnet Mask**
  Shows the subnet mask of this route.
- **Gateway**
  Shows the gateway for this route. For sink routes, the information "Sink" is displayed instead of the IP address.
- **Interface**
  Shows the interface for 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:
  - Connected: Connected routes
  - Static: Static routes
  - RIP: Routes via RIP
  - OSPF: Routes via OSPF
  - Other: Other routes

6.3.15.2 NAT Translations

Overview

This page displays the active NAT connections.

Description of the displayed values



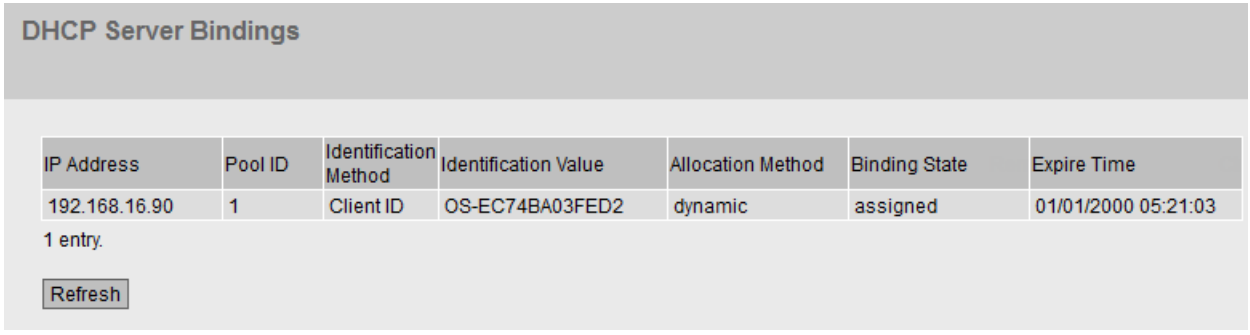
Interface	Inside Local Address	Inside Local Port	Inside Global Address	Inside Global Port	Outside Local/Global Address	Outside Local/Global Port	Last Use Time[s]
vlan1	10.0.0.2	161	140.80.100.1	161	140.80.58.23	59269	11
vlan1	10.0.0.2	49156	140.80.100.1	49156	140.80.57.72	123	46
vlan1	10.0.0.9	80	140.80.103.1	80	140.80.57.73	49620	49
vlan1	10.0.0.9	80	140.80.103.1	80	140.80.57.73	49621	49
vlan1	10.0.0.9	80	140.80.103.1	80	140.80.57.73	49623	47
vlan1	10.0.0.9	80	140.80.103.1	80	140.80.57.73	49624	46
vlan1	10.0.0.9	80	140.80.103.1	80	140.80.57.73	49625	46
vlan1	10.0.0.9	80	140.80.103.1	80	140.80.57.73	49626	46
vlan1	10.0.0.9	80	140.80.103.1	80	140.80.57.73	49627	46
vlan1	10.0.0.9	80	140.80.103.1	80	140.80.57.73	49628	46

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.

6.3.16 DHCP Server

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



Description

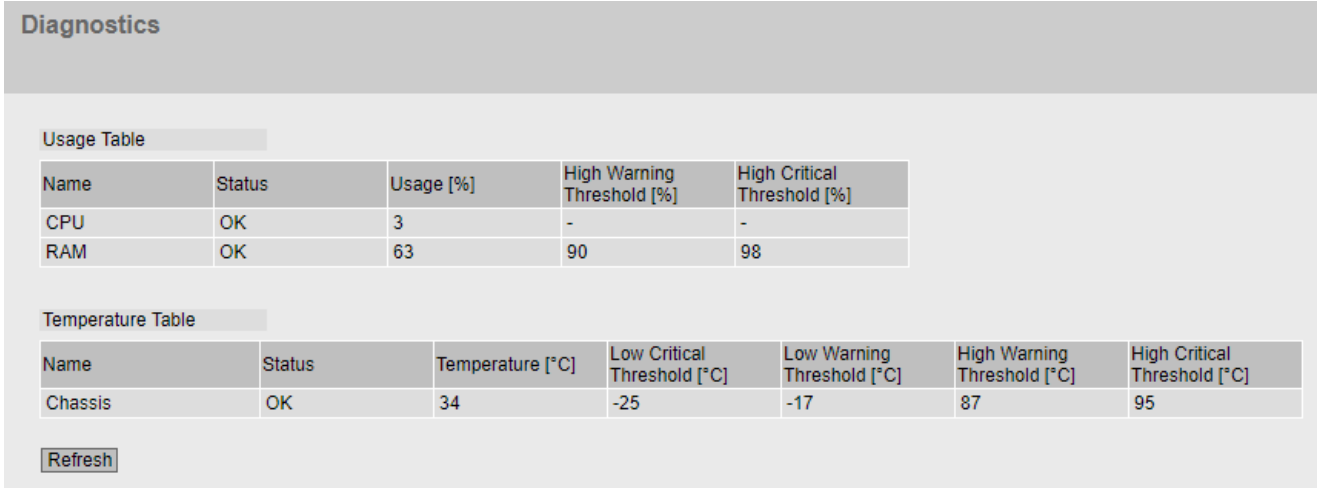
- **IP Address**
  Shows the IPv4 address assigned to the DHCP client.
- **Pool ID**
  Shows the number of the IPv4 address band.
- **Identification Method**
  Shows the method according to which the DHCP client is identified.
  - MAC address
    Identification is based on the MAC address.
  - DHCP client ID
    Identification is based on a freely defined DHCP client ID.
  - 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.
- **Identification value**
  Shows the MAC address ot he 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.

6.3.17 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.



Description

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

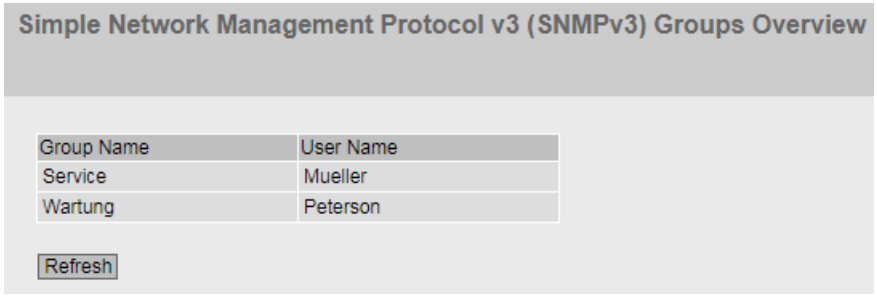
- **Name**
  Shows the name of the module.
- **Status**
  Depending on the relationship between the threshold values and the current usage, the following status values are displayed in ascending priority:
  - **OK**
    The usage is within the preset threshold values.
  - **WARNING**
    The upper threshold 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 needs to 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.
  With plugable 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 lower or upper threshold value of the severity level "Warning" was exceeded. 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 lower or upper threshold value of the severity level "Critical" was exceeded. The device needs to 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. "-" 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 This means that with the same devices with similar ambient temperatures the value can differ.
- **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 this value is exceeded, the status changes to "WARNING". You can configure that you are informed by a message.
- **Upper Threshold [°C] (Critical)**
  If this value is exceeded, the status changes to "CRITICAL". You can configure that you are informed by a message.

6.3.18 SNMP

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



Description

The table has the following columns:

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

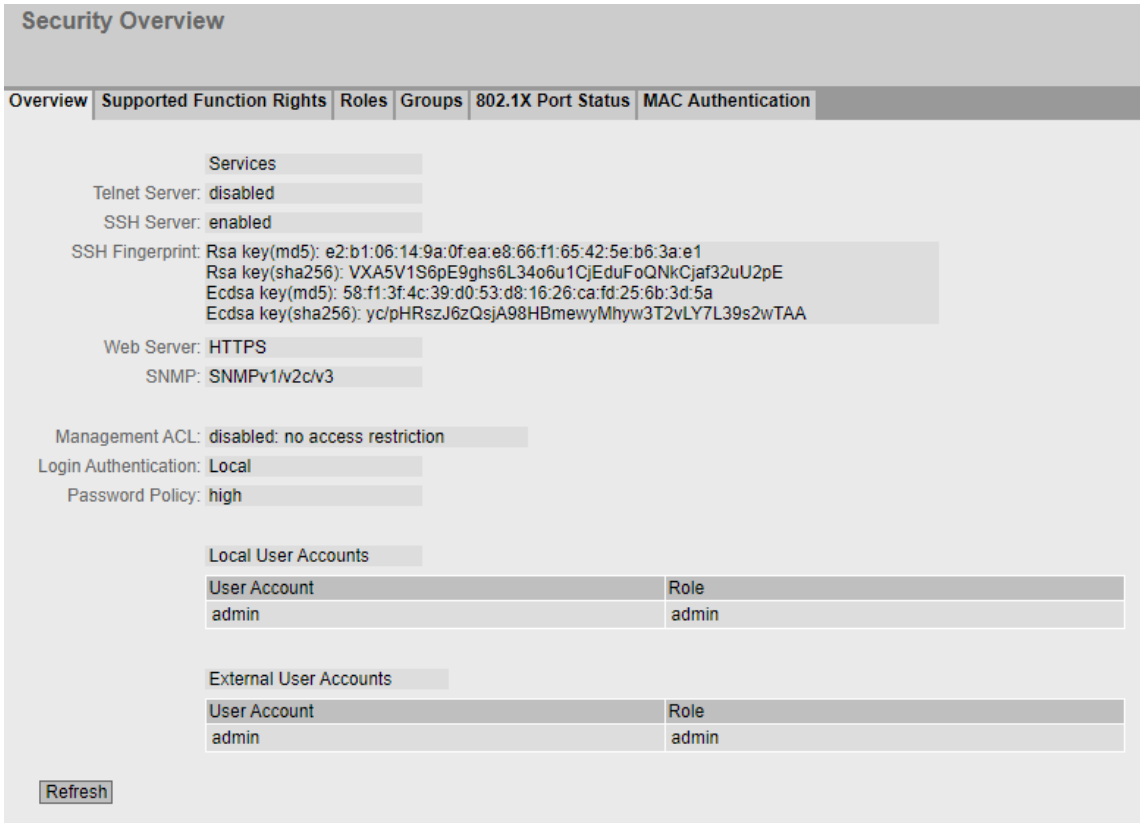
6.3.19 Security

6.3.19.1 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.



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 "admin" is linked to the role "admin". 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

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

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:

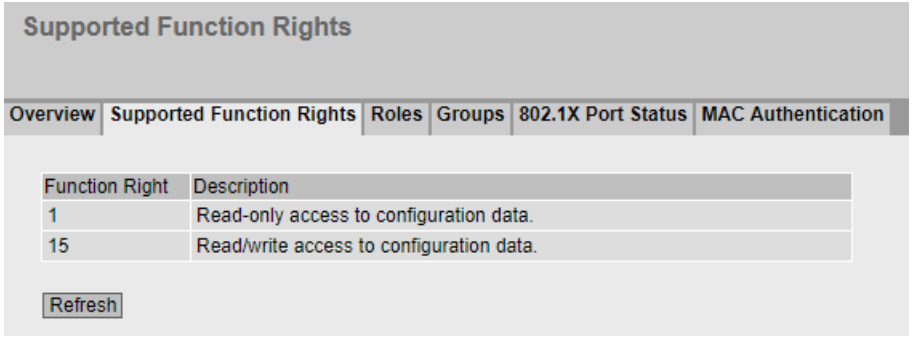
- **User Account**
  Shows the name of the local user.
- **Role**
  Shows the role of the user. You can obtain more information on the function rights of the role in "Information > Security > Roles".

6.3.19.2 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

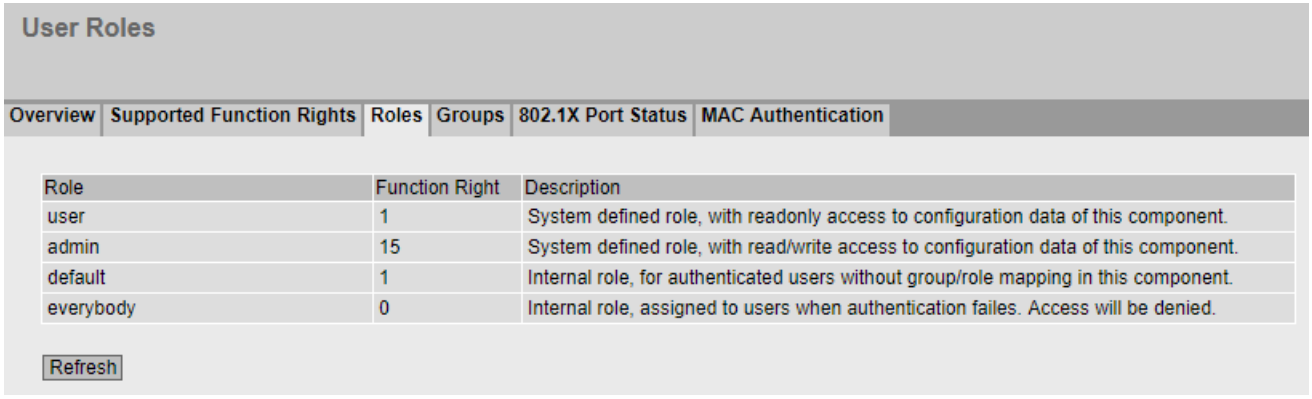
- **Function Right**
  Shows the number of the function right. Different rights relating to the device parameters are assigned to the numbers.
- **Description**
  Shows the description of the function right.

6.3.19.3 Roles

Note

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

The page shows the roles valid locally on the device.



Description

The table contains the following columns:

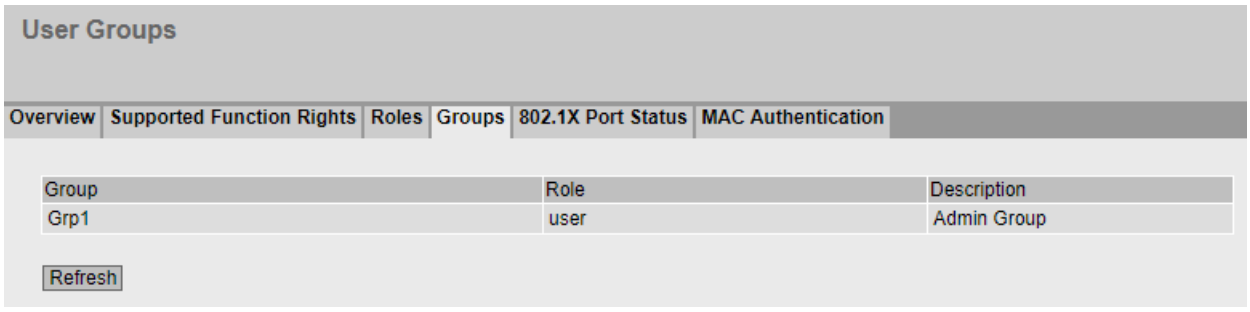
- **Role**
  Shows the name of the role.
- **Function Right**
  Shows the function right of the role:
  - 1
    Users with this role can read device parameters but cannot change them.
  - 15
    Users with this role can both read and change device parameters.
  - 0
    This is a role that the device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

6.3.19.4 Groups

Note

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

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.



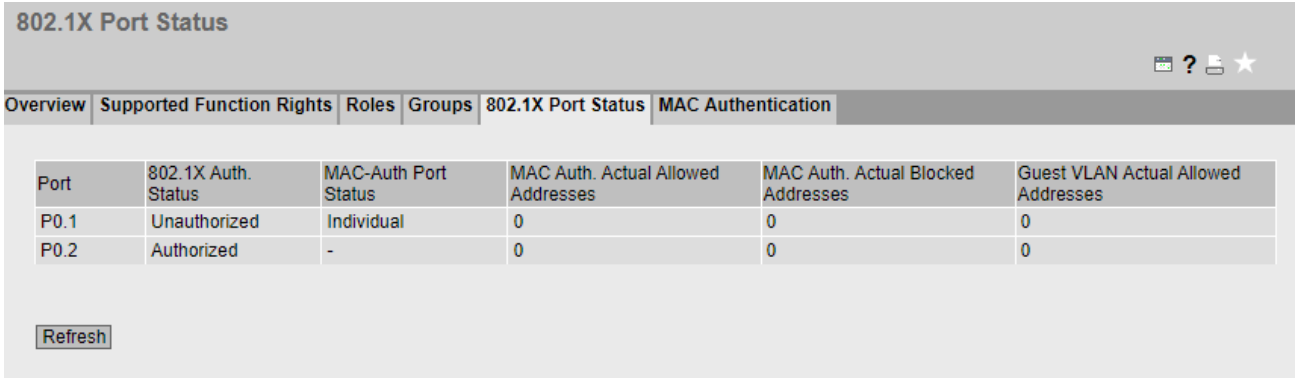
Description of the displayed values

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.

6.3.19.5 802.1X Port Status

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



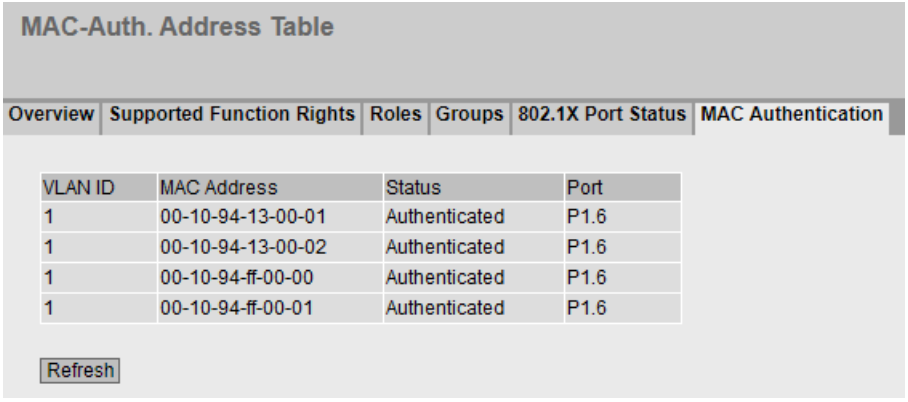
Description

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 ≥ 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.

6.3.19.6 MAC Authentication Address Table

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



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.

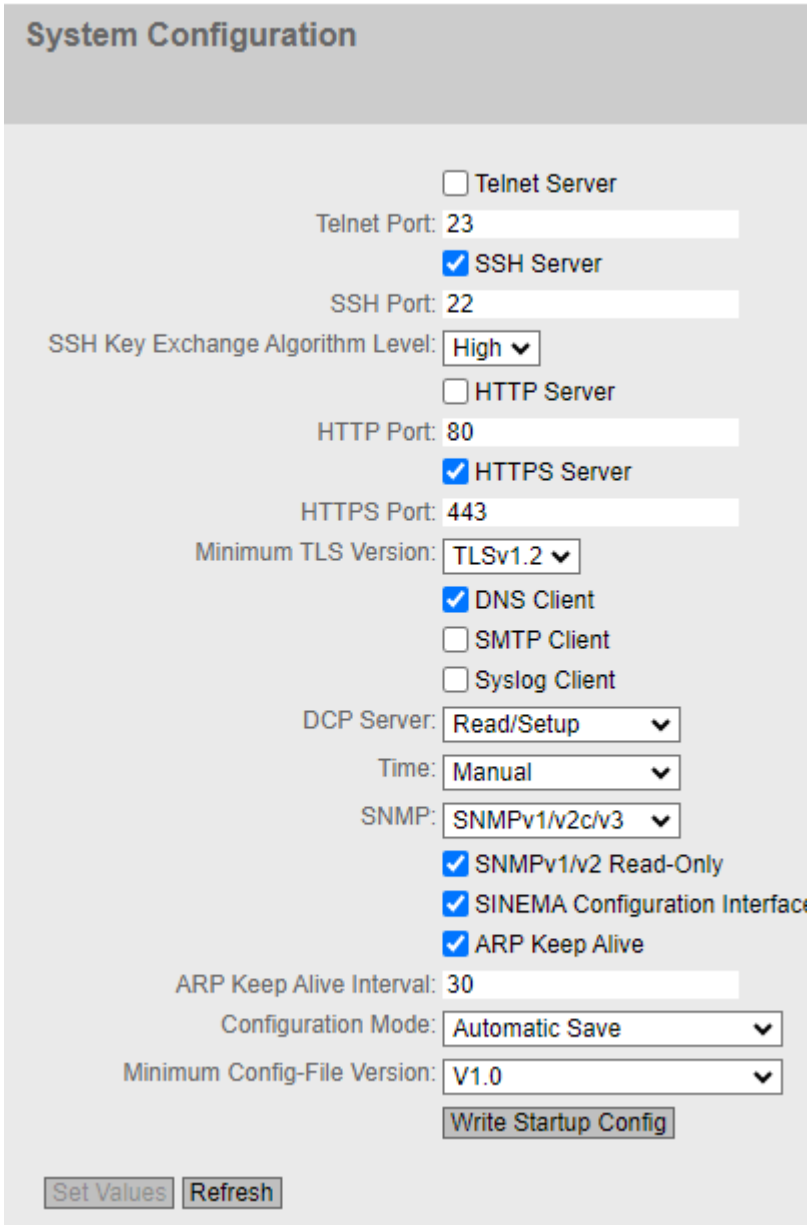
6.4 The "System" menu

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.



Description

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 possible settings 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 you experience problems connecting to SSH clients (TeraTerm, PuTTY, STS) when the level is set to "High", a possible cause is that the SSH clients do not support the exchange algorithms of the "High" setting.

  Make sure that you are using the latest 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 not changed.
  - Read/Setup
    As long as the default password of the administrator 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 via 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 using STEP 7 Basic/Professional.
- **ARP Keep Alive**
  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.
- **ARP Keep Alive Interval**
  Interval in seconds at which the check is performed cyclically. If you enter a value here, the "ARP Keep Alive" check box is selected automatically.
  Range of values: 30 ... 86400 seconds
  Default: 30 seconds

- **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 before you restart the device, the configuration is automatically saved.
    In addition to this, the following message appears in the display area "Changes will be saved automatically in x seconds. Press 'Write Startup Config' to save immediately."

    Note

    Interrupting the save

    Saving starts only after the timer in the message has elapsed. How long saving takes depends on the device.

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

  - 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 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 either the changes made have 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 mode.

- **Minimum Config-File Version**
  Specify the minimum version that a configuration file must have to be loaded into the device. The versions differ in the signature of the file header. Configuration files of Version 2.0 have better protection against tampering.
  The saving of a configuration file is independent of this setting. Configuration files that were saved with a firmware version ≤ V4.3 always equate to V1.0. Configuration files that were saved with a firmware version ≥ V4.4 always equate to V2.0.
  - V1.0
    With this setting, you can load configuration files with V1.0 and V2.0 into the device.
  - V2.0
    With this setting, you can load only configuration files with V2.0 into the device.

Configuration procedure

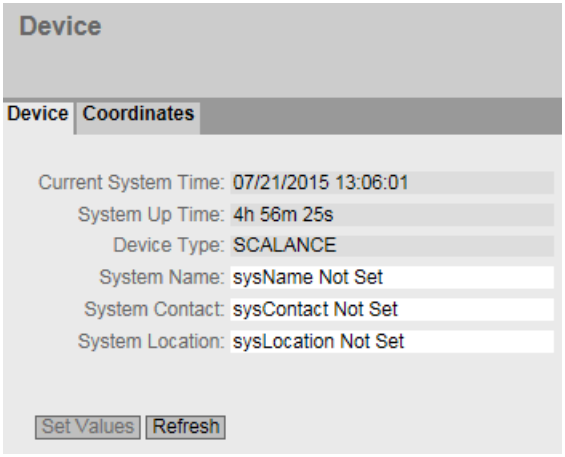
1. To use the required function, select the corresponding check box.
2. Select the options you require from the drop-down lists.
3. Click the "Set Values" button.

6.4.2 General

6.4.2.1 Device

General device information

This page contains the general device information.



The 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

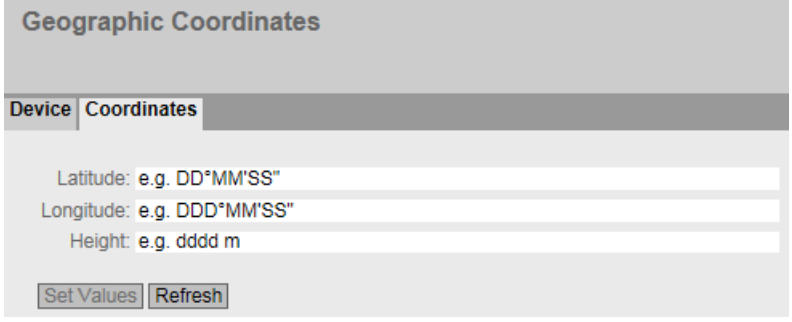
Information on geographic coordinates

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.



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° 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° 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° 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° 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.

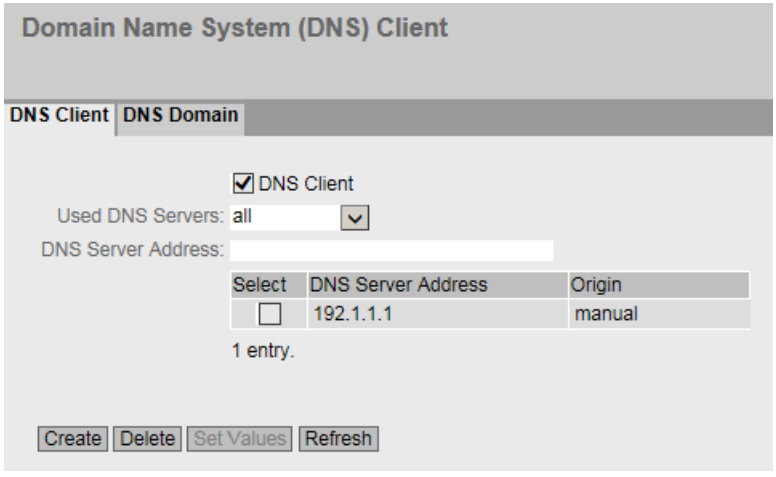
If there is more than one DNS server, the order in the table specifies the order in which the servers are queried. The top server is queried first. A total of seven DNS servers can be configured on the device. Manually configured DNS servers are given preference.

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.

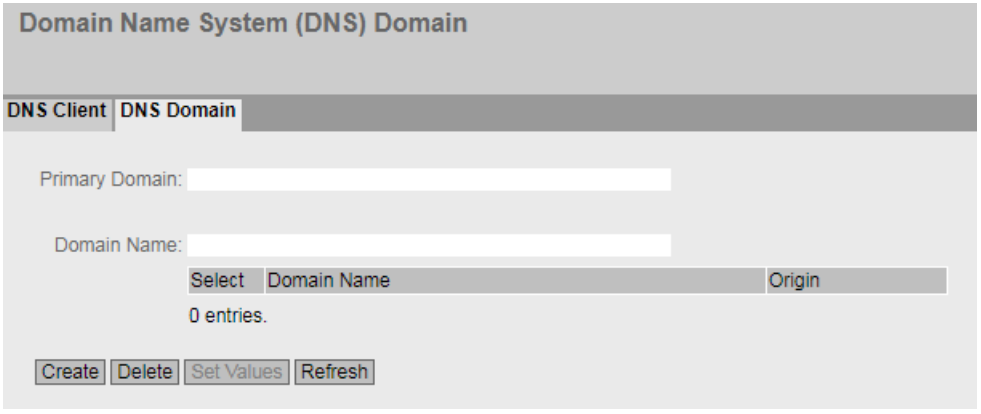
Filtering DNS servers

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.

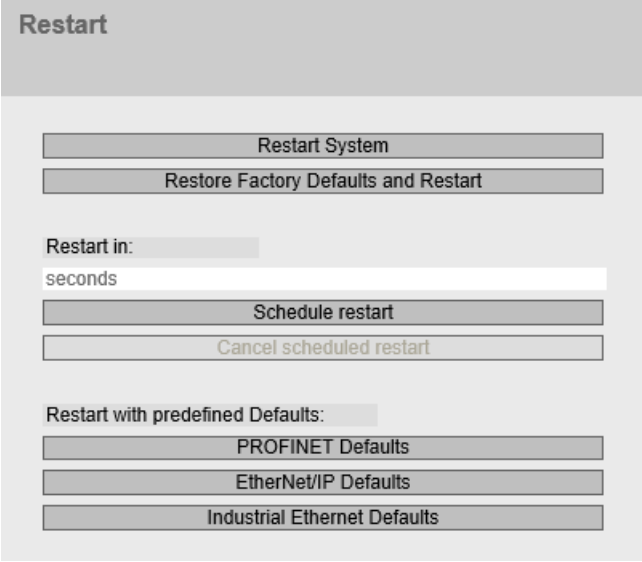
Specify additional domain

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 factory setting or reset the default settings of various profiles.



Restart

Note the following points about restarting a device:

- You can only restart the device with administrator privileges.
- A device should only be restarted with the buttons of this menu or with the appropriate CLI commands and not by a power cycle on the device.
- If the device is in "Trial" mode, configuration modifications must be saved manually before a restart. Any modifications you have made only become active on the device after clicking the "Set values" button on the relevant WBM page and are only active until the next restart of the device. To save all changes, click "Write Startup Config" on the "System > Configuration" page.
- If the device is in "Automatic Save" mode, the last changes are saved automatically before a restart.

Restore Factory Defaults

By resetting all the settings to the factory settings, 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 were set specially for a profile are displayed before the restart.

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

Description

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 System**
  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, for example, 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 settings depend on the device.
- **Restart in:**
  Specify here the time in seconds 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.
- **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 timer is not automatically updated.
- **Cancel scheduled restart**
  With this button, you disable the timer for the scheduled restart.

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 file types contains the following areas.

Area	File type	Description	Upload	Save	Delete[1)]
Update	Firmware	The firmware is signed and encrypted. This ensures that only firmware created by Siemens can be downloaded to the device. An installed firmware version can be updated to a previous version in this way. After the downgrade process is complete, the device is reset to factory settings following a restart.	X	X	--

Area	File type	Description	Upload	Save	Delete[1)]
Configuration	Config	This file contains the start configuration. Among other things, this file contains the definitions of the users, roles, groups and function rights. The passwords are stored in the "Users" file.	X	X	--
	ConfigPack	Detailed configuration information, for example, startup configuration, users, certificates, favorites, firmware of the device (if saved as well).	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 accordingly. 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	--
	WBMFav	WBM favorites This file contains the favorites that you created in the WBM. You can download this file and upload it to other devices.	X	X	X

Area	File type	Description	Upload	Save	Delete[1)]
Certificate & Key	HTTPSCert	Default HTTPS certificates including key The preset and automatically created HTTPS certificates are self-signed. 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. The following file types can be loaded into the device. • .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)". **It is recommended that you use password-protected certificates in the PKCS#12 format.** The following certificates are supported: • ECDSA certificates created with secp521r1 (NIST P-521) • RSA certificates with a maximum key length of 2048 bits • ECC certificates with a key length of 256 bits	X	X	X
	SSHPrivate-KeyECDSA	SSH private key (ECDSA) The SSH key ecdsa-sha2-nistp521 is supported. 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)".	X	X	X
	SSHPrivateKeyR-SA	SSH private key (RSA) with and without password The following SSH keys are supported: • rsa-sha2-512 • rsa-sha2-256 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)".	X	X	X

Area	File type	Description	Upload	Save	Delete[1)]
Service & 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) Electronic data sheet for describing devices in the EtherNet/IP mode	--	X	--
	GSDML	PROFINET information on the device properties	--	X	--
	MIB	Private MSPS MIB file "Scalance_m_msps.mib"	--	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 device. 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, it has the status "Not Accepted" because 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

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

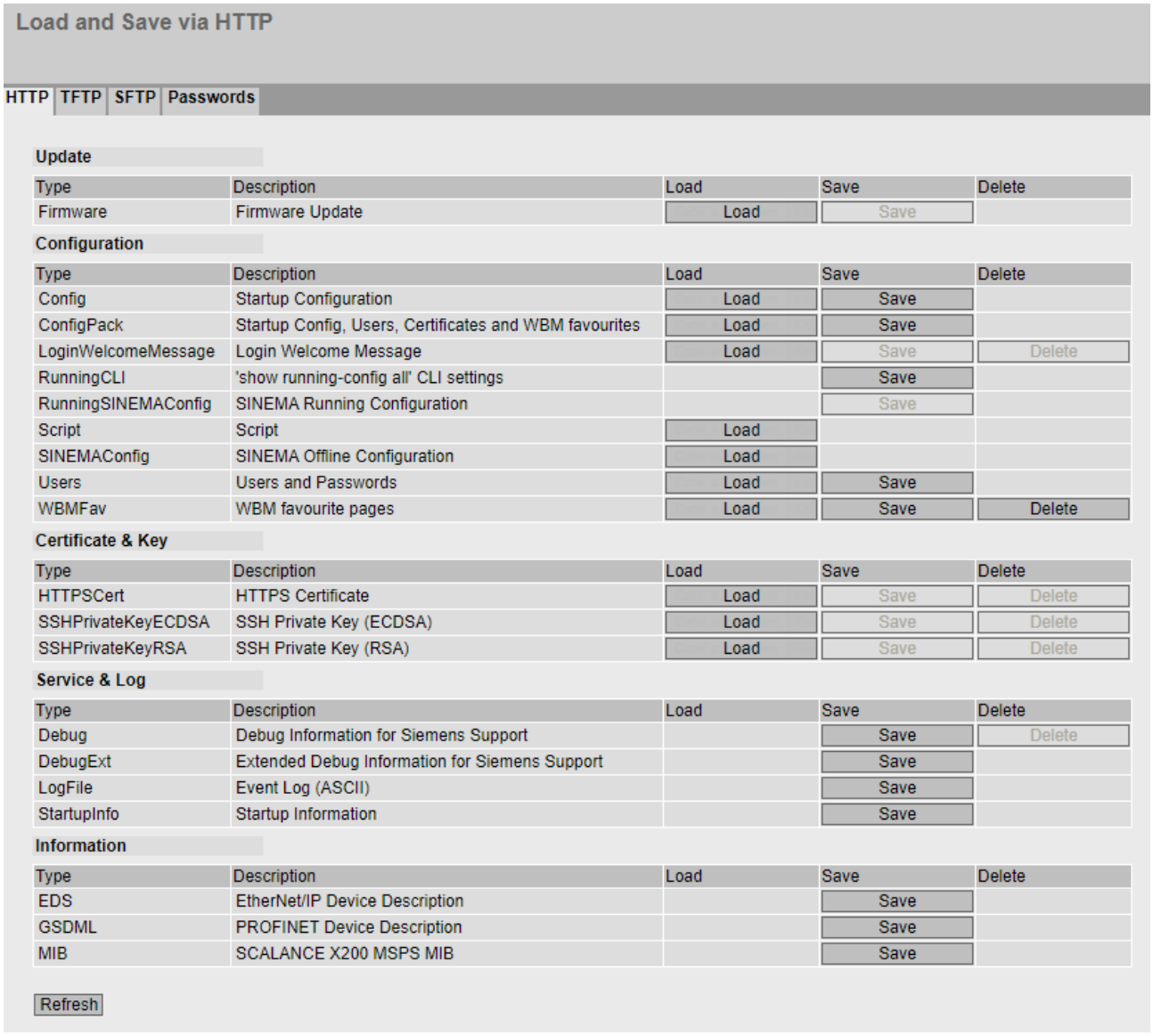
You use the two file types "RunningSINEMAConfig" and "SINEMAConfig" to exchange configuration data between a device (WBM) and STEP 7 Basic/Professional via a file.

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	
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	
WBMFav	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 X200 MSPS MIB		Save	

Refresh

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 for 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 for 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 for 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 is output. Click the "OK" button and run the restart. 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 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 data using HTTP

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

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.

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 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, it has the status "Not Accepted" because 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

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

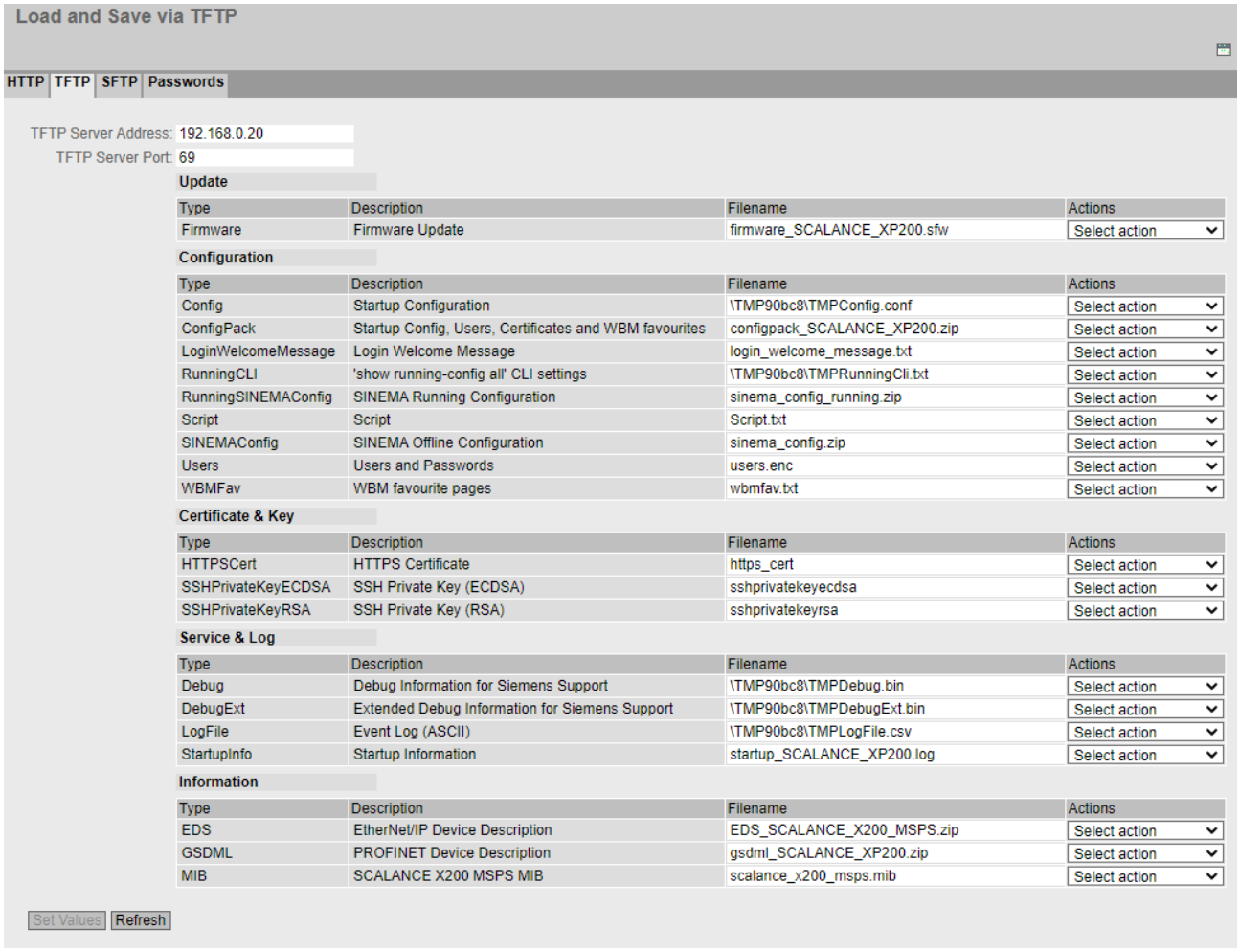
You use the two file types "RunningSINEMAConfig" and "SINEMAConfig" to exchange configuration data between a device (WBM) and STEP 7 Basic/Professional via a file.

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.



Description

The page contains the following boxes:

- **TFTP Server Address**
  Enter the IP address or the FQDN (Fully Qualified Domain Name) of the TFTP server with which you exchange data.
- **TFTP Server Port**
  Enter the port of the TFTP server via 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 of the TFTP server in the "TFTP Server Address" input box.
2. Enter the port of the TFTP server to be used in the "TFTP Server Port" input box.
3. If applicable, enter the name of a file in which you want to save or from which you want to take the data 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 action.
6. If a restart is necessary, a message to this effect is output. Click the "OK" button and 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.

1. Click "Load".
2. In the dialog window, select the file with the previous version of the currently loaded firmware.
3. Confirm the device restart at the end of the load process.
   The device is reset to the factory settings of the version to be loaded and then restarts.

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

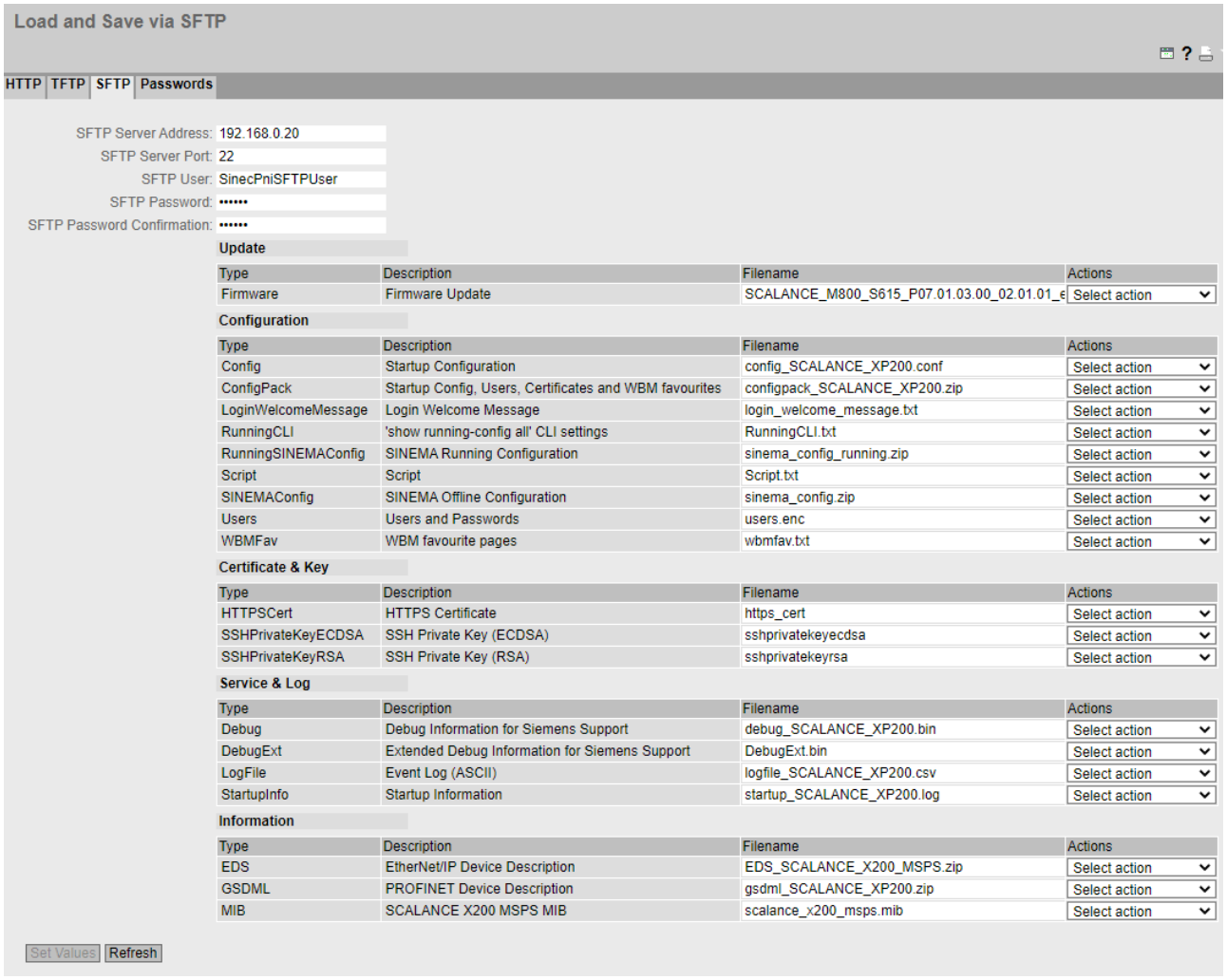
You use the two file types "RunningSINEMAConfig" and "SINEMAConfig" to exchange configuration data between a device (WBM) and STEP 7 Basic/Professional via a file.

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: 192.168.0.20
SFTP Server Port: 22
SFTP User: SinecPniSFTPUser
SFTP Password: ••••••
SFTP Password Confirmation: ••••••

Update

Type	Description	Filename	Actions
Firmware	Firmware Update	SCALANCE_M800_S615_P07.01.03.00_02.01.01_e	Select action

Configuration

Type	Description	Filename	Actions
Config	Startup Configuration	config_SCALANCE_XP200.conf	Select action
ConfigPack	Startup Config, Users, Certificates and WBM favourites	configpack_SCALANCE_XP200.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
WBMFav	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_XP200.bin	Select action
DebugExt	Extended Debug Information for Siemens Support	DebugExt.bin	Select action
LogFile	Event Log (ASCII)	logfile_SCALANCE_XP200.csv	Select action
StartupInfo	Startup Information	startup_SCALANCE_XP200.log	Select action

Information

Type	Description	Filename	Actions
EDS	EtherNet/IP Device Description	EDS_SCALANCE_X200_MSPS.zip	Select action
GSDML	PROFINET Device Description	gsdml_SCALANCE_XP200.zip	Select action
MIB	SCALANCE X200 MSPS MIB	scalance_x200_msps.mib	Select action

Set Values | Refresh

Description

The page contains the following boxes:

- **SFTP Server Address**
  Enter the IP address or the FQDN (Fully Qualified Domain Name) 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 is output. Click the "OK" button and 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

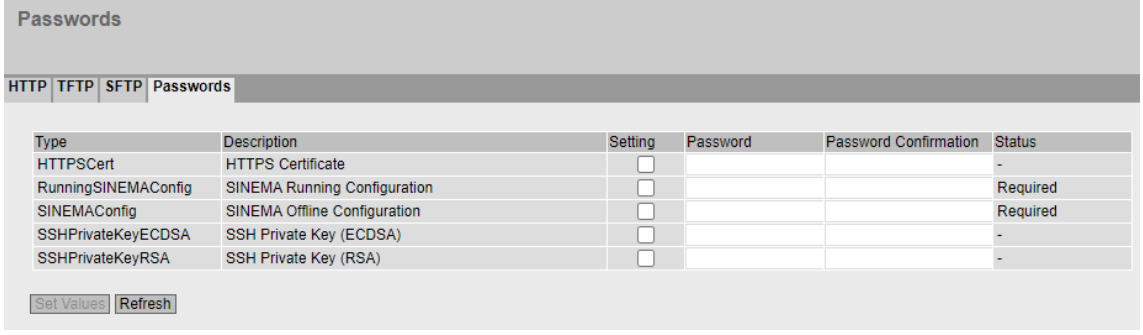
Configuration data has a checksum. If you change the data, you can no longer upload it to the IE switch.

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.

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.



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

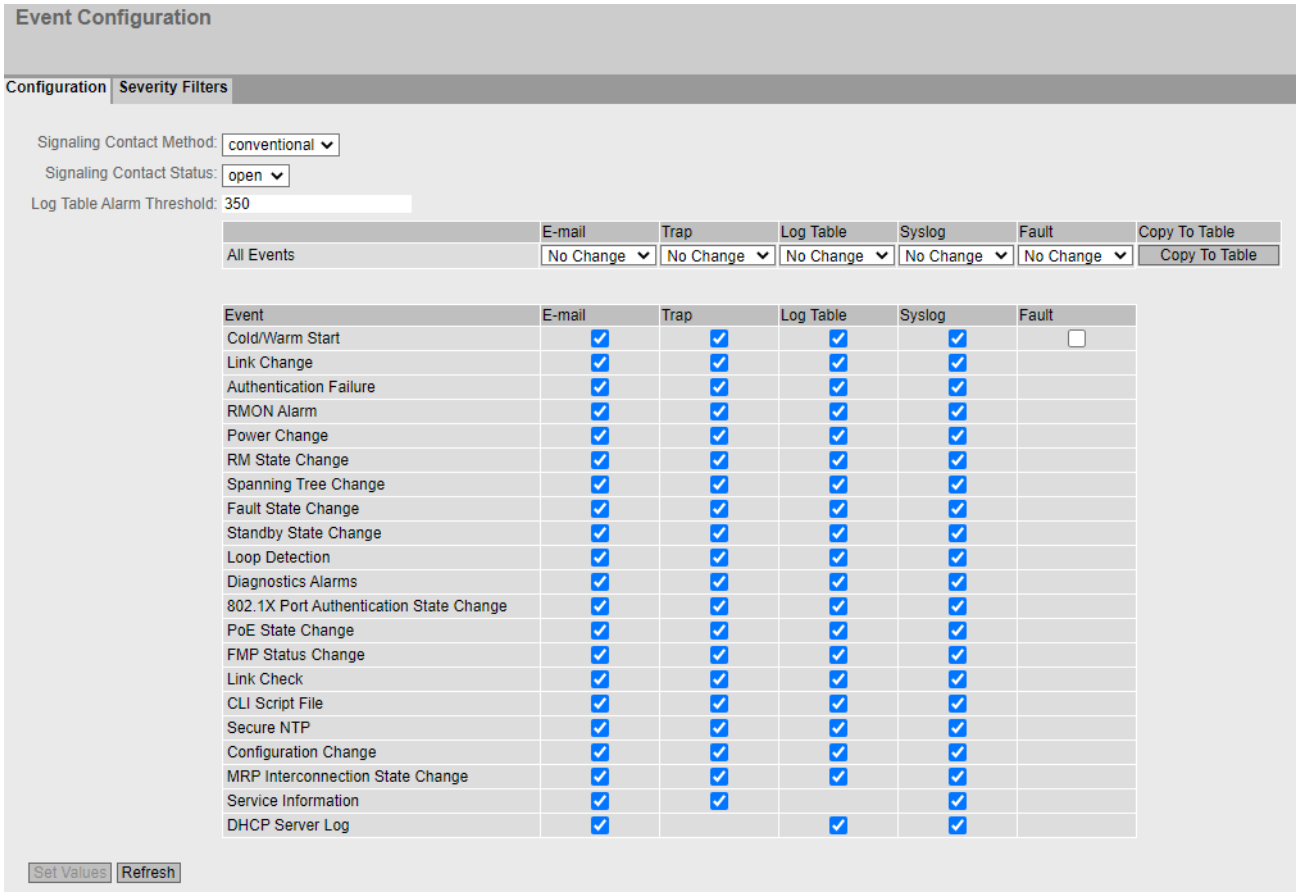
1. Enter the password in "Password".
2. To confirm the password, enter the password again in "Password Confirmation".
3. Enable the "Setting" option.
4. Click the "Set Values" button.

6.4.7 Events

6.4.7.1 Configuration

Selecting system events

On this page, you specify how a device reacts to system events. To enable or disable the options, click the relevant check boxes of the columns.



Description of the displayed boxes

The page contains the following boxes:

- **Signaling Contact Method**
  Select the behavior of the signaling contract from the drop-down list. The following reactions are possible:
  - Standard
    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**
  To change the status of the signaling contact, select the "User defined" method from the "Signaling Contact Method" drop-down list.
  Select the status of the signaling contact from the drop-down list. The following statuses are possible:
  - closed
    Signaling contact is closed.
  - open
    Signaling contact is open.
- **Log Table Alarm Threshold**
  Specify the number of entries at which a log message is generated.
  If the specified limit will be reached with the next entry, an alarm message is output, e.g. if 300 is specified, the message that limit 300 has been reached is output after entry 299.

With Table 1, you can select or clear all check boxes of a column of Table 2 at once. Table 1 has the following columns:

- **All Events**
  Shows that the settings are valid for all events of table 2.
- **E-mail / Trap / Log Table / Syslog / Fault**
  Enable or disable the required type of notification for all events. If "No Change" is selected, the entries of the corresponding column in table 2 remain unchanged.
- **Copy to Table**
  If you click the button, the setting is adopted for all events of table 2.

Table 2 has the following columns:

- **Event**
  The column contains the following values:
  - Cold/Warm Start
    The device has been turned on or restarted by the user. In the error memory of the device, a new entry is generated with the type of restart performed.
  - Link Change
    This event occurs only when the port status is being monitored and has changed, see "System > Fault Monitoring > Link Change".
  - Authentication Failure
    This event occurs when access with an incorrect password is attempted.
  - RMON Alarm
    An alarm or event has occurred in connection with the remote monitoring of the system.
  - Power Change
    This event occurs only when power supply lines 1 and 2 are monitored. If the monitored cable has no voltage, an error is displayed. The event also occurs when the PoE power supply has failed. You can find additional information in the section "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 Spanning Tree topology has changed.
  - Fault State Change
    The fault state has changed. The fault state 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).
  - Loop Detection
    A loop was detected in the network segment.
  - Diagnostics Alarms
    A diagnostics value has fallen below or exceeded a certain limit.
  - 802.1X Port Authentication State Change
    This event occurs with 802.1X authentications.
  - PoE State Change
    The status of PoE has changed.

    Note

    You can only configure this event in devices that support PoE.

  - FMP Status Change
    The value of the received power or the power loss has exceeded or fallen below a certain limit.

    Note

    You can only configure this event in devices that support FMP.

  - Link Check
    A disruption was detected on an optical transmission link.

    Note

    You can only configure this event in devices with optical interfaces.

  - CLI Script File
    An error was detected in the CLI script file.
  - 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, e.g. messages about the time of time synchronization, password change or general configuration change, 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.
- **Fault**
  The device triggers a fault. The error LED lights up

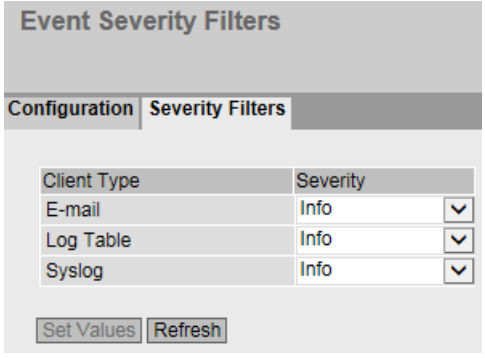
Configuration procedure

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
   - Fault
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.



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:

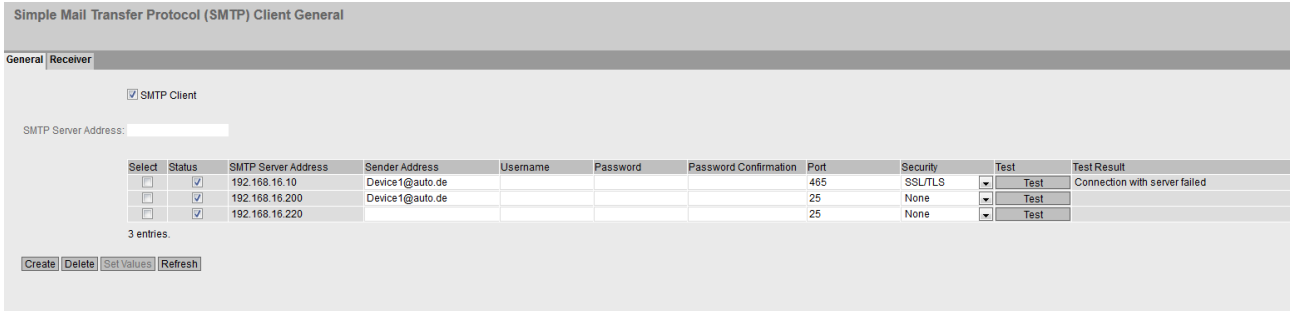
1. Select the required values from the drop-down lists of the second table column after the client types.
2. Click the "Set Values" button.

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.



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

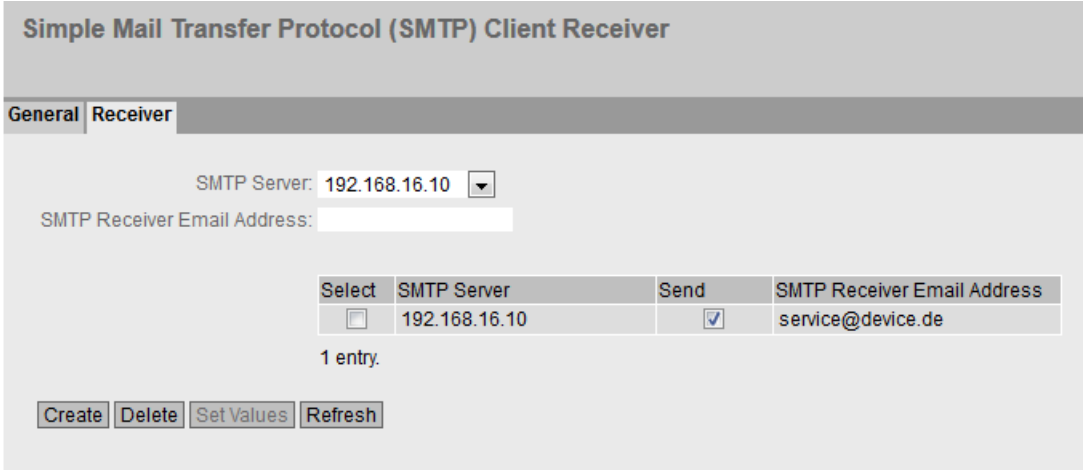
Depending on the properties and configuration of the SMTP server, it may be necessary to adapt the "Sender E-Mail Address" input for the e-mails. Check with the administrator of the SMTP server.

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.



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.

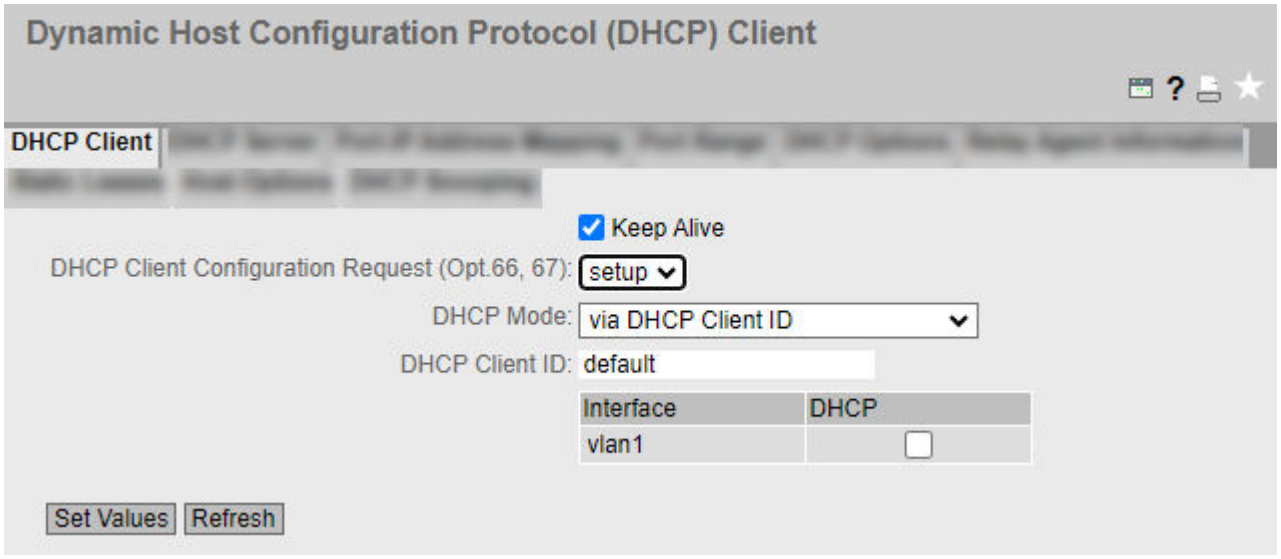
6.4.9 DHCP

6.4.9.1 DHCP Client

Setting the DHCP mode

If the device is configured as a DHCP client, it starts a DHCP request. As reply to the request, 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.

Description



The page contains the following boxes:

- **Keep Alive**
  Keep Alive is enabled 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 when 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 when the lease time expires.
- **DHCP Client Configuration 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
Security risk - risk of unauthorized access and/or misuse The function can potentially be used to change the functionality of the device, thereby causing failure of the 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. To prevent unauthorized access and/or misuse, disable the function if you are not using it (**Off**). In a device with default setting (**Setup**), no further configuration file is loaded from the DHCP server after the first login with the default user profile **admin** and the assignment of a new password, even if the options 66 and 67 are still contained in the DHCP requests of the DHCP client.

  - 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 the same as when **On** is set, 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 the same as when **Off** is set: 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 request.
  - 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 in 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.
- **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.

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)" option, if the DHCP client is 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 in this configuration file.

6.4.9.2 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.

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 bindings

If you deactivate or delete an IPv4 address band or turn the DHCP server off and on again, the DHCP server assignments are deleted see "Information > DHCP Server".

The structure of this page depends on the device. For this reason, devices are divided into two groups:

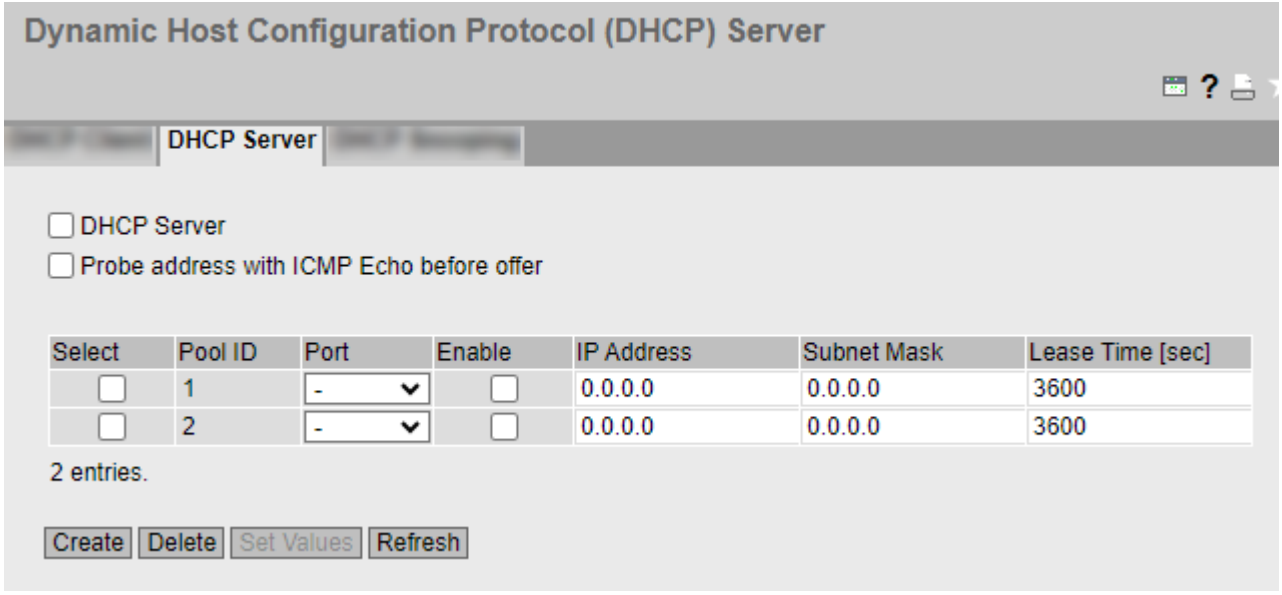
- SCALANCE XB-200, SCALANCE XR-300WG and SCALANCE XF-200BA
- SCALANCE XC-200, SCALANCE XF-200G, SCALANCE XP-200 and SCALANCE XP-200G

Requirement

- The connected devices are configured so that they obtain the IP address from a DHCP server.
- The Base Bridge Mode 802.1Q VLAN Bridge is enabled. For more information, refer to "Layer 2 > VLAN > General (Page 305)".

SCALANCE XB-200, SCALANCE XR-300WG and SCALANCE XF-200BA

On this page, you specify tIPv4 addresses that are assigned via certain ports.



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.

- **Probe address with ICMP Echo before offer**
  When selected, the DHCP server checks whether or not 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 for 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).
- **Port**
  Specify the port via which IPv4 address of this DHCP pool will be assigned.
- **Enable**
  Specify whether or not this IPv4 address will be used.

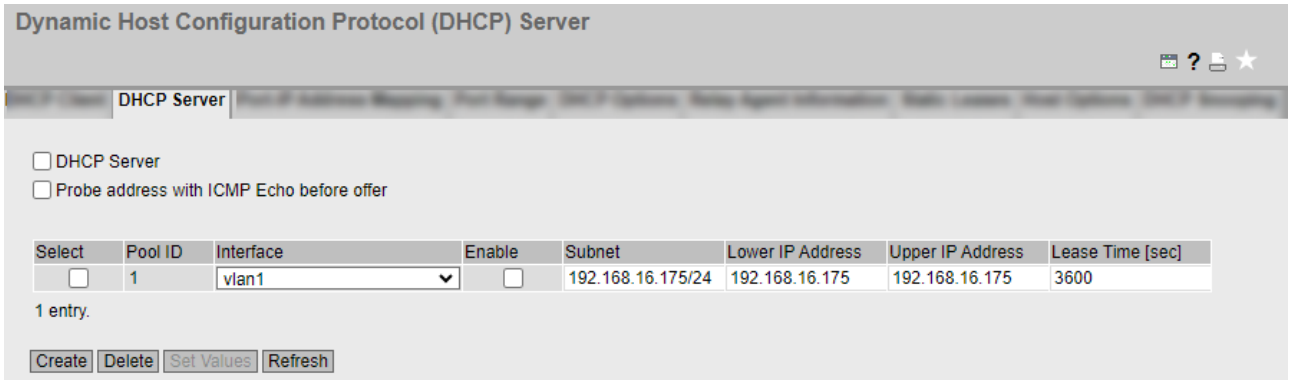
  Note

  If you enable the IPv4 address, its settings in this DHCP tab are grayed out and can no longer be edited.

- **IP Address**
  Enter the IPv4 address that will be assigned via the specified port.
- **Subnet**
  Enter the subnet mask matching the IPv4 address. Use the CIDR notation.
- **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.

SCALANCE XC-200, SCALANCE XF-200G, SCALANCE XP-200 and SCALANCE XP-200G

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".



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.

- **Probe address with ICMP Echo before offer**
  When selected, the DHCP server checks whether or not 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

  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).
- **Interface**
  Select a VLAN IP interface. The IPv4 addresses are assigned dynamically via this interface. The requirement for the assignment is that the IPv4 address of the interface is located in the subnet of the IPv4 address band. If this is not the case, the interface does not assign any IPv4 addresses.

- **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.

  Note

  Effects on other tabs

  When you configure the boxes "Subnet", "Lower IP Address" and "Upper IP Address", the row of the corresponding DHCP pool in the "Port-IP Address Mapping" tab is deleted. if you delete the configuration, the row in the "Port-IP Address Mapping" tab is available again.

- **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.

Configure DHCP server on SCALANCE XB-200, XR-300WG and XF-200BA

1. Click the "Create" button.
   A new row with a unique number (Pool ID) is created.
2. Select the required port.
3. Enter the IPv4 address and the subnet mask.
4. Enter the lease time.
5. Click the "Set Values" button.
6. Select the "Enable" check box on this tab.
7. Click the "Set Values" button.

Configure DHCP server on SCALANCE XC-200, XF-200G, XP-200 and XP200G

1. Click the "Create" button.
   A new row with a unique number (Pool ID) is created.
2. Select a VLAN IP interface.
3. Click the "Set Values" button.
   In the "Port-IP Address Mapping" tab a new row is created for the Pool ID. In the "Port" tab, all ports can be selected that currently belong to the selected VLAN.
   In the "Port Range" tab a new row is created for the Pool ID. 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:
   Configure the 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.

   Configure the DHCP pool for an IPv4 address
   - 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 on the "DHCP Server" tab.
5. Make the settings you require for the pool in the other DHCP tabs.

Enable DHCP pool

1. In the "DHCP Server" tab, select the check box "Enable".
2. Click the "Set Values" button.

Deleting a DHCP pool

Note

You can only delete entries that are not enabled.

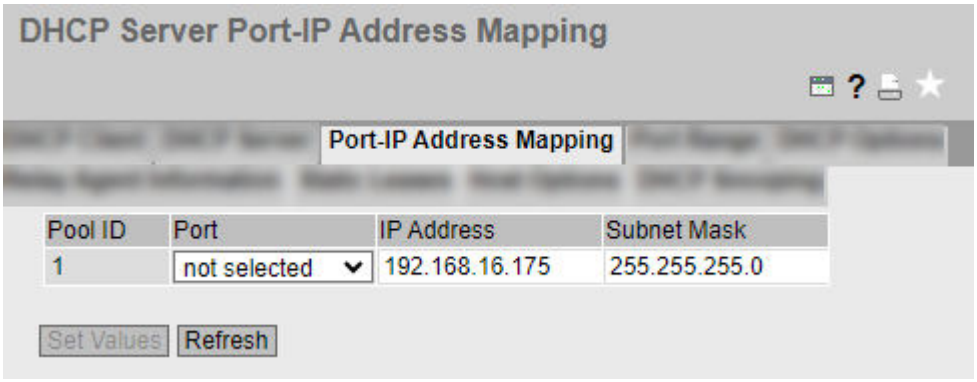
1. Enable the "Select" check box in the row to be deleted.
   Repeat this for all entries you want to delete.
2. Click the "Delete" button.
   The entry is deleted.

6.4.9.3 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".



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.
- **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

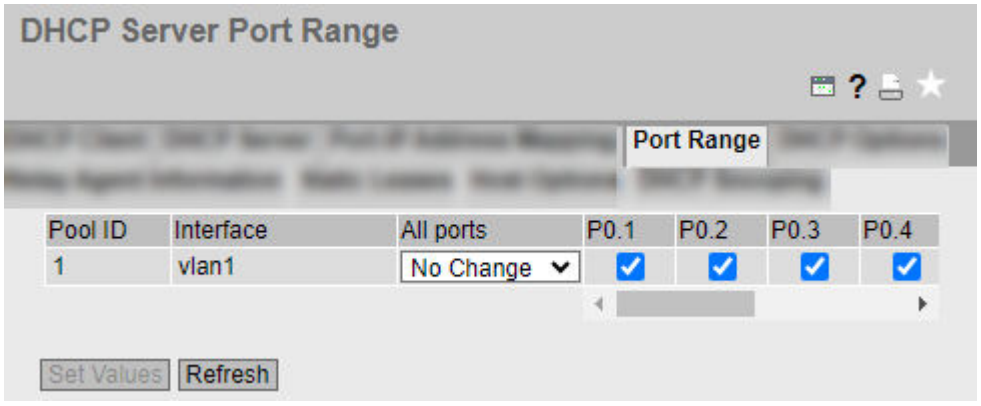
Assign an IP address to the port

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.

6.4.9.4 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.



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.

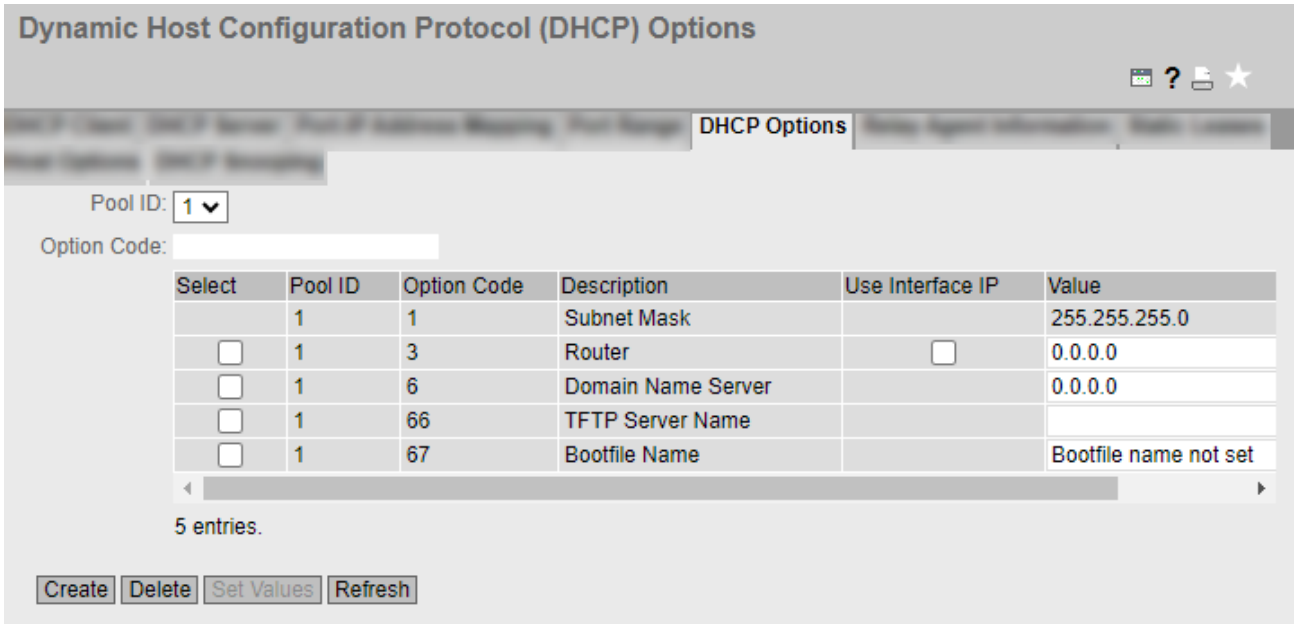
Configuring all ports

1. Select the required entry in the "All ports" drop-down list.
2. Click the "Set Values" button.

6.4.9.5 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 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 66
- Option 67

Procedure

Creating a DHCP option

1. Select a Pool ID.
2. Enter the option code.
3. Click the "Create" button.
4. Enter a value.
5. If applicable, select the "Use Interface IP" check box for option 3.
6. Click the "Set Values" button.

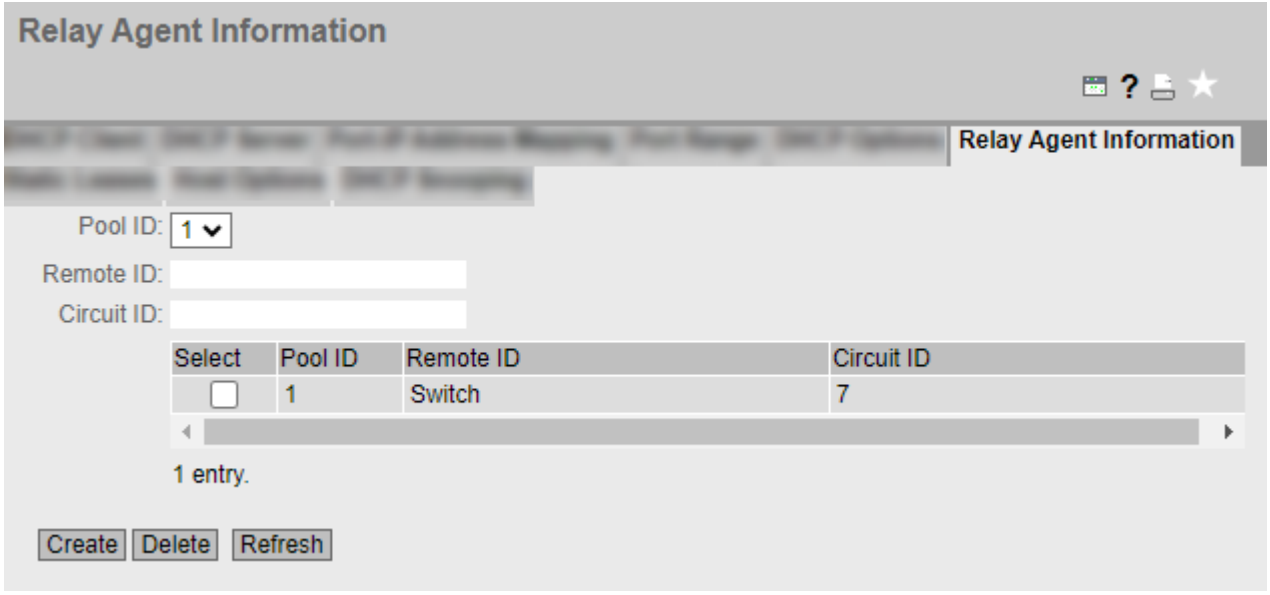
Deleting a DHCP option

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.

6.4.9.6 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

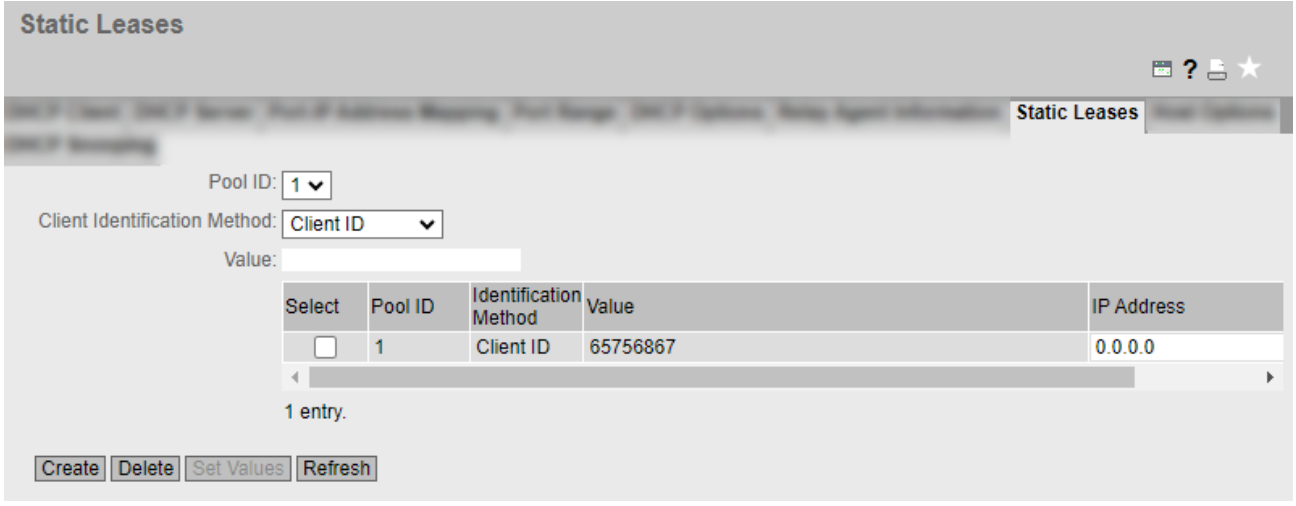
1. Select a Pool ID.
2. Enter the remote ID.
3. Enter the circuit ID.
4. Click the "Create" button.

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.

6.4.9.7 Static Leases

On this page you define that DHCP clients are assigned a preset IPv4 address depending on their client ID or MAC address.



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.
- **Value**
  Enter the MAC address (Ethernet MAC) or the client 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.
- **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

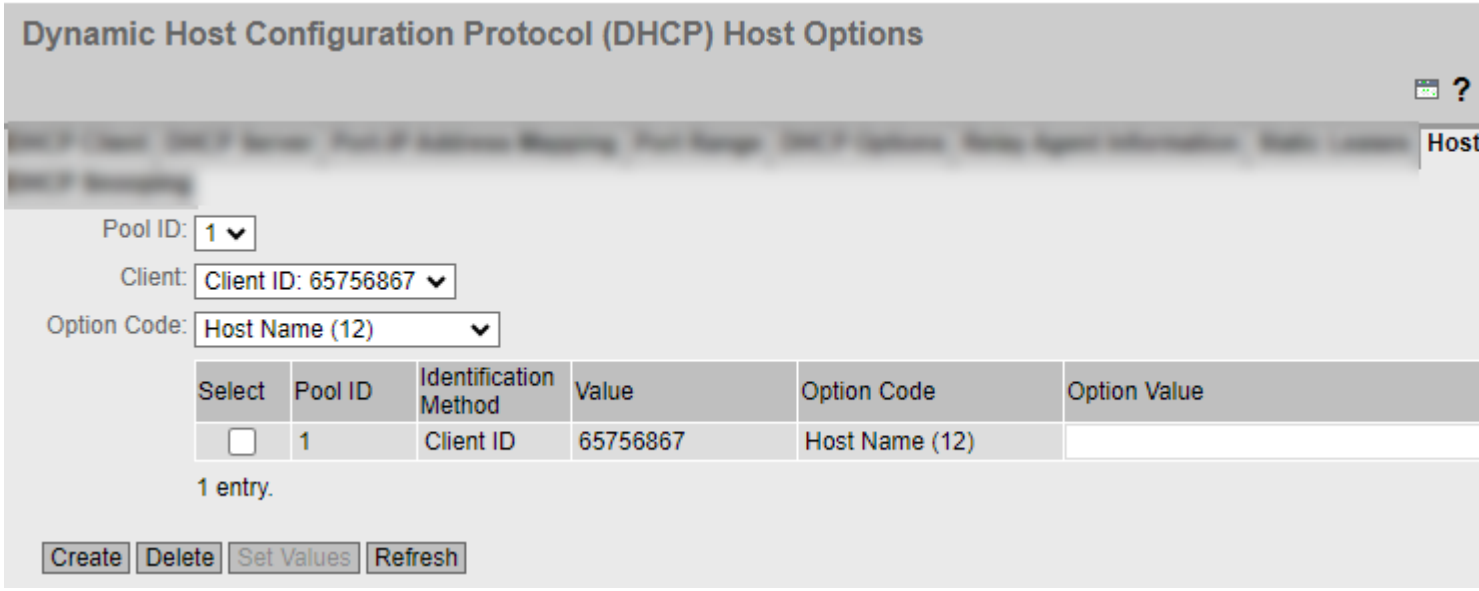
1. Select a Pool ID.
2. Select the Client identification method.
3. Enter the value.
4. Click the "Create" button.
5. Specify the IPv4 address that will be assigned to the client.
6. Click the "Set Values" button.

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.

6.4.9.8 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.



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.

- **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.

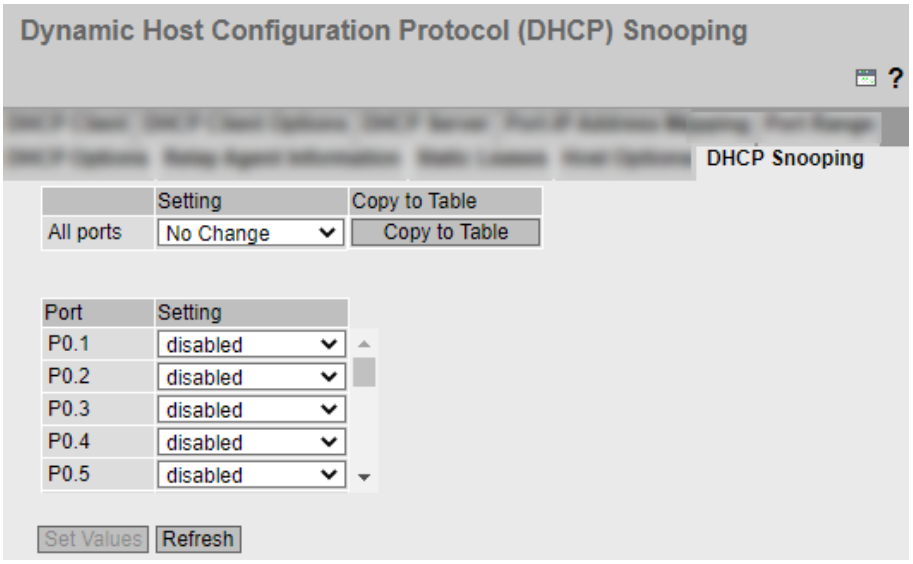
Delete option

1. Select the check box of the row you want to delete.
2. Click the "Delete" button.

6.4.9.9 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.



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.

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 91)".

6.4.10.1 General

Configuration of SNMP

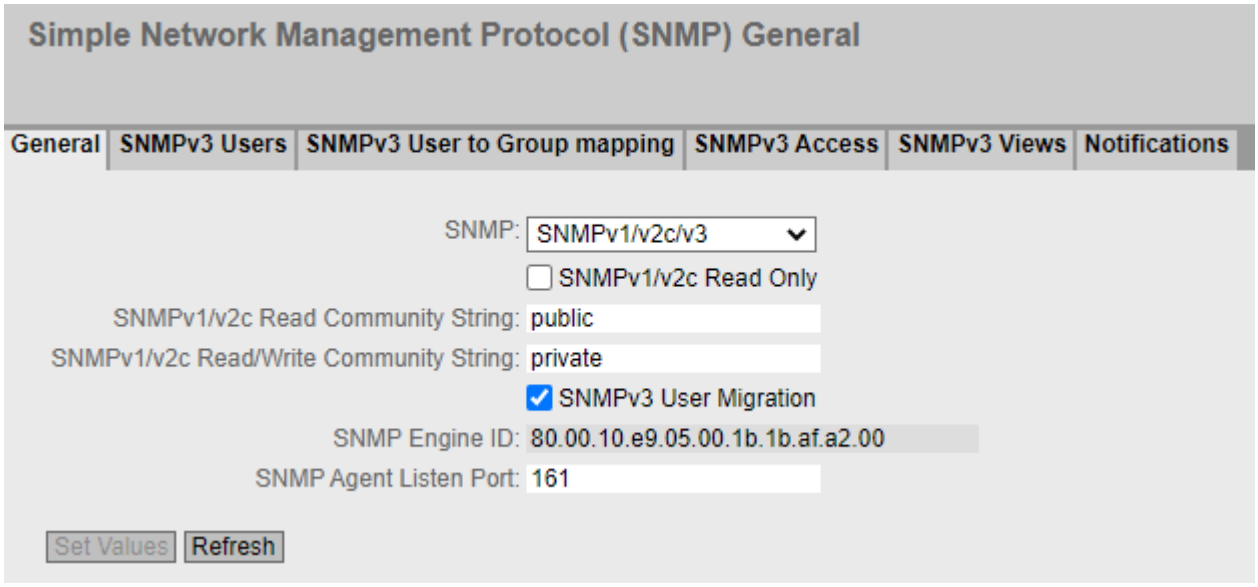
Note

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.



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.

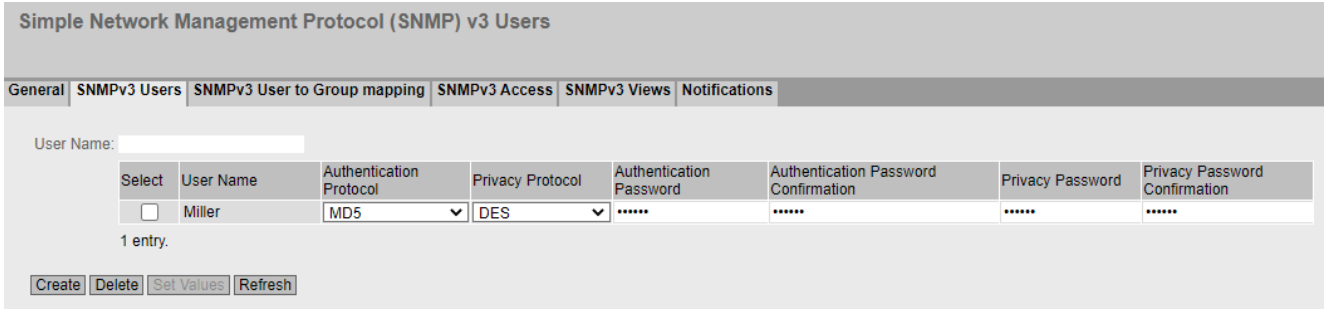
Procedure

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.



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.

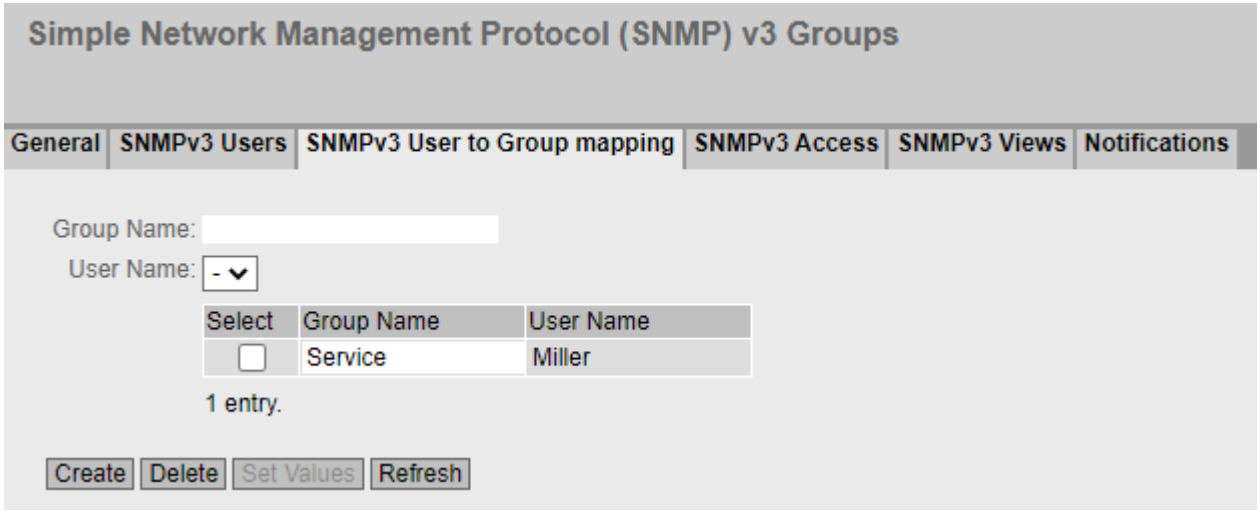
Delete user

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.



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.

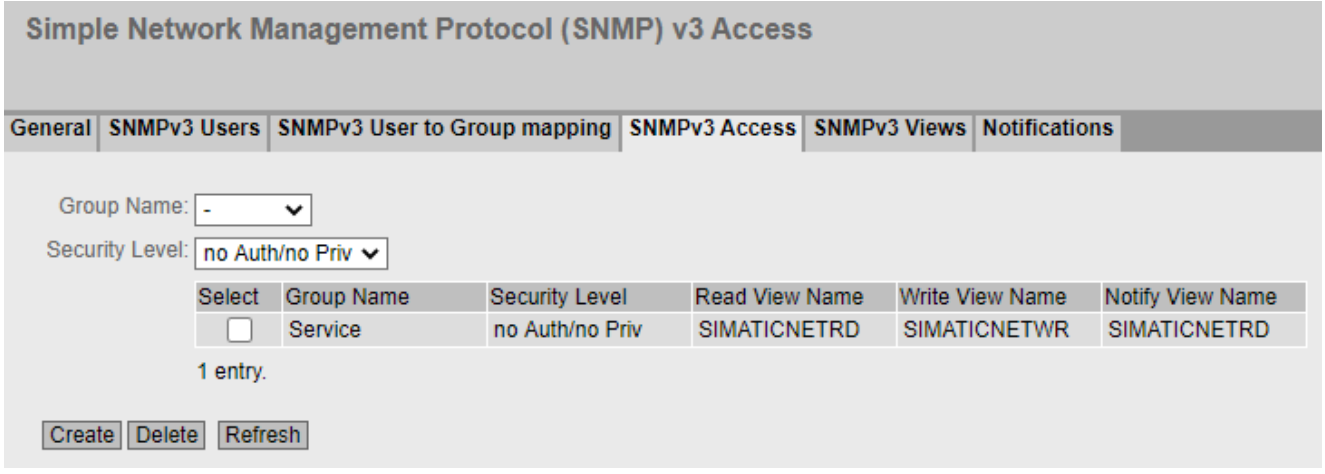
6.4.10.4 SNMPv3 Access

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.



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.

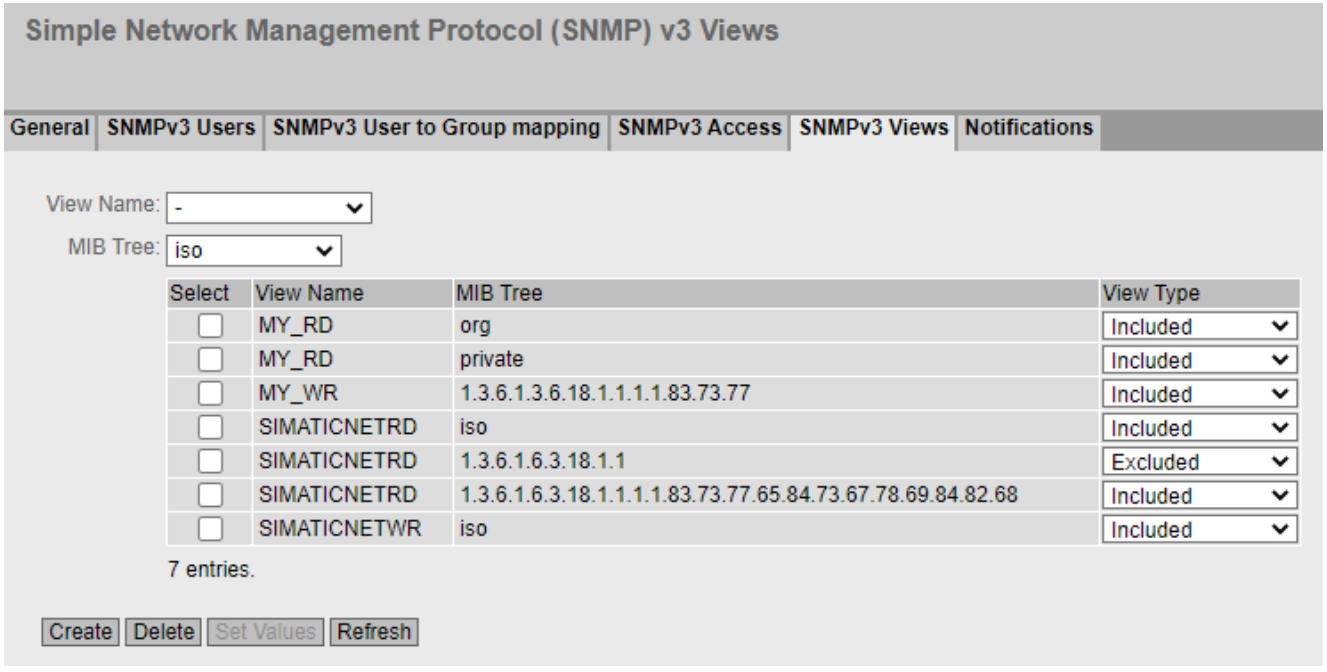
Deleting a group

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.



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.

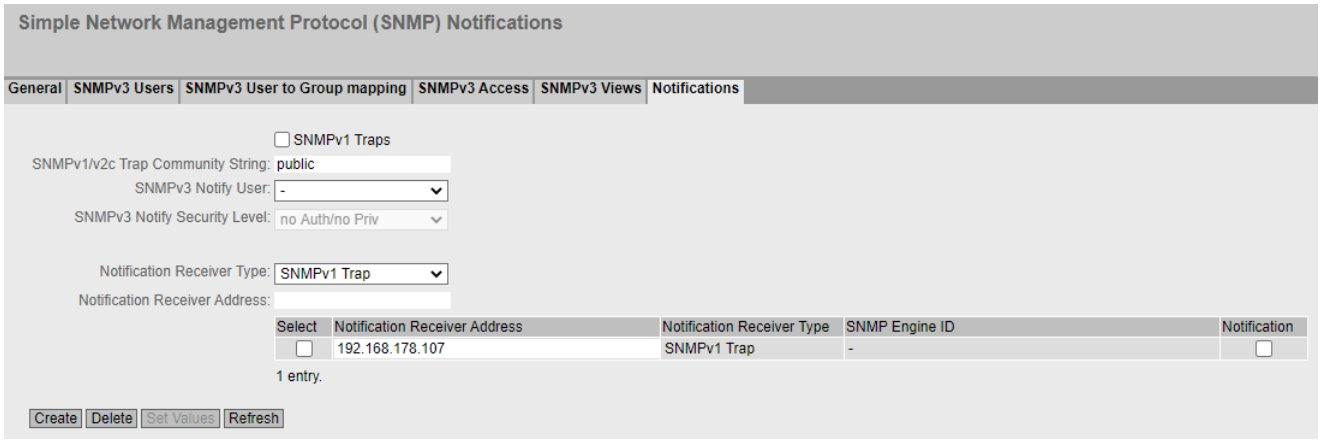
The table has the following columns:

- **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.



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. 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

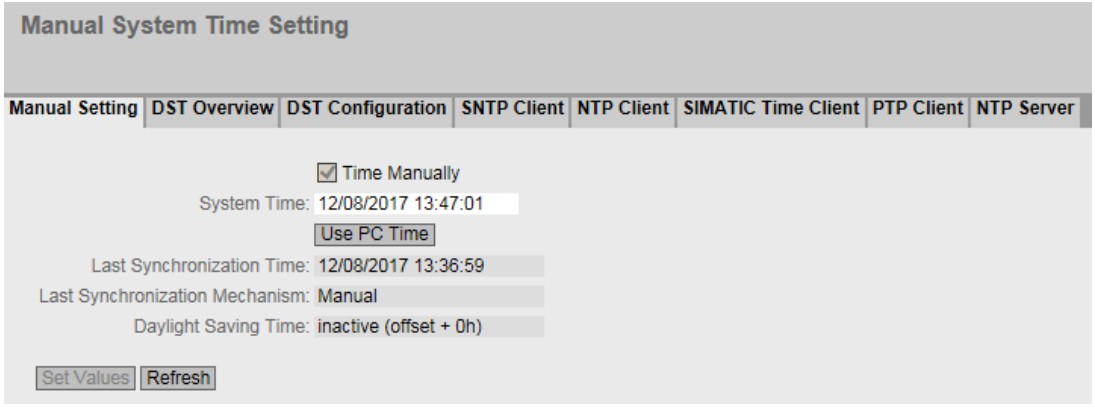
There are different methods that can be used to set the system time of the device. Only one method can be active at any one time.

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.

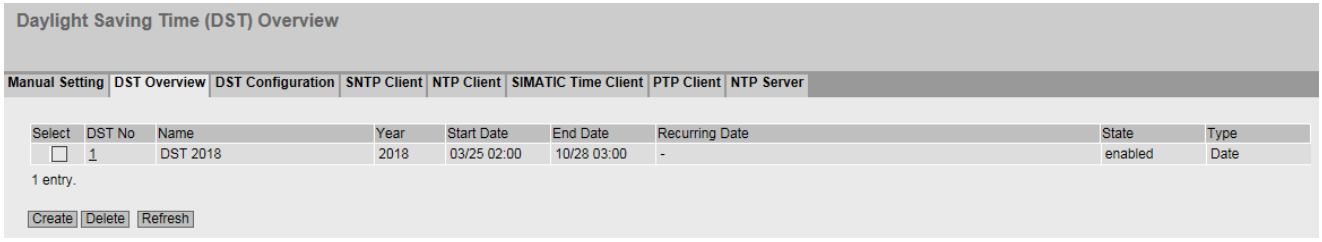
Procedure

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.



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

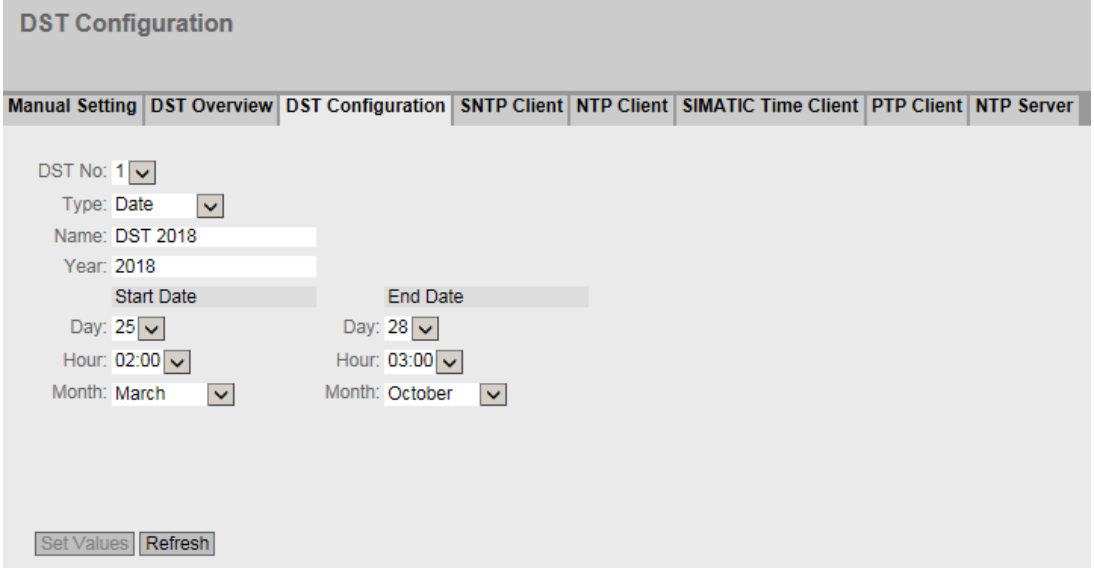
Note

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.

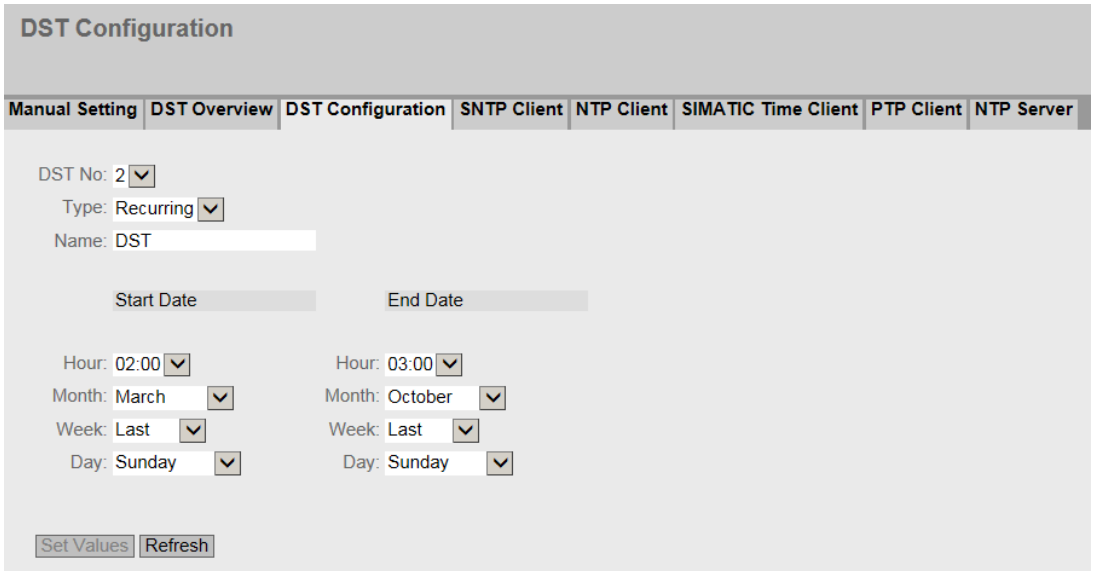
Settings with "Date" selected



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



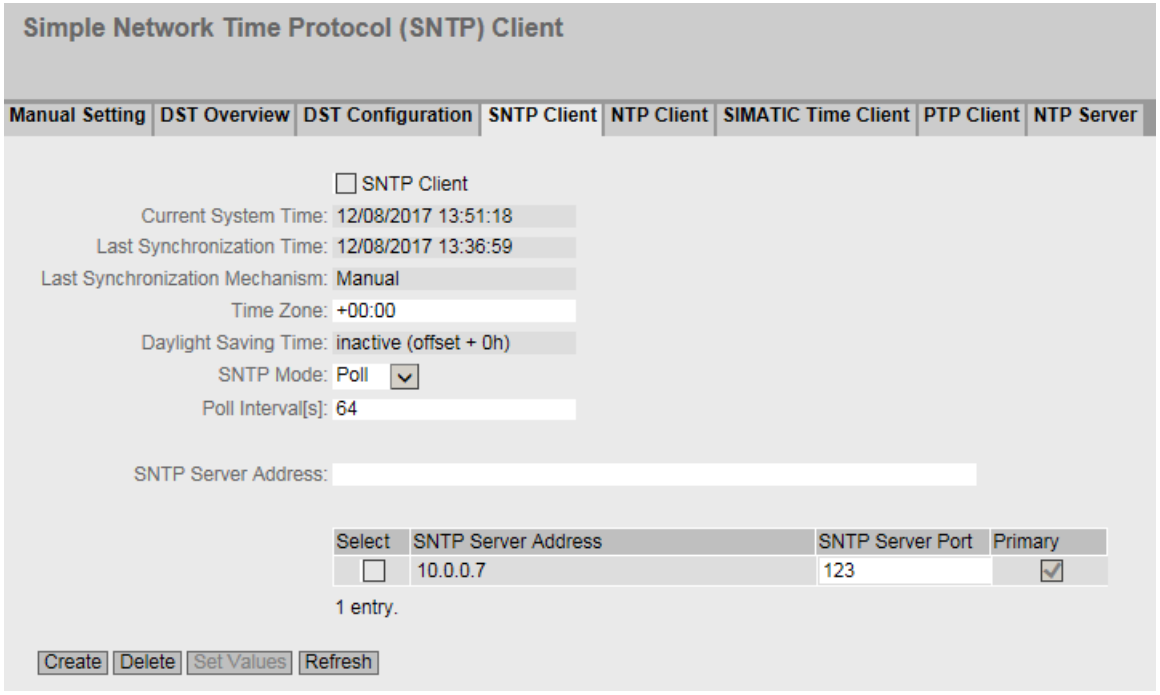
You can create a rule for the daylight saving time changeover.

- **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.



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

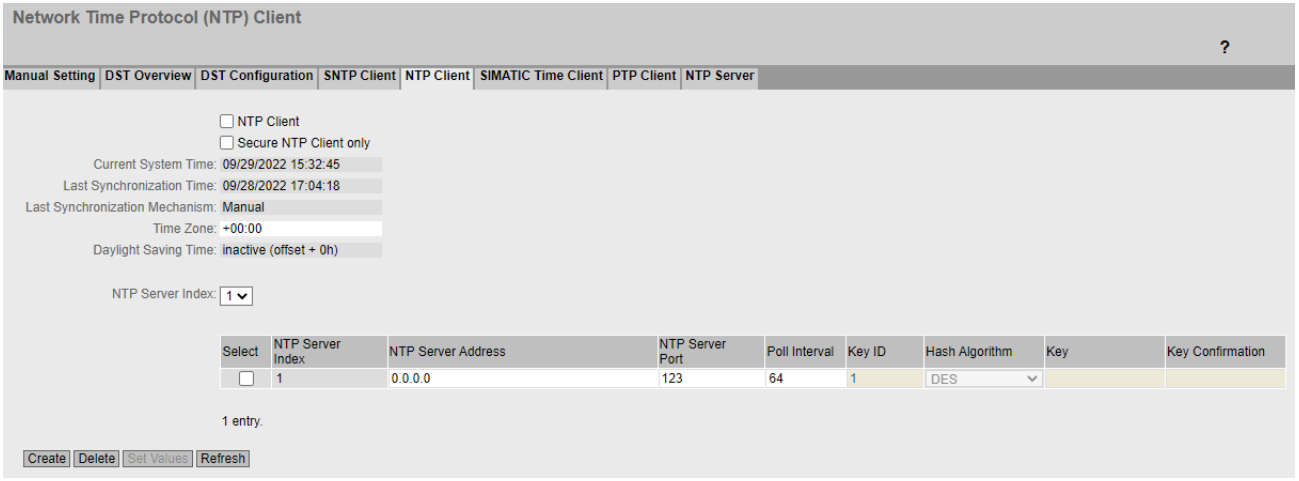
1. Click the "SNTP Client" check box to enable the automatic time setting.
2. In the "Time Zone" input box, enter the local time difference to world time (UTC). The input format is "+/-HH:MM" (for example +02:00 for CEST), because the SNTP server always sends the UTC time. This time is then recalculated 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.

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.



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

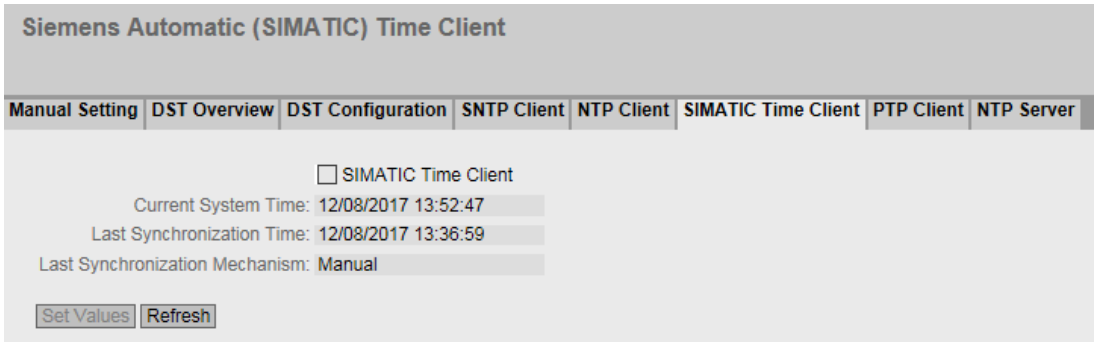
To synchronize the time of day via a secure NTP server, the following additional steps are necessary:

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.

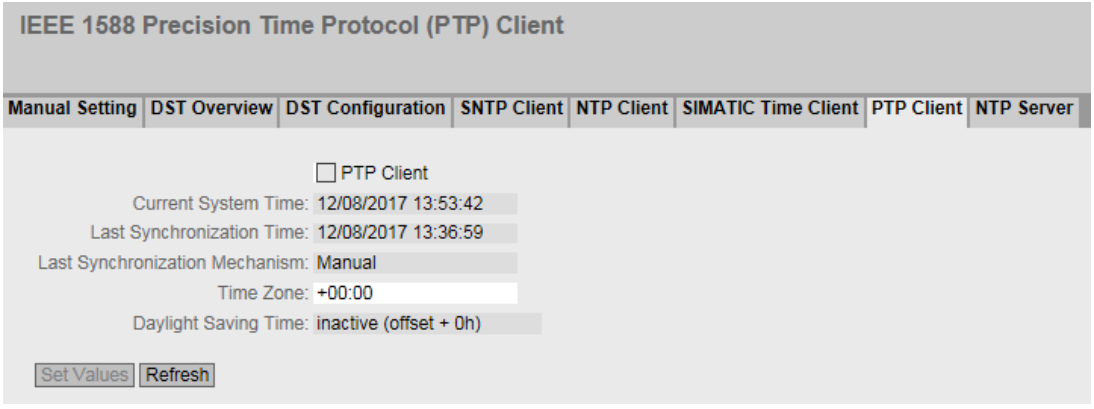
6.4.11.7 PTP Client

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.



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

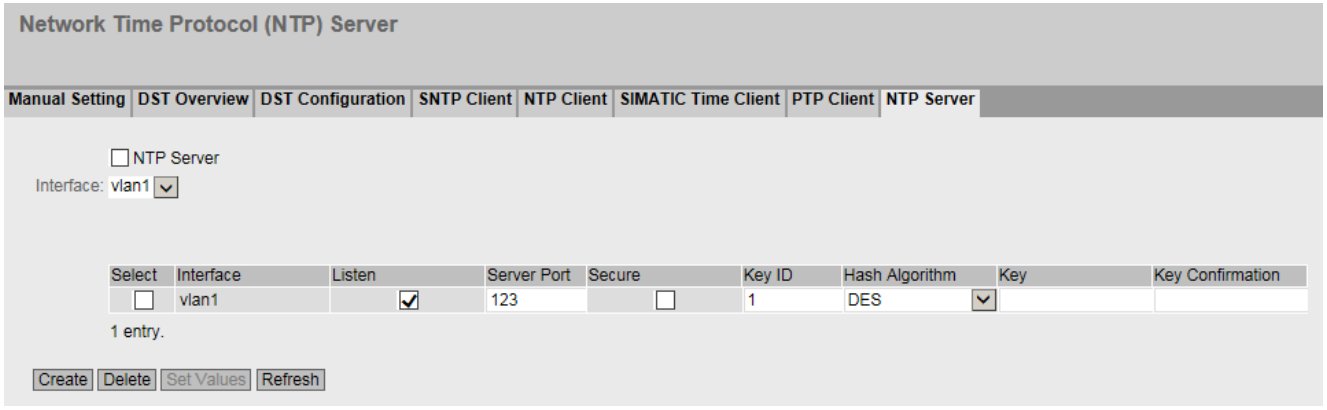
On this WBM page, you configure the device as an NTP server or as an NTP server of the type "NTP (secure)". The other devices can call up the time made available by the device via this NTP server. This means that the supplied devices are not dependent on a connection to an external time server.

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.



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)".

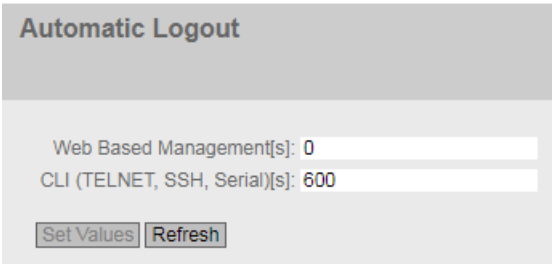
- **Key ID**
  Enter the ID of the authentication key.
- **Hash Algorithm**
  Specify the format for the authentication key.
- **Key**
  Enter the authentication key. The length depends on the hash algorithm.
  The following minimum lengths are recommended for the hash algorithm:
  - DES: ASCII 8 characters
  - MD5: ASCII 16 characters
  - SHA1: ASCII 20 characters
- **Key Confirmation**
  Enter the authentication key for confirmation.

6.4.12 Auto 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.



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

Availability of the buttons

Depending on your IE switch, different buttons and functions are available, see section "System functions hardware equipment (Page 17)".

Functionality of the button

You will find a detailed description of the function available with the button in the device operating instructions.

On this page, the functionality of the button can be enabled or disabled.

Description of the displayed boxes

The following functions are possible:

- **Restore Factory Defaults**
  if you select the check box, you can execute the function "Restore Factory Defaults" via the button.

  ⚠ CAUTION

  Button function "Restore Factory Defaults" active during startup

  If you have disabled this function in your configuration, disabling is only valid during operation. When starting up, 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 then needs to be reconfigured. An inserted PLUG is also deleted and returned to the delivery state.

- **Set Fault Mask**
  If you select the check box, you can define the fault mask via the button.

Steps in configuration

1. To use the functionality, select the corresponding check box.
2. Click the "Set Values" button.

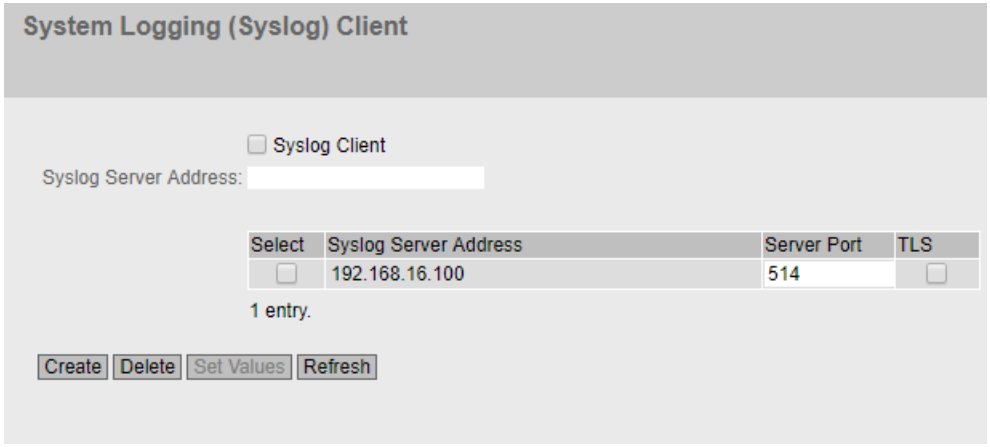
6.4.14 Syslog Client

Syslog according to RFC 5424 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.



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.

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

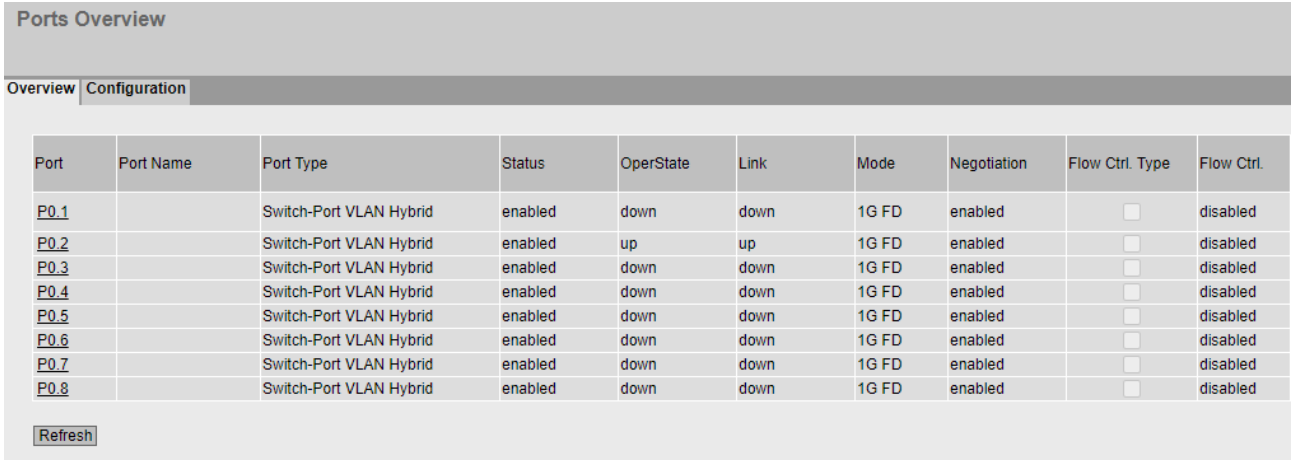
1. Select the check box in the row to be deleted.
2. Click the "Delete" button. All selected entries are deleted and the display is refreshed.

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.



Port	Port Name	Port Type	Status	OperState	Link	Mode	Negotiation	Flow Ctrl. Type	Flow Ctrl.
P0.1		Switch-Port VLAN Hybrid	enabled	down	down	1G FD	enabled		disabled
P0.2		Switch-Port VLAN Hybrid	enabled	up	up	1G FD	enabled		disabled
P0.3		Switch-Port VLAN Hybrid	enabled	down	down	1G FD	enabled		disabled
P0.4		Switch-Port VLAN Hybrid	enabled	down	down	1G FD	enabled		disabled
P0.5		Switch-Port VLAN Hybrid	enabled	down	down	1G FD	enabled		disabled
P0.6		Switch-Port VLAN Hybrid	enabled	down	down	1G FD	enabled		disabled
P0.7		Switch-Port VLAN Hybrid	enabled	down	down	1G FD	enabled		disabled
P0.8		Switch-Port VLAN Hybrid	enabled	down	down	1G FD	enabled		disabled

(Continuation of table)

Maximum Nodes	Learnt Nodes	Nodes Monitoring Action	Nodes Monitoring State	MAC Address	Blocked by	Unicast MAC Learning
100	0	power down timeout	on	08-00-07-70-84-b1	Link down	enabled
0	13	no	off	08-00-07-70-84-b2	-	enabled
0	0	no	off	08-00-07-70-84-b3	Link down	enabled
0	0	no	off	08-00-07-70-84-b4	Link down	enabled
0	0	no	off	08-00-07-70-84-b5	Link down	enabled
0	0	no	off	08-00-07-70-84-b6	Link down	enabled
0	0	no	off	08-00-07-70-84-b7	Link down	enabled
0	0	no	off	08-00-07-70-84-b8	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
  - Switch-Port PVLAN Host
  - Switch-Port PVLAN Promiscuous
  - Switch-Port VLAN Access
- **Combo Port Media Type**
  This column contains a value only in case of combo ports.
  Shows the mode of the combo port:
  - auto
  - rj45
  - sfp

- **Status**
  Shows 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.
- **OperState**
  Displays the current operating state. The operating state depends on the configured "Status" and the "Link". The available options are as follows:
  - 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 connection to the network, a "Link Integrity Signal" is being received.
  - down
    The connection is interrupted, for example, because the connected device is turned off.
- **Mode**
  Shows the transmission parameters of the port.
- **Negotiation**
  Shows whether the automatic configuration is enabled or disabled.
- **Flow Ctrl. Type**
  Shows whether flow control is enabled or disabled for the port.
- **Flow Ctrl.**
  Shows whether flow control is working on this port.
- **Maximum Nodes**
  The number of learned 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 have been learned for this port.

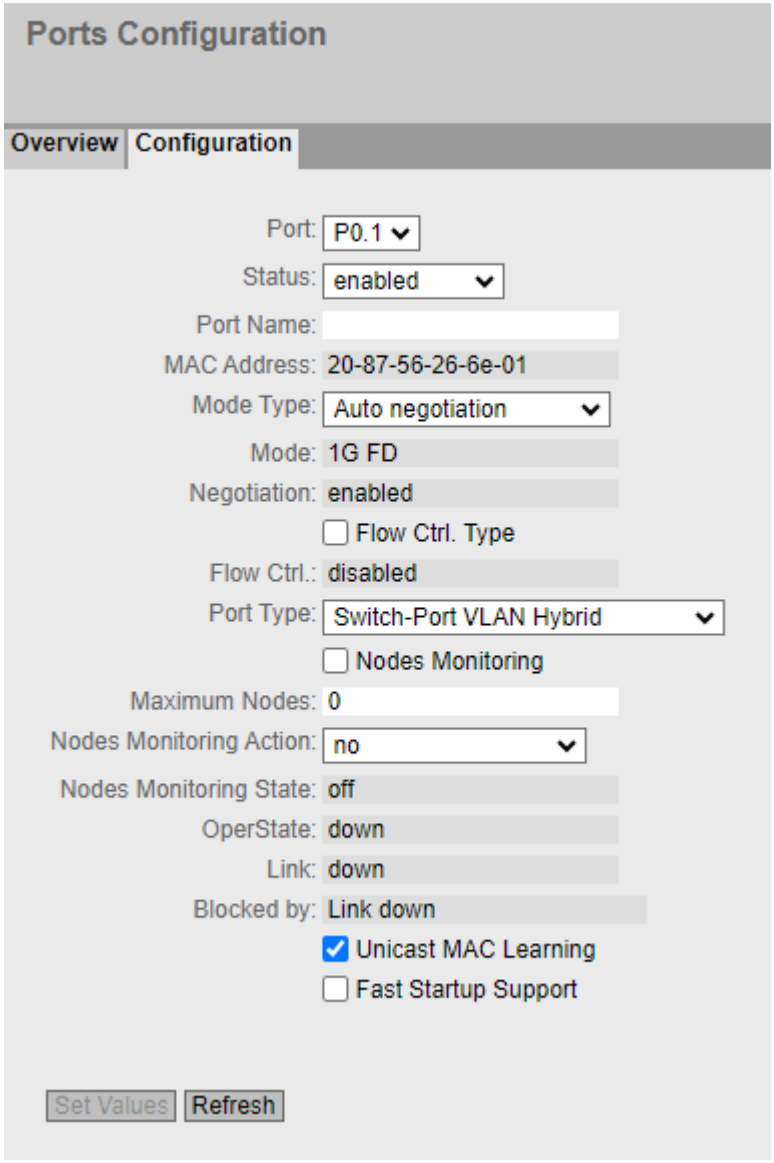
- **Nodes Monitoring Action**
  Shows the action that has been configured for when the number of monitored nodes is exceeded:
  - No
    No action when exceeded
  - Power down
    Switches the port off.
  - Power down timeout
    Switches the port off and checks the status again every 10 minutes.
- **Nodes Monitoring State**
  Shows the status of network node monitoring.
  - Off
    Monitoring is not enabled.
  - On
    Monitoring is enabled.
  - Exceeded
    The maximum number of possible MAC addresses has been exceeded.
  - Unknown
    The status of the function is unknown.
- **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 a result.
  - Link Check
    A disruption was detected on an optical transmission link, and the port status "disable" was configured as a result.
  - 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 in response to the 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".
- **NOA**
  This function is not available for all device groups, see section "System functions and hardware equipment".
  Shows the network to which the port belongs.
- **Unicast MAC Learning**
  Shows whether the learning of unicast addresses is enabled or disabled for a port.

6.4.15.2 Configuration

Configuring ports

On this page, you can configure all 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.

    Note

    Reduced current consumption

    For every optical port that you set to "link down", the current consumption of the device is reduced by 30 mA.

  - 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. Before the port and the partner port can communicate with each other, the settings must match at both ends.
  If you set the mode to "Auto negotiation", these parameters are automatically negotiated with the connected partner port. If you disable the "Auto negotiation" function, the "MDI/MDI-X Autocrossover" function remains active.

  Note

  "Auto negotiation" mode

  If the connected partner does not support Auto negotiation, the port at which this partner is connected must be set permanently to the values of the partner (transmission speed, duplexity).

  Note

  Transmission modes with SCALANCE XR-300WG PoE

  With the 10 Gigabit ports of the SCALANCE XR-300WG PoE, the "2.5 Gbps full duplex" and "5 Gbps full duplex" transmission modes are also possible. The "Auto negotiation" function can also set these two transmission modes.

- **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, with the SCALANCE XR-300WG also 2500 Mbps and 5000 Mbps on the 10 gigabit ports. 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.
- **Flow Ctrl. Type**
  Enable or disable the flow control function for the port.

  Note

  To use the flow control function, enable flow control at the appropriate input and output ports.

  If a packet is sent from an input port with flow control enabled to an output port with flow control enabled, the packet is not discarded if there is an overload. If flow control is enabled only on the input port, the packet can be discarded if there is an overload.

  Note

  Turning flow control on/off with "Auto negotiation"

  You can only enable or disable flow control when the "Auto negotiation" function is turned off. Afterwards you can enable "Auto negotiation" again.

- **Flow Ctrl.**
  Shows whether flow control is working on this port.

- **Port Type** (not available for all device groups)
  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.
  - 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 other 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.

- **Combo Port Media Type** (not available for all device groups)
  Specify the mode of the combo port:
  - auto
    If you select this mode, the pluggable transceiver port has priority.
    As soon as a pluggable transceiver is plugged in, an existing connection at the fixed RJ45 port is terminated. If no pluggable transceiver is plugged in, a connection can be established via the fixed RJ45 port.
  - rj45
    If you select this mode, the fixed RJ45 port is used regardless of the pluggable transceiver port.
    If a pluggable transceiver is plugged in, it is disabled, and the power turned off.
  - sfp
    If you select this mode, the pluggable transceiver port is used regardless of the fixed RJ45 port.
    If an RJ45 connection is established, it is terminated because the power of the RJ45 port is turned off.

  The factory setting for the combo ports is the auto mode.

  Note

  Automatic adaptation due to PROFINET configuration

  When establishing a PROFINET connection, the setting of the combo port media type is adapted automatically:
  - If a pluggable transceiver is configured, the combo port media type is set to "sfp".
  - If the built-in RJ45 port is configured, the combo port media type is set to "rj45".

  So that the automatic adaptation can be made, the combo port media type must be set to "auto".

  Configure the combo port media type accordingly using the WBM or CLI.

- **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 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 "Nodes Monitoring" check box is selected automatically. The value "0" clears the "Nodes Monitoring" check box automatically.
- **Nodes Monitoring Action**
  Action that is triggered when the number of monitored nodes is exceeded. The action is revoked as soon as the number is no longer exceeded.
  - No
    No action when exceeded
  - Power down
    Switches the port off.
  - Power down timeout
    Switches the port off and checks the status again every 10 minutes.

- **Nodes Monitoring State**
  Shows the status of network node monitoring.
  - Off
    Monitoring is not enabled.
  - On
    Monitoring is enabled.
  - Exceeded
    The maximum number of possible MAC addresses has been exceeded.
  - Unknown
    The status of the function is unknown.
- **OperState**
  Displays the current operating state. The operating state depends on the configured "Status" and the "Link". The available options are as follows:
  - 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 available options are as follows:
  - up
    The port has a valid link to the network, a "Link Integrity Signal" signal is being received.
  - down
    The connection is interrupted, 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 a result.
  - Link Check
    A disruption was detected on an optical transmission link, and the port status "disable" was configured as a result.
  - 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 in response to the 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 State Change
    The port is an MRP Interconnection port with the status "blocking".

- **NOA**
  This function is not available for all device groups, see section "System functions and hardware equipment".

  Note

  You can only configure this function if the device is operating in Transparent Bridge mode (Layer 2 > VLAN > "General" > "Base Bridge Mode" drop-down list: 802.1D Transparent Bridge). In the "802.1Q VLAN Bridge" mode in a NOA configuration, an error message is displayed.

  NOA (NAMUR Open Architecture) is a concept for data exchange in the process industry with the purpose of transferring data from the field level to a cloud. A SCALANCE XC-200 can take on the function of a NOA IT/OT switch and separate pure IT networks from pure OT networks. Communication to both networks is also possible. The switch separates the networks based on ports, which means a port either belongs to the IT network or to the OT network or to both networks. Select which network the port belongs to in the drop-down list. To export the IT data or the OT data, one port must be configured accordingly in each case. Select one of the following options:

  – Both
    The port belongs to the IT network and the OT network.
  – IT
    The port belongs to the IT network.
  – OT
    The port belongs to the OT network.

- **Unicast MAC Learning**
  Enables unicast address learning for a port.
- **Fast startup support** (only gigabit device variants)
  Speeds up connection establishment at a transmission speed of 100 Mbps by disabling the "Auto negotiation" and "MDI/MDI-X Autocrossover" functions.
  Enable this option to reduce the connection time.
  Fast startup support cannot be enabled on ring, standby or interconnection ports.

Changing the port configuration

Click the appropriate box to change the configuration.

Note

Optical ports always work with the full duplex mode and with maximum transmission speed. 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

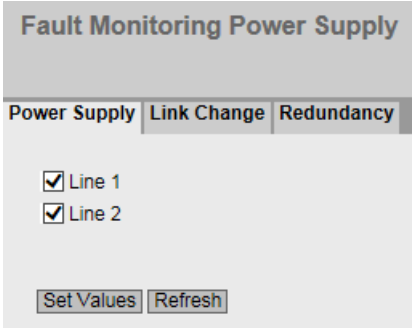
Configure whether or not the power supply should be monitored by the messaging system. Depending on the hardware variant, there are one or two power connectors (Supply 1 / Supply 2). With a redundant power supply, configure the monitoring separately for each individual feed-in line.

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

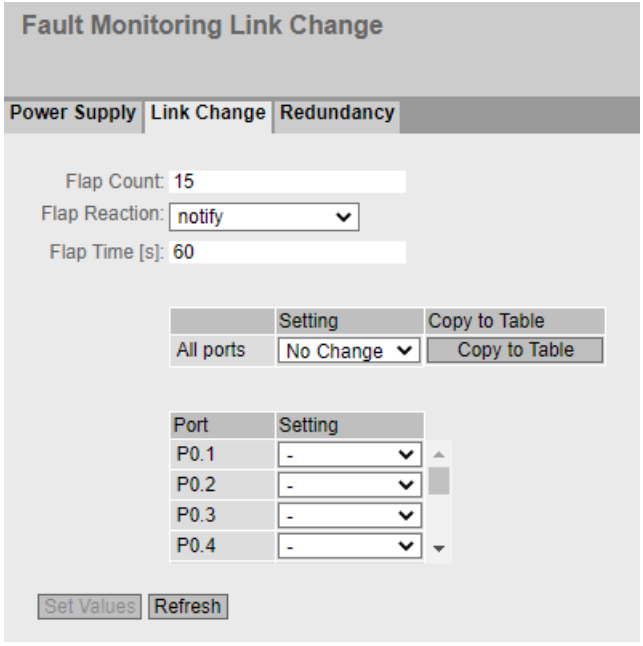
Configuration of fault monitoring of status changes on connections

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

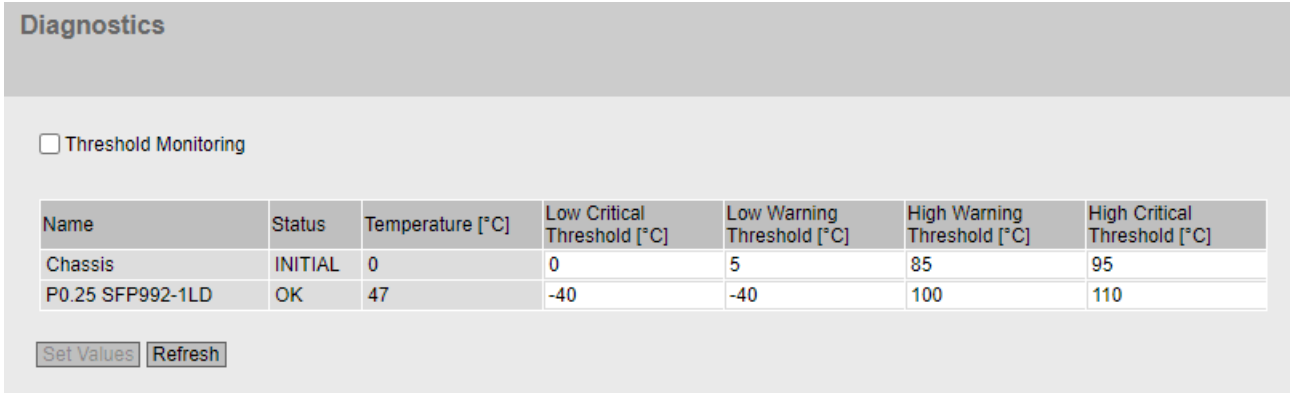
- **Redundancy Lost**
  When the check box is selected, the error LED is activated for the respective ring manager in case of a ring switchover (MRP or HRP, blocked port is closed).

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.

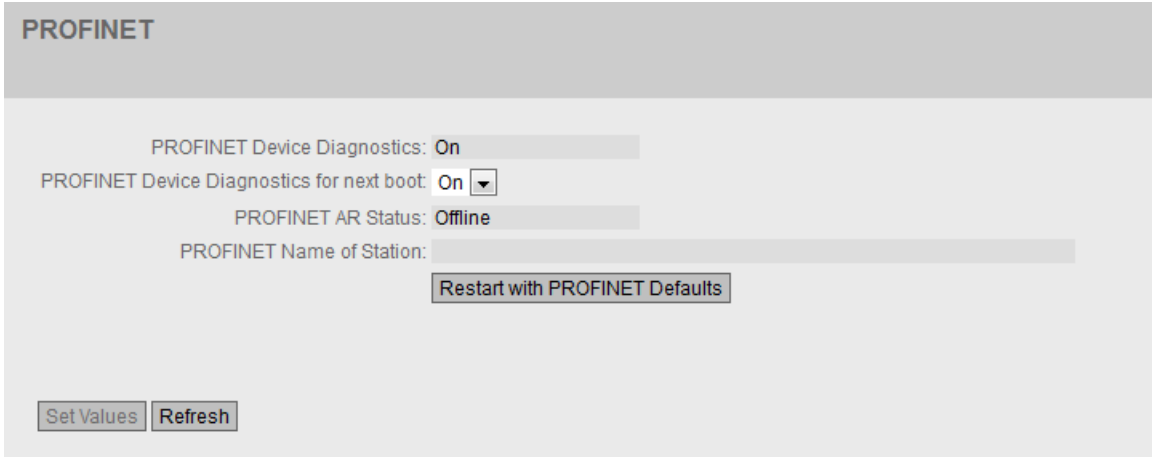
The table contains the following columns:

- **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.



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.

- **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.

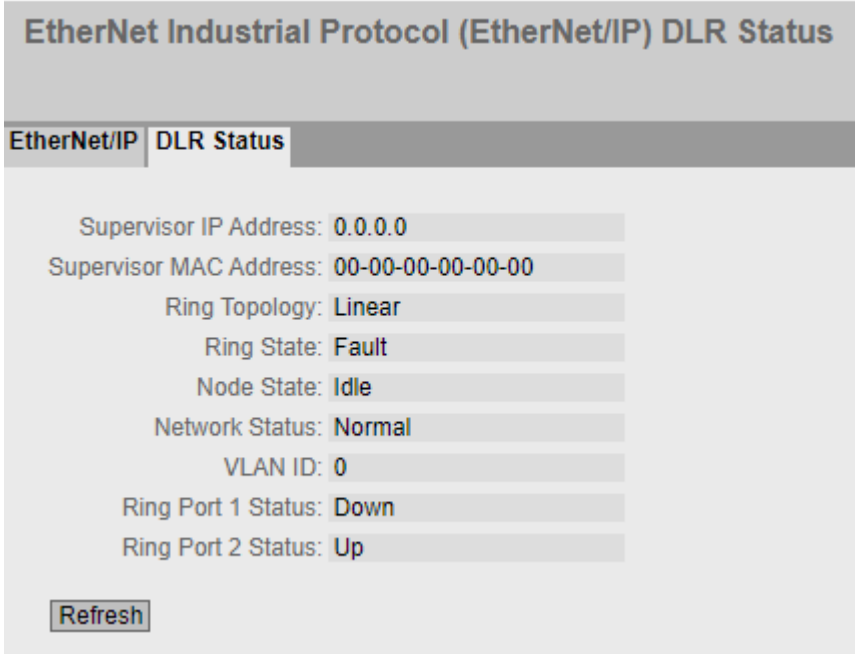
NOTICE
By resetting the settings to the default settings of a profile, the IP address is also lost. The device can then only be addressed via the serial interface, SINEC PNI or via DHCP. With the appropriate connection, a previously correctly configured device can cause circulating frames after the reset 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.

- **EtherNet/IP DLR Vlan**
  Select the "VLAN0" entry from the drop-down list for the DLR VLAN.
  The drop-down list is only available on devices with the following article numbers:

6GK5 204-2AA00-2GF2	6GK5 206-2BS00-2FC2	6GK5 216-0BA00-2AC2
6GK5 204-2AA00-2YF2	6GK5 208-0BA00-2AB2	6GK5 216-0BA00-2FC2
6GK5 205-3BB00-2AB2	6GK5 208-0BA00-2AC2	6GK5 216-0BA00-2TB2
6GK5 205-3BB00-2TB2	6GK5 208-0BA00-2FC2	6GK5 216-0HA00-2AS6
6GK5 205-3BD00-2AB2	6GK5 208-0BA00-2TB2	6GK5 216-0HA00-2ES6
6GK5 205-3BD00-2TB2	6GK5 208-0HA00-2AS6	6GK5 216-0HA00-2TS6
6GK5 205-3BF00-2AB2	6GK5 208-0HA00-2ES6	6GK5 216-0UA00-5ES6
6GK5 205-3BF00-2TB2	6GK5 208-0HA00-2TS6	6GK5 224-0BA00-2AC2
6GK5 206-2BB00-2AB2	6GK5 208-0UA00-5ES6	6GK5 324-0BA00-2AR3
6GK5 206-2BB00-2AC2	6GK5 213-3BB00-2AB2	6GK5 324-0BA00-3AR3
6GK5 206-2BB00-2TB2	6GK5 213-3BB00-2TB2	6GK5 328-4FS00-2AR3
6GK5 206-2BD00-2AB2	6GK5 213-3BD00-2AB2	6GK5 328-4FS00-2RR3
6GK5 206-2BD00-2AC2	6GK5 213-3BD00-2TB2	6GK5 328-4FS00-3AR3
6GK5 206-2BD00-2TB2	6GK5 213-3BF00-2AB2	6GK5 328-4FS00-3RR3
6GK5 206-2BF00-2AB2	6GK5 213-3BF00-2TB2	6GK5 328-4SS00-2AR3
6GK5 206-2BF00-2TB2	6GK5 216-0BA00-2AB2	6GK5 328-4SS00-3AR3
6GK5 206-2BS00-2AC2		

  The listed devices support the DLR VLAN only in 802.1D Transparent Bridge mode. On the "Layer 2 > VLAN > General" page, set the Base Bridge mode to 802.1D Transparent Bridge and configure VLAN0 as DLR VLAN via the WBM or in the CLI with the command `ethernetip dlr vlan`.
  The DLR VLAN is supported by all other devices without restrictions and no configuration needs to be performed.

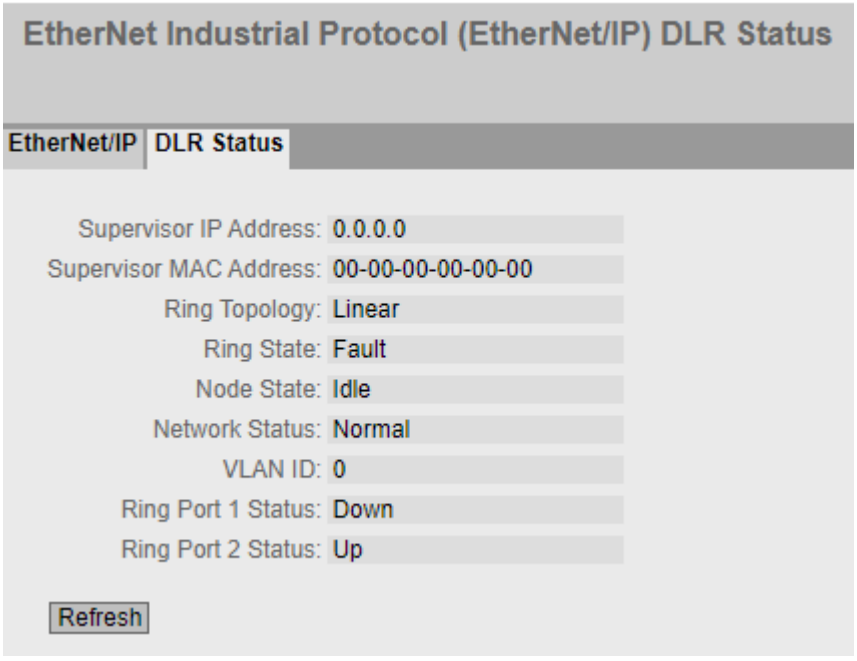
- **Restart with EtherNet/IP Defaults**
  Click this button to restore the default settings of the EtherNet/IP profile and to restart the device. You must confirm the restart in a dialog box. The dialog box displays the settings specially made for operation with the EtherNet/IP protocol.

NOTICE
Failure of the data traffic after resetting to default settings 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. With the appropriate attachment, a previously correctly configured device can cause circulating frames after the reset and therefore the failure of the data traffic.

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.



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 shown for the enabled EtherNet/IP DLR VLAN and as long as a supervisor has been detected. The configuration of the VLAN ID for DRL depends on the device:
  - **SCALANCE XR-300WG PoE, SCALANCE XC-200 with the identification "G" in the type designation (Gigabit versions) and SCALANCE XC216-4C**
    The DLR VLAN is independent of the VLAN configuration of the device.
  - **All other devices**
    The DLR VLAN depends on the VLAN configuration of the device.
    You can find the article numbers of the affected devices in the section EtherNet/IP (Page 271).

  Note

  If no DLR VLAN was configured, the EtherNet/IP DLR ports are automatically added as members to all VLANs with an ID in the range 1 ... 4095, regardless of whether a VLAN exists in the device configuration. In the WBM, the EtherNet/IP DLR ports are displayed in all existing VLANs with the label "E".

- **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
Do not remove or insert a PLUG during operation A PLUG may only be removed or inserted when the device is turned off. The device checks whether or not a PLUG is present at one second intervals. If the PLUG is removed during operation, loss of data may occur.

Information about the configuration of the C-PLUG

This page provides detailed information about the configuration stored on the C-PLUG. It is also possible to reset the PLUG to "factory defaults" 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.

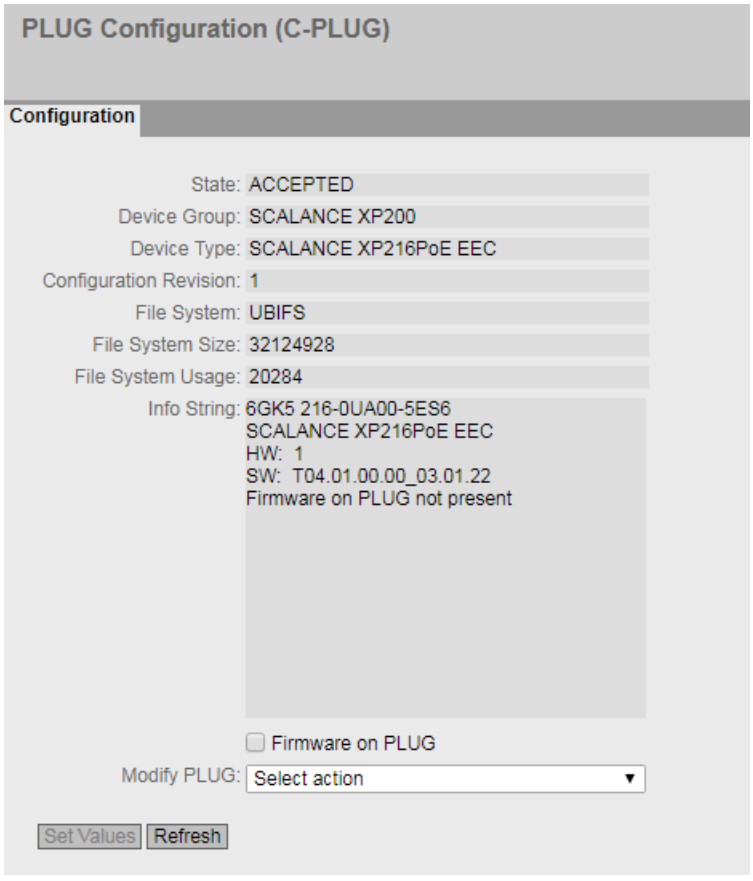
If you decide against executing the function after making your selection, click the "Refresh" button. As a result the data of this page is read from the device again and the selection is canceled.

Note

Incompatibility with older firmware versions with PLUG inserted

During the installation of an older firmware version, the configuration data can be lost. In this case, reset the device to the factory settings after the firmware has been installed.
In this situation, when a PLUG is inserted in the device, following the restart, this has the status "NOT ACCEPTED" because 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 "System > PLUG".



Description of the displayed boxes

The table has the following rows:

- **Status**
  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 C-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 C-PLUG previously.
- **Device type**
  Shows the device type within the product line that used the C-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, order 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.
- **Firmware on PLUG**
  When the function is enabled (default), the firmware will be stored on the PLUG. This means that automatic firmware updates/downgrades can be made with the PLUG. The box "Infor String" shows whether or not the firmware is stored on the PLUG.
- **Modify PLUG**
  Select the setting from the drop-down list. You have the following options for changing the configuration on the C-PLUG:
  - Write Current Configuration to the 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 C-PLUG and triggers low-level formatting.

Configuration procedure

1. You can only make settings in this box if you are logged on as "Administrator". Here, you decide how you want to change the content of the PLUG.
2. If you want to save the firmware on the PLUG select the check box "Firmware on PLUG".
3. Select the required option from the "Modify PLUG" drop-down list.
4. 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.

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.

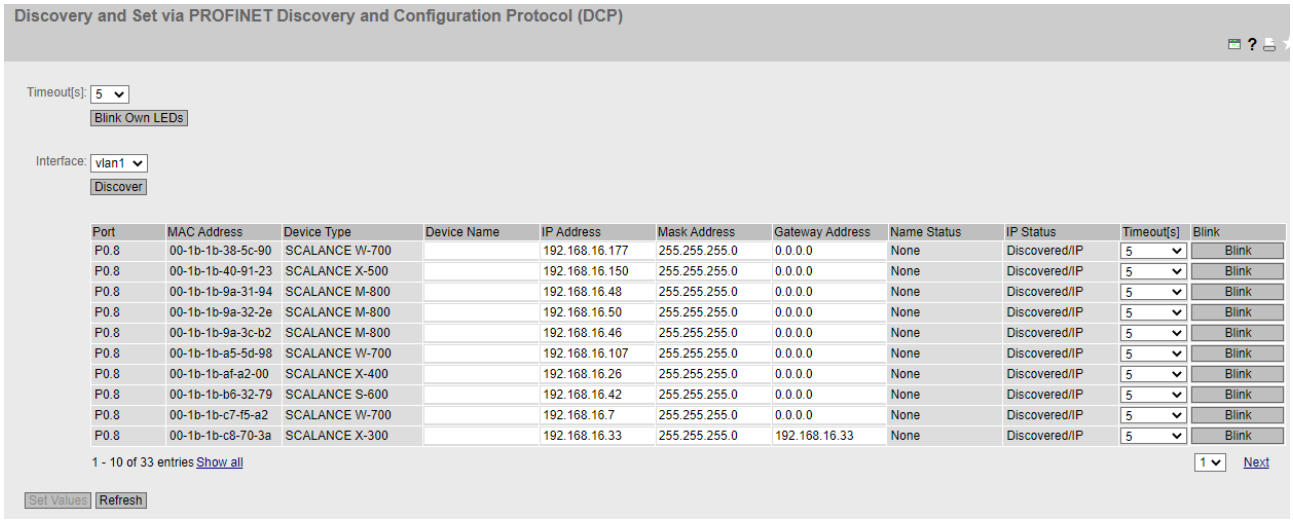
6.4.22 DCP Discovery

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".



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.
  - Discoverd: 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.

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".

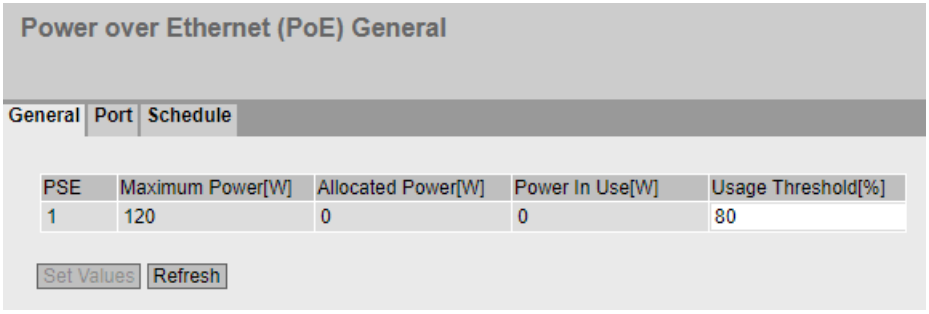
6.4.23 Power over Ethernet (PoE)

6.4.23.1 General

Settings for Power over Ethernet (PoE)

On this page, you see information about the power that the IE switch supplies with PoE.

The PoE variants of the SCALANCE XP-200 represent PSEs (Power Sourcing Equipment).



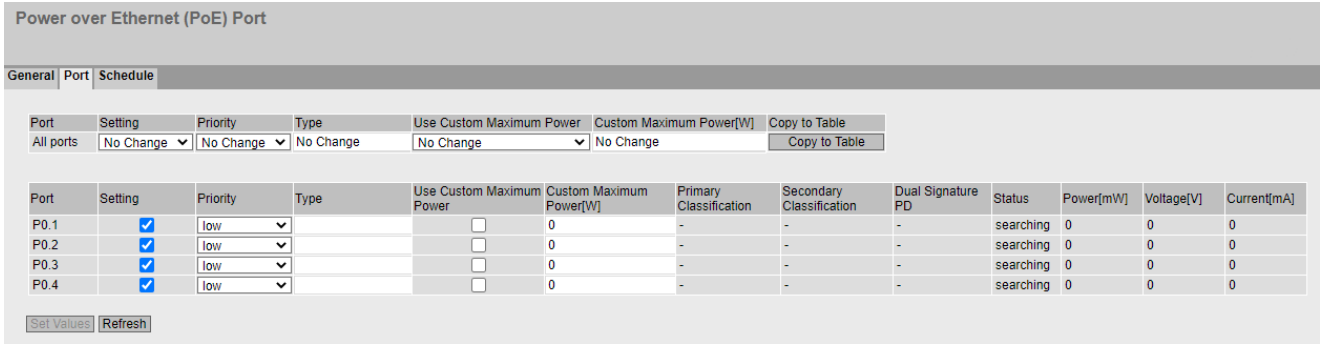
Description of the displayed boxes

- **PSE (read-only)**
  Shows the number of the PSE.
- **Maximum Power [W]**
  Maximum power that a PSE provides to supply PoE devices. For the device type SCALANCE XR326-2C PoE WG, you can configure the maximum power; for the other devices, this box is read only.
- **Allocated Power [W] (read-only)**
  Sum of the power reserved by the PoE devices according to the "Classification".
- **Power in Use [W] (read-only)**
  Sum of the power used by the end devices.
- **Usage Threshold [%]**
  As soon as the power being used by the end devices exceeds the percentage shown here, an event is triggered.

6.4.23.2 Port

Settings for the ports

For each individual PoE port, you can specify whether the power will be supplied via Ethernet. You can also set a priority for each connected consumer. Devices for which a high priority was set take preference over other devices for the power supply.
On this page, you can see detailed information on the individual PoE ports.



Description of the displayed boxes

The page contains two tables. In table 1, you can make settings and assign them to all ports at the same time. In table 2, you can make different settings for each port.

Table 1 has the following columns:

- **Port**
  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.
- **Priority**
  Select the required priority.
  If "No Change" is selected, the entry in table 2 remains unchanged.
- **Type**
  Here, you can enter a string to describe the connected device in greater detail. The maximum length is 255 characters.
- **Use Custom Maximum Power**
  Select whether the custom maximum power is used.
  If "No Change" is selected, the entry in table 2 remains unchanged.
- **Custom Maximum Power [W]**
  Enter the maximum power that a port makes available to supply a connected device.
  This value is only taken into account when the "Use Custom Maximum Power" check box is selected.
  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**
  Shows the configurable PoE 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 the PoE power supply for this port or interrupt it.
- **Priority**
  From the drop-down list, select which priority this port will have for the power supply.
  The following settings are possible, in ascending order of relevance:
  - Low
  - High
  - Critical

  If the power of the connected power supply is inadequate to supply all connected devices, devices with a higher priority are given preference.
  If the same priority is set for two ports, the port with the lower number will be preferred when necessary.
- **Type**
  Here, you can enter a string to describe the connected device in greater detail. The maximum length is 255 characters.
- **Use Custom Maximum Power**
  If you enable this check box for a port, the user-defined maximum power is used.
- **Custom Maximum Power [W]**
  Enter the maximum power that a port makes available to supply a connected device.
  This value is only taken into account when the "Use Custom Maximum Power" check box is selected.
  The user-defined power is compared to the range of values of the class indicated by the connected device:
  - If the user-defined power is within the class of the connected device, the user-defined value is used.
  - If the user-defined power is above the class of the connected device, the highest value of the class is used.
  - If the user-defined power is below the class of the connected device, the lowest value of the class is used.

  If the power consumption of the connected device exceeds the defined or used maximum power, the connected device is turned off.
- **Classification** (read-only)
  With devices that can supply energy consumers of the standards IEEE802.af Type 1 or IEEE802.at Type 2.
  The classification specifies the class of the device. From this, it is possible to recognize the maximum power of the device.

- **Primary Classification** (read-only)
  With devices that can supply energy consumers of the standards IEEE802.af Type 1, IEEE802.at Type 2 or IEEE802.3bt Type 3.
  The primary classification of the device at this port.
- **Secondary Classification** (read-only)
  With devices that can supply energy consumers of the standards IEEE802.af Type 1, IEEE802.at Type 2 or IEEE802.3bt Type 3.
  The secondary classification of the device at this port.
- **Dual Signature PD** (read-only)
  With devices that can supply energy consumers of the standards IEEE802.af Type 1, IEEE802.at Type 2 or IEEE802.3bt Type 3.
  Specifies whether the connected energy consumer is a single signature PD or a dual signature PD.
  - **Yes**
    The power supply for the device at this port must correspond to the primary classification and the secondary classification.
  - **No**
    The power supply for the device at this port must correspond to the primary classification.
- **Status** (read-only)
  Shows the current status of the port.
  The following states are possible:
  - disabled
    The PoE power supply is deactivated for this port.
  - delivering
    The PoE power supply is activated for this port and a device is connected.
  - searching
    The PoE power supply is activated for this port but there is no device connected.

  Note

  If a device is connected to a port with PoE capability, a check is made to determine whether the power of the port is adequate for the connected device.

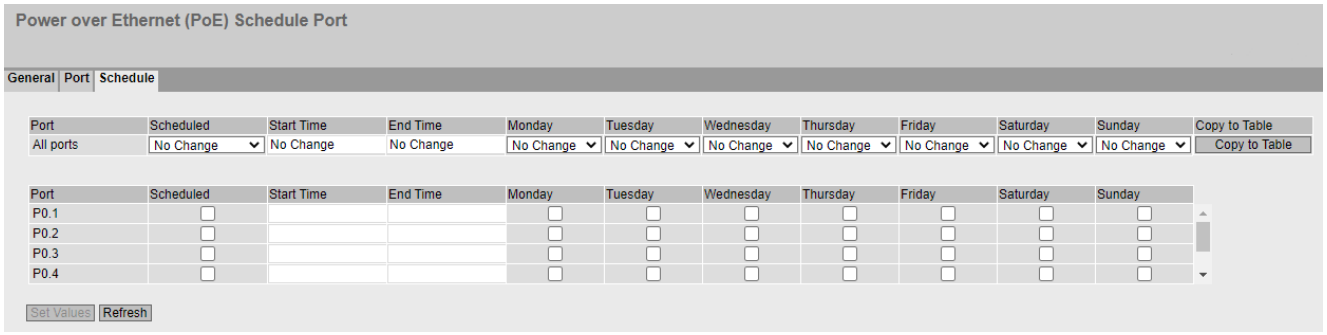
  If the power of the port is inadequate, although PoE is enabled in "Setting", the port nevertheless has the status "disabled". This means that the port was disabled by the PoE power management.

- **Power [mW]** (read-only)
  Shows the power that the SCALANCE provides at this port.
- **Voltage [V]** (read-only)
  Shows the voltage applied to this port.
- **Current [mA]** (read-only)
  Shows the current with which a device connected to this port is supplied.

6.4.23.3 Schedule

Time restrictions for Power over Ethernet (PoE)

On this page, you configure the period of time in which power supply over the individual PoE ports is possible. If consumers are in uninterrupted operation, energy consumption can be reduced in this way.



Description of the displayed boxes

The page contains two tables. In table 1, you can make settings and assign them to all ports at the same time. In table 2, you can make different settings for each port.

Table 1 has the following columns:

- **Port**
  Shows that the settings are valid for all ports.
- **Setting**
  The following options are possible:
  - **Enabled**
    All check boxes in the second column of Table 2 are selected.
  - **Disabled**
    All check boxes in the second column of Table 2 are cleared.
  - **No Change**
    The entries in table 2 remains unchanged.
- **Start Time**
  Enter the start time for power supply via PoE in the format **hh:mm**. If "No Change" is selected, the entries in table 2 remain unchanged.
- **End Time**
  Enter the end time for power supply via PoE in the format **hh:mm**. If "No Change" is selected, the entries in table 2 remain unchanged.
  If the value for the end time is less than the value for the start time or when both values are the same, the end of the PoE power supply is on the next weekday.

- **Monday ... Sunday**
  The following options are possible:
  - **Enabled**
    All check boxes in the column for the corresponding weekday of Table 2 are selected.
  - **Disabled**
    All check boxes in the column for the corresponding weekday of Table 2 are cleared.
  - **No Change**
    The entries 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**
  Shows the configurable PoE 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**
  When the check box is selected, the respective port makes power supply via PoE available only in the configured time period.
- **Start Time**
  Enter the start time for power supply via PoE in the format **hh:mm**.
- **End Time**
  Enter the end time for power supply via PoE in the format **hh:mm**.
- **Monday ... Sunday**
  Select the check boxes for the days of the week on which power supply via PoE should be available.

6.4.24 Port Diagnostics

6.4.24.1 Cable Tester

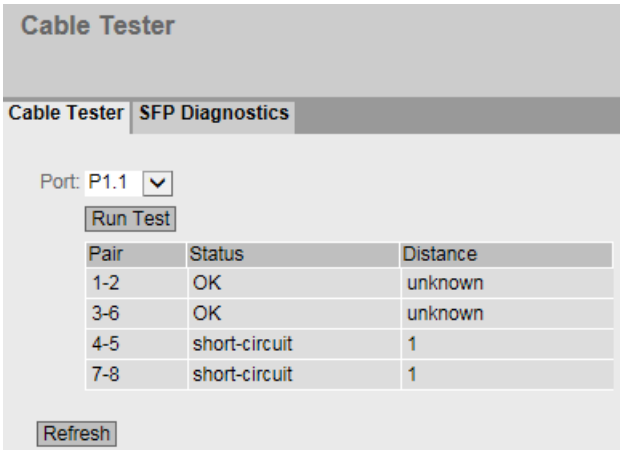
With this page, each individual Ethernet port can run independent fault diagnostics on the cable. This test is performed without needing to remove the cable, connect a cable tester and install a loopback module at the other end. Short-circuits and cable breaks can be localized to within a few meters.

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; in this case, the connection needs to be re-established 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.

  The wire pair assignment - pin assignment is as follows (DIN 50173):

  Pair 1 = pin 1-2

  Pair 2 = pin 3-6

  Pair 3 = pin 4-5

  Pair 4 = pin 7-8

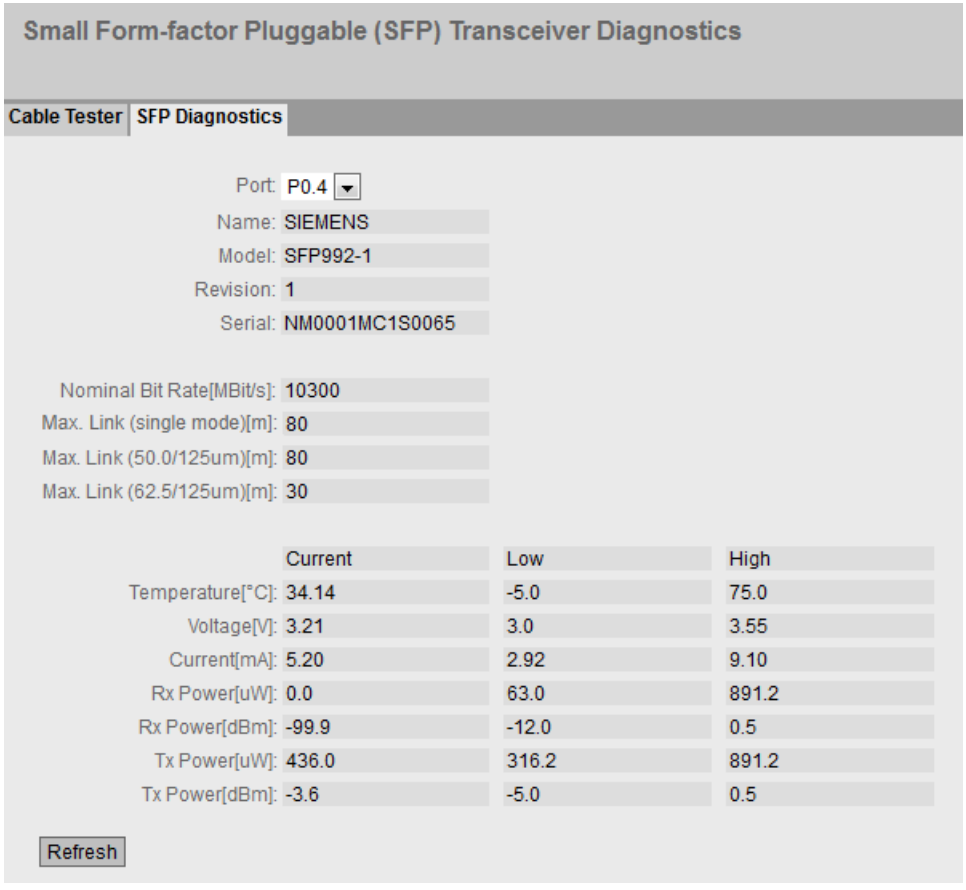
- **Status**
  Displays the status of the cable.
- **Distance**
  Displays the distance to the open cable end, cable break, or short-circuit in meters. The value for the distance has a tolerance of +/- 1 m.
  If the status is "OK", the length is specified with "unknown".

6.4.24.2 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.



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.

6.5 The "Layer 2" menu

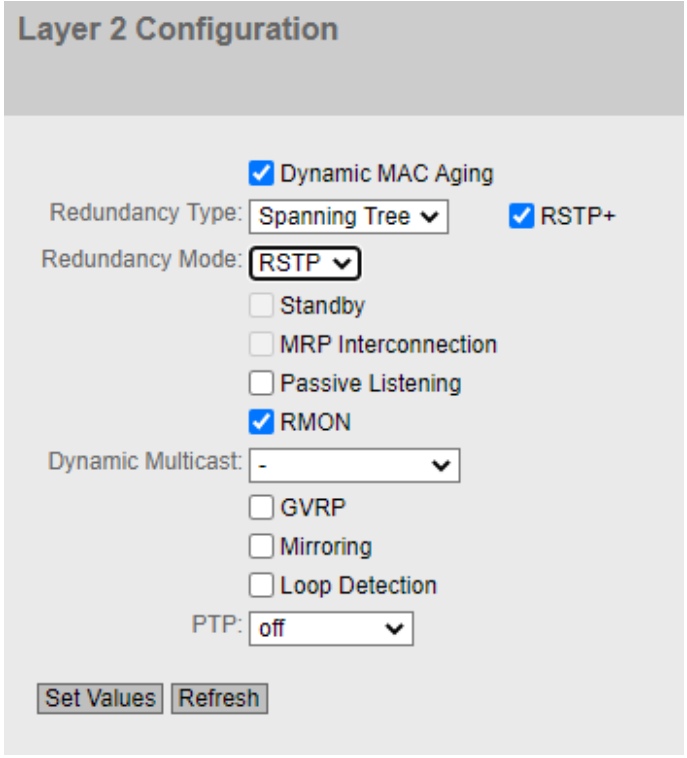
6.5.1 Configuration

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.



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".

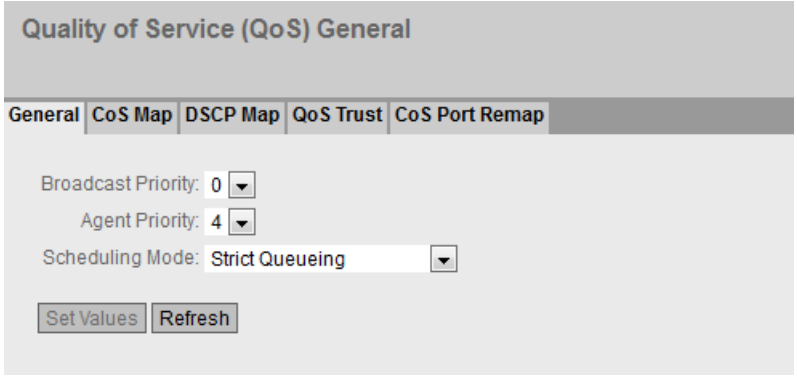
6.5.2 Quality of Service (QoS)

You should also refer to the chapter "Technical Basics", section "Quality of service (Page 93)".

6.5.2.1 General

Transmission priorities

On this page, you can specify the priorities of different frames. In addition to this, depending on the priority you can set the method according to which the processing order of the frames is specified.



Description of the displayed values

The page contains the following boxes:

- **Broadcast Priority**
  Specify the priority of broadcast frames. The switch sorts the frame into a Queue according to this prioritization. You configure the assignment of the priority to a queue on the page "Layer 2 > QoS > CoS Map".
- **Agent Priority**
  Specify the priority of agent frames. The switch sorts the frame into a queue according to this prioritization . You configure the assignment of the priority to a queue on the page "Layer 2 > QoS > CoS Map".
- **Scheduling Mode**
  Select the order in which the frames are processed in the queues.
  - Strict Queueing
    As long as there are frames with high priority in the queue, only these high-priority frames are processed.
  - Weighted Fair Queueing
    Even if there are frames with high priority in the queue, frames with a lower priority will be processed occasionally.

Note

Devices for which you cannot set the scheduling mode use the "Strict Queueing" method.

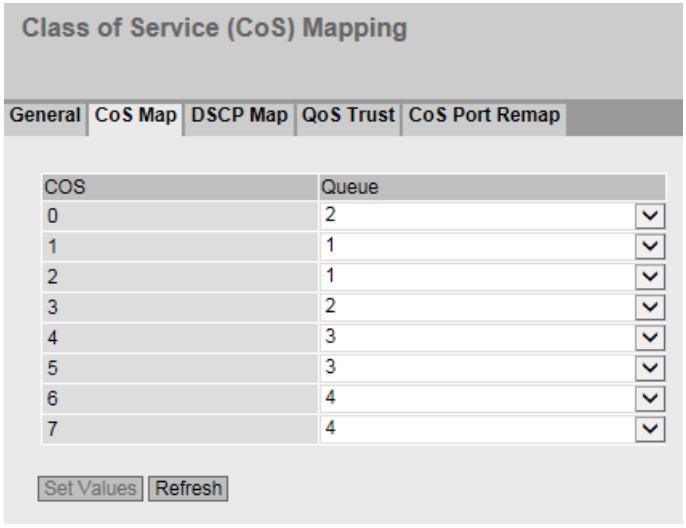
Steps in configuration

1. From the drop-down lists "Broadcast Priority" and "Agent Priority" select the priority with which the frames will be processed internally.
2. In the "Scheduling Mode" drop-down list select the method according to which the processing order of the frames is decided.
3. Click the "Set Values" button.

6.5.2.2 CoS Map

CoS Map

On this page, you can assign CoS priorities to different queues.



Description of the displayed boxes

The table has the following columns:

- **CoS**
  Shows the CoS priority of the incoming frames.
- **Queue**
  From the drop-down list, select the queue that is assigned to the CoS priority.
  The higher the number of the Queue, the higher the processing priority.

The service classes (CoS) are assigned to the queues as default as follows:

COS	Devices with 4 queues	Devices with 8 queues
0	Queue 2	Queue 2
1	Queue 1	Queue 1
2	Queue 1	Queue 3
3	Queue 2	Queue 4
4	Queue 3	Queue 5
5	Queue 3	Queue 6
6	Queue 4	Queue 7
7	Queue 4	Queue 8

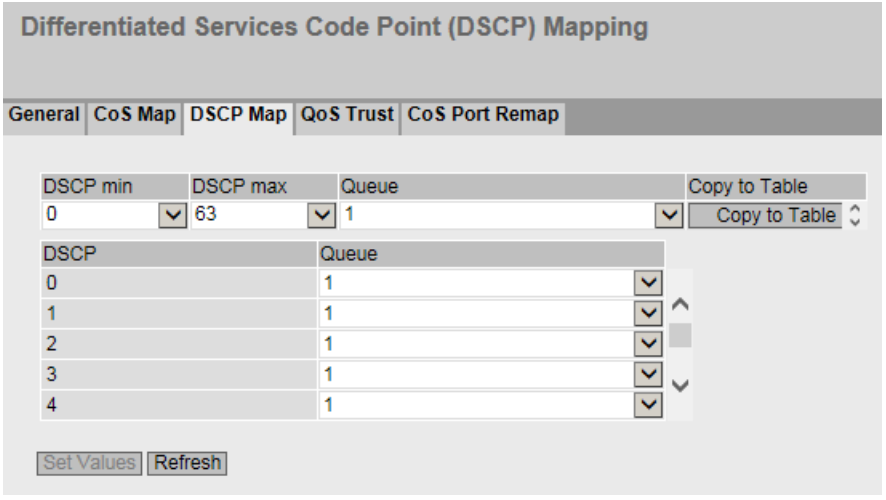
Configuration procedure

1. For each value in the "CoS" column, select the queue from the "Queue" drop-down list.
2. Click the "Set Values" button.

6.5.2.3 DSCP Map

DSCP queue

On this page, you can assign DSCP priorities to different Queues.



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 frames.
- **Queue**
  From the drop-down list, select the queue that is assigned to the DSCP priority.
  The higher the queue number the higher the processing priority

The DSCP priorities are assigned to the queues as default as follows:

DSCP codes	Devices with 4 queues
0 - 15	Queue 1
16 - 31	Queue 2
32 - 47	Queue 3
48 - 63	Queue 4

DSCP codes	Devices with 8 queues
0 - 7	Queue 2
8 - 15	Queue 1
16 - 23	Queue 3
24 - 31	Queue 4
32 - 39	Queue 5
40 - 47	Queue 6
48 - 55	Queue 7
56 - 63	Queue 8

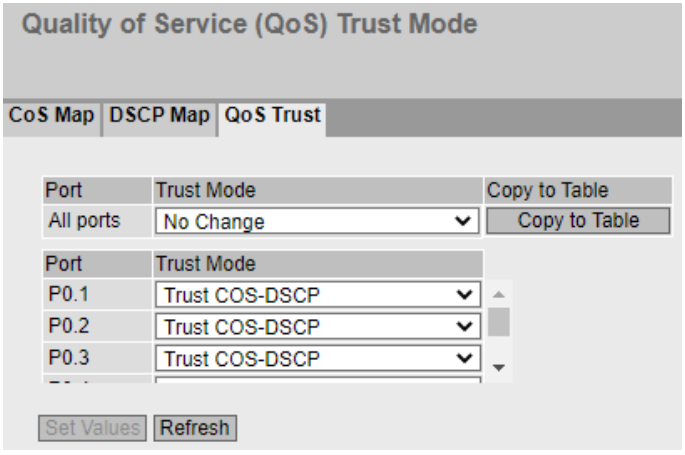
Steps in configuration

1. For each value in the "DSCP" column, select the queue from the "Queue" drop-down list.
2. Click the "Set Values" button.

6.5.2.4 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.



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.

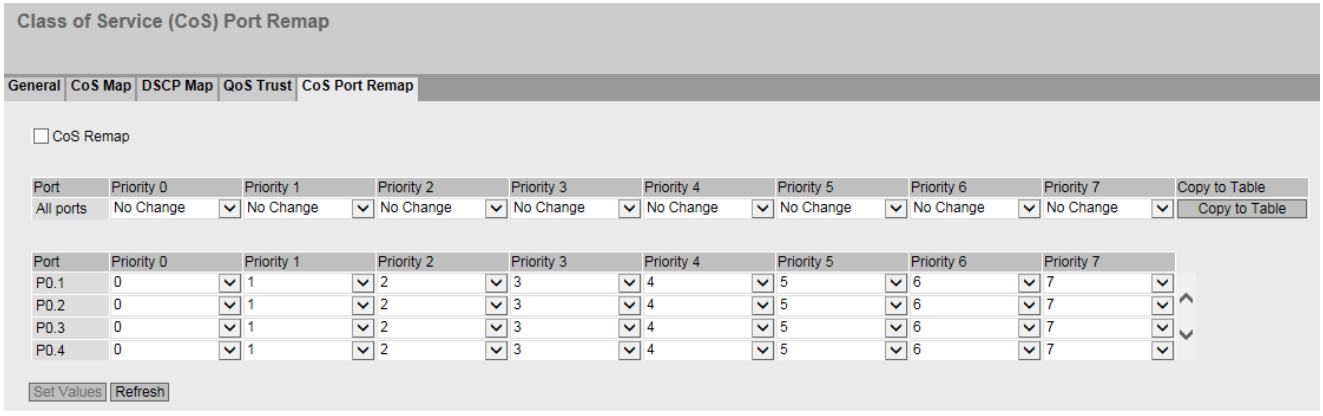
Configuration procedure

1. Select the required Trust Mode from the drop-down list.
2. Click the "Set Values" button.

6.5.2.5 CoS Port Remap

Changing priority when sending

On this page depending on the priority when receiving, you can change the priority of a frame with which it is sent. The new priority effects only the following devices that receive the frame.



Description of the displayed boxes

The page contains the following boxes:

- **CoS Remap**
  Enable or disable frames being sent with changed priorities according to Table 2.

Table 1 has the following columns:

- **Port**
  Shows that the settings are valid for all ports of table 2.
- **Priority 0 - 7**
  The priority in the column stands for the priority with which a frame is received.
  - 0 - 7
    Select the priority with which a frame will be sent.
  - No Change
    No change in 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 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.
- **Priority 0 - 7**
  The priority in the column stands for the priority with which a frame is received.
  In the drop-down list select the priority with which a frame will be sent.

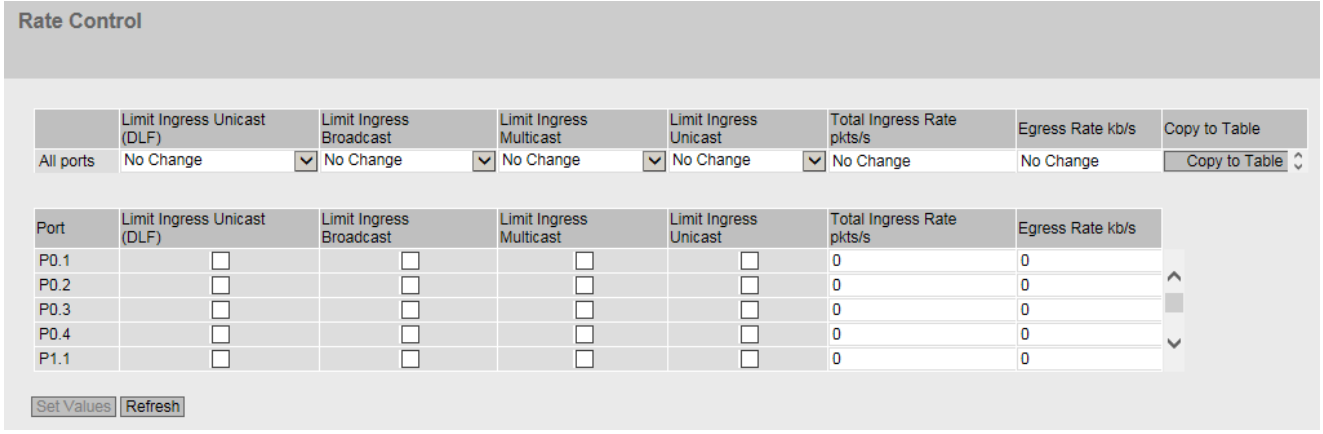
Steps in configuration

1. Select the "CoS Remap" check box.
2. Using the drop down lists select the priority for sending for each receive priority per port.
3. 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 for the individual ports. You can specify the category of frame for which these limit values will apply.



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 kb/s**
  Specify the data rate for all incoming frames. If "No Change" is entered, the entry in table 2 remains unchanged
- **Egress Rate kb/s**
  Specify the data rate for all outgoing frames. If "No Change" is entered, the entry in 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.
- **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 kb/s**
  Specify the data rate for all incoming frames.

  Note

  The device limits data traffic to the entered value only if at least one check box in the following columns has been selected for the relevant port:

  - 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, 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.

Steps in configuration

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

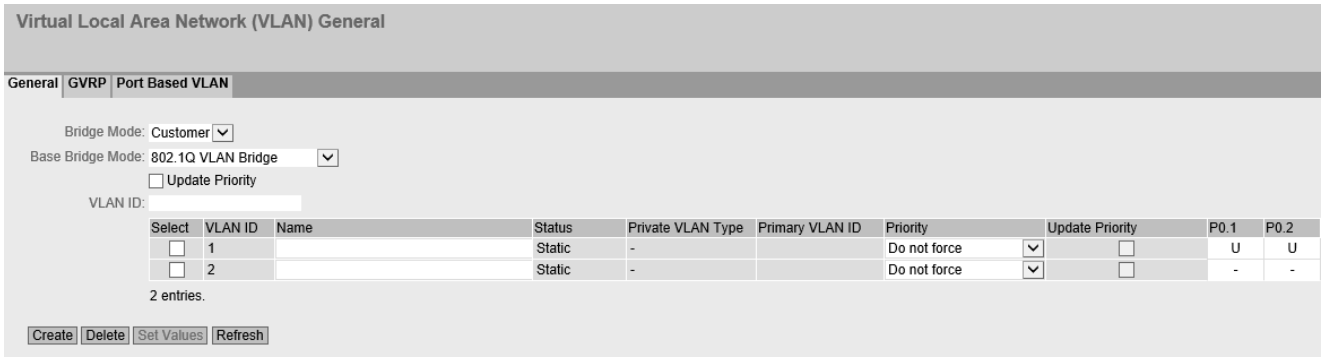
On this page, you specify whether the device forwards frames with VLAN tags transparently (IEEE 802.1D/VLAN-unaware mode) or takes VLAN information into account (IEEE 802.1Q/ VLAN-aware mode). If the device is in the "802.1Q VLAN Bridge" mode, you can define VLANs and specify the use of the ports.

The possible settings on this page depend on what you select in the "Base Bridge Mode" box.

Note

Changing the Agent VLAN ID

If the configuration PC is connected directly to the device via Ethernet and you change the agent VLAN ID, the device is no longer reachable via Ethernet following the change.



Description of the displayed boxes

The page contains the following boxes:

- **Bridge Mode**
  Select the role of the device. The following roles are available:
  - 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. In this role, you can use the function Q-in-Q VLAN tunnel.

    Note

    The Provider role has the following effects on the VLAN tag: All data packets that are not sent from an access port receive a VLAN tag. If the VLAN configuration of the other devices is not adapted accordingly, network loops can occur or network segments may no longer be reachable.

- **Base Bridge Mode**

  Note
  Changing Base Bridge Mode

  Note the paragraph "Changing Base Bridge Mode" in this section. This section describes how a change affects the existing configuration.

  Select the required mode from the drop-down list. The following modes are possible:
  - 802.1Q VLAN Bridge
    Sets the mode "VLAN-aware" for the device. In this mode, VLAN information is taken into account.
  - 802.1D Transparent Bridge
    Sets the mode "VLAN-unaware" for the device. In this mode, VLAN tags are not changed but are forwarded transparently. The VLAN priority is evaluated for CoS. In this mode, you cannot create any VLANs. Only a management VLAN is available: VLAN 1.
- **Update Priority**
  When you select this check box, the value in the "Priority" column is entered in the VLAN tags of all incoming frames for this VLAN as new Class of Service.
- **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.

- **Name**
  Enter a name for the VLAN. The name only provides information and has no effect on the configuration.
  Length: Max. 32 characters
- **State**
  Shows the status type of the entry in the internal port filter table. Here, "Static" means that the VLAN was entered statically by the user.
- **Private VLAN Type**
  Shows the type of the PVLAN.
- **Primary VLAN ID**
  With secondary PVLANs, shows the ID of the corresponding primary PVLAN.
- **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**
  This column shows the status of the "Update Priority" check box at the start of the page for all VLANs. A VLAN-specific setting is not possible.
- **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 "-".
  - M
    The port is a member of the VLAN. Frames sent in this VLAN are forwarded with the corresponding VLAN tag.
  - R
    The port is a member of the VLAN. A GVRP frame is used for the registration.
  - 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.
  - F
    The port is not a member of the specified VLAN and cannot become a member of this VLAN even if it is configured as a trunk port.
  - T
    This option is only displayed and cannot be selected in the WBM.
    This port is a trunk port making it a member in all VLANs.

Changing Base Bridge Mode

VLAN-unaware (802.1D transparent bridge) → VLAN-aware (802.1Q VLAN bridge)

If you change the Base Bridge Mode from VLAN-unaware to VLAN aware, this has the following effects:

- All static and dynamic unicast entries are deleted.
- All static and dynamic multicast entries are deleted.
- With Spanning Tree, you can set the following protocol compatibility: STP, RSTP and MSTP.

VLAN-aware (802.1Q VLAN bridge) → VLAN-unaware (802.1D transparent bridge)

If you change the Base Bridge Mode from VLAN-aware to VLAN-unaware, this has the following effects:

- All VLAN configurations are deleted.
- A management VLAN is created: VLAN 1.
- All static and dynamic unicast entries are deleted.
- All static and dynamic multicast entries are deleted.
- With Spanning Tree, you can set the following protocol compatibility: STP and RSTP.
- You cannot use GVRP.
- You cannot use guest VLAN.
- The VLAN assignment cannot be adopted from the RADIUS server.
- You cannot configure the port type.
- Defined access rules must be valid for all VLANs. On the "Security > Management ACL" page, the value "1-4094" must be defined for the parameter "VLANs Allowed".

802.1Q VLAN bridge: 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 there is a further switch at this port, the frame should have a tag added (trunk port).

Configuration procedure

1. If "802.1Q VLAN bridge" is not set, select the entry "802.1Q VLAN Bridge" from the "Base Bridge Mode" drop-down list. Click the "Set Values" button.
2. Enter an ID in the "VLAN ID" input box.
3. Click the "Create" button. A new entry is generated in the table. As default, the boxes have the entry "-".

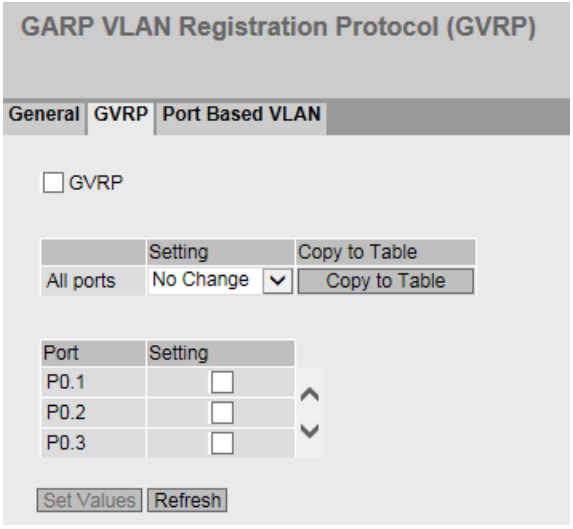
4. If applicable, enter a name for the VLAN.
5. Specify the use of the port in the VLAN. If, for example you select "M", the port is a member of the VLAN. Frames sent in this VLAN are forwarded with the corresponding VLAN tag.
6. Click the "Set Values" button.

6.5.4.2 GVRP

Configuration of GVRP functionality

Using a GVRP frame, a different device can register at the port of the device for a specific VLAN ID. 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.



Description of the displayed boxes

The page contains the following boxes:

- **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.

Steps in configuration

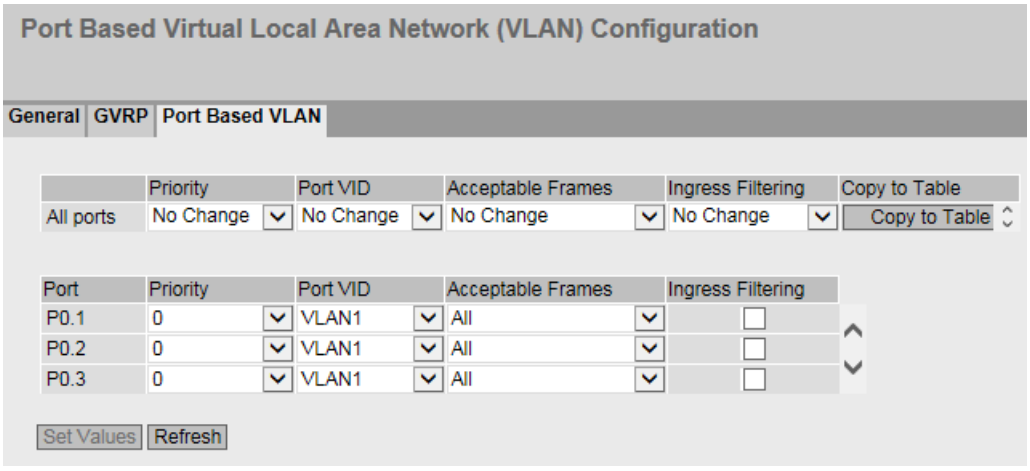
1. Click "GVRP" check box.
2. Click the check box after the port in the "Setting" column to enable or disable GVRP for this port.
   Repeat this for every port for which you want to enable or disable the function.
3. Click the "Set Values" button.

6.5.4.3 Port-based VLAN

Processing received frames

On this page, you specify the configuration of the port properties for receiving frames.

You can only configure the settings on this page if on the "General" tab you selected the "Base Bridge Mode" "802.1Q VLAN Bridge".



Description of the displayed boxes

Table 1 has the following columns:

- **1st column**
  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**
  When 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.
- **Priority**
  The CoS priority (Class of Service) used in a VLAN tag. If a frame is received without a tag, it will be assigned this priority. The 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).
  From the drop-down list, select the priority given to untagged frames.
- **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. Otherwise, the forwarding rules apply according to the configuration.
  - All
    The device forwards all frames.
  - Untagged and Priority Tagged Only
    The device discards all tagged frames. The device forwards all untagged frames and frames with 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.
- **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.

Steps in configuration

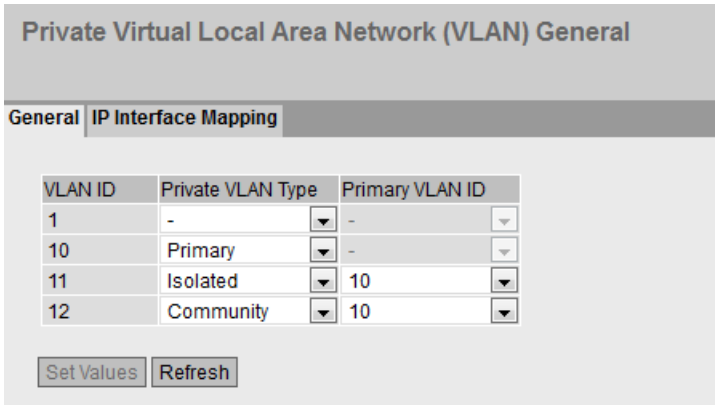
1. In the row of the port to be configured, click on the relevant cell in the table to configure it.
2. Enter the values to be set in the input boxes as follows.
3. Select the values to be set from the drop-down lists.
4. Click the "Set Values" button.

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.



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

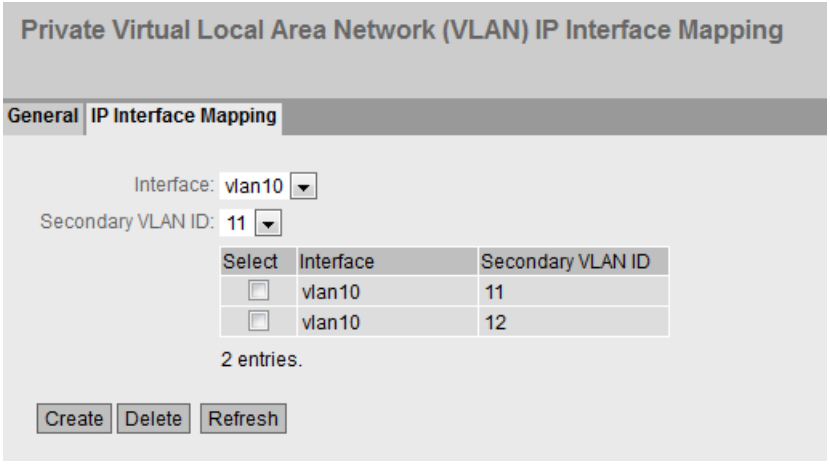
Private VLAN configuration page

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.



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.

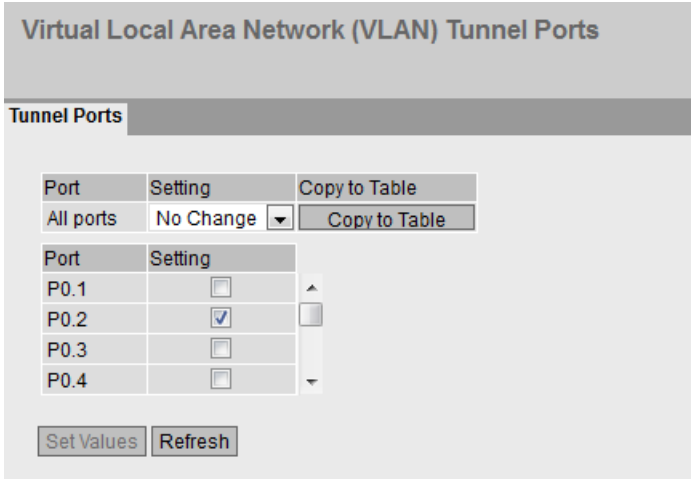
3. Select a secondary VLAN ID.
4. Click the "Create" button.

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.



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 or disable the mirroring function and make the basic settings.

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.

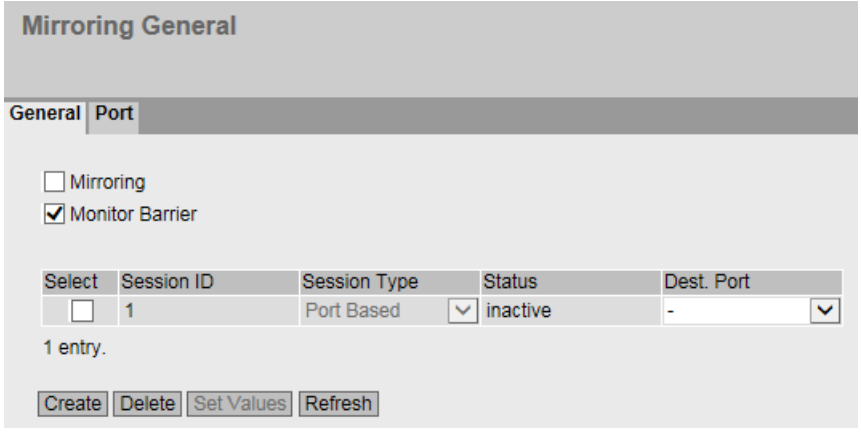
Note the data rate

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.

Several source ports from the same VLAN

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.

Settings



The page contains the following boxes:

- **Mirroring**
  Click this check box to enable or disable mirroring.

  Note

  You need to disable port mirroring if you want to connect a normal end device to the monitor port.

- **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.

  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 configure these functions manually even if monitor barrier is turned on. The data traffic on the monitor port is 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. You can create precisely one session.
- **Session Type**
  Shows the type of mirroring session.
- **Status**
  Shows whether or not mirroring is enabled.
- **Dest. Port**
  From the drop-down list, select the output port to which data will be mirrored in this session.

Procedure

Creating a mirroring session

1. Activate mirroring.
2. Click the "Create" button to create an entry in the table.
   The session ID is assigned automatically.
3. Select a destination port.
4. Click the "Set Values" button to save and activate the selected settings.
5. Change to the following tab to make further detailed settings for the session ID.

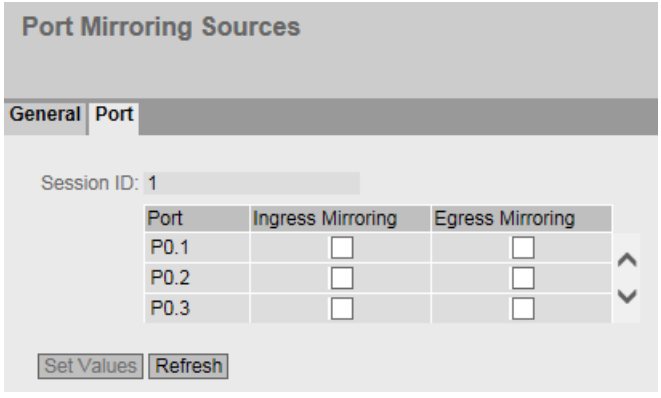
Deleting a mirroring session

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 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 boxes:

- **Session ID**
  Shows the session.
- **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.

- **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

Mirroring with ring ports

If you enable the mirroring function for a ring port, the ring port sends test frames even in the "link down" status.

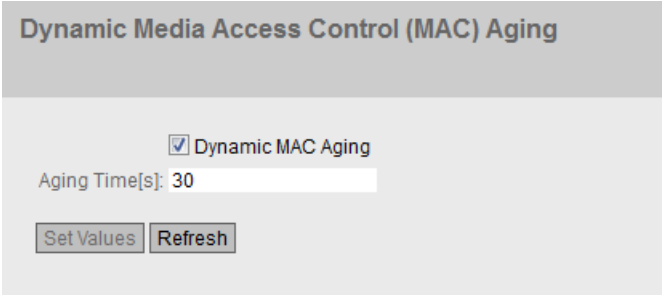
Steps in configuration

1. 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.
2. Click the "Set Values" button.

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.



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 in steps of 15. After this time, a learned address is deleted if the device does not receive any further frames from this sender address.
  Range of values: 15 - 630 (seconds)
  Factory setting: 30

Note

Rounding of the values, deviation from desired value

When you input the Aging Time, note that it is rounded to correct values. If you enter a value that cannot be divided by 15, the value is automatically rounded down.

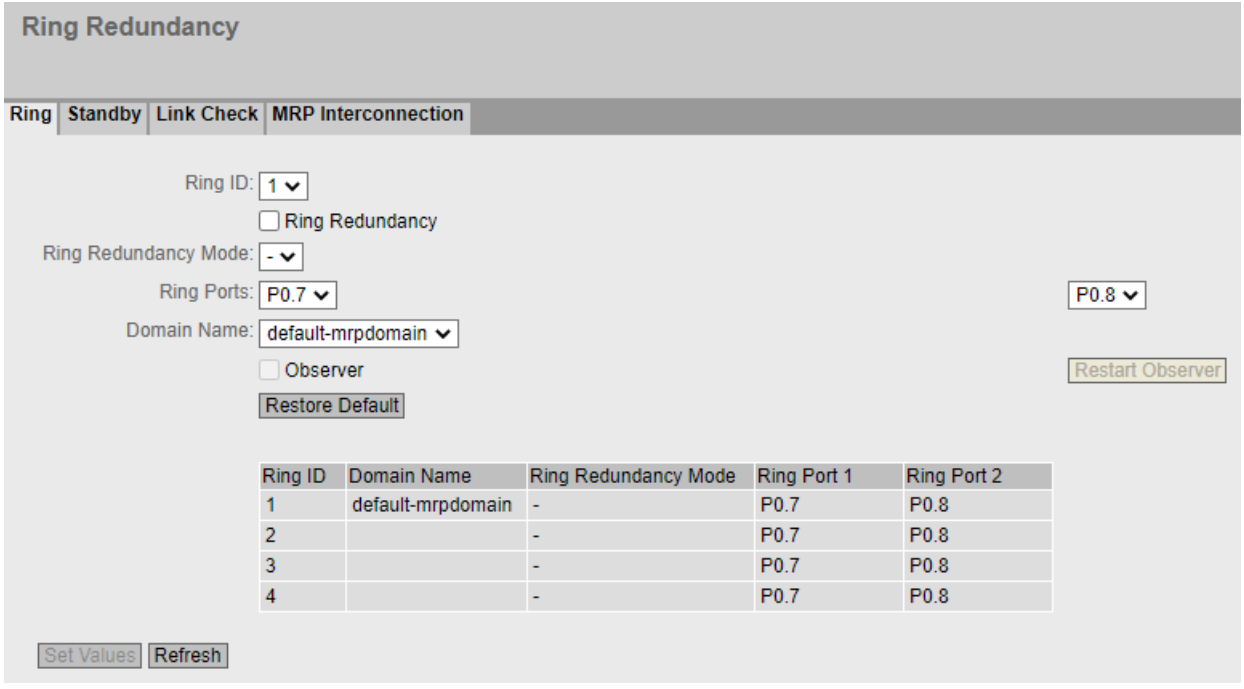
Steps in configuration

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

Configuration of ring redundancy



- **Ring ID**
  Select the ID of the ring you want to configure.
- **Ring Redundancy**
  If you select 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 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.

  – HRP Client
    The device adopts the HRP Client role.

  – MRP Manager
    The device adopts the role of MRP Manager. The device cannot take on the client role automatically.

  – 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.

- **Ring ports**
  Here, you set the ports to be used as ring ports in ring redundancy.

  Note

  Agent VLAN ID of the ring ports

  You need to configure the Agent VLAN ID for the ring ports. You can therefore configure a VLAN ID in the value range between 1 and 4094 also for the ring ports.

  The ring port you select in the left-hand drop-down list is the "Isolated Port" in HRP.
  The factory setting defines the following ring ports:

Devices	Factory setting ring ports
SCALANCE XB208 SCALANCE XB216	P0.1 and P0.2
SCALANCE XB205-3	P0.7 and P0.8
SCALANCE XB206-2	P0.7 and P0.8
SCALANCE XB213-3	P0.15 and P0.16
SCALANCE XC206-2G PoE SCALANCE XC206-2G PoE EEC SCALANCE XC206-2SFP SCALANCE XC206-2SFP G SCALANCE XC206-2SFP EEC SCALANCE XC206-2SFP G EEC SCALANCE XC208 SCALANCE XC208G SCALANCE XC208EEC SCALANCE XC208G EEC SCALANCE XC208G PoE SCALANCE XC216 SCALANCE XC216EEC SCALANCE XC216-4C SCALANCE XC216-4C G SCALANCE XC216-4C G EEC SCALANCE XC224 SCALANCE XC224-4C G SCALANCE XC224-4C G EEC	P0.1 and P0.2
SCALANCE XC216-3G PoE	P0.4 and P0.5
SCALANCE XC206-2	P0.7 and P0.8
SCALANCE XF-200BA	P1.1 and P2.1
SCALANCE XF204G	P0.1 and P0.2
SCALANCE XP208 SCALANCE XP208G	P0.1 and P0.2
SCALANCE XP216	P0.10 and P0.12

Devices	Factory setting ring ports
SCALANCE XR324WG SCALANCE XR328-4C WG (GE)	P0.1 and P0.2
SCALANCE XR326-2C PoE WG SCALANCE XR328-4C WG	P0.25 and P0.26

Port groups for devices with more than 8 ports

The ring ports of an MRP ring should belong to the same logical port group.

XB-200

Device	Article number	Port group
SCALANCE XB216	6GK5 216-0BA00-2AB2 6GK5 216-0BA00-2TB2	**Group 1** Port 1 ... Port 8 **Group 2** Port 9 ... Port 16
SCALANCE XB213-3 (SC)	6GK5 213-3BD00-2AB2 6GK5 213-3BD00-2TB2	
SCALANCE XB213-3 (ST/BFOC)	6GK5 213-3BB00-2AB2 6GK5 213-3BB00-2TB2	
SCALANCE XB213-3LD	6GK5 213-3BF00-2AB2 6GK5 213-3BF00-2TB2	

XC-200

Device	Article number	Port group
SCALANCE XC216	6GK5 216-0BA00-2AC2	**Group 1** Port 1 ... Port 4 Port 9 ... Port 12 **Group 2** Port 5 ... Port 8 Port 13 ... Port 16
SCALANCE XC216 EEC	6GK5 216-0BA00-2FC2	
SCALANCE XC224	6GK5 224-0BA00-2AC2	**Group 1** Port 1 ... Port 8 **Group 2** Port 9 ... Port 12 Port 17 ... Port 20 **Group 3** Port 13 ... Port 16 Port 21 ... Port 24

XP-200

Device	Article number	Port group
SCALANCE XP216	6GK5 216-0HA00-2AS6	**Group 1**
SCALANCE XP216	6GK5 216-0HA00-2TS6	Port 1 ... Port 5, Port 7
SCALANCE XP216 EEC	6GK5 216-0HA00-2ES6	**Group 2**
SCALANCE XP216 PoE EEC	6GK5 216-0UA00-5ES6	Port 6, Port 8, Port 9, Port 11, Port 13, Port 15
		Group 3
		Port 10, Port 12
		Port 14, Port 16

XR-300WG

Device	Article number	Port group
SCALANCE XR324WG	6GK5 324-0BA00-2AR3	**Group 1**
SCALANCE XR324WG	6GK5 324-0BA00-3AR3	Port 1 ... Port 4
		Port 13 ... Port 16
		Group 2
		Port 5 ... Port 8
		Port 17 ... Port 20
		Group 3
		Port 9 ... Port 12
		Port 21 ... Port 24
SCALANCE XR328-4C WG	6GK5 328-4FS00-2AR3	**Group 1**
SCALANCE XR328-4C WG	6GK5 328-4FS00-2RR3	Port 1 ... Port 4
SCALANCE XR328-4C WG	6GK5 328-4FS00-3AR3	Port 13 ... Port 16
SCALANCE XR328-4C WG	6GK5 328-4FS00-3RR3	**Group 2**
SCALANCE XR328-4C WG	6GK5 328-4SS00-2AR3	Port 5 ... Port 8
SCALANCE XR328-4C WG	6GK5 328-4SS00-3AR3	Port 17 ... Port 20
		Group 3
		Port 9 ... Port 12
		Port 21 ... Port 24
		Group 4
		Port 25 ... Port 28

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. For SIMATIC S7-1500R:
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. For information on which IE switches can be used as H-Sync forwarder, refer to the section "System functions and hardware equipment".
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

- **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 list 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.
- **DNA Redundancy**
  Enable/disable DNA redundancy. You can only enable DNA redundancy when the following requirements are met:

  – Ring redundancy is enabled.

  – "MRP Manager" or "MRP Client" is configured as Ring Redundancy Mode.
  DNA redundancy is only possible with MRP.

Note

You can find a detailed step-by-step description of the configuration of DNA redundancy in the section "Technical basics → Redundancy mechanism → Dual Network Access redundancy (DNA redundancy)".

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.

Configuration procedure

1. Select the "Ring Redundancy" check box.
2. Select the redundancy mode.
3. Specify the ring ports.
4. Click the "Set Values" button.

Restoring factory settings

EtherNet/IP / Industrial Ethernet variants

If you have restored the factory defaults, ring redundancy is disabled and the ring port settings are reset. Spanning Tree is enabled.

PROFINET variants

If you have restored the factory defaults, ring redundancy is enabled. If you reset to the factory settings, the ring port settings are also reset. If you used other ports previously as ring ports before resetting, a previously correctly configured device can cause circulating frames and therefore the failure of the data traffic.

Changing over the status of the ring ports with the redundancy manager (HRP)

If you configure a redundancy manager, set the status of the ring ports. 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

Note

Changing ring ports on the SCALANCE XF200-BA DNA

To change the preconfigured ring ports, disable DNA redundancy first.

To change the ring ports, follow the steps below:

1. Open the ring.
2. Select the new ring ports.
3. Change the cable connections.
4. Close the ring.

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.

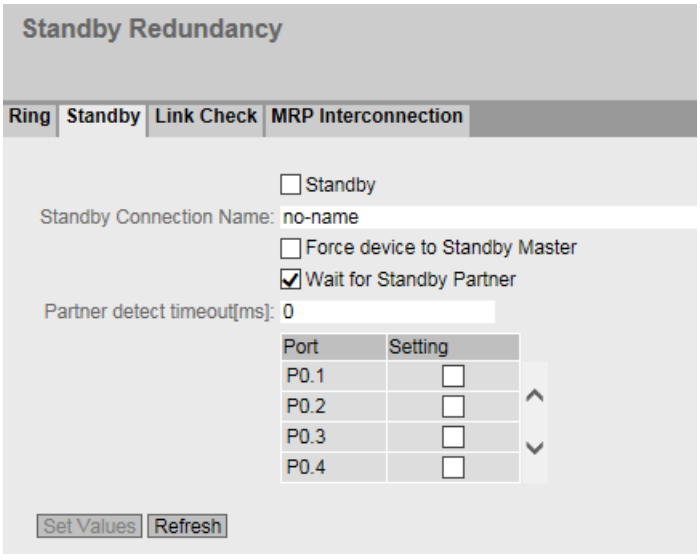
For the "Standby Connection Name", a name unique within the ring must be assigned for both partners. This identifies the two modules that belong together as standby partners.

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.



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 Link Check

Requirements

Note

Changing the media type with a combo port: Optical → electrical

If Link Check is active for a combo port with the media type "SFP" and you want to enable the "RJ45" media type, disable Link Check first.

- You cannot enable Link Check on ports with 10 Gbps.
- You can only enable the Link Check function with optical ring ports of an HRP or MRP ring.
- Link Check must be enabled on two neighboring devices (connection partners) within an HRP or MRP ring.
- The ring ports on which you enable Link Check must be connected.
- Link Check is not available with multiple rings. Link Check can only be enabled in rings with ID 1 if no other ring is active.

Monitoring optical connections in the ring

With the Link Check function, you can monitor the transmission quality of optical sections within an HRP or MRP ring, identify disturbed connections and under certain conditions turn them off. When the disturbed section is turned off, the redundancy manager can close the ring and restore communication.

NOTICE
Make sure that the frames used by Link Check for monitoring the optical connections are not supplanted by an overload of high-priority frames in the network. An overload of high priority frames can be caused by the following, for example: • Network loops that can cause duplication of the high-priority frames • Changing the priorities for forwarding frames

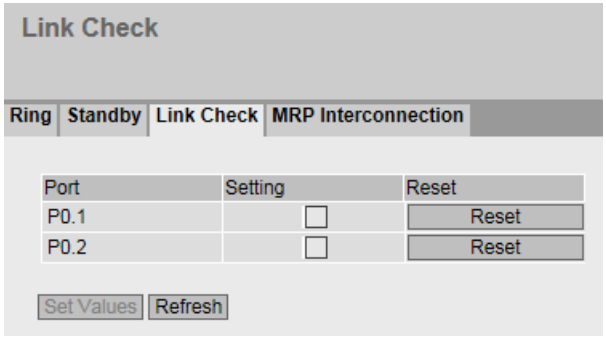
Note

Do not enable Link Check on only one of two connection partners. This can lead to incorrect behavior.

Note

If Link Check is enabled on all devices of a ring at the same time, and several connections within the ring have problems, this leads to fragmentation of the ring.

1. During commissioning enable the Link Check function for one connection section after the other by enabling Link Check for the two connection partners connected to a line.
2. To ensure an error-free connection, wait 1 min. before you enable Link Check for the next connection.



Description of the displayed boxes

The table contains 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**
  With this check box, you enable or disable the Link Check function for a port.
  When connection monitoring is enabled, you can see the number of sent and received Link Check test frames on the "Information > Redundancy > Link Check" page.
- **Reset**
  After resetting Link Check, the function is restarted on the port and the statistics are reset. If you use the "Reset" button, the reset must be performed on both connection partners within 30 s.

Note

When you use the "Reset" button, loops can form temporarily resulting in a loss of data traffic. The loop is automatically cleared again.

If this is not acceptable for your application, reset Link Check by pulling the cable and plugging it in again.

Configuration procedure

Enabling Link Check

Follow the steps below to activate the monitoring of a ring port:

1. Select the appropriate check box in the "Setting" column.
2. Click the "Set Values" button.

Disabling Link Check

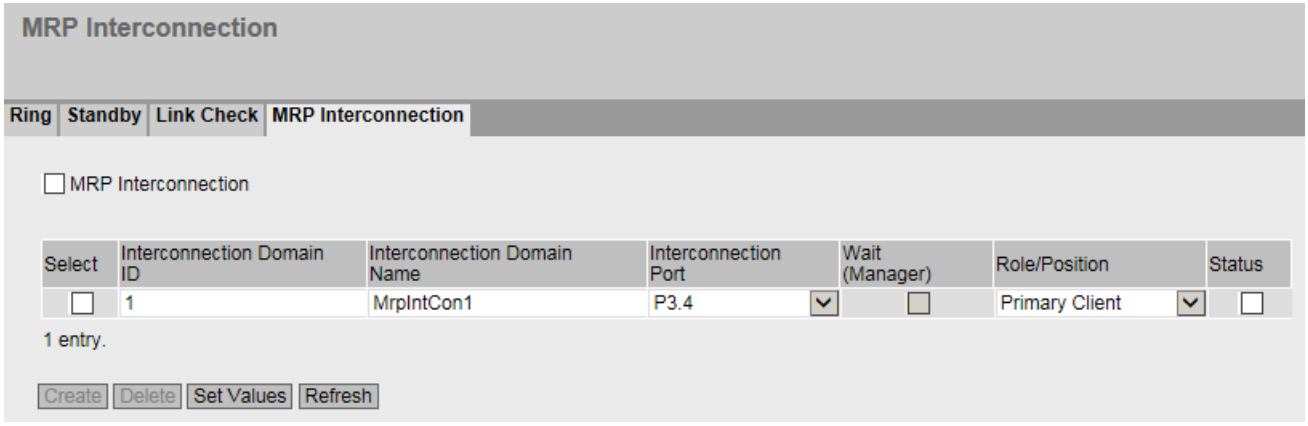
Follow the steps below to deactivate the monitoring of a ring port:

1. Deactivate the appropriate check box in the "Setting" column.
2. Click the "Set Values" button.

6.5.9.4 MRP-Interconnection

Redundant linking of rings

On this page, you create, delete and configure MRP Interconnection connections.



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.
  - The following maximum values are in effect for the number of enabled MRP interconnections:
    SCALANCE XC-200, SCALANCE XC-300, SCALANCE XF-200BA, SCALANCE XP-200, SCALANCE XM-400 and SCALANCE XR-500
    Two connections
    SCALANCE XB-200 and SCALANCE XR-300WG
    One connection

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.
4. 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.

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

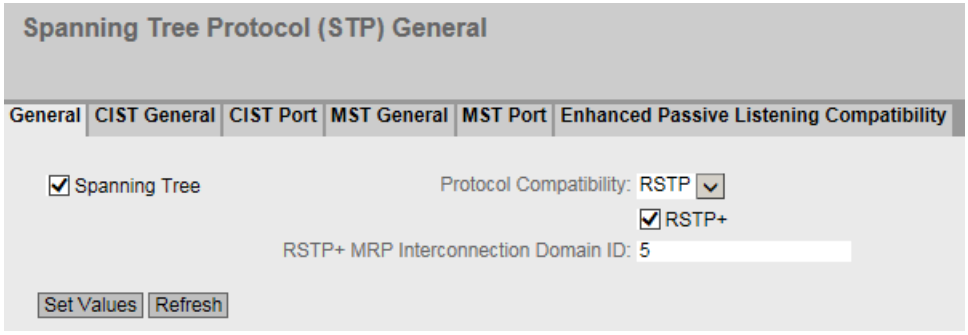
6.5.10.1 General

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.



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 324)" 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

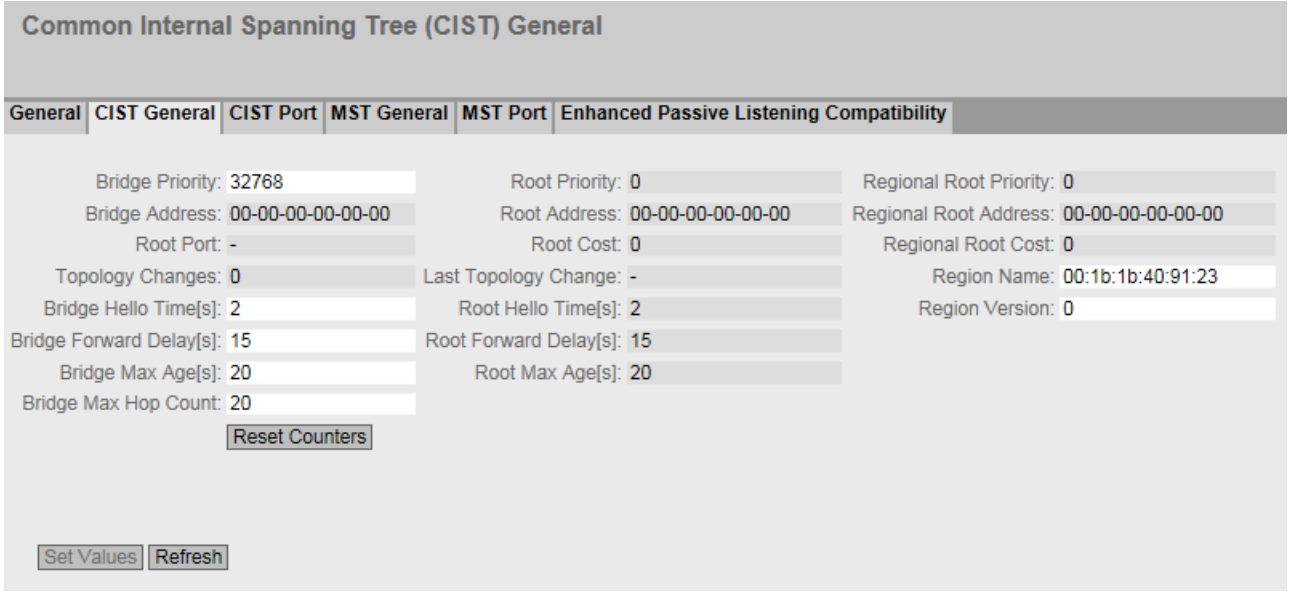
1. Select the "Spanning Tree" check box.
2. From the "Protocol Compatibility" drop-down list, select the type of compatibility.
3. Click the "Set Values" button.

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.



Description

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.

- **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

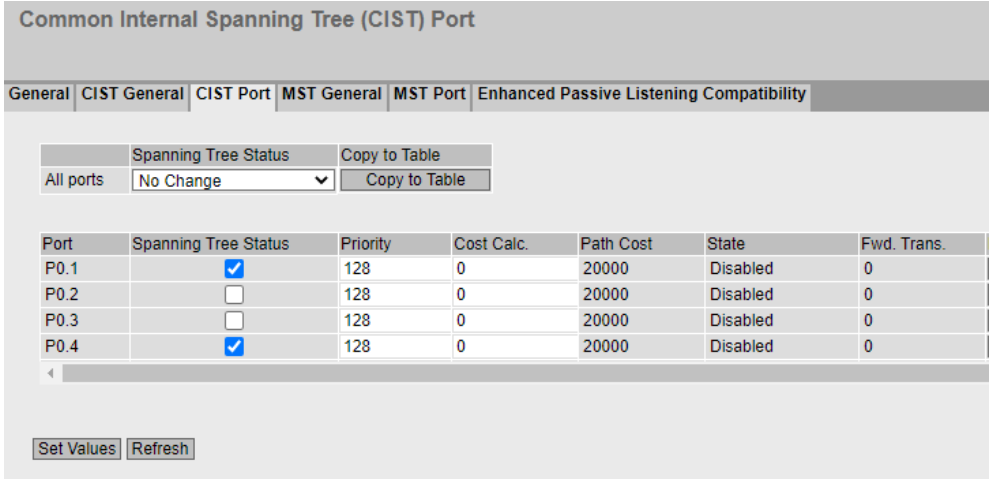
1. Enter the data required for the configuration in the input boxes.
2. Click the "Set Values" button.

6.5.10.3 CIST Port

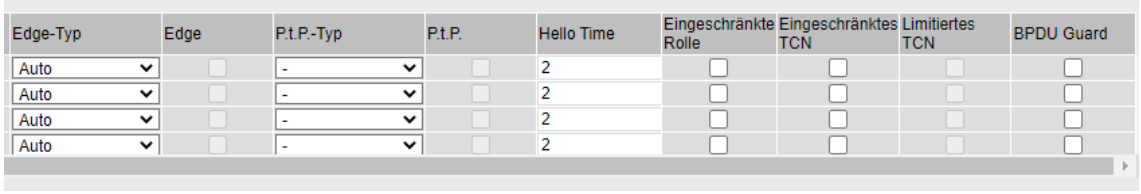
MSTP-CIST port configuration

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.



(Continuation of table)



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.

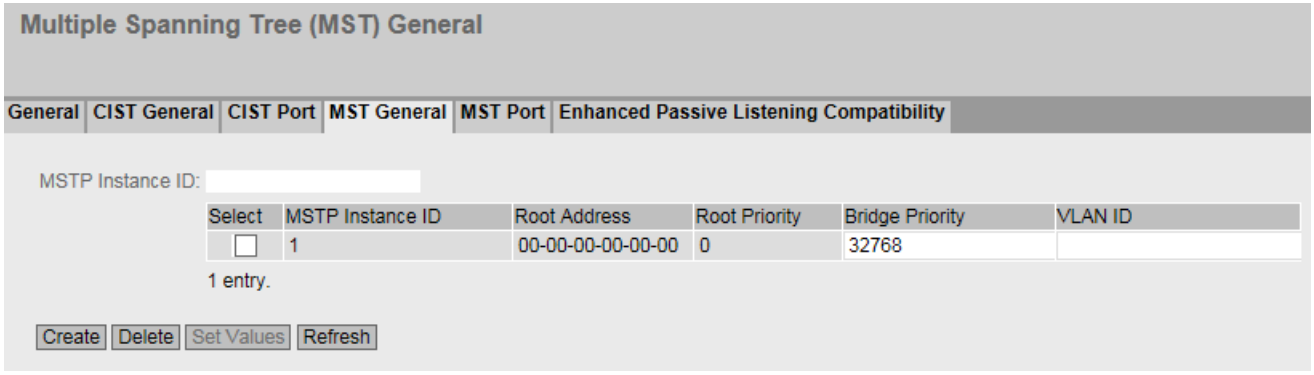
Configuration procedure

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.



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.

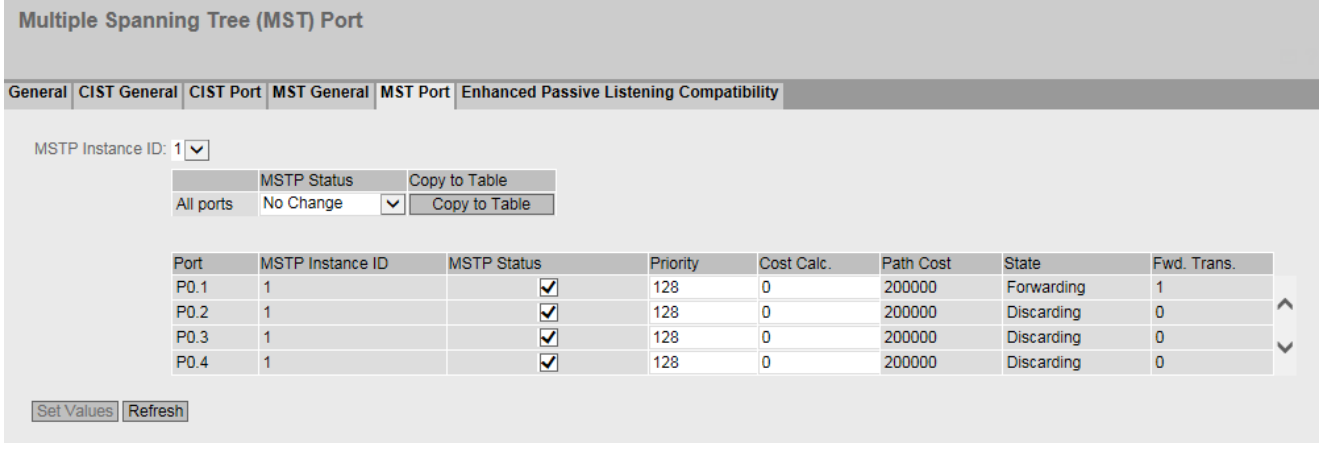
Deleting entries

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.



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 = 2,000,000

  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 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.

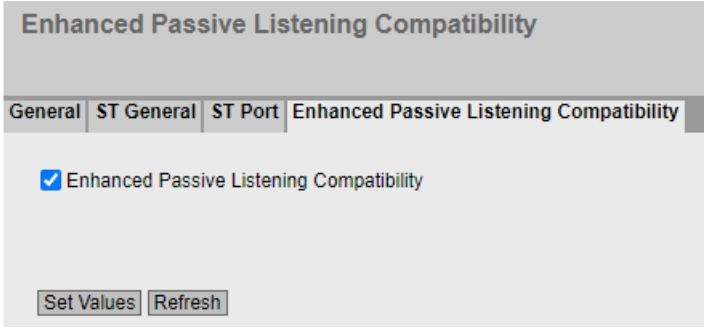
6.5.10.6 Enhanced Passive Listening Compatibility

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 will be sent via edge ports; this is, however, necessary for the passive listening function on ring nodes.

Enabling the function

On this page, you can enable the "Enhanced Passive Listening Compatibility" function.



Description of the displayed boxes

The page contains the following box:

- **Enhanced Passive Listening Compatibility**
  Enable or disable this function for the entire device.

Steps in configuration

1. Enable or disable "Enhanced Passive Listening Compatibility"
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".

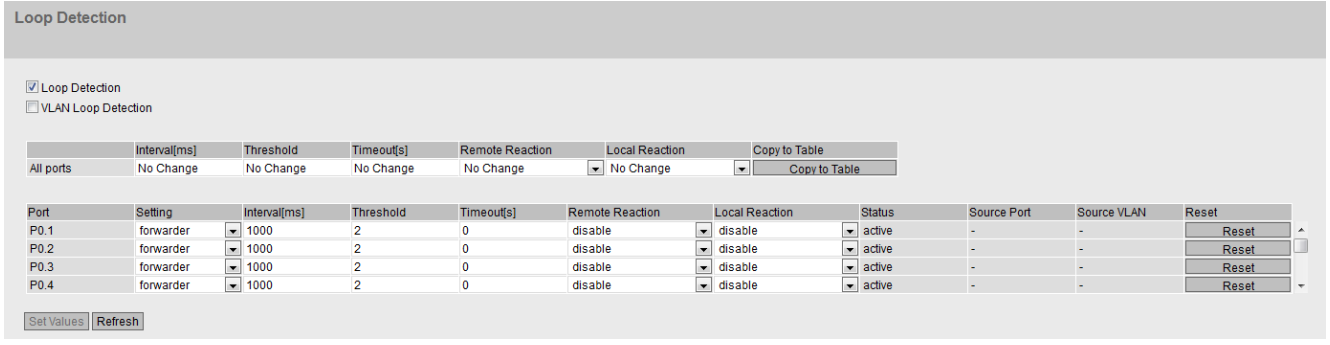
Note

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



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 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 correctly to a partner device, the Link Aggregation Control Protocol (LACP) from the IEEE 802.3AD standard is used.

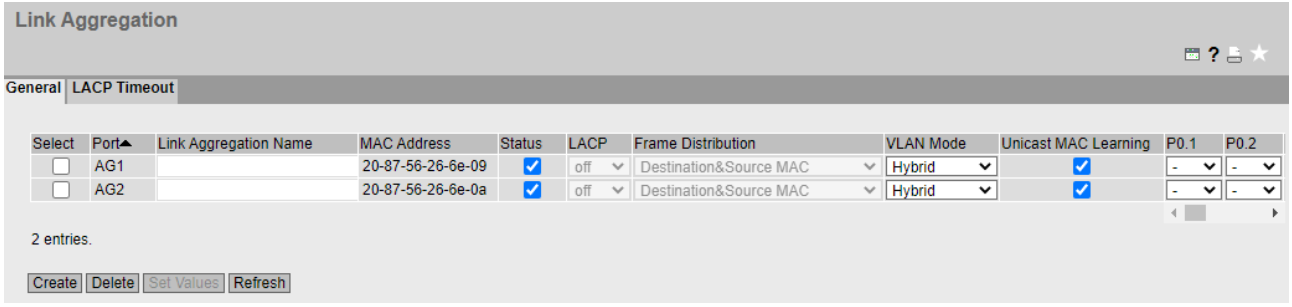
Note

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

This page displays all the configured link aggregations.



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.
- **Status**
  Enable or disable the link aggregation.

- **LACP**
  - On
    Enables the sending of LACP frames.
  - Off
    Disables the sending of LACP frames.
- **Frame Distribution** - Destination&Source MAC
  The distribution of packets to the individual links of a aggregation is based on a combination of the destination and source MAC address.
- **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.
- **Port**
  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".

Steps in configuration

Basics prior to configuration

1. First, identify the ports you want to connect 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 a link aggregation

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.

Changing a link aggregation

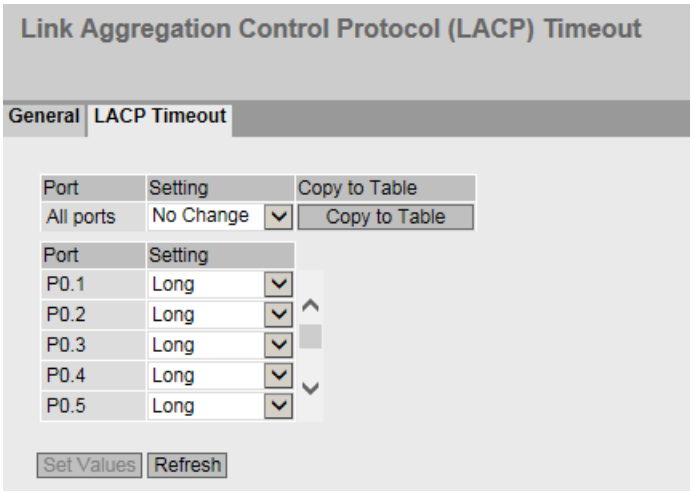
1. In the overview, click on the relevant table entry to change the configuration of a created link aggregation.
2. Make all the changes.
3. Click the "Set Values" button.

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 LACPDUs 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.



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

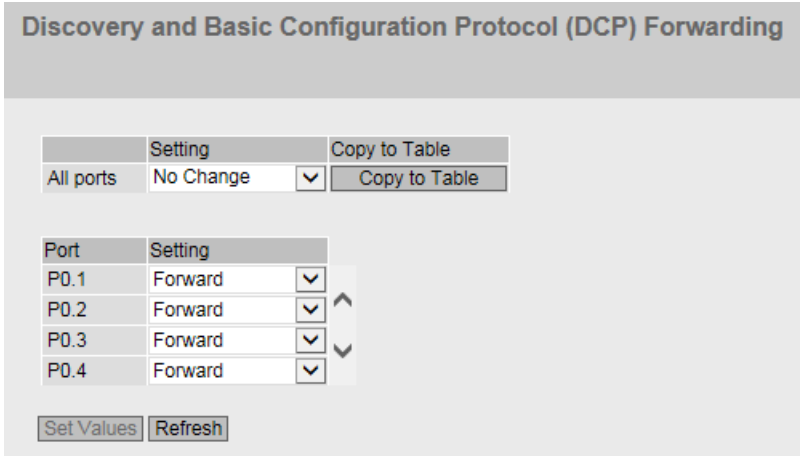
The DCP protocol is used by STEP 7 and SINEC PNI for configuration and diagnostics. When shipped, DCP is enabled on all ports; in other words, DCP frames are forwarded at all ports. With this option, you can disable the forwarding of the frames for individual ports, for example to exclude individual 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.



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

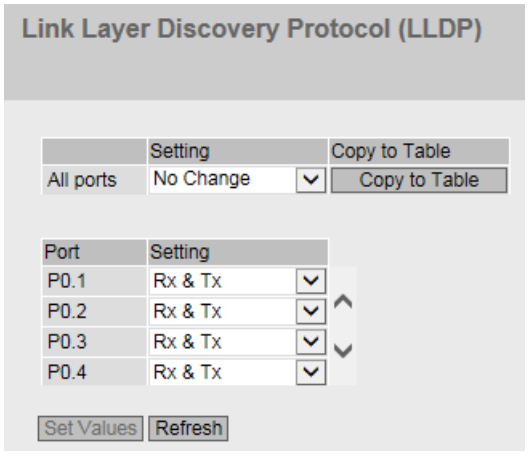
LLDP (Link Layer Discovery Protocol) is defined in the IEEE 802.1AB standard.

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.
- **Settting**
  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.

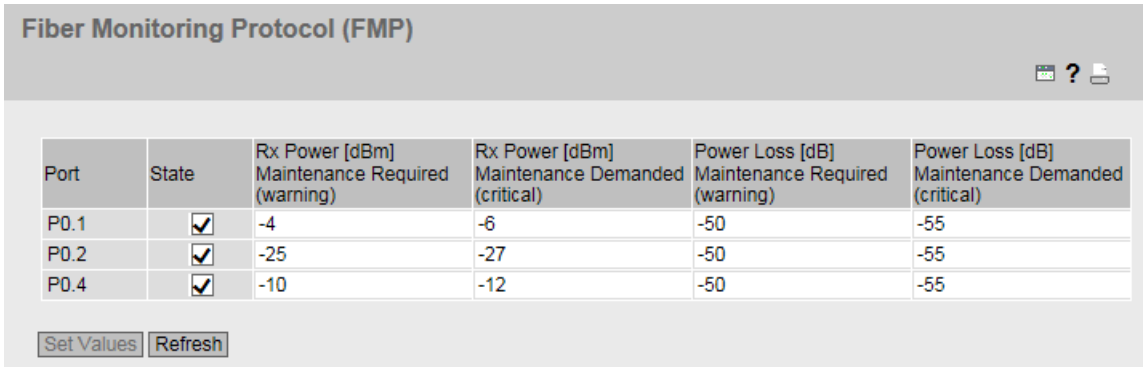
If Fiber Monitoring is enabled on the connection partner, the connection partner transfers the current value for the transmit power of the port to the device. The device compares the value it has received for the transmit power with the actually received power. The difference between the receive power 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.



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

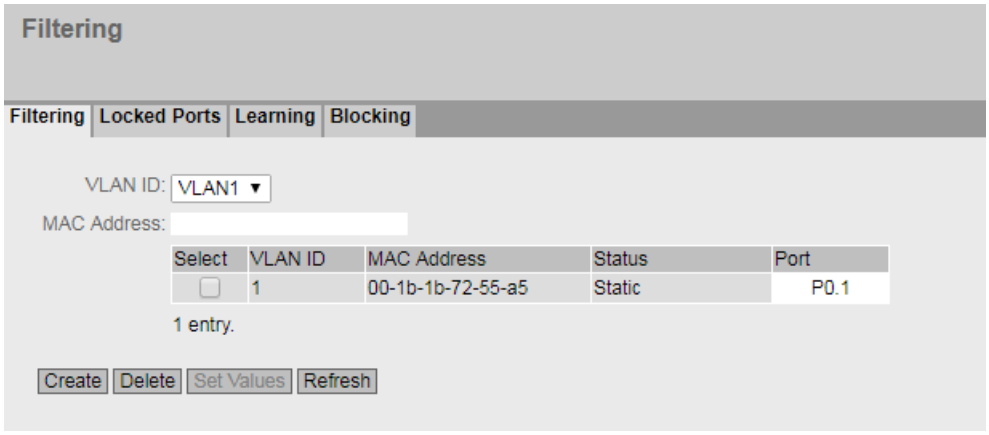
This table shows the source addresses of unicast address frames entered statically by the user during parameter assignment.

On this page, you also define the static unicast filters.

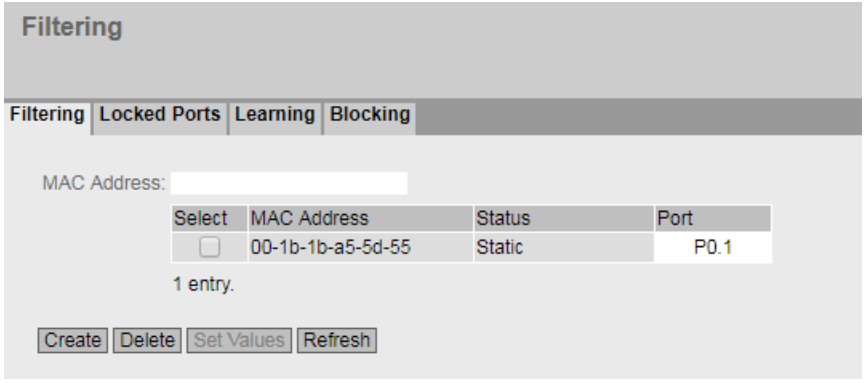
Dependency on the "Base bridge mode"

The displayed boxes depend on which "Base bridge mode" is set. If you change the "Base bridge mode" the existing entries are lost. The following figures show the different contents of the WBM page for the two operating modes "802.1Q VLAN Bridge" and "802.1D Transparent Bridge".

Base bridge mode: 802.1Q VLAN Bridge



Base bridge mode: 802.1D Transparent Bridge



Description of the displayed boxes

The page can contain the following boxes:

- **VLAN ID**
  Select the VLAN ID for 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.

The 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** - 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**
  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.

Configuration procedure

To edit the entries, follow the steps below.

Creating a new entry

1. In "Base bridge mode: 802.1Q VLAN Bridge" select the appropriate 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. Click the "Refresh" button.
5. Select the relevant port from the drop-down list.
6. 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.

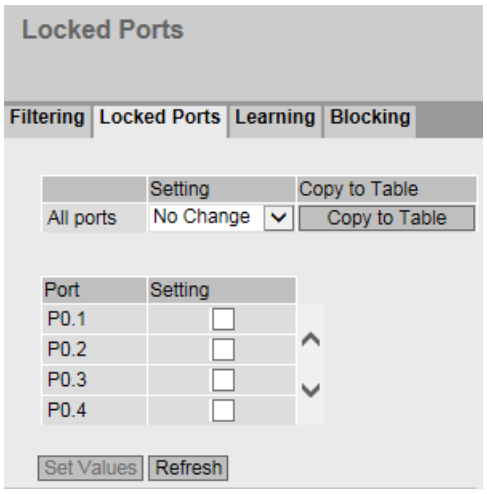
6.5.16.2 Locked Ports

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.

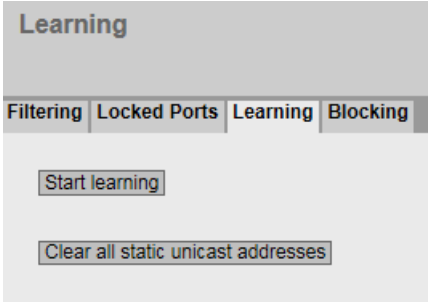
6.5.16.3 Learning

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.

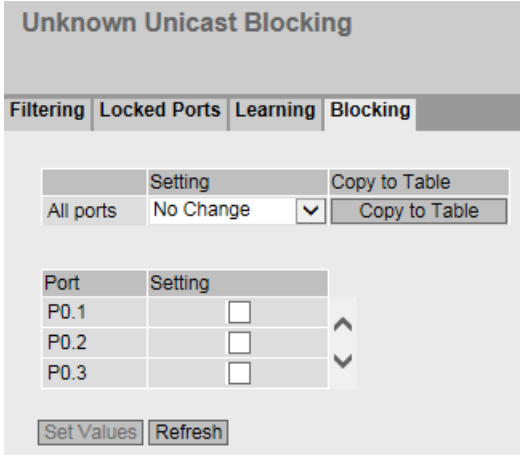
   Note

   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. The following options are available for 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 parameter assignment frames (IGMP Configuration).
- Active dynamic assignment of addresses by GMRP frames.

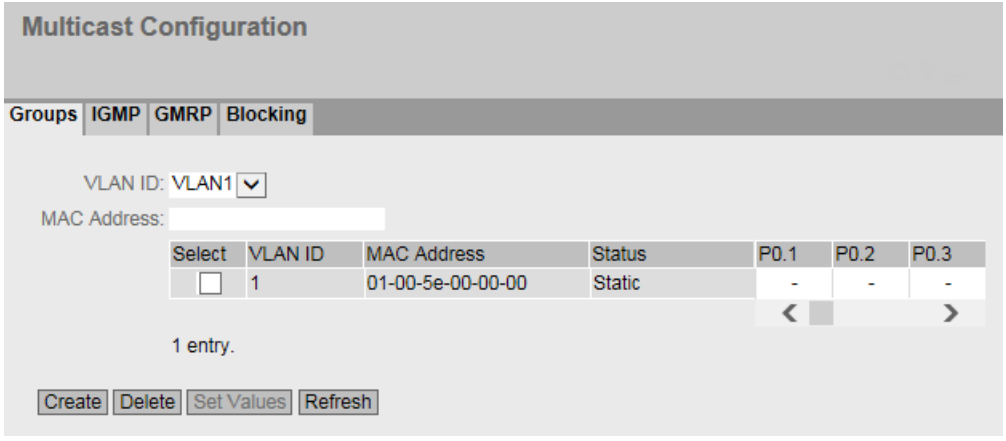
The result of all these methods is that multicast frames are sent only to ports for which an appropriate address is entered.

The "Multicast" menu item, shows the multicast frames currently entered in the filter table and their destination ports that the user set in the parameters.

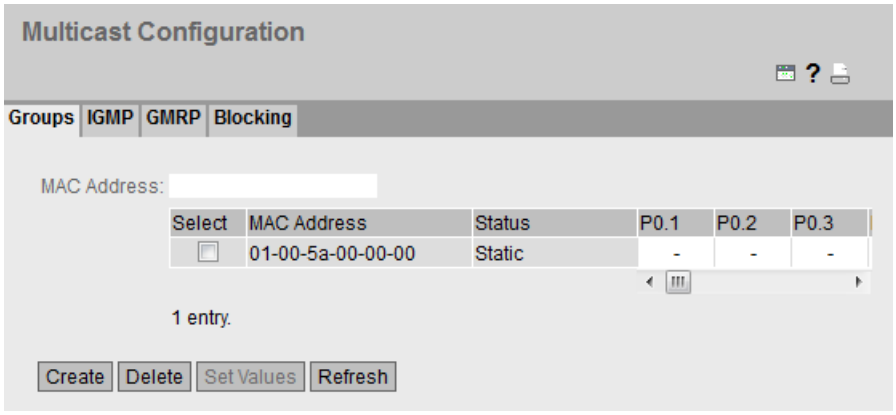
Dependency on the "Base bridge mode"

The displayed boxes depend on which "Base bridge mode" is set. If you change the "Base bridge mode" the existing entries are lost. The following figures show the different contents of the WBM page for the two operating modes "802.1Q VLAN Bridge" and "802.1D Transparent Bridge".

Base bridge mode: 802.1Q VLAN Bridge



Base bridge mode: 802.1D transparent bridge



Description of the displayed boxes

The page can contain 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 MAC 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 port. Within every 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.
  - I
    (IGMP) Member of the multicast group, registration was by an IGMP frame. This value is only dynamically assigned.
  - –
    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.

Configuration procedure

Creating a new entry

Note

You cannot create any static multicast entries if GMRP is enabled.

1. In "Base bridge mode: 802.1Q VLAN Bridge", select the required VLAN ID from the "VLAN ID"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.

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.

Creating layer 2 multicast addresses with a script and GMRP

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 fully completed and the layer 2 multicast addresses have been created.

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

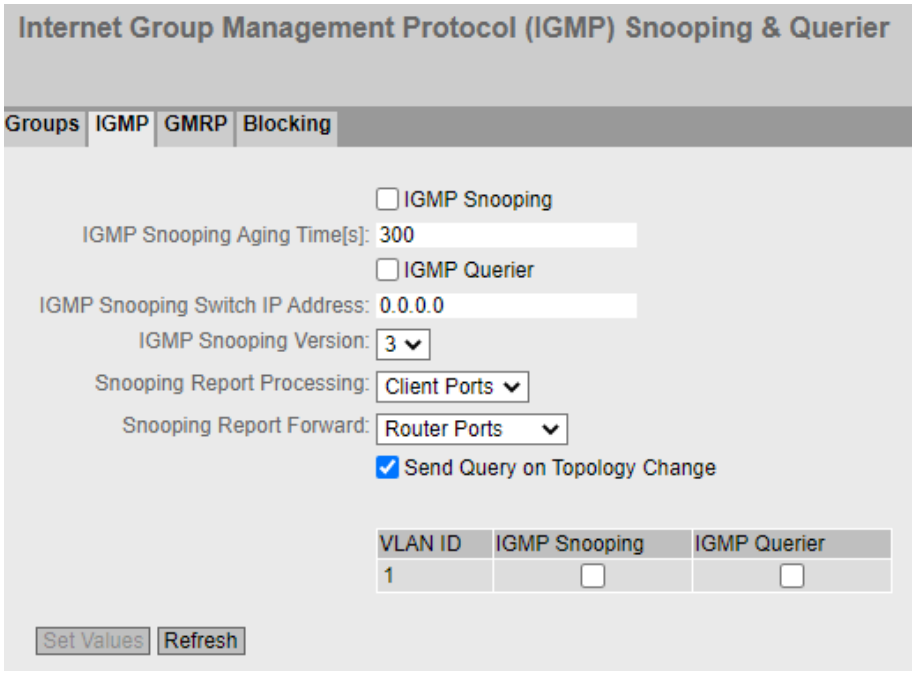
The IE switch as IGMP querier

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



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 Querier with multiple 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

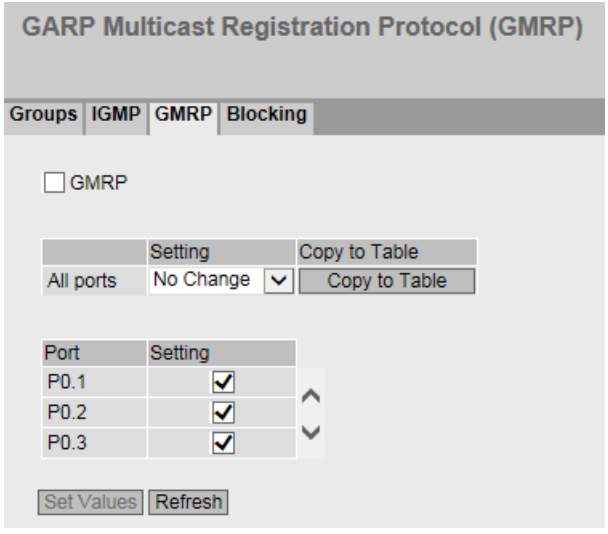
1. Clear the "IGMP Querier" check box.

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.



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**
  If 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.

Steps in configuration

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.

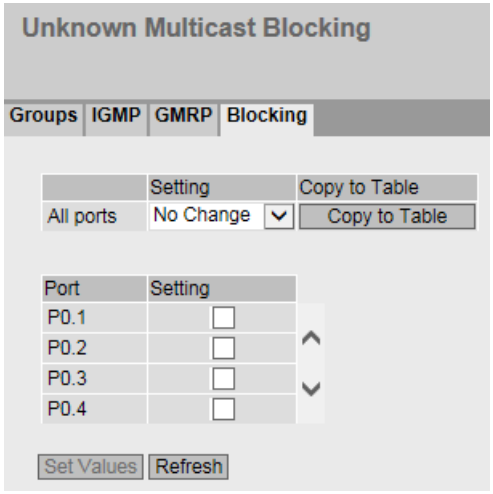
Enabling the sending of GMRP frames for all ports

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 Multicast blocking

Disabling the forwarding of unknown multicast frames

On this page, you can block the forwarding of unknown multicast 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 multicast frames is enabled.
  - Disabled
    Blocking of 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.

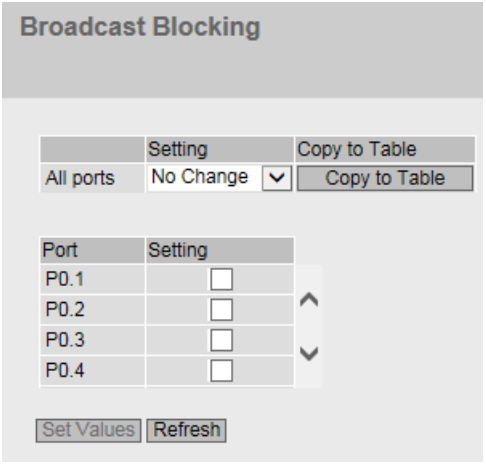
6.5.18 Broadcast

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.



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

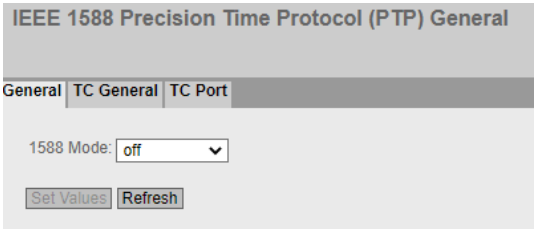
1. In the "Setting" drop-down list in table 1, select the "Enabled" entry.
2. Click the "Copy to Table" button. The check box is enabled for all ports in table 2.
3. To apply the changes, click the "Set Values" button.

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.

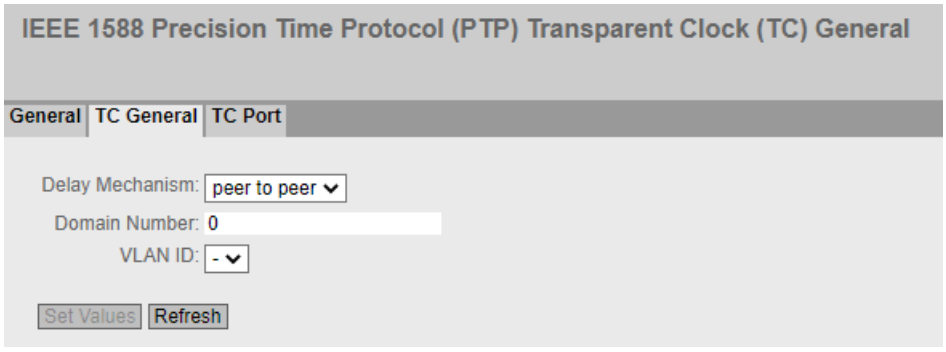
Mode 1588
You can make the following settings:

- **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.



Configuration of the IEEE 1588 transparent clock

- **Delay Mechanism**
  Specify the delay mechanism the device will work with:
  - end to end
    The delay request response mechanism will be used.

    Note

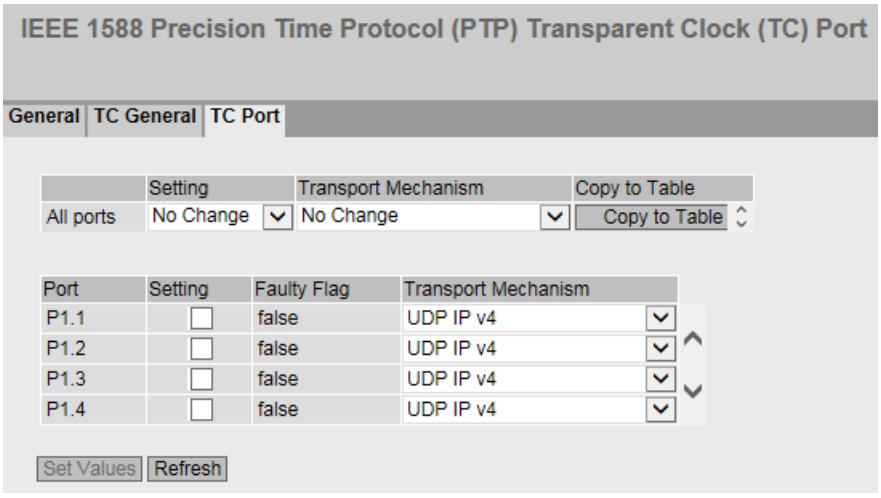
    With end-to-end synchronization with more than 2 slaves, freak values > 100 ns can occur in the offset.

  - 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.
- **VLAN ID**
  The setting option depends on the configured Base Bridge Mode ("Layer 2 Menu > VLAN > General"):
  - 802.1D Transparent Bridge
    "-" is displayed in the drop-down list because the VLAN tag does not have any effect in this mode. The device synchronizes itself in every VLAN.
  - 802.1Q VLAN Bridge
    All configured VLANs are contained in the drop-down list. 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.



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

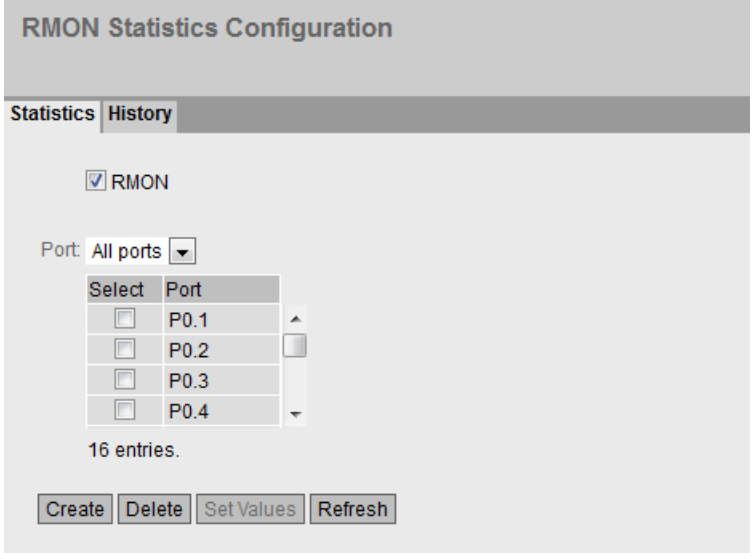
6.5.20.1 Statistics

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.

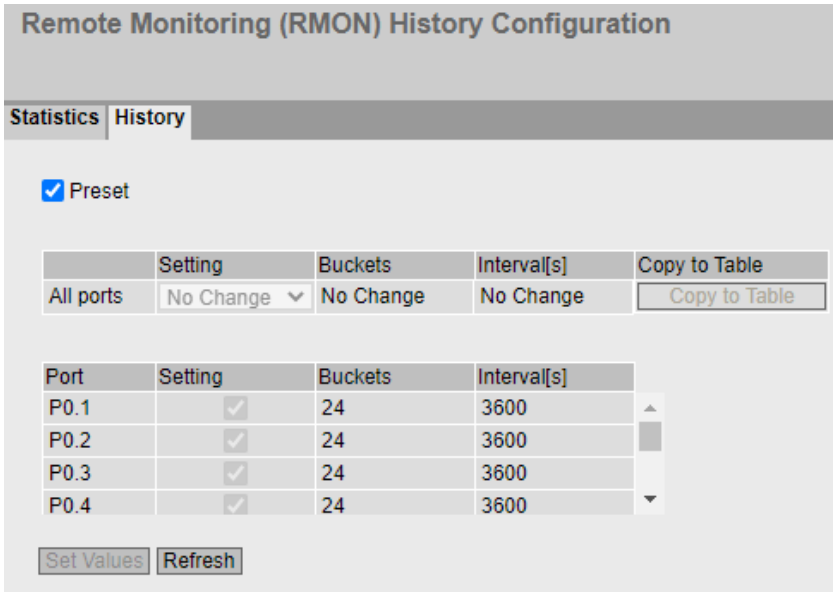
6.5.20.2 History

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.

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

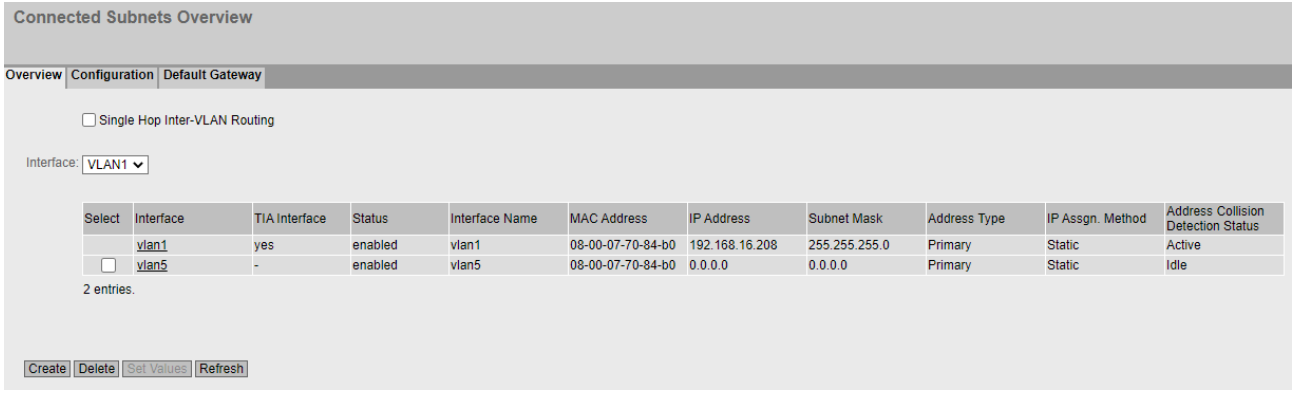
6.6.1 Subnets

6.6.1.1 Overview

Creating subnets

On this page, you can create several VLAN IP interfaces for the device.

A subnet always relates to a VLAN. The IP address is assigned in the "Configuration" tab.



Description of the displayed values

The page contains the following boxes:

- **Single-Hop Inter-VLAN-Routing**
  Enable or disable routing between local IP interfaces.
- **Interface**
  Select the interface for which you want to configure another IP subnet.

The table has the following columns:

- **Select**
  Select the row you want to delete.
- **Interface**
  Shows the interface.
- **TIA Interface**
  Shows whether 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.

- **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.

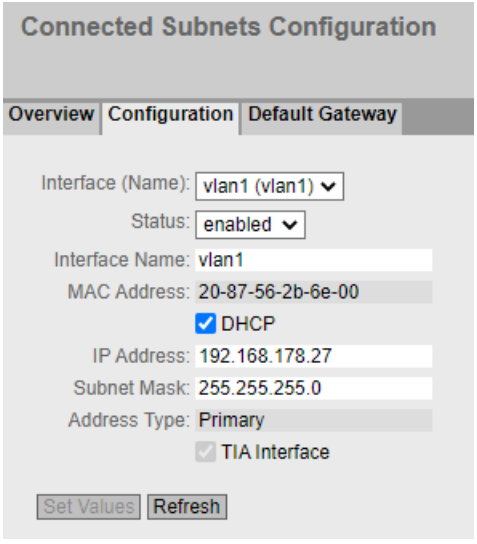
  This column shows the current status of the function. The following values are possible:
  - Idle
    The interface is not enabled and does not have an IPv4 address.
  - Starting
    This status indicates the start-up phase. In this phase, the device initially sends a query as to whether the planned 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.
  - Disabled
    The function for detection of address collisions is disabled.

Configuration procedure

1. Select the interface from the "Interface" drop-down list.
2. Click the "Create" button. A new row is inserted in the table.
3. Click the "Set Values" button.
4. Configure the subnet in the "Configuration" tab.

6.6.1.2 Configuration

On this page, you configure the IPv4 interface.



Description of the displayed values

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.
- **TIA Interface**
  Select whether or not this interface should become the TIA interface.

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.

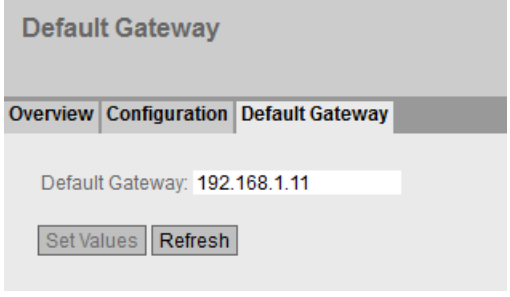
6.6.1.3 Default gateway

Creating subnets

On this page, you define the default gateway.

Note

If you configure a static IP address for the default gateway, DHCP is automatically disabled for the TIA interface. This prevents the gateway address from being overwritten by DHCP. If necessary, you can enable DHCP again subsequently.



Description of the displayed values

The page contains the following boxes:

- **Default Gateway**
  Enter the IP address of the interface that is used as the default gateway.

Steps in configuration

1. Enter the default gateway.
2. Click the "Set Values" button.

6.6.2 DHCP Relay Agent

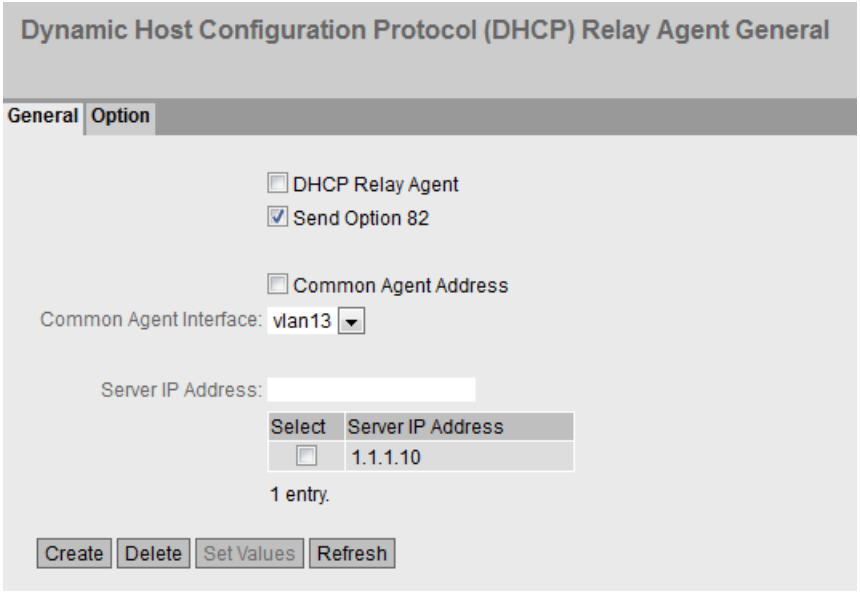
6.6.2.1 General

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.



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

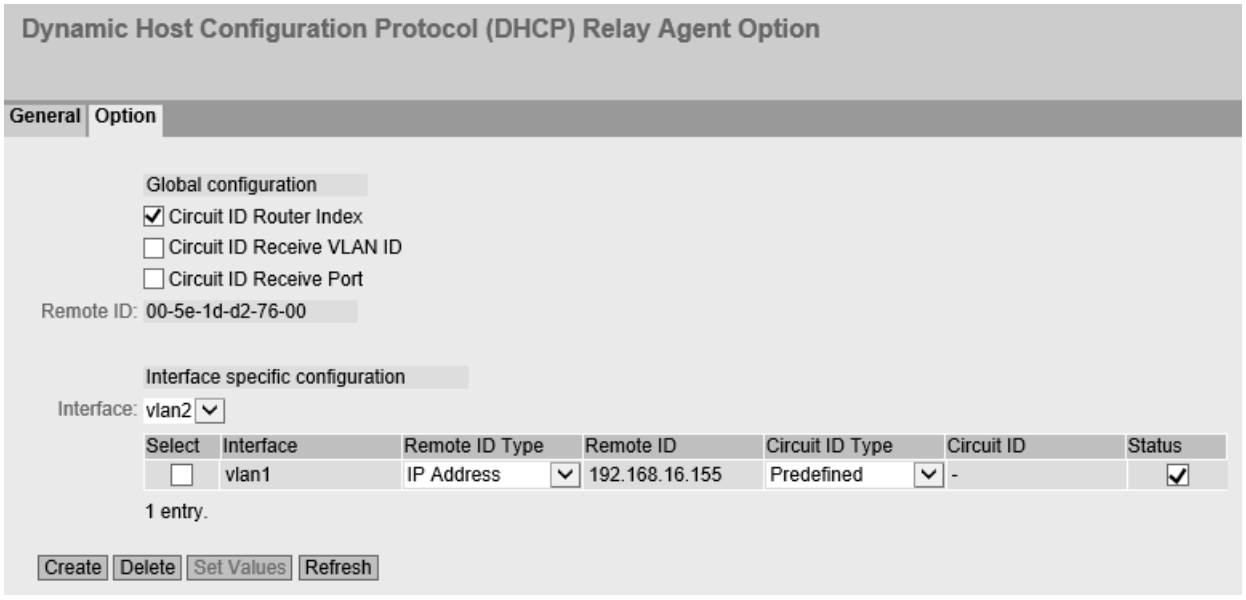
1. Enter the IPv4 address of the DHCP server in the "Server IP Address" input box.
2. Click the "Create" button. A new entry is generated in the table.
3. Select the "DHCP Relay Agent" check box.
4. Select the "Send Option 82" check box.
5. Click the "Set Values" button.

6.6.2.2 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.



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:

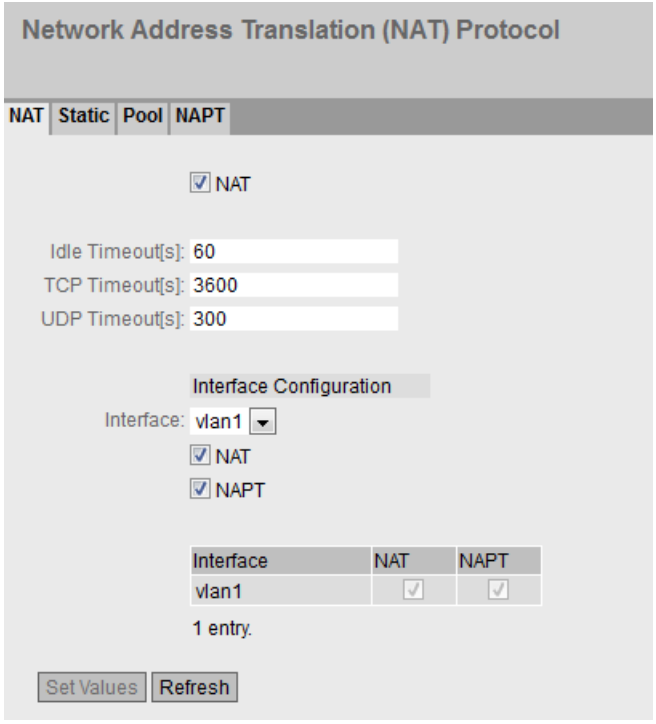
1. Enable the required option in "Global configuration".
   - Circuit ID Router Index
   - Circuit ID Receive VLAN ID
   - Circuit ID Receive Port
2. Click the "Set Values" button.
3. Select the interface from the "Interface" drop-down list.
4. Click the "Create" button. A new row is inserted in the 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.

6.6.3 NAT

6.6.3.1 NAT

On this WBM page, you specify the basic settings for NAT.



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.

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

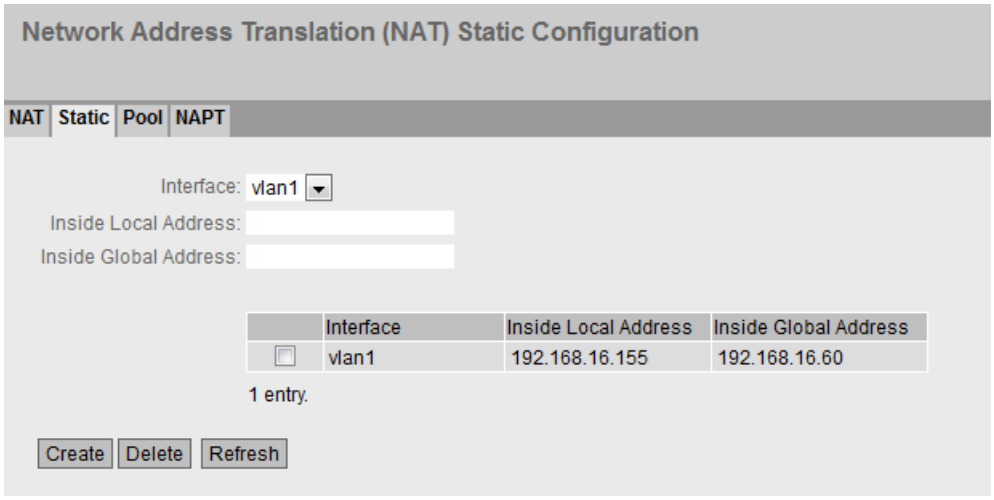
To configure NAT/NAPT, do the following:

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.



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

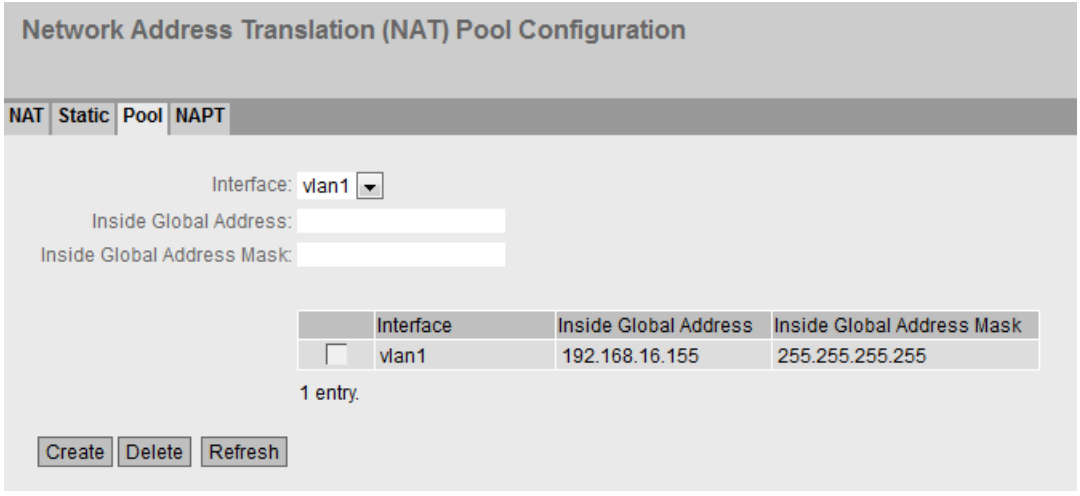
To create a 1:1 address translation, proceed as follows:

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.



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.

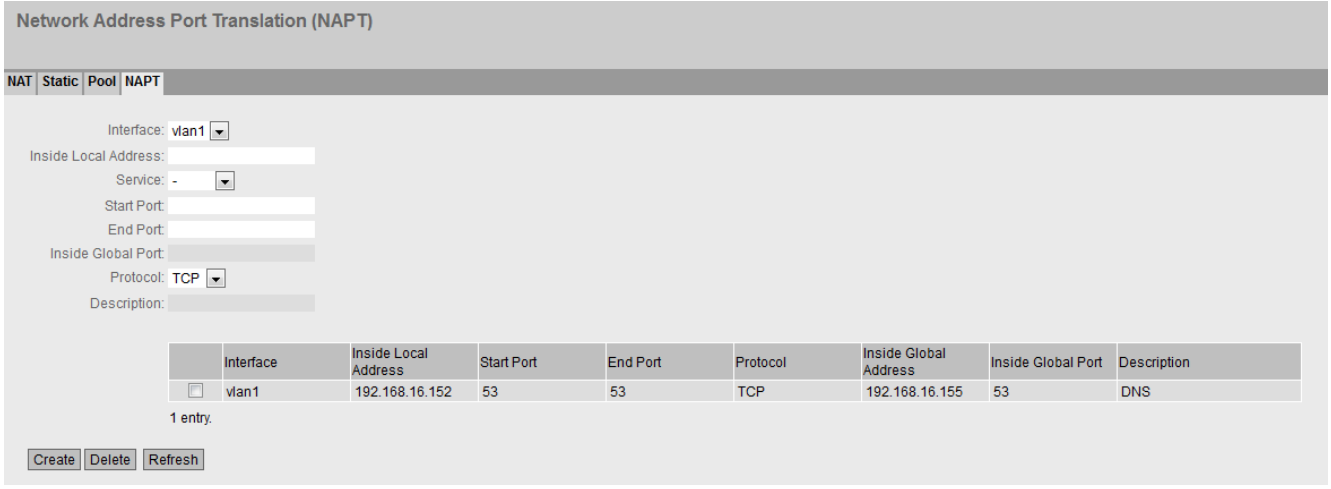
Procedure

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 NAPT

On this WBM page, you configure static port translations.



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.

6.7 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.

Note

When you transfer the configuration of a device to STEP 7 (TIA Portal), the configured users are not transferred.

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 and authorization of users by servers on which user data can be stored centrally.

A RADIUS server for industrial networks is included in the SINEC INS (Infrastructure Network Services) software tool. SINEC INS provides all services necessary for managing industrial networks, for example, RADIUS, Syslog, NTP, DHCP, TFTP, SFTP and DNS server.

The authentication of users via a RADIUS server is 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.

Assignment of a VLAN via RADIUS or guest VLAN in Base Bridge mode "802.1Q VLAN Bridge"

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

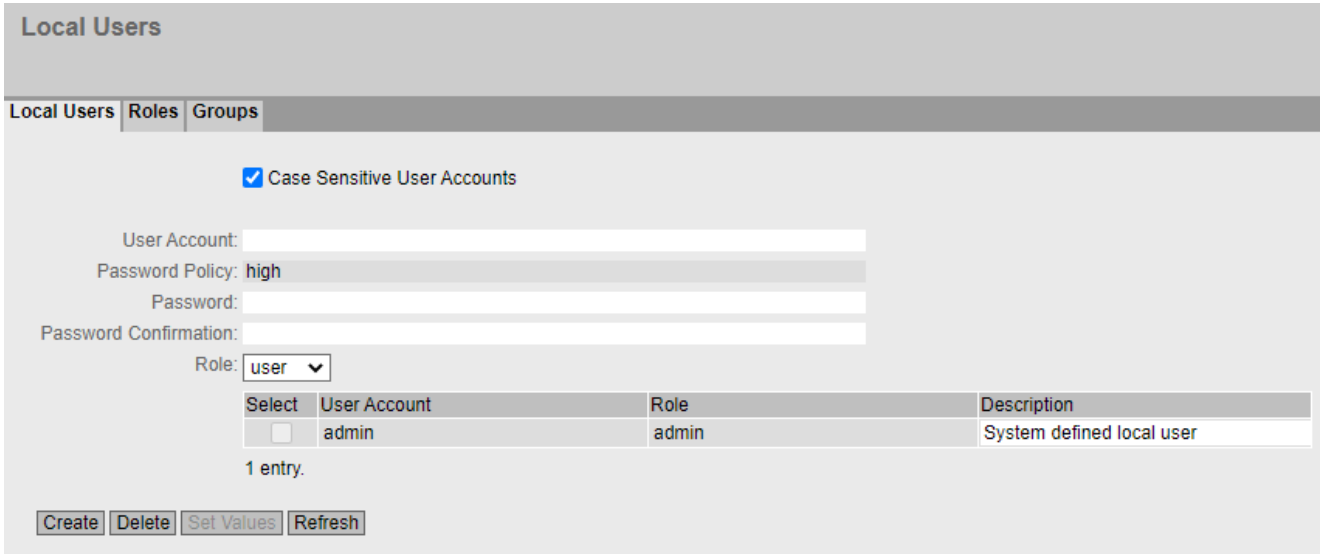
6.7.2.1 Local Users

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.



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.

Note

User "user" preset in the factory

As of firmware version 2.1, the default user set in the factory "user" is no longer available when the product ships.

If you update a device to firmware V2.1, the user "user" is initially still available. If you reset the device to the factory settings ("Restore Factory Defaults and Restart"), the user "user" is deleted.

You can create new users with the role "user".

- **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. Use passwords with a high password strength.

- **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.

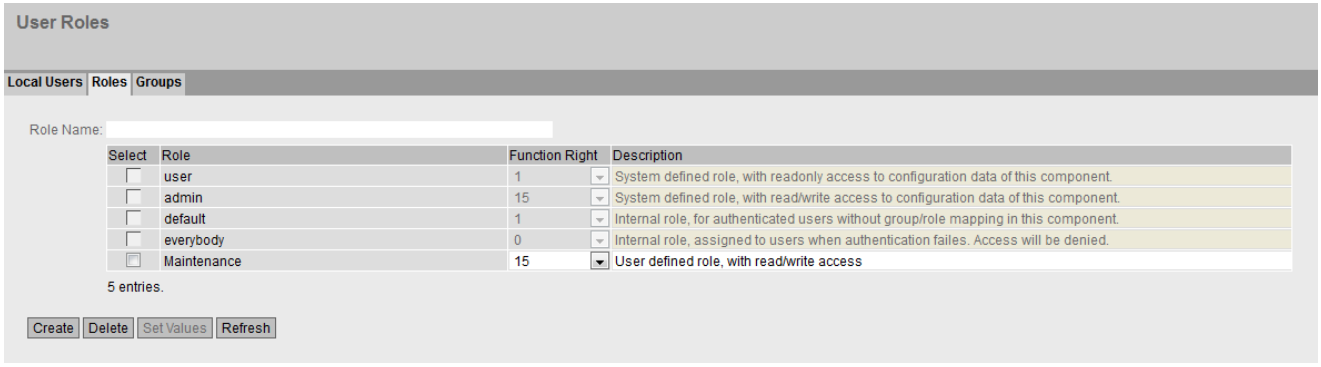
6.7.2.2 Roles

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.



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

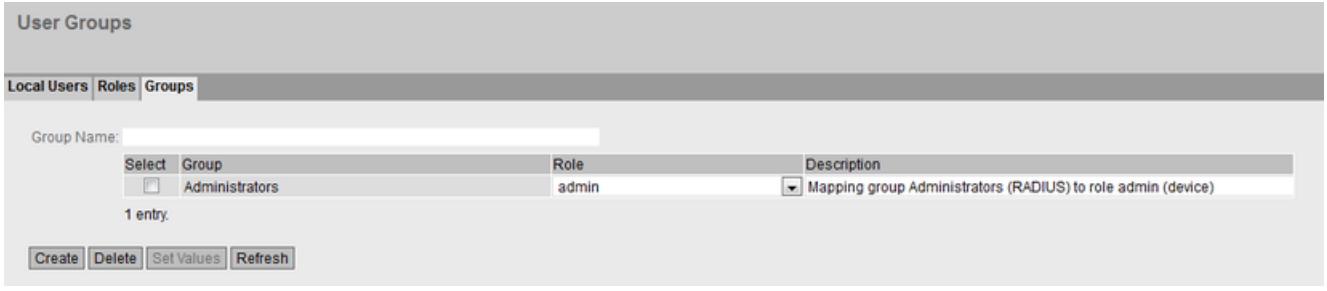
On this page you link a group with a role.

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

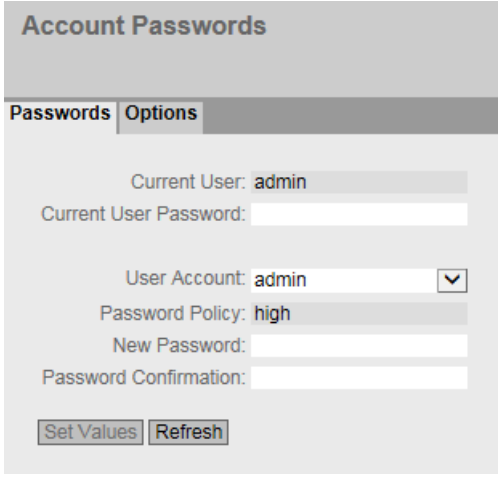
6.7.3.1 Passwords

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.



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

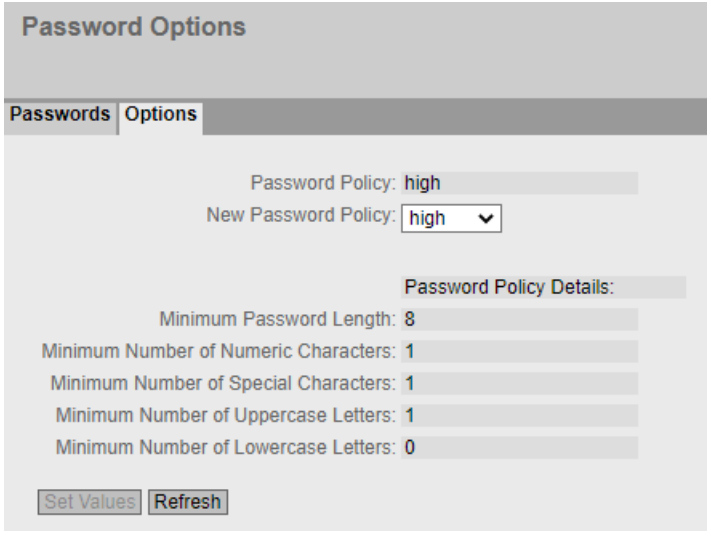
Changing the password in "Trial" mode

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.



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.

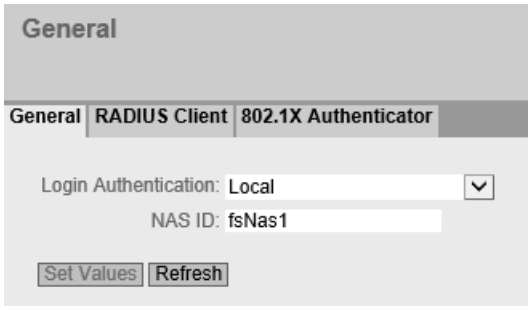
6.7.4 AAA

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.

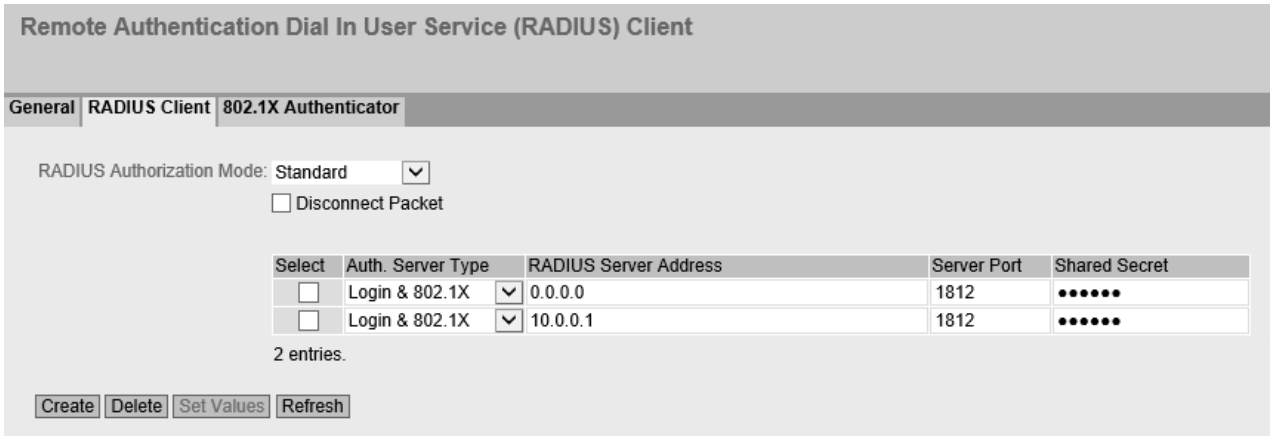
6.7.4.2 RADIUS Client

Authentication over an external server

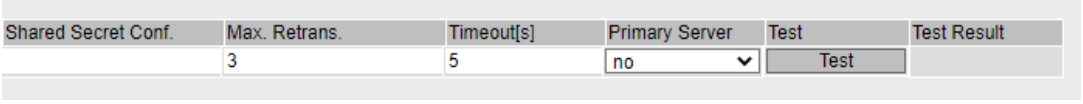
The concept of RADIUS is based on an external authentication server.

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.



Continuation of table:



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 405).
  - 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

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

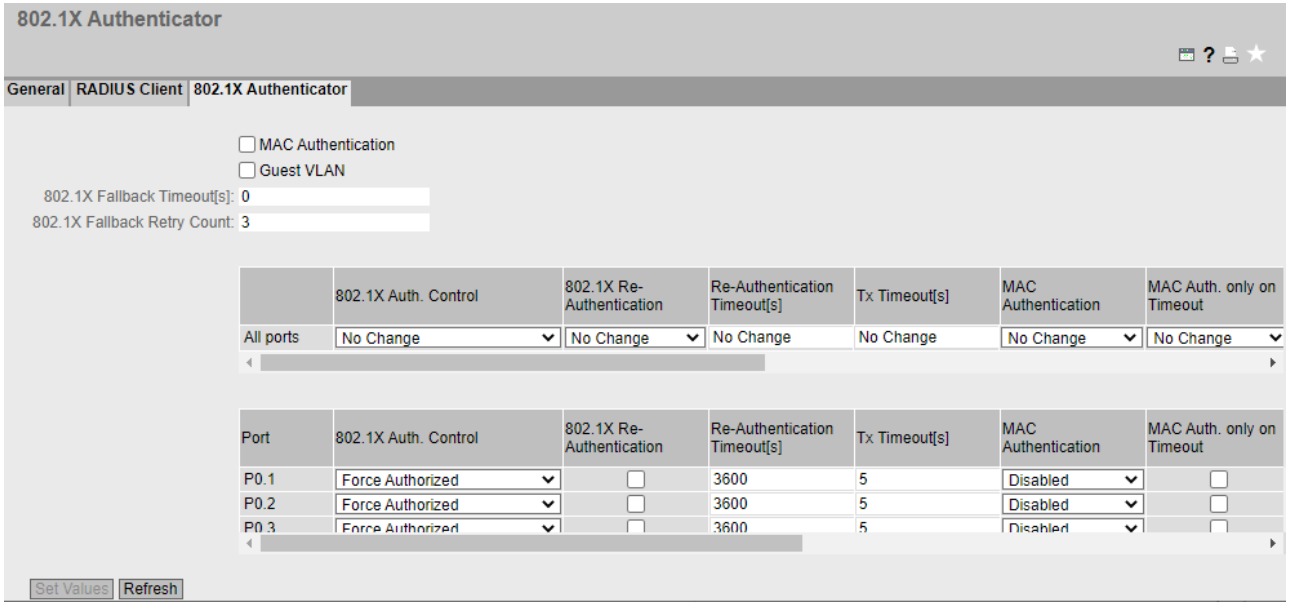
Setting up network access

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.

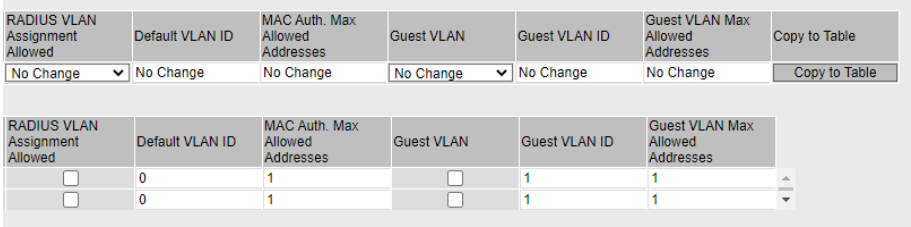
When authenticating using 802.1X, both the end device and the authentication server must support the EAP protocol (Extensive Authentication Protocol).

Enabling authentication for individual ports

By enabling the relevant options, you specify for each port whether network access protection according to IEEE 802.1X is enabled on this port.



Continuation of table:



Description of the displayed boxes

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**
  Select the required setting.
  If "No Change" is selected, the entry in table 2 remains unchanged.
- **Tx Timeout**
  Select the required setting.
  If "No Change" is selected, the entry in table 2 remains unchanged.
- **MAC Authentication**
  Select the required setting.
  If "No Change" is selected, the entry in table 2 remains unchanged.
- **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 by 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 have been 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**
  Specify the time interval in seconds after which the device is reauthenticated at the relevant port.
  The default value is 3600 seconds.
- **Tx Timeout**
  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**
  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 ≥ 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 ≤ 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**
  If this check box is selected, MAC authentication is only possible after an 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.

- **RADIUS VLAN Assignment Allowed**
  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 405) is rejected.
  If a port is assigned to a VLAN dynamically using this function during authentication, assignment using the VLAN ID or the VLAN name is possible. Configure the following values on the RADIUS server:
  - Tunnel-Type = VLAN
  - Tunnel-Medium-Type = IEEE-802
  - Tunnel-Private-Group-Id = VLAN ID or VLAN name

  The IE switch distinguishes as follows:
  - VLAN ID: The RADIUS server transfers a numeric string for the parameter "Tunnel-Private-Group-Id".
  - VLAN name: The RADIUS server transfers an alphanumeric string for the parameter "Tunnel-Private-Group-Id".
- **Default VLAN ID**
  If a VLAN ID is transmitted by the RADIUS server following 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. In addition, 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. There are two options:
  - **The value "0" is configured for 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 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**
  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.

- **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 405) is rejected.
  This function is also known as "Authentication failed VLAN".
- **Guest VLAN ID**
  Specify 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.

Configuration procedure

Enabling 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.

Enabling authentication for all ports

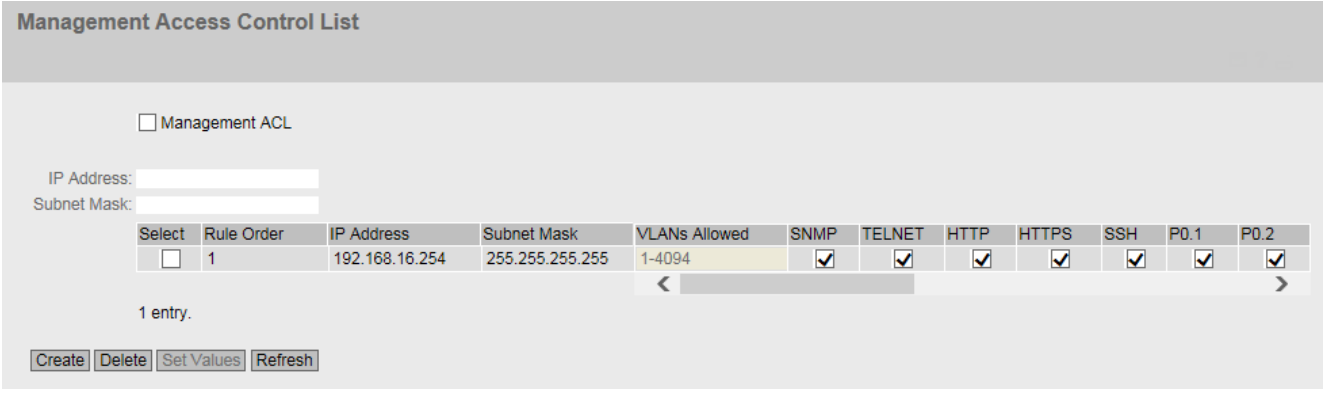
1. Select the required options in table 1.
2. Click the "Copy to Table" button. The relevant settings are adopted for all ports in table 2.
3. To apply the changes, click the "Set Values" button.

6.7.5 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. A maximum of 10 rules can be specified.



Note

If IP addresses or address bands are defined in the rules, no other IP addresses can access the management automatically.

Description

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**
  - In the Base Bridge mode "802.1Q VLAN Bridge"
    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.
  - In the Base Bridge mode "802.1D Transparent Bridge"
    You cannot define any access rules relating to VLANs. The rules apply to all VLANs.

    Note

    Compatibility with older firmware versions

    If you have defined certain VLANs with a firmware version < 1.2, the configuration of the VLANs will be replaced during a firmware update with the default value "1-4094".

- **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.

Configuration procedure

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.

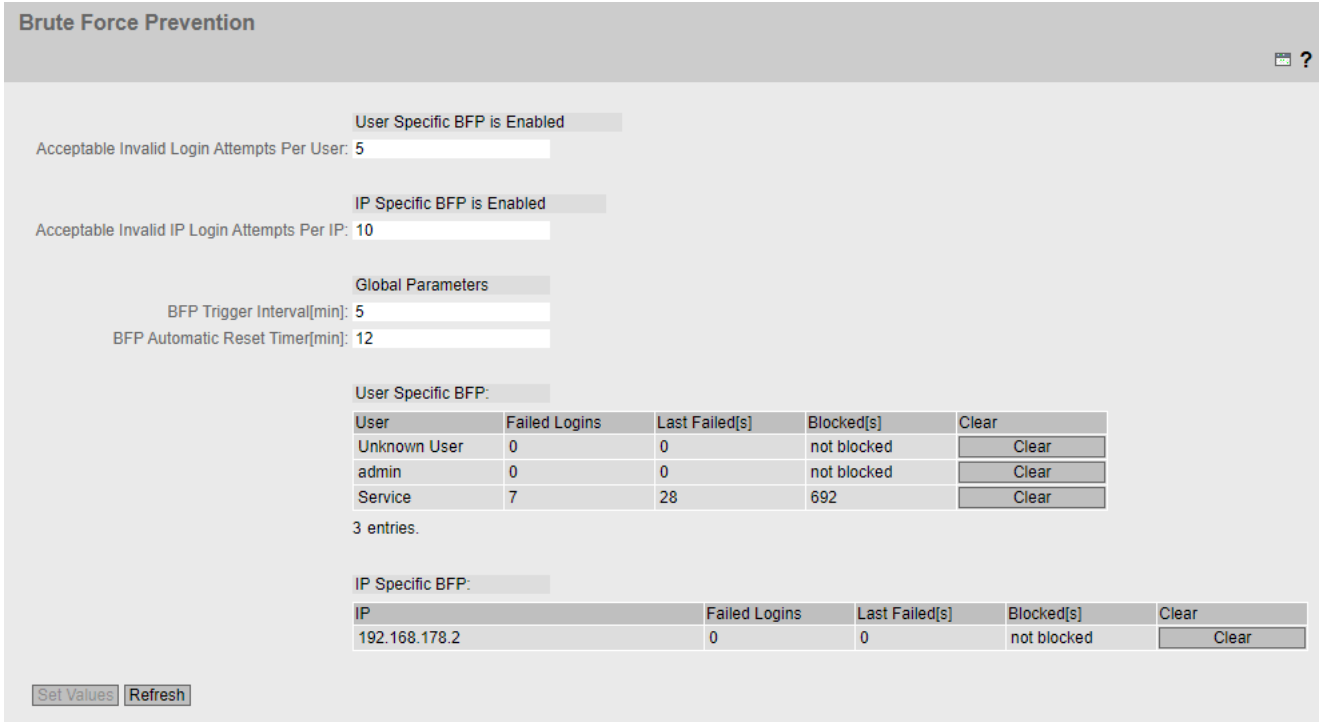
Delete rule

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.

6.7.6 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.



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

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.

Operating the button

To load new firmware, you require the button. When pressing the button, remember the information in the appropriate operating instructions.

Press the "RESET" button on the SCALANCE XB-200 with only slight force.

Press the "SELECT/SET" button on the SCALANCE XC-200.

Press the "SET" button on the SCALANCE XF-200BA.

Press the "RESET" button on the SCALANCE XF-200G with only slight force.

Press the "RESET" button on the SCALANCE XP-200 as far as the pressure point.

Press the "RESET" button on the SCALANCE XP-200G as far as the pressure point.

Press the "RESET" button on the SCALANCE XR-300WG.

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 "Downloading new firmware using TFTP without WBM and CLI (Page 435)".

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. 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 on 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 on 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"

A

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	DI1
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	Passwort 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	Passwort 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 DI1 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

Appendix B "Ciphers used"

B

B.1 Ciphers used

The following tables list the encryption methods (ciphers) used by the SCALANCE X device.

SSL

HTTPS WBM Server

Category	IANA name	Hexadecimal value	Enabled by default
Encryption suite	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	c030	✓
Encryption suite	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	c02f	✓
Encryption suite	TLS_AES_256_GCM_SHA384	1302	✓
Encryption suite	TLS_CHACHA20_POLY1305_SHA256	1303	✓
Encryption suite	TLS_AES_128_GCM_SHA256	1301	✓
Protocol version	TLSv1.2	-	✓
Protocol version	TLSv1.3	-	✓

SMTP Client (secure)

Category	IANA name	Hexadecimal value	Enabled by default
Encryption suite	TLS_AES_128_GCM_SHA256	1301	✓
Encryption suite	TLS_CHACHA20_POLY1305_SHA256	1303	✓
Encryption suite	TLS_AES_256_GCM_SHA384	1302	✓
Encryption suite	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	c02c	✓
Encryption suite	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	c02b	✓
Encryption suite	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	c02f	✓
Encryption suite	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	c030	✓
Protocol version	TLSv1.2	-	✓
Protocol version	TLSv1.3	-	✓

Syslog (secure) Client

Category	IANA name	Hexadecimal value	Enabled by default
Encryption suite	TLS_AES_128_GCM_SHA256	1301	✓
Encryption suite	TLS_CHACHA20_POLY1305_SHA256	1303	✓

Category	IANA name	Hexadecimal value	Enabled by default
Encryption suite	TLS_AES_256_GCM_SHA384	1302	✓
Encryption suite	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	c02c	✓
Encryption suite	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	c02b	✓
Encryption suite	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	c02f	✓
Encryption suite	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	c030	✓
Protocol version	TLSv1.2	-	✓
Protocol version	TLSv1.3	-	✓

SSH

SSH Server

Category	IANA name	Hexadecimal value	Enabled by default
Encryption method (enc)	aes256-ctr	-	✓
Host key	ecdsa-sha2-nistp521	-	✓
Key exchange (kex)	curve25519-sha256	-	✓
Key exchange (kex)	curve25519-sha256@libssh.org	-	✓
Key exchange (kex)	ecdh-sha2-nistp256	-	✓
Key exchange (kex)	ecdh-sha2-nistp384	-	✓
Key exchange (kex)	ecdh-sha2-nistp521	-	✓
MAC	hmac-sha2-256	-	✓
Protocol version	SSHv2.0	-	✓

SSH CLI Client

Category	IANA name	Hexadecimal value	Enabled by default
Encryption method (enc)	aes256-ctr	-	✓
Host key	ecdsa-sha2-nistp521	-	✓
Host key	ecdsa-sha2-nistp256	-	✓
Key exchange (kex)	curve25519-sha256	-	✓
Key exchange (kex)	curve25519-sha256@libssh.org	-	✓
Key exchange (kex)	ecdh-sha2-nistp256	-	✓
Key exchange (kex)	ecdh-sha2-nistp384	-	✓
Key exchange (kex)	ecdh-sha2-nistp521	-	✓
MAC	hmac-sha2-256	-	✓
Protocol version	SSHv2.0	-	✓

SNMP

SNMP Server

Category	Process	Hexadecimal value	Enabled by default
Authentication	HMAC-MD5-96	-	-
Authentication	HMAC-SHA-96	-	-
Encryption	des-cbc	-	-
Encryption	aes128-cbc	-	-

RADIUS

RADIUS Client

Category	Process	Hexadecimal value	Enabled by default
Integrity algorithm	MD5	-	-
Integrity algorithm	HMAC-SHA1	--	-

Index

F

G

H

I

L

M

N

P

Q

R

S

T

U

V

W