

# SIEMENS

## SIMATIC NET

### Industrial Ethernet switches SCALANCE XM400/X-500 Web Based Management




Configuration Manual

<u>Introduction</u>	<b>1</b>
<u>Description</u>	<b>2</b>
<u>Assignment of an IP address</u>	<b>3</b>
<u>Technical basics</u>	<b>4</b>
<u>Configuring with Web Based Management</u>	<b>5</b>
<u>Troubleshooting/FAQ</u>	<b>6</b>

## 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.

 <b>DANGER</b>
indicates that death or severe personal injury <b>will</b> result if proper precautions are not taken.
 <b>WARNING</b>
indicates that death or severe personal injury <b>may</b> result if proper precautions are not taken.
 <b>CAUTION</b>
indicates that minor personal injury can result if proper precautions are not taken.
<b>NOTICE</b>
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:

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

### Trademarks

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

### Disclaimer of Liability

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

# Table of contents

<b>1</b>	<b>Introduction</b> .....	<b>7</b>
1.1	Information on the configuration manual .....	7
1.2	Security information .....	9
<b>2</b>	<b>Description</b> .....	<b>11</b>
2.1	Product characteristics.....	11
2.2	Requirements for installation and operation .....	12
2.3	C-PLUG / KEY-PLUG .....	13
2.4	Power over Ethernet (PoE).....	14
<b>3</b>	<b>Assignment of an IP address</b> .....	<b>17</b>
3.1	Structure of an IP address .....	17
3.2	Initial assignment of an IP address .....	18
3.3	Address assignment with DHCP .....	19
3.4	Address assignment with the Primary Setup Tool .....	20
<b>4</b>	<b>Technical basics</b> .....	<b>21</b>
4.1	Configuration limits .....	21
4.2	VLAN.....	22
4.3	VLAN tagging.....	23
4.4	SNMP .....	26
4.5	Spanning Tree.....	28
4.5.1	RSTP, MSTP, CIST .....	29
4.6	Routing function .....	30
4.6.1	OSPFv2.....	31
4.7	Redundancy mechanism .....	35
4.7.1	HRP.....	35
4.7.2	MRP .....	36
4.7.2.1	MRP - Media Redundancy Protocol .....	36
4.7.2.2	Configuration in WBM .....	38
4.7.2.3	Configuration in STEP 7 .....	39
4.7.3	Standby .....	42
4.8	Link aggregation.....	43
<b>5</b>	<b>Configuring with Web Based Management</b> .....	<b>45</b>
5.1	Web Based Management .....	45
5.2	Login .....	47
5.3	The "Information" menu .....	49

5.3.1	Start page.....	49
5.3.2	Versions.....	54
5.3.3	I&M.....	55
5.3.4	ARP table.....	57
5.3.5	Log table.....	58
5.3.6	Faults.....	60
5.3.7	Redundancy.....	61
5.3.7.1	Spanning Tree.....	61
5.3.7.2	VRRP Statistics.....	64
5.3.7.3	Ring redundancy.....	66
5.3.7.4	Standby redundancy.....	68
5.3.8	Ethernet statistics.....	70
5.3.8.1	Packet size.....	70
5.3.8.2	Packet type.....	72
5.3.8.3	Packet Error.....	73
5.3.9	Routing.....	74
5.3.9.1	Routing Table.....	74
5.3.9.2	OSPFv2 Interfaces.....	75
5.3.9.3	OSPFv2 Neighbors.....	77
5.3.9.4	OSPFv2 Virtual Neighbors.....	79
5.3.9.5	OSPFv2 LSDB.....	80
5.4	The "System" menu.....	82
5.4.1	Configuration.....	82
5.4.2	General.....	85
5.4.2.1	Device.....	85
5.4.2.2	Coordinates.....	86
5.4.3	Agent IP.....	88
5.4.4	Restart.....	90
5.4.5	Load & Save.....	91
5.4.5.1	HTTP.....	91
5.4.5.2	TFTP.....	94
5.4.6	Events.....	97
5.4.6.1	Configuration.....	97
5.4.6.2	Severity Filters.....	100
5.4.7	SMTP client.....	101
5.4.8	DHCP client.....	103
5.4.9	SNMP.....	104
5.4.9.1	General.....	104
5.4.9.2	Traps.....	106
5.4.9.3	Groups.....	107
5.4.9.4	Users.....	109
5.4.10	System time.....	111
5.4.10.1	Manual setting.....	111
5.4.10.2	SNTP client.....	113
5.4.10.3	NTP client.....	116
5.4.10.4	SIMATIC time client.....	118
5.4.11	Auto logout.....	119
5.4.12	Select/Set button configuration.....	119
5.4.13	Syslog client.....	121
5.4.14	Ports.....	123
5.4.14.1	Overview.....	123
5.4.14.2	Configuration.....	125

5.4.15	Fault monitoring .....	128
5.4.15.1	Power Supply .....	128
5.4.15.2	Link Change .....	129
5.4.15.3	Redundancy .....	131
5.4.16	PNIO .....	132
5.4.17	PLUG configuration .....	133
5.4.18	PLUG license .....	136
5.4.19	Ping .....	138
5.4.20	PoE .....	139
5.4.20.1	General .....	139
5.4.20.2	Port.....	140
5.4.21	Port Diagnostics .....	143
5.4.21.1	Cable tester.....	143
5.4.21.2	SFP diagnostics .....	145
5.5	The "Layer 2" menu .....	147
5.5.1	Configuration.....	147
5.5.2	Qos.....	151
5.5.2.1	CoS queue mapping .....	151
5.5.2.2	DSCP mapping .....	152
5.5.3	Rate control.....	153
5.5.4	VLAN.....	155
5.5.4.1	General .....	155
5.5.4.2	GVRP .....	158
5.5.4.3	Port-based VLAN .....	160
5.5.4.4	Protocol Based VLAN Group .....	162
5.5.4.5	Protocol Based VLAN Port.....	163
5.5.4.6	Ipv4 Subnet Based VLAN .....	164
5.5.5	Mirroring .....	166
5.5.5.1	General .....	166
5.5.5.2	Port.....	168
5.5.5.3	VLAN.....	170
5.5.5.4	MAC Flow.....	171
5.5.5.5	IP Flow .....	172
5.5.6	Dynamic MAC aging .....	173
5.5.7	Ring redundancy .....	174
5.5.7.1	Ring redundancy .....	174
5.5.7.2	Standby .....	177
5.5.8	MSTP .....	179
5.5.8.1	General .....	179
5.5.8.2	CIST general.....	180
5.5.8.3	CIST port.....	182
5.5.8.4	MST general.....	186
5.5.8.5	MST port .....	187
5.5.8.6	Enhanced Passive Listening Compatibility .....	189
5.5.9	Loop Detection .....	191
5.5.10	Link aggregation.....	194
5.5.11	DCP forwarding.....	197
5.5.12	LLDP .....	199
5.5.13	Unicast .....	201
5.5.13.1	Filtering .....	201
5.5.13.2	Locked ports.....	203
5.5.13.3	Learning .....	205

5.5.13.4	Unicast blocking .....	206
5.5.14	Multicast .....	208
5.5.14.1	Groups.....	208
5.5.14.2	IGMP .....	211
5.5.14.3	GMRP.....	212
5.5.14.4	Multicast blocking.....	214
5.5.15	Broadcast .....	216
5.6	The "Layer 3" menu .....	218
5.6.1	Configuration .....	218
5.6.2	Subnets .....	219
5.6.2.1	Overview .....	219
5.6.2.2	Configuration .....	220
5.6.3	Static routes .....	222
5.6.4	DHCP Relay Agent .....	224
5.6.4.1	General.....	224
5.6.4.2	Option.....	225
5.6.5	VRRP .....	227
5.6.5.1	Router.....	227
5.6.5.2	Configuration .....	230
5.6.5.3	Addresses Overview .....	232
5.6.5.4	Addresses Configuration.....	233
5.6.6	OSPFv2.....	234
5.6.6.1	Configuration.....	234
5.6.6.2	Areas .....	236
5.6.6.3	Area Range .....	237
5.6.6.4	Interfaces.....	239
5.6.6.5	Interface authentication.....	241
5.6.6.6	Virtual Links.....	242
5.6.6.7	Virtual link authentication .....	244
5.7	The "Security" menu .....	246
5.7.1	Passwords.....	246
5.7.2	AAA .....	247
5.7.2.1	General.....	247
5.7.2.2	Radius client.....	247
5.7.2.3	802.1x authenticator.....	250
5.7.3	Port ACL MAC.....	252
5.7.3.1	Rules Configuration.....	252
5.7.3.2	Port Ingress Rules.....	253
5.7.3.3	Port Egress Rules .....	255
5.7.4	Port ACL IP .....	257
5.7.4.1	Rules Configuration.....	257
5.7.4.2	Port Ingress Rules.....	259
5.7.4.3	Port Egress Rules .....	261
5.7.5	Management ACL .....	263
<b>6</b>	<b>Troubleshooting/FAQ.....</b>	<b>265</b>
6.1	Firmware update via WBM or CLI not possible.....	265
	<b>Index .....</b>	<b>267</b>

# Introduction

## 1.1 Information on the configuration manual

### Validity of the configuration manual

This Configuration Manual covers the following products:

- SCALANCE X500
  - SCALANCE XR552-12M
  - SCALANCE XR528-6M

The devices are available with or without routing functions. For the devices without routing functions, the functions can be enabled by a KEY-PLUG.

- SCALANCE XM400
  - SCALANCE XM408-8C
  - SCALANCE XM416-4C

The devices are available only without routing functions. The routing functions can be enabled by a KEY-PLUG.

This Configuration Manual applies to the following software version:

- SCALANCE X-500 firmware as of version 3.0
- SCALANCE XM400 firmware as of Version 3.1

### 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 provides you with the information you require to configure the IE switches.

## Orientation in the documentation

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

- Configuration Manual:
  - SCALANCE XM400/X-500 Command Line Interface

This document contains the CLI commands that are supported by the IE switches SCALANCE XM400 and SCALANCE X-500.

- Operating instructions:
  - SCALANCE XR-500M
  - MM900 media modules for SCALANCE XR-500M
  - Fan unit FAN597-1 for SCALANCE XR-500M
  - Power supply PS598-1 for SCALANCE XR-500M
  - SCALANCE XM400
  - Extender for SCALANCE XM400

These documents contain information on installing and connecting up and approvals for the products.

The following documentation is also available from SIMATIC NET on the topic of Industrial Ethernet:

- System manual "Industrial Ethernet / PROFINET"
- System manual "Industrial Ethernet / PROFINET - Passive network components"

All these documents are available in digital form on the SCALANCE X-500 CD.

## SIMATIC NET glossary

Explanations of the specialist terms used in this documentation can be found in the SIMATIC NET glossary.

You will find the SIMATIC NET glossary here:

- SIMATIC NET Manual Collection

The DVD ships with certain SIMATIC NET products.

- On the Internet under the following entry ID:

50305045 (<http://support.automation.siemens.com/WW/view/en/50305045>)



## 1.2 Security information

Siemens provides automation and drive products with industrial security functions that support the secure operation of plants or machines. They are an important component in a holistic industrial security concept. With this in mind, our products undergo continuous development. We therefore recommend that you keep yourself informed with respect to our product updates. Please find further information and newsletters on this subject at: <http://support.automation.siemens.com>.

To ensure the secure operation of a plant or machine it is also necessary to take suitable preventive action (e.g. cell protection concept) and to integrate the automation and drive components into a state-of-the-art holistic industrial security concept for the entire plant or machine. Any third-party products that may be in use must also be taken into account. Please find further information at: <http://www.siemens.com/industrialsecurity>



## Description

### 2.1 Product characteristics

#### Properties of the IE switches

- The Ethernet interfaces support the following modes:
  - 10 Mbps and 100 Mbps both in full and half duplex
  - 1000 Mbps full duplex
  - Autocrossing
  - Autopolarity
- Redundancy protocols Multiple Spanning Tree Protocol (MSTP), Rapid Spanning Tree Protocol (RSTP) and Spanning Tree Protocol (STP)

This allows a subnet to be connected redundantly to a higher-level company network with reduced requirements for the reconfiguration time (in the range of seconds).
- Routing protocol Open Shortest Path First (OSPF) and redundancy protocol Virtual Router Redundancy Protocol (VRRP)

If the IE switches have routing functions, they support the OSPF routing protocol and the VRRP redundancy protocol. This means that industrial, routed subnets can also be connected redundantly to a higher-level company network.
- 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. Port-based, protocol-based and subnet-based VLANs are available.
- Load limitation when using multicast protocols, for example video transmission  
By learning the multicast sources and destinations (IGMP snooping, IGMP querier), the IE switches can also filter multicast data traffic and limit the load in the network. Multicast and broadcast traffic can be limited.
- Time-of-day synchronization
- Diagnostics messages (log table entries, e-mail) 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.
- Link aggregation (IEEE 802.1AX) for bundling data streams
- 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).

2.2 Requirements for installation and operation

**Layer 3 functions**

The following functions are only available on devices with routing functions:

- Routing
- OSPF
- VRRP

The following SCALANCE X-500 devices have routing functions:

Device	Order number
XR552-12M	6GK5 552-0AR00-2AR2
	6GK5 552-0AR00-2HR2
XR528-6M	6GK5 528-0AR00-2AR2
	6GK5 528-0AR00-2HR2

For the SCALANCE XM400 devices, the functions can be enabled by a KEY-PLUG.

## 2.2 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 PC on which the Primary Setup Tool (PST) is installed is necessary for the initial assignment of an IP address to the IE switches. For the other configuration settings, a computer with Telnet or an Internet browser is necessary.

#### Serial interface

The IE switches have a serial interface. An IP address is unnecessary to be able to access the device via the serial interface. A serial cable ships with the products.

Set the following parameters for the connection:

- Bits per second: 115200
- Data bits: 8
- Parity: None
- Stop bits: 1
- Flow control: None

## 2.3 C-PLUG / KEY-PLUG

### Configuration information on the C-PLUG / KEY-PLUG

The C-PLUG / KEY-PLUG is used to transfer the configuration of the old device to the new device when a device is replaced.

**NOTICE****Do not remove or insert a C-PLUG / KEY-PLUG during operation!**

A C-PLUG / KEY-PLUG may only be removed or inserted when the device is turned off. The device checks whether or not a C-PLUG / KEY-PLUG is present at one second intervals. If it is detected that the C-PLUG / KEY-PLUG was removed, there is a restart. If a valid C-PLUG / KEY-PLUG was inserted in the device, the device changes to a defined error state following the restart.

When the new device starts up with the C-PLUG / KEY-PLUG, it then continues automatically with exactly the same configuration as the old device. One exception to this can be the IP configuration if it is set over DHCP and the DHCP server has not been reconfigured accordingly.

A reconfiguration is necessary if you use functions based on MAC addresses.

---

**Note**

In terms of the C-PLUG / KEY-PLUG, the SCALANCE devices work in two modes:

- **Without C-PLUG / KEY-PLUG**  
The device stores the configuration in internal memory. This mode is active when no C-PLUG / KEY-PLUG is inserted.
  - **With C-PLUG / KEY-PLUG**  
The configuration stored on the C-PLUG / KEY-PLUG is displayed over the user interfaces. If changes are made to the configuration, the device stores the configuration directly on the C-PLUG / KEY-PLUG and in the internal memory. This mode is active as soon as a C-PLUG / KEY-PLUG is inserted. When the device is started with a C-PLUG / KEY-PLUG inserted, the device starts up with the configuration data on the C-PLUG / KEY-PLUG.
-

---

**Note**

**Incompatibility with previous versions with C-PLUG / KEY-PLUG inserted**

During the installation of a previous version of the firmware, 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 C-PLUG / KEY-PLUG is inserted in the device, following the restart, this has the status "Not Accepted" since the C-PLUG / KEY-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 C-PLUG / KEY-PLUG is no longer required, the C-PLUG / KEY-PLUG can be deleted or rewritten manually.

---

**License information on the KEY-PLUG**

In addition to the configuration, the KEY-PLUG also contains a license that allows the use of layer 3 functions.

## 2.4 Power over Ethernet (PoE)

### General

"Power over Ethernet" (PoE) is a power supply technique for network components according to IEEE 802.3af or IEEE 802.3at. The power is supplied over the Ethernet cables that connect the individual network components together. This makes an additional power cable unnecessary. PoE can be used with all PoE-compliant network components that require a power of max. 25.50 W.

### Cable used for the power supply

- **Variant 1 (redundant wires)**  
In Fast Ethernet, the wire pairs 1, 2 and 3, 6 are used to transfer data. Pairs 4, 5 and 7, 8 are then used to supply power. If there are only four wires available, the voltage is modulated onto the wires 1, 2 and 3, 6 (see variant 2). This alternative is suitable for a data transmission rate of 10/100 Mbps. This type of power supply is not suitable for 1 Gbps since with gigabit all 8 wires are used for data transfer.
- **Variant 2 (phantom power)**  
With phantom power, the power is supplied over the pairs that are used for data transfer, in other words, all eight (1 Gbps) or four (10/100 Mbps) wires are used both for the data transfer and the power supply.

A PoE-compliant end device must support both variant 1 and variant 2 over redundant wires. A PoE-compliant switch can supply the end device either using:

- Variant 1 or
- Variant 2 or
- Variant 1 and variant 2.


## Endspan

With endspan, the power is supplied via a switch that can reach a device over an Ethernet cable. The switch must be capable of PoE, for example a SCALANCE X108PoE, SCALANCE X308-2M PoE, SCALANCE XR552-12M.

## Midspace

Midspace is used when the switch is not PoE-compliant. The power is supplied by an additional device between the switch and end device. In this case, only data rates of 10/100 Mbps can be achieved because the power is supplied on redundant wires.

A Siemens power insert can also be used as the interface for the power input. Since a power insert supports a power supply of 24 VDC, it does not conform with 802.3af or IEEE 802.3at. The following restrictions relating to the use of power inserts should be noted:

 <b>WARNING</b>
<p><b>Operate the power insert only when the following conditions apply:</b></p> <ul style="list-style-type: none"> <li>• with extra low voltages SELV, PELV complying with IEC 60364-4-41</li> <li>• in USA/CAN with power supplies complying with NEC class 2</li> <li>• in USA/CAN, the cabling must meet the requirements of NEC/CEC</li> <li>• Current load maximum 0.5 A</li> </ul>

## Cable lengths

Table 2- 1 Permitted cable lengths (copper cable - Fast Ethernet)

Cable type	Accessory (plug, outlet, TP cord)	Permitted cable length
IE TP torsion cable	with IE FC Outlet RJ-45 + 10 m TP cord	0 to 45 m + 10 m TP cord
	with IE FC RJ-45 Plug 180	0 to 55 m
IE FC TP Marine Cable IE FC TP Trailing Cable IE FC TP Flexible Cable	with IE FC Outlet RJ-45 + 10 m TP cord	0 to 75 m + 10 m TP cord
	with IE FC RJ-45 Plug 180	0 to 85 m
IE FC TP standard cable	with IE FC Outlet RJ-45 + 10 m TP cord	0 to 90 m + 10 m TP cord
	with IE FC RJ-45 Plug 180	0 to 100 m

2.4 Power over Ethernet (PoE)

Table 2- 2 Permitted cable lengths (copper cable - gigabit Ethernet)

Cable type	Accessory (plug, outlet, TP cord)	Permitted cable length
IE FC standard cable, 4×2, 24 AWG IE FC flexible cable, 4×2, 24 AWG	with IE FC RJ-45 Plug 180, 4x2	0 to 90 m
IE FC standard cable, 4×2, 22 AWG	with IE FC Outlet RJ-45 + 10 m TP cord	0 to 60 m + 10 m TP cord
IE FC flexible cable, 4×2, 22 AWG	with IE FC Outlet RJ-45 + 10 m TP cord	0 to 90 m + 10 m TP cord

Table 2- 3 Fitting connectors

PIN	IE FC outlet RJ-45	IE FC RJ-45 modular outlet	Use	
			1000BaseT	10BaseT, 100BaseTX
1	Yellow	Green/white	D1+	Tx+
2	Orange	Green	D1-	Rx+
3	White	Orange/white	D2+	Tx-
6	Blue	Orange	D2-	Rx-
4	-	Blue	D3-	-
5	-	Blue/white	D3+	-
7	-	Brown/white	D4-	-
8	-	Brown	D4+	-



## Assignment of an IP address

### 3.1 Structure of an IP address

#### Address classes

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

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

XXX.XXX.XXX.XXX

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

#### Subnet mask

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

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

Example of a class B network:

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

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

### *3.2 Initial assignment of an IP address*

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".

---

## **3.2 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 (default)
- Primary Setup Tool
- STEP 7
- CLI via the serial interface  
For further information on assigning the IP address using the CLI, refer to the documentation SCALANCE XM400/X-500 Command Line Interface.
- NCM PC

---

#### **Note**

When the product ships and following "Restore Factory Defaults and Restart", 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.

---

## 3.3 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. Once this period has elapsed, the client must either request a new IP address or extend the lease time of the existing IP address.
- 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. The address can be assigned via the MAC address, the DHCP client ID or the system name. You configure the parameter in "System > DHCP Client".
- the DHCP options 66, 67 are supported
  - DHCP option 66: Assignment of a dynamic TFTP server name
  - DHCP option 67: Assignment of a dynamic boot file name

---

#### Note

DHCP uses a mechanism with which the IP address is assigned for only a short time (lease time). If the device does not reach the DHCP server with a new request on expiry of the lease time, the assigned IP address, the subnet mask and the gateway continue to be used.

The device therefore remains accessible under the last assigned IP address even without a DHCP server. This is not the standard behavior of office devices but is necessary for problem-free operation of the plant.

Since the DHCP client also sends a RELEASE to the server, the server can assign this address to a further device so that inconsistencies can occur within the network.

Remedy:

After disabling DHCP, you should therefore

- change the IP address of the device to an address not assigned by DHCP
- or
- remove the IP address assigned to the device from the address pool of the DHCP server.

Working with a mixture of dynamic address assignment and statically assigned addresses is not advisable.

---

## **3.4 Address assignment with the Primary Setup Tool**

### **Introduction**

The PST (Primary Setup Tool) is capable of assigning such an address to unconfigured devices that do not yet have an IP address.

### **Requirement**

The devices can be reached via Ethernet.

---

#### **Note**

For more detailed information, refer to the Primary Setup Tool configuration manual.

You will find the PST at Siemens Industry Automation and Drives Service & Support on the Internet under entry ID 19440762. The URL for this entry is:

<http://support.automation.siemens.com/WW/view/en/19440762>  
(<http://support.automation.siemens.com/WW/view/en/19440762>)

---

## Technical basics

### 4.1 Configuration limits

#### Configuration limits of the device

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

The usability of various functions depends on the device type you are using and whether or not a KEY-PLUG is inserted.

	Configurable function	Maximum number	
<b>System</b>	Syslog server	3	
	E-mail server	3	
	SNMPv1 trap recipient	10	
<b>Layer 2</b>	Virtual LANs (port-based; including VLAN 1)	257	
	Protocol-based VLAN groups per port	12	
	IPv4 subnet-based VLANs	150	
	Multiple Spanning Tree instances	16	
	Link aggregations or Etherchannels each with a maximum of 8 ports per aggregation	8	
	Ports in a link aggregation	8	
	Static MAC addresses in the forward database (FDB)	256	
	Multicast addresses without active GMRP	512	
	Multicast addresses with active GMRP	50	
	VLANs whose data traffic can be mirrored to a monitor port	255	
	<b>Security</b>	IP addresses from a RADIUS server	3
		Management ACLs (access rules for management)	10
		Rules for port ACL MAC	128
Ingress and egress rules for port ACL MAC		256	
Rules for port ACL IP		128	
Ingress and egress rules for port ACL IP		256	
<b>Layer 3</b>	Layer 3 interfaces	127	
	Entries in the hardware routing table	4096	
	Static routes	100	
	Possible routes to the same destination	8	
	DHCP Relay Agent interfaces	127	
	DHCP Relay Agent servers	4	
	VRRP router interfaces (VLAN interfaces only)	52	
OSPF areas per device	5		

	Configurable function	Maximum number
	OSPF area range entries per OSPF area (intra-area summary)	3
	OSPF interfaces	40
	OSPF interfaces per OSPF area	40
	OSPF virtual links (within an autonomous system)	8
	OSPF interface authentication key	200 (40 interfaces each with 5 keys)
	OSPF virtual link authentication key	40 (8 virtual links each with 5 keys)

## 4.2 VLAN

### 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 23)). This expansion includes not only the VLAN ID but also priority information.

### Options for the VLAN assignment

There are various options for the assignment to VLANs:

- Port-based VLAN  
Each port of a device is assigned a VLAN ID. You configure port-based VLAN in "Layer 2 > VLAN > Port-based VLAN (Page 160)".
- Protocol-based VLAN  
Each port of a device is assigned a protocol group. You can configure protocol-based VLAN in "Layer 2 > VLAN > Protocol Based VLAN Port (Page 163)".
- Subnet-based VLAN  
The IP address of the device is assigned a VLAN ID. You configure subnet-based VLAN in "Layer 2 > VLAN > Ipv4 Subnet Based VLAN (Page 164)".

### processing the VLAN assignment

If more than one VLAN assignment is created on the device, the assignments are processed in the following order:

1. Subnet-based VLAN
2. Protocol-based VLAN
3. Port-based VLAN

The frame is first examined for the IP address. If a rule on the "Ipv4 Subnet Based VLAN" tab applies, the frame is sent to the corresponding VLAN. If no rule applies, the protocol type of the frame is examined. If a rule on the "Protocol Based VLAN Port" tab applies, the frame is sent to the corresponding VLAN. If no rule applies, the frame is sent via the port-based VLAN. The rules for the port-based VLAN are specified on the "Port Based VLAN" tab.

## 4.3 VLAN tagging

### Expansion of the Ethernet frames by four bytes

For CoS (Class of Service, frame priority) and VLAN (virtual network), the IEEE 802.1 Q 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. With the IE switches, the standard MTU size is 1536 bytes. The MTU size can be changed to values from 64 to 9216 bytes.

The end devices 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:

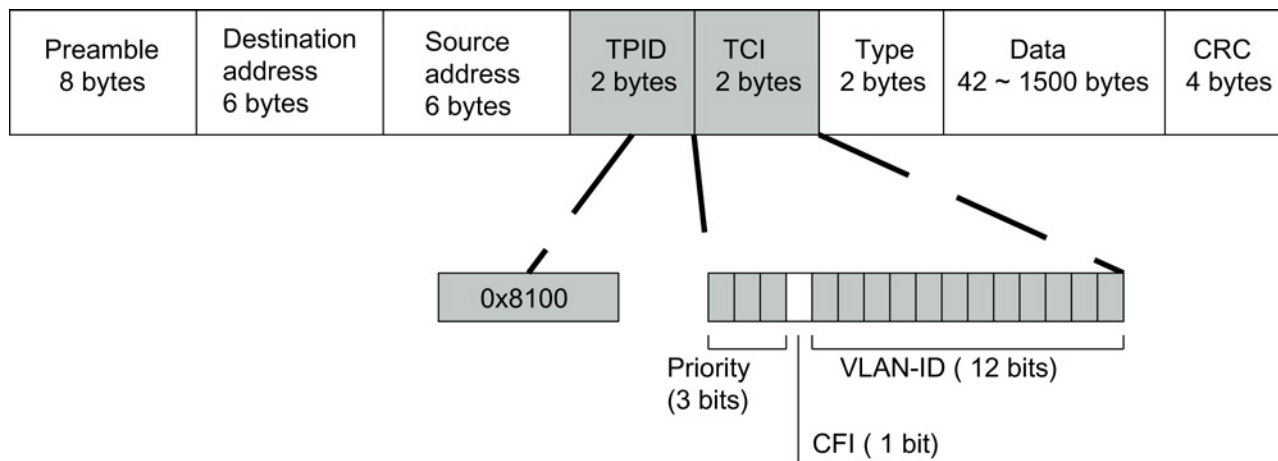


Figure 4-1 Structure of the expanded Ethernet frame

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:

#### CoS prioritization

The tagged frame has 3 bits for the priority that is also known as Class of Service (CoS). The priority according to IEEE 802.1p is as follows:

CoS bits	Type of data
000	Non time-critical data traffic (less than best effort [basic setting])
001	Normal data traffic (best effort [background])
010	Reserved (standard)
011	Reserved ( excellent effort )
100	Data transfer with max. 100 ms delay
101	Guaranteed service, interactive multimedia
110	Guaranteed service, interactive voice transmission
111	Reserved

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 eight parallel queues in which the frames with different priorities can be processed. First, the frames with the highest priority ("Strict Priority" method) 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 responsible 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 4095 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.
4095	Reserved

## 4.4 SNMP

### Introduction

With the aid of the Simple Network Management Protocol (SNMP), you monitor and control network elements from a central station, for example routers, 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

For security reasons, do not use the standard values "public" or "private". Change the values following the initial installation.

---

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 for a data record from the agent
- GETNEXT  
Calls up the next data record.

- GETBULK (available as of SNMPv2)  
Requests multiple data records at one time, 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 agent returns the data requested by the manager.
- TRAP  
If a certain event occurs, the SNMP agent sends traps.

SNMPv1 and SNMPv2 and SNMPv3 use UDP (User Datagram Protocol). The data is described in a Management Information Base (MIB).

### SNMP v3

Compared with the previous versions SNMP v1 and SNMP v2, SNMP v3 introduces a comprehensive security concept.

SNMP v3 supports:

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

## 4.5 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 stations. 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 Unit) 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.

## 4.5.1 RSTP, MSTP, CIST

### Rapid Spanning Tree Protocol (RSTP)

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

This is achieved by using the following functions:

- Edge ports (end node port)  
Edge ports are ports connected to an end device.  
A port that is defined as an edge port is activated immediately after connection establishment. If a spanning tree BPDU is received at an edge port, the port loses its role as edge port and it takes part in (R)STP again. If no further BPDU is received after a certain time has elapsed (3 x hello time), the port returns to the edge port status.
- Point-to-point (direct communication between two neighboring devices)  
By directly linking the devices, a status change (reconfiguration of the ports) can be made without any delays.
- Alternate port (substitute for the root port)  
A substitute for the root port is configured. If the connection to the root bridge is lost, the device can establish a connection over the alternate port without any delay due to reconfiguration.
- 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 is a term from the multiple spanning tree. CIST identifies the internal instance used by the switch that is comparable in principle with an internal RSTP instance.

## 4.6 Routing function

### Introduction

The term routing describes the specification of routes for communication between different networks; in other words, how does a data packet from subnet A get to subnet B.

SCALANCE X supports the following routing functions:

- **Static routing**  
With static routing, the routes are entered manually in the routing table.
- **Router redundancy**  
With standardized VRRP (Virtual Router Redundancy Protocol), the availability of important gateways is increased by redundant routers.
- **Dynamic routing**  
The entries in the routing table are dynamic and are updated continuously. The entries are created by the routing protocol.
  - OSPF v2 (Open Shortest Path First)

### Static routing

The route is entered manually in the routing table. Enter the route in the routing table on the WBM page "Routes (Page 222)".

### Router redundancy with VRRP

With the Virtual Router Redundancy Protocol (VRRP), the failure of a router in a network can be countered.

Several VRRP routers in a network segment are put together as a logical group that forms a virtual router (VR). The group is defined using the virtual ID (VRID). Within the group, the VRID must be the same. The VRID can no longer be used for other groups.

The virtual router is assigned a virtual IP address and a virtual MAC address. One of the VRRP routers within the group is specified as the master router. The master router has priority 255. The other VRRP routers are backup routers. The master router assigns the virtual IP address and the virtual MAC address to its network interface. The master router sends VRRP packets (advertisements) to the backup routers at specific intervals. With the VRRP packets, the master router signals that it is still alive. The master router also replies to the ARP queries.

If the virtual master router fails, a backup router takes over the role of the master router. The backup router with the highest priority becomes the master router. If the priority of the backup routers is the same, the higher MAC address decides. The backup router becomes the new virtual master router.

The new virtual master router adopts the virtual MAC and IP address. This means that no routing tables or ARP tables need to be updated. The consequences of a device failure are therefore minimized.

You configure VRRP in "Layer 3 > VRRP (Page 227)".

## 4.6.1 OSPFv2

### Dynamic routing with OSPF v2

OSPF (Open Shortest Path First) is a cost-based routing protocol. To calculate the shortest and most cost-effective route, the Short Path First algorithm by Dijkstra is used. OSPF was developed by the IETF (Internet Engineering Task Force). You configure OSPFv2 in "Layer 3 > OSPFv2 (Page 234)".

OSPF v2 divides an autonomous system (AS) into different areas.

### Areas in OSPF

The following areas exist:

- **Backbone**  
The backbone area is area 0.0.0.0. All other areas are connected to this area. The backbone area is connected either directly or via virtual connections with other areas. All routing information is available in the backbone area. As a result, the backbone area is responsible for forwarding information between different areas.
- **Stub Area**  
This area contains the routes within its area within the autonomous system and the standard route out of the autonomous system. The destinations outside this autonomous system are assigned to the standard route.
- **Totally Stubby Area**  
This area knows only the routes within its area and the standard route out of the area.
- **Not So Stubby Area (NSSA)**  
This area can forward (redistribute) packets from other autonomous systems into the areas of its own autonomous system. The packets are further distributed by the NSSA router.

### Routers of OSPF

OSPF distinguishes the following router types:

- **Internal router (IR)**  
All OSPF interfaces of the router are assigned to the same area.
- **Area Border Router (ABR)**  
The OSPF interfaces of the router are assigned to different areas. One OSPF interface is assigned to the backbone area. Where possible, routes are grouped together.

- Backbone Router (BR)  
At least one of the OSPF interfaces is assigned to the backbone area.
- Autonomous System Area Border Router (ASBR)  
One interface of the router is connected to a different AS, for example an AS that uses the routing protocol RIP.

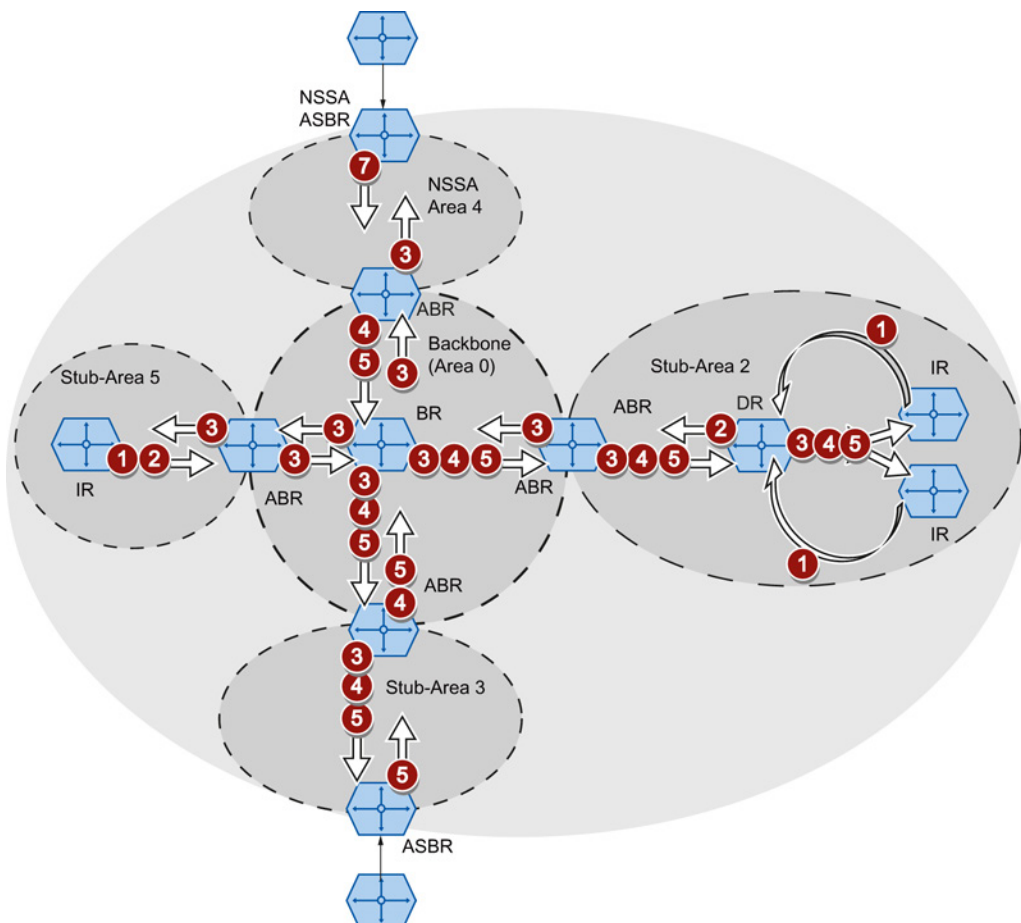
### Virtual connection

Each area must be physically connected to the backbone area. In some situations a physical connection is not possible. The remote router is connected to a backbone router via a virtual connection. In the area through which the virtual connection runs, there is no designated router or designated backup router.

### LSA types

Within the autonomous system, packets are exchanged that contain information about the connections of a router and the connection status message. The packets are also known as LSAs (Link State Advertisements). The LSAs are always sent from the router to the neighbor router.

If there are changes in the network, LSAs are sent to all routers in the network. The information depends on the LSA type.





- 1 Router LSA (LSA Type 1)**

The LSA Type 1 is only sent within an area. For each active connection of the router that belongs to the area in consideration, an LSA Type 1 is generated. The LSA Type 1 contains information about the status and the costs of the connection, for example IP address, network mask, network type
- 2 Network LSA (LSA Type 2)**

The LSA Type 2 is sent only within an area. For each network that belongs to the relevant area, the router generates an LSA Type 2. If several routers are interconnected in a network, the LSA Type 2 is sent by the designated router (DR). The LSA Type 2 includes the network address, the network mask and a list of routers that are connected to the network
- 3 Summary LSA (LSA Type 3 / LSA Type 4)**

The Summary LSA is generated by the area border router and sent into the area. The Summary LSA contains information about routes outside the area but inside the AS. Where possible, the routes are grouped together.

  - Summary LSA (LSA Type 3)  
The LSA Type 3 describes the routes to the networks and advertises the standard route to the areas.
  - AS Summary LSA (LSA Type 4)  
The LSA Type 4 describes the routes to the ASBR.
- 5 External LSA (LSA Type 5 / LSA Type 7)**

The External LSA is generated by the ASBR. The LSA type depends on the area.

  - 7** • AS External LSA (LSA Type 5)  
The LSA Type 5 is sent by the AS border router into the areas of the autonomous system except the Stub and NSSA areas. The LSA contains information about routes to a network in another AS. The routes are either created manually or learned externally. The ASBR uses LSA Type 5 to distribute standard routes to the backbone area.
  - NSSA External LSA (LSA Type 7)  
The LSA Type 7 is generated by the AS border router of an NSSA. The router is also known as the NSSA ASBR. The LSA Type 7 is sent only within the NSSA. If the P bit in LSA Type 7 = 1, these LSAs are converted to LSA Type 5 by the ABR and sent to the backbone area.

## Establishing the neighborhood

The router runs through the following statuses to establish a connection to the neighbor router.

### 1. Attempt state / Init state

The router activates OSPF and begins to send and receive Hello packets. Based on the received Hello packets, the router learns which OSPF routers are in its vicinity. The router checks the content of the Hello packet. The Hello packet also contains the list of the neighbor routers (neighbor table) of the "sender".

### 2. Two way state

If, for example, the ID of the area, the area type and the settings for the times match, a connection (adjacency) can be established to the neighbor. In a point-to-point network, the connection is established directly. If several neighbor routers can be reached in a network, the designated router (DR) and the designated backup router (DBR) are identified based on Hello packets. The router with the highest router priority becomes the designated router. If two routers have the same router priority, the router with the lower router ID becomes the designated router. The router establishes a connection to the designated router.

### 3. Exchangestart state

The neighbor routers decide which router starts communication. The router with the higher router ID becomes master.

### 4. Exchange state

The neighbor routers send packets that describe the content of their neighborhood database. The neighborhood database (link state database - LSDB) contains information on the topology of the network.

### 5. Loading state

The router completes the received information. If the router still has questions relating to the status of a specific connection, it sends a link state request. The neighbor router sends a response (link state update). The response contains a suitable LSA. The router confirms receipt of the response (link state acknowledge).

### 6. Full State

The information exchange with the neighbor router is completed. The neighborhood database of the neighbor router is the same. Based on the Short Path First algorithm, the router calculates a route to every destination. The route is entered in the routing table.

## Check the neighborhood

The Hello packets are only used to establish the neighborhood relations. Hello packets are used to check the connection to the neighbor router by sending them cyclically. If no Hello packet is received within a certain interval (dead interval), the connection to the neighbor is marked as "down". The relevant entries are deleted.

## Updating the neighborhood database

Once the neighborhood database is established, LSAs are sent to all routers in the network if there are changes in the topology.

## 4.7 Redundancy mechanism

### 4.7.1 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 0.3 seconds.

#### **Standby redundancy**

Standby redundancy is a method with which two 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 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.
- All devices must be interconnected via their ring ports.
- 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.

## 4.7.2 MRP

### 4.7.2.1 MRP - Media Redundancy Protocol

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

IEC 62439-2 Edition 1.0 (2010-02) 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 0.2 seconds.

### Requirements

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. In topologies with X300 IE switches, up to 100 nodes are supported.  
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.
- "MRP" must be activated on all devices in the ring (see section "Configuration in STEP 7 (Page 39)").
- 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.

## Topology

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

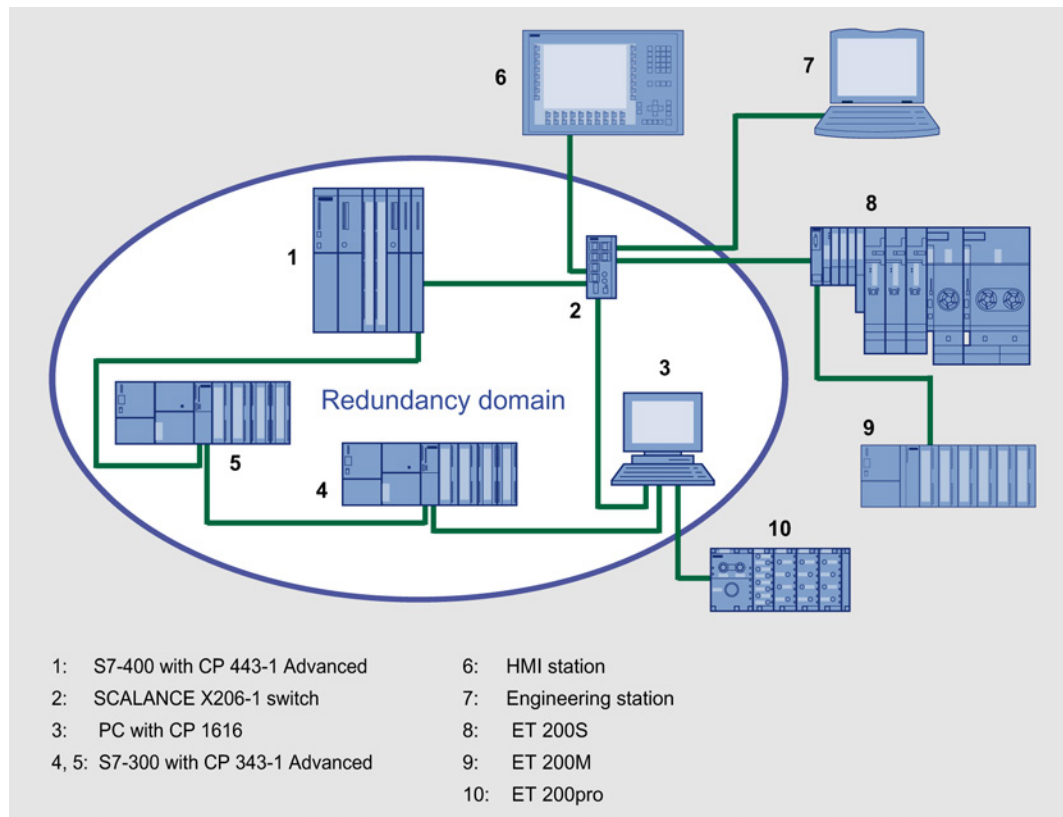


Figure 4-2 Example of a ring topology with the MRP media redundancy protocol

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 1616.

### 4.7.2.2 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 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".
  - 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.

---

#### Configuration

In WBM, you configure MRP on the following pages:

- Configuration (Page 147)
- Ring redundancy (Page 174)

### 4.7.2.3 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****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

Leave the default entry "mrpdomain 1" from the factory settings 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.

If you leave the setting for "Domain" as the factory set "mrpdomain-1", the defaults for "Role" and "Ring ports" also remain active.

The MRP settings remain in effect following a restart of the device or following a power down and hot restart.

## Role

The choice of role depends on the following use cases.

- You want to use MRP in a ring topology 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 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 "redundancy manager".
  - For all other devices in the ring topology, select the role of "Client".

---

### Note

To ensure problem-free operation when using a non-Siemens device as the redundancy manager in the ring, make sure that you assign the fixed role of "Client" to all other devices in the ring, before you close the ring. Otherwise, there may be circulating data frames that will cause a failure in the network.

---

- 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

Brand new Siemens devices and those reset to the factory settings have the MRP role "Manager (Auto)" (CPs) or "Automatic Redundancy Detection" (SCALANCE X). If you are operating a non-Siemens device as the redundancy manager in the ring, this may cause loss of the data traffic.

---

## 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.

- CPs adopt the "Manager (Auto)" MRP role.
- With switches, the redundancy method Automatic Redundancy Detection (ARD) is activated.

If other ports were used previously as ring ports before resetting, with the appropriate attachment, a previously correctly configured device can cause circulating frames and therefore the failure of the data traffic.

## 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.

- Interruption / return (redundancy manager only)

If the ring is interrupted and when the original configuration returns, diagnostic interrupts are generated.

The occurrence of both interrupts within 0.2 seconds indicates an interruption in the ring.

## Parameter assignment of the redundancy is not set by STEP 7 (redundancy alternatives)

This option only affects switches. Select this option if you want to set the properties for media redundancy using alternative mechanism or tools such as Web based Management (WBM), CLI or SNMP.

If you enable this option, existing redundancy settings from WBM, CLI or SNMP, 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.

### 4.7.3 Standby

#### General

SCALANCE X switches support not only ring redundancy within a ring but also redundant linking of two rings or open network segments (linear bus). In the redundant link, two rings are connected together over two 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

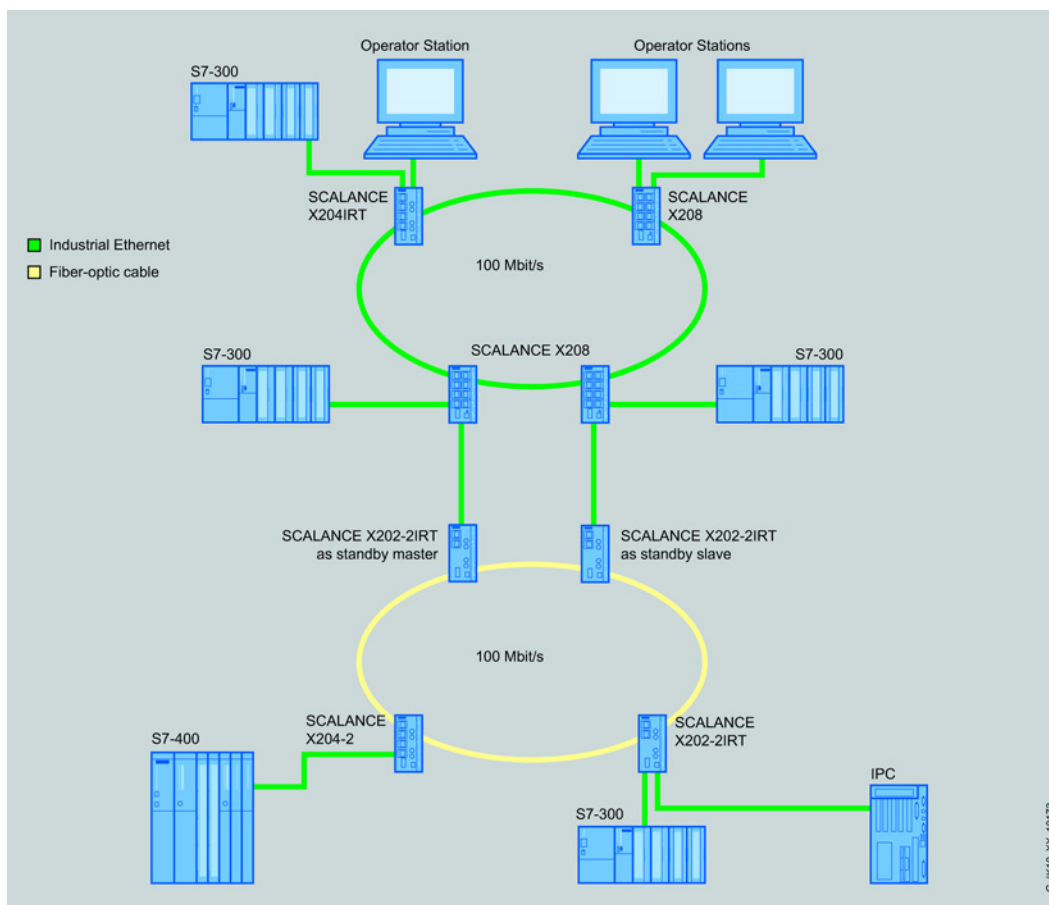


Figure 4-3 Example of redundant linking of two SCALANCE X-200 IRT rings

For a redundant link as shown in the figure, two devices must be configured as standby redundancy switches within a network segment. Here, network segments are rings with a redundancy manager (RM, in the example, the SCALANCE X202-2IRT switches). Instead of rings, network segments might also be linear.

The two X202 devices 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.

## **4.8 Link aggregation**

### **Link aggregation**

With link aggregation, several parallel physical connections with the same transmission speed are grouped together to form a logical connection with a higher transmission speed. This method based on IEEE 802.3ad is also known as port trunking or channel bundling.

Link aggregation works only with full duplex connections with the same transmission speed in point-to-point mode. This achieves multiplication of the bandwidth or transmission speed. If part of the connection fails, the data traffic is handled via the remaining parts of the connection.

To control and monitor, the Link Aggregation Control Layer (LACL) and the Link Aggregation Control Protocol (LACP) are used.



# Configuring with Web Based Management

## 5.1 Web Based Management

### How it works

The device has an integrated HTTP server for Web Based Management (WBM). If a device is addressed over an Internet browser, it returns HTML pages to the client PC depending on the user input.

The user enters the configuration data in the HTML pages sent by the device. The device evaluates this information and generates reply pages dynamically.

The advantage of this method is that only an Internet browser is required on the client.

---

#### Note

##### Secure connection

WBM also allows you to establish a secure connection via HTTPS.

Use HTTPS for protected data transmission. If you wish to access WBM only via a secure connection, activate the option "HTTPS Server only" under "System > Configuration".

---

### Requirements

#### WBM display

- The device has an IP address
- There is a connection between the device and the client PC. With the Windows ping command, you can check whether or not a connection exists.
- Access via HTTPS is enabled.
- JavaScript is activated in the Internet browser.
- The Internet browser must not be set so 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. In the Internet Explorer, you can make the appropriate setting in the "Options > Internet Options > General" menu in the section "Browsing history" with the "Settings" button. Under "Check for newer versions of stored pages:", select "Automatically".
- If a firewall is used, the relevant ports must be opened.
  - For access using HTTP: Port 80
  - For access using HTTPS: Port 443

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

- MS IE 9
- Mozilla Firefox ESR17

---

**Note**

**Compatibility view**

In Microsoft Internet Explorer, disable the compatibility view to ensure correct display and to allow problem-free configuration using WBM.

---

**Display of the WBM on mobile devices**

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

Resolution	Operating system	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:

- Safari on iOS 6 (iPhone, iPad Mini, iPod Touch 4th Generation)
- Chrome 25 on Android (Galaxy Nexus 4, Galaxy Nexus 7)

---

**Note**

**Display of the WBM and working with it on mobile devices**

The display on the WBM pages and how you work with them on mobile devices may differ compared with the same pages on desktop devices. Some pages also have an optimized display for mobile devices.

---

## 5.2 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 client PC. With the ping command, you can check whether or not a connection exists.
2. In the address box of the Web browser, enter the IP address or the URL of the device. If there is a problem-free connection to the device, the login page of Web Based Management (WBM) is displayed.

### Logging on using the Web browser

#### Selecting the language of the WBM

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, only English is available. Other languages will follow in a later version.

---

The screenshot shows the Siemens WBM login interface. At the top left is the Siemens logo. In the top right corner, there is a language selection dropdown menu set to 'English' and a 'Go' button. On the left side, there is a sidebar with 'Name' and 'Password' input fields and a 'Login' button. The main content area has a large 'LOGIN' heading, followed by 'Name:' and 'Password:' labels with corresponding input fields, and a 'Login' button. At the bottom, there is a link to 'Switch to secure HTTP'.

## Login with HTTP

There are two ways in which you can log in via HTTP. 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 when logging in whichever of the above options you choose:

1. Enter the following in the "Name" input box:
  - "admin": With this user type, you can change the settings of the device (read and write access to the configuration data).
  - "user": With this user type, you cannot change any of the settings of the device (read access to the configuration data).
2. Enter your password in the "Password" input box.  
When you log in for the first time or following a "Restore Factory Defaults and Restart", enter the standard password in the "Password" input box.
  - "admin": standard password "admin"
  - "user": standard password "user"
3. Click the "Login" button or confirm your entry with "Enter".  
When you log in for the first time following a "Restore Factory Defaults and Restart", you will be prompted to change the password. The new password must be at least 6 characters long. You need to repeat the password as confirmation. The password entries must match. Click the "Set Values" to complete the action and activate the new password.

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

## Login with HTTPS

Web Based Management also allows you to connect to the device over the secure connection of the HTTPS protocol. Follow these steps:

1. Click on the link "Switch to secure HTTP" on the login page or enter "https://" and the IP address of the device in the address box of the Internet browser.  
  
The "Certification Error Warning" is displayed and asks you whether you want to continue the action.
2. Click the "Yes" button if you want to continue.  
The Login page of Web-Based Management appears.
3. Enter the following in the "Name" input box:
  - "admin": With this user type, you can change the settings of the device (read and write access to the configuration data).
  - "user": With this user type, you cannot change any of the settings of the device (read access to the configuration data).



4. Enter your password in the "Password" input box.  
When you log in for the first time or following a "Restore Factory Defaults und Restart", enter the standard password in the "Password" input box.
  - "admin": standard password "admin"
  - "user": standard password "user"
5. Click the "Login" button or confirm your entry with "Enter".  
When you log in for the first time following a "Restore Factory Defaults and Restart", you will be prompted to change the password. The new password must be at least 6 characters long. You need to repeat the password as confirmation. The password entries must match. Click the "Set Values" to complete the action and activate the new password.

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

## 5.3 The "Information" menu

### 5.3.1 Start page

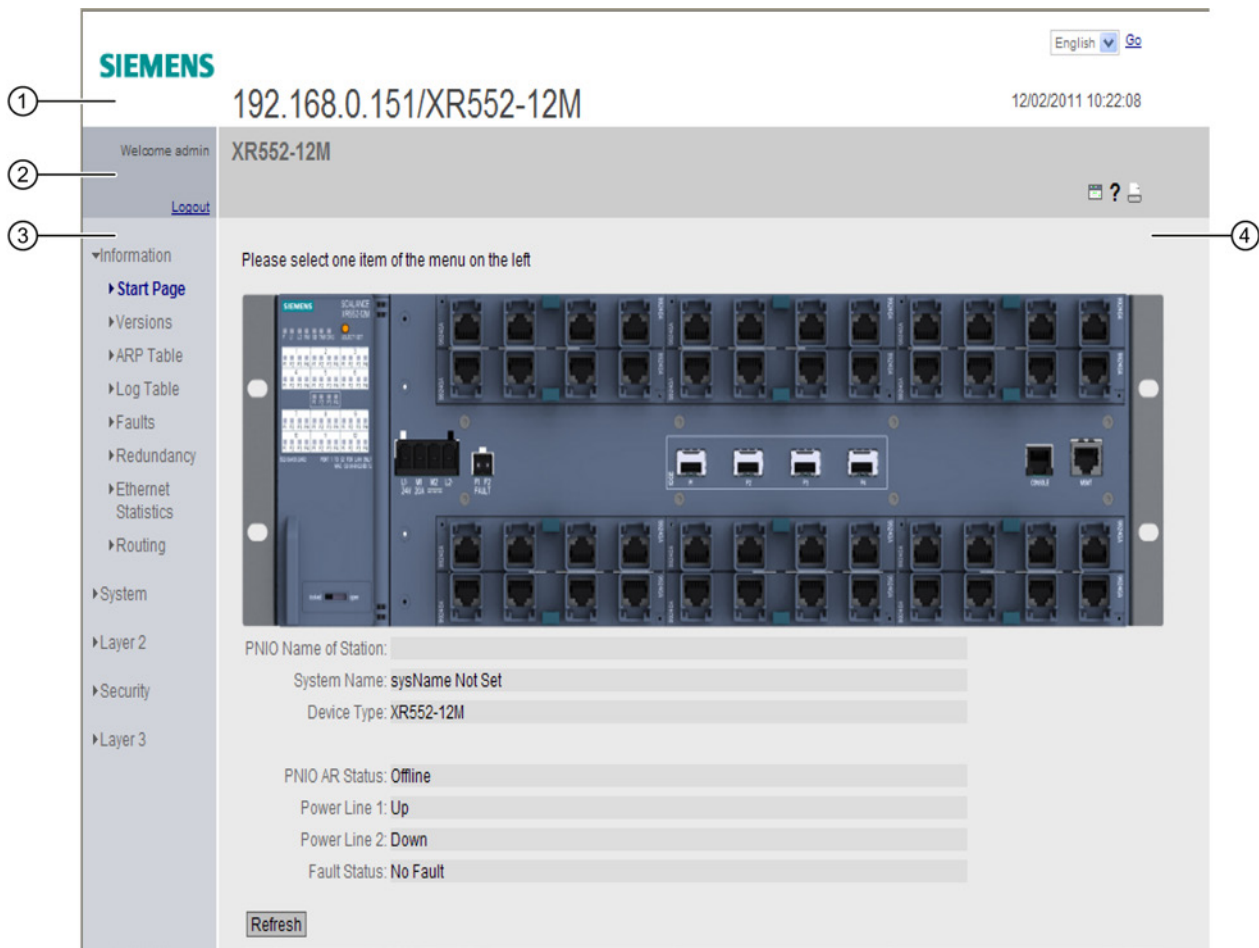
#### View of the Start page

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
- Display of: "System Location/System Name"
  - "System Location" contains the location of the device.  
With the settings when the device ships, the in-band port 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 time and date

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

## Display area (2)

In the upper part of the display area, you can see the full title of the currently selected menu item.

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

- **Printer** 

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 browser.

---

- **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.

- **LED simulation** 

Each component of a 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. Unoccupied slots or unused connectors are displayed as a gray LED. The meaning of the LED displays is described in the operating instructions.

If you click the simulated "Select/Set" button, you can change the display mode (LEDs DM or D1/D2).

If you click this button, you open the window for the LED simulation. You can show this window during a change of menu and move it as necessary. To close the LED simulation, click the close button in the LED simulation window.

- **Logging out**

You can log out from any WBM page by clicking the "Logout" link.

## 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.

Content area (4)

The content area shows a graphic of the device:

- SCALANCE X500

The graphic of the SCALANCE X-500 is static.

- SCALANCE XM400

The graphic of the SCALANCE XM400 is dynamic. The basic device is always shown. If extenders are connected to the basic device, these are also shown.

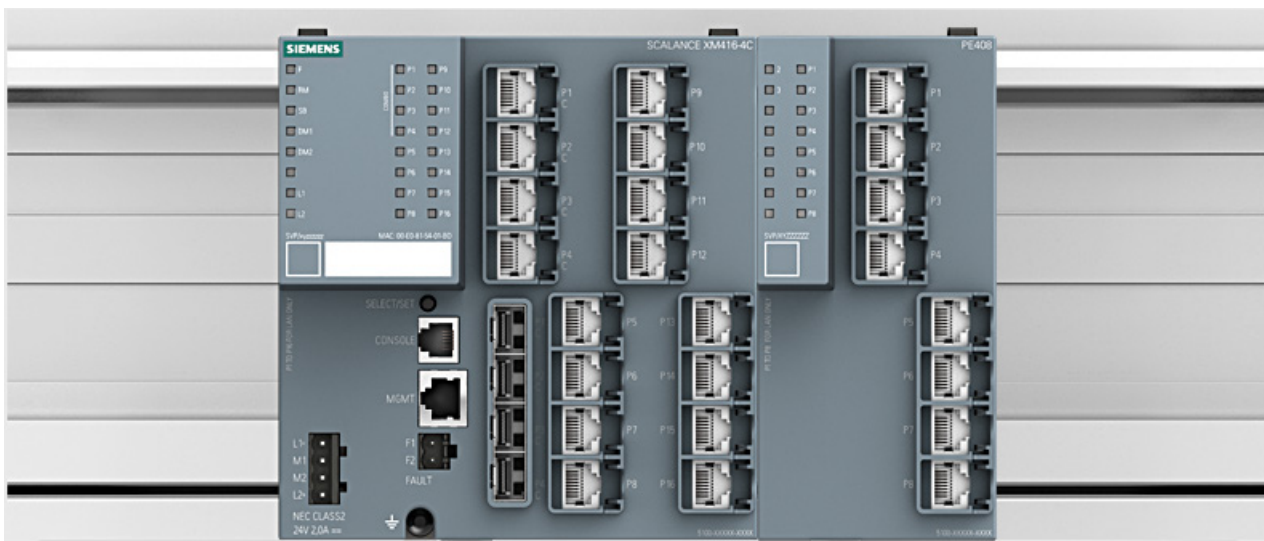


Figure 5-1 Example of a device graphic: SCALANCE XM416-4C with one port extender PE408

In the navigation area, click a menu to display the pages of the WBM in the content area.

The following is displayed below the device graphic:

- PNIO Name of Station  
Shows the PROFINET IO device name.
- System Name  
Shows the system name of the device.
- Device Type  
Shows the type of the device.
- PNIO AR Status  
Shows the PROFINET IO application relation status.
  - Online  
There is a connection to a PROFINET IO controller. The PROFINET IO controller has downloaded its configuration data to the device. The device can send status data to the PROFINET IO controller.  
In this status, the parameters set by the PROFINET IO controller cannot be configured on the device.
  - Offline  
There is no connection to the PROFINET IO controller.

- Power Line 1 / Power Line 2
  - Up  
Power supply 1 or 2 is applied
  - Down:  
Power supply 1 or 2 is not applied or is below the permitted voltage.
- Faults 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" login.

---

- **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.
- **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. Deleting also results in an update of the page in the WBM.
- **Page down with "Next"**  
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 up with "Prev"**  
The number of data records that can be displayed on a page is limited. Click the "Prev" button to page up through the data records.

### 5.3.2 Versions

#### Versions of hardware and software

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

Version Information			
Hardware	Name	Revision	Order ID
Basic Device	SCALANCE XR552-12M (L3)	3	6GK5 552-0AR00-2AR2
Slot3	MM992-4CUC	1	6GK5 992-4GA00-8AA0
Software	Description	Version	Date
Firmware	SCALANCE XR500 Firmware	T03.00.00.00_41.01.02	03/12/2013 20:00:01
Bootloader	SCALANCE XR500 Bootloader	T03.00.00.00_40.01.04	03/05/2013 20:00:09
Firmware_Running	Current running Firmware	T03.00.00.00_41.01.02	03/12/2013 20:00:01

#### Description of the displayed values

Table 1 has the following columns:

- **Hardware**
  - Basic Device  
Shows the basic device
  - PX.X  
X.X = port in which the SFP module is inserted.
  - Slot X  
"X" = slot number: Module plugged into this slot.
- **Name**  
Shows the name of the device or module.
- **Revision**  
Displays the hardware version of the device.
- **Order ID**  
Shows the order number of the device or module.

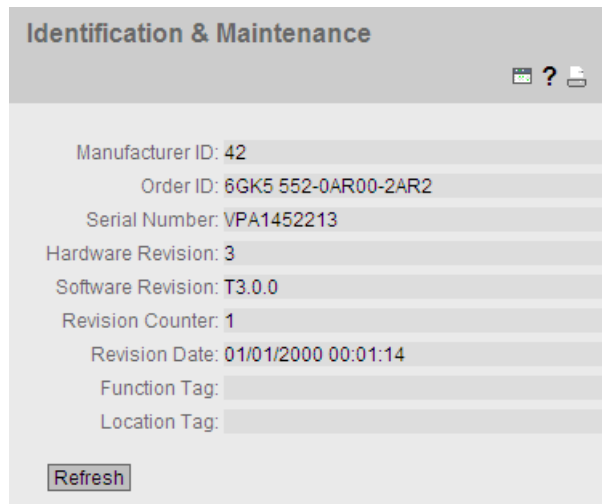
Table 2 has the following columns:

- **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.
- **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.

### 5.3.3 I&M

#### Identification and Maintenance data

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



#### 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 Revision**  
Shows the software version.
- **Revision Counter**  
Shows the revision counter: Counter for revisions since the initial commissioning
- **Revision Date**  
Revision date: 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 (location identifier) of the device. The location identifier (LID) is created during configuration of the device with HW Config of STEP 7.



## 5.3.4 ARP table

### Assignment of MAC address and IP address

With the Address Resolution Protocol (ARP), there is a unique assignment of MAC address to IP 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.

Address Resolution Protocol (ARP) Table			
Interface	MAC Address	IP Address	Media Type
vlan1	00-13-ce-63-59-bf	192.168.0.97	Dynamic
vlan1	6c-62-6d-6f-38-31	192.168.0.100	Dynamic

2 entries.

### Description

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 target device.
- **IP Address**  
Shows the IP address of the target device.
- **Media Type**  
Shows the type of connection.
  - Dynamic  
The device recognized the address data automatically.
  - Static  
The addresses were entered as static addresses.

### 5.3.5 Log table

#### Logging events

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

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

You cannot configure anything on this page.

**Log Table**

Severity Filters

Info  
 Warning  
 Critical

Restart	System Up Time	Severity	Log Message
4	23:33:46	4 - Warning	OSPF Interface 'Vlan1': Network 0.0.0.1 (Router 0.0.0.1) trans
4	23:33:09	4 - Warning	VRRP Interface 'Vlan1': Virtual Router 1 (VLAN 1) transitioned
4	23:33:09	6 - Info	MSTP Port State Change,
4	23:33:09	6 - Info	MSTP Port State Change,
4	23:33:08	6 - Info	IP communication is possible. Remote logging activated.
4	23:33:06	4 - Warning	VRRP Interface 'Vlan1': Virtual Router 1 (VLAN 1) transitioned
4	23:33:06	4 - Warning	OSPF Interface 'Vlan1': Network 0.0.0.1 (Router 0.0.0.1) trans
4	23:33:06	6 - Info	New Fault state: "Link up on P3.4."
4	23:33:06	6 - Info	Link up on P3.4.
4	23:33:03	4 - Warning	IP communication is not possible. Remote logging deactivat Please check IP configuration and network connectivity.

1 - 10 of 131 entries. [Show all](#) 1 [Next](#)

#### 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**  
Information
- **Warning**  
Warnings
- **Critical**  
Critical

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

## Description of the displayed values

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

If the system time is set, the time is also displayed at which the event occurred.

## Description of the buttons and input boxes

### "Clear" button

Click this button to delete the content of the event log file. The display is also cleared. The restart counter is only reset after you have restored the device to the factory settings and restarted the device.

---

### Note

The number of entries in this table is restricted to 400. When this number is reached, the oldest entries are discarded. The table remains permanently in memory.

---

### "Entries per page" input box

Enter the number of displayed entries per page. The default is 10.

### "Show all" button

Click this button to display all the entries on the WBM page. Note that displaying all messages can take some time.

### "Next" button

Click this button to go to the next page.

### "Prev" button

Click this button to go to the previous page.

### Drop-down list for page change

From the drop-down list, select the page you want to go to.

### 5.3.6 Faults

#### Error status

This page displays any errors that occur. Errors of the "Cold/Warm Start" event can be deleted following confirmation.

If there are no more unanswered error/fault messages, the fault LED goes off.

The time calculation always begins after the last system start. When the system is restarted, a new entry with the type of restart is created in the fault memory.

Fault Time	Fault Description	Clear Fault State
23s	Fan module faulty.	Clear Fault State
41s	Cold start performed.	Clear Fault State
49s	Link up on P3.4.	Clear Fault State

#### Description

The "No. of Signaled Faults" box shows the number of faults that have occurred since the last startup. Click the "Reset Counters" button to reset this value.

The table contains the following columns:

- **Fault Time**  
Shows the time the device has been running since the last restart when the described fault occurred.
- **Fault Description**  
Display of the fault status for the device.
- **Clear Fault State**  
To delete files of the "Cold/Warm Start" event, click the "Clear Fault State" button.

## 5.3.7 Redundancy

### 5.3.7.1 Spanning Tree

#### Introduction

The page shows the current information about the Spanning Tree and the settings of the root bridge.

Spanning Tree

Spanning Tree VRRP Statistics Ring Redundancy Standby

Spanning Tree Mode: **MSTP**

Instance ID: 0

Bridge Priority: 32768

Bridge Address: 08-00-06-4b-01-00

Root Priority: 32768

Root Address: 08-00-06-4b-01-00

Root Cost: 0

Bridge Status: **This bridge is the root**

Regional Root Priority: 32768

Regional Root Address: 08-00-06-4b-01-00

Regional Root Cost: 0

Port	Role	State	Oper. Version	Priority	Path Cost	Edge Type	P.LP. Type
P1.9	Designated	Forwarding	MSTP	128	200000	Edge Port	P.LP

Refresh

#### 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 > MSTP > 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 ports leading away from the root bridge.
  - 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.

- **State**

Displays the current status of the port. The values are only displayed. The parameter depends on the configured protocol. The following statuses 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**

Describes the type of spanning tree in which the port operates
- **Priority**

If the path calculated by 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.  
If the value in the "Cost Calc" field is "0", the automatically calculated value is displayed. Otherwise, the value of the "Cost Calc" field 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:

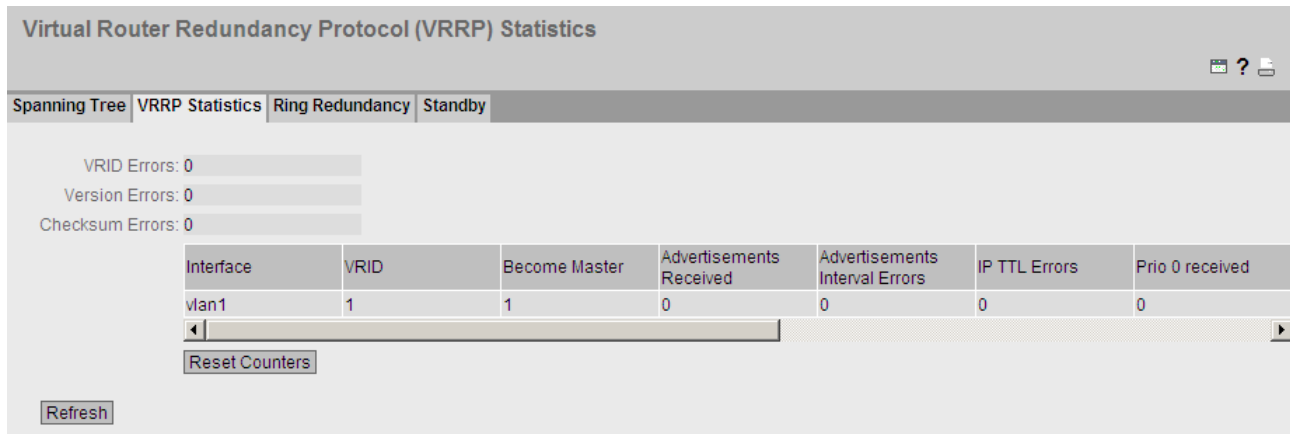
  - 10,000 Mbps = 2,000
  - 1000 Mbps = 20,000
  - 100 Mbps = 200,000
  - 10 Mbps = 2,000,000.

- **Edge Type**  
Shows the type of the connection. The following values are possible:
  - Edge Port  
There is an end device at this port.
  - No Edge Port  
There is a Spanning Tree or Rapid Spanning Tree device at this port.
- **P.t.P. Type**  
Shows the type of 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.

### 5.3.7.2 VRRP Statistics

#### Introduction

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



#### Description of the displayed values

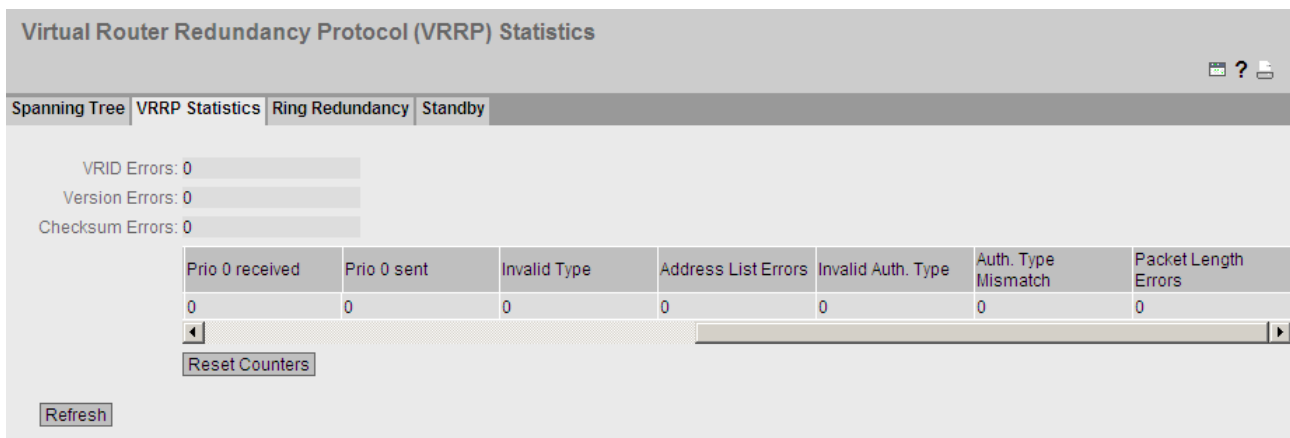
The following fields are displayed:

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



The table has the following columns:

- **Interfaces**  
Interface to which the settings relate.
- **VRID**  
Shows the ID of the virtual router.  
Valid values are 1 to 255.
- **Become Master**  
Shows how often this virtual router changed to the "Master" status.
- **Advertisements Received**  
Shows how often a VRRP packet was received that contained a bad address list.
- **Advertisements Interval Errors**  
Shows how many bad VRRP packets were received whose interval does not match the value set locally.
- **IP TTL Errors**  
Shows how many bad VRRP packets were received whose TTL (Time to live) value in the IP header is incorrect.
- **Prio 0 received**  
Shows how many VRRP packets with priority 0 were received. VRRP packets with priority 0 are sent when a master router is shut down. These packets allow a fast handover to the relevant backup router.
- **Prio 0 sent**  
Shows how many VRRP packets with priority 0 were sent. Packets with priority 0 are sent when a master router is shut down. These packets allow a fast handover to the relevant backup router.

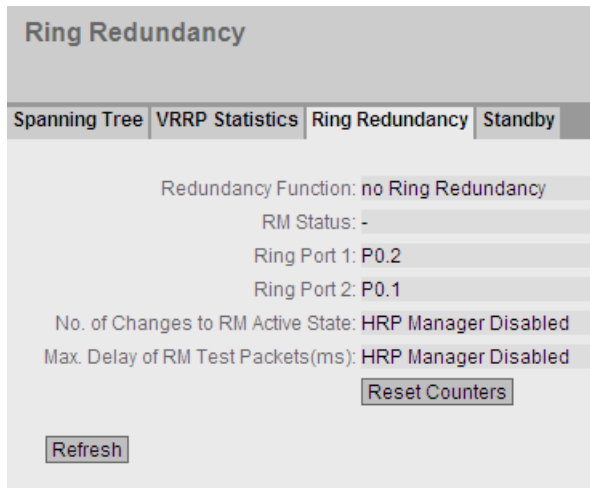


- **Invalid Auth. Type**  
Shows how many bad VRRP packets were received whose authentication type was not type 0. Type 0 means "no authentication".
- **Auth. Type Mismatch**  
Shows how many bad VRRP packets were received whose authentication type does not match.
- **Packet Length Error**  
Shows how many bad VRRP packets were received whose length is not correct.

### 5.3.7.3 Ring redundancy

#### Information on ring redundancy

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



The table has the following columns:

- **Redundancy Function**

The "Redundancy Function" column shows the role of the device within the ring:

- No Ring Redundancy (off)  
The IE switch is operating without redundancy function.
- HRP Client  
The IE switch is operating as an HRP client.
- HRP Manager  
The IE switch is operating as an HRP manager.
- MRP Client  
The IE switch is operating as an MRP client.
- MRP Manager  
The IE switch is operating as an MRP manager.

- **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 (RM function 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.

- If media redundancy in ring topologies is completely disabled, ring ports configured last are displayed and the text "Ring Redundancy disabled" is displayed.

- **Ring Port 1 and Ring Port 2**

The "Ring Port 1" and "Ring Port 2" columns show the ports being used as ring ports.

- **No. of Changes to RM Active State**

Indicates how often the redundancy manager changed to the active status. If ring redundancy is disabled or the device is not the HRP manager, the text "HRP Manager Disabled" appears in this box.

- **Max. Delay of RM Test Packets(ms)**

Shows the maximum delay of the test packets in milliseconds. If ring redundancy is disabled or the device is not the HRP manager, the text "HRP Manager Disabled" appears in this box.

- Click the "Reset Counters" button to reset the counters on this page.

### 5.3.7.4 Standby redundancy

#### Information on standby redundancy

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

---

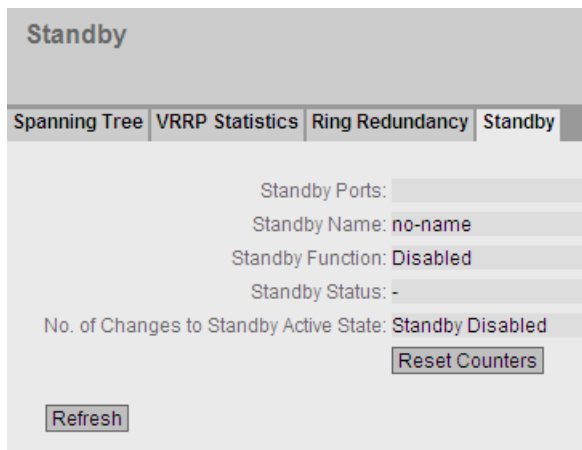
**Note****Device with the higher MAC address becomes master**

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:



The meaning of the displayed boxes is as follows:

- **Standby Port**

The "Standby Port" display box 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:**  
Standby link is disabled. The device is operating neither as master nor slave. The standby port is working 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:**  
Existing connection to the partner device has been lost. In this case there is either a physical fault (for example, device failure, link down) or the configuration on the partner device was modified (for example different connection name, standby link disabled).

- **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.

- **No. of Changes to Standby Active State**

Indicates how often the redundancy manager changed to the standby status. If ring redundancy is disabled, the text "Standby Disabled" appears in this box.

- Click the "Reset Counters" button to reset the counters on this page.

### 5.3.8 Ethernet statistics

#### 5.3.8.1 Packet size

##### Frames sorted by length

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

**Ethernet Statistics: Packet Size**

Packet Size	Packet Type	Packet Error				
Port	64	65-127	128-255	256-511	512-1023	1024-max
P0.1	364789	87385	8147	102960	9684	69842
P0.2	0	0	0	0	0	0
P0.3	0	0	0	0	0	0
P0.4	0	0	0	0	0	0
P1.1	104117	45085	126	17535	21	11
P1.2	211416	60841	5521	55533	1024	26649
P1.3	0	0	0	0	0	0
P1.4	104117	44917	141	34819	19	17
P2.1	0	0	0	0	0	0
P2.2	0	0	0	0	0	0
P2.3	0	0	0	0	0	0
P2.4	0	0	0	0	0	0
P3.1	0	0	0	0	0	0
P3.2	0	0	0	0	0	0
P3.3	0	0	0	0	0	0
P3.4	0	0	0	0	0	0
P4.1	0	0	0	0	0	0

Reset Counter

Refresh

##### Description of the displayed values

The table has the following columns:

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

---

##### Note

##### Display of frame statistics

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

---

- **Frame lengths**

The other columns after the port number contain the absolute numbers of incoming 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.

---

## Description of the button

**"Reset Counter" button**

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

### 5.3.8.2 Packet type

#### Received frames sorted by type

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

Ethernet Statistics: Packet Type			
Packet Size	Packet Type	Packet Error	
Port	Unicast	Multicast	Broadcast
P0.1	0	0	0
P0.2	0	0	0
P0.3	0	0	0
P0.4	0	0	0
P1.1	7486	720	28
P1.2	0	0	0
P1.3	5793	739	25
P1.4	2306	207	74
P2.1	0	0	0
P2.2	0	0	0

Reset Counter

Refresh

#### Description of the displayed values

The table has the following columns:

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

#### Description of the button

##### "Reset Counters" button

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



### 5.3.8.3 Packet Error

#### Bad received frames

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

Ethernet Statistics: Packet Error						
Packet Size	Packet Type	Packet Error				
Port	CRC	Undersize	Oversize	Fragments	Jabbers	Collisions
P0.1	0	0	0	0	0	0
P0.2	0	0	0	0	0	0
P0.3	0	0	0	0	0	0
P0.4	0	0	0	0	0	0
P1.1	0	0	0	0	0	0
P1.2	0	0	0	0	0	0
P1.3	0	0	0	6	0	6
P1.4	0	0	0	0	0	0

Reset Counter

Refresh

#### Description of the displayed values

The table has the following columns:

- **Port**  
Shows the available ports and link aggregations. The port is made up of the module number and the port number, for example port 0.1 is module 0, port 1.
- **Error types**  
The other columns after the port number contain the absolute numbers of the incoming frames according to their error type.

In the columns of the table, a distinction is made according to the following error types:

- **CRC**  
Packets whose content does not match the CRC checksum.
- **Undersize**  
Packets with a length less than 64 bytes.
- **Oversize**  
Packets discarded because they were too long.
- **Fragments**  
Packets with a length less than 64 bytes and a bad CRC checksum.
- **Jabbers**  
VLAN-tagged packets with an incorrect CRC checksum that were discarded because they were too long.

- Collisions  
Detected collisions.

### Description of the button

#### "Reset Counters" button

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

## 5.3.9 Routing

### 5.3.9.1 Routing Table

#### Introduction

This page shows the routing table of the device.

Layer 3: Routing Table					
Routing Table	OSPFv2 Interfaces	OSPFv2 Neighbors	OSPFv2 Virtual Neighbors	OSPFv2 LSDB	
Destination Network	Subnet Mask	Gateway	Interface	Metric	Routing Protocol
120.80.0.0	255.255.0.0	0.0.0.0	vlan1	0	Connected
152.80.1.0	255.255.255.0	162.80.1.1	P3.1	2	OSPF
162.80.1.0	255.255.255.0	0.0.0.0	P3.1	0	Connected
172.80.1.0	255.255.255.0	0.0.0.0	vlan3	0	Connected
182.80.1.0	255.255.255.0	172.80.1.2	vlan3	2	OSPF

#### 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.
- **Interface**  
Shows the interface for this route.

- **Metric**  
Shows the metric of the route. The higher 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

### 5.3.9.2 OSPFv2 Interfaces

#### Overview

This page shows the configuration of the OSPF interface.

Open Shortest Path First v2 (OSPFv2) Interfaces						
Routing Table	OSPFv2 Interfaces	OSPFv2 Neighbors	OSPFv2 Virtual Neighbors	OSPFv2 LSDB		
IP Address	Area ID	Interface Status	OSPF Status	Designated Router	Backup Designated Router	Events
120.80.1.18	0.0.0.0	Designated Router	enabled	120.80.1.18	0.0.0.0	2
162.80.1.2	3.0.0.0	Designated Router	enabled	162.80.1.2	162.80.1.1	3
172.80.1.1	3.0.0.0	Backup D. Router	enabled	172.80.1.2	172.80.1.1	4

#### Description of the displayed values

The table has the following columns:

- **IP Address**  
Shows the IP address of the OSPF interface
- **Area ID**  
Shows the Area ID to which the OSPF interface belongs.

- **Interface Status**  
Shows the status of the interface:
  - Down  
The interface is not available.
  - Loop back  
Loop back interface
  - Waiting  
Starting up and negotiating the interface.
  - Point to Point  
Point-to-point link
  - Designated Router  
The router is a designated router and generates network LSAs.
  - Backup D. Router  
The router is the backup router for the designated router.
  - Other D. Router  
The Interface has started up. The router is neither a designated nor a designated backup router.
- **OSPF Status**  
Shows the status of OSPF.
  - Enabled: OSPF is enabled on the interface.
  - Disabled: OSPF is disabled on the interface.
- **Designated Router**  
Shows the IP address of the designated router for this OSPF interface.
- **Backup Designated Router**  
Shows the IP address of the designated backup router for this OSPF interface.
- **Events**  
Shows the number of status changes of OSPF.

### 5.3.9.3 OSPFv2 Neighbors

#### Overview

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

Open Short Path First v2 (OSPFv2) Neighbors							
Routing Table	OSPFv2 Interfaces	OSPFv2 Neighbors	OSPFv2 Virtual Neighbors	OSPFv2 LSDB			
IP Address	Router ID	Status	Assoc. Area Type	Priority	Hello Suppr.	Retrans Queue	Events
162.80.1.1	1.1.1.1	full	Normal	1	2	0	6
172.80.1.2	3.3.3.3	full	Normal	1	2	0	6

Refresh

#### Description of the displayed values

The table has the following columns:

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

---

**Note**

**Normal status**

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

---

- **Assoc. Area Type**

Shows the area type via which the neighbor-neighbor relation is maintained. The following area types exist:

- Standard
- Stub
- NSSA
- Backbone

- **Priority**

Shows the priority of the neighbor router. This is only significant when selecting the designated router on a network. For virtual neighbor routers, this information is irrelevant.

- **Hello Suppr.**

Shows the suppressed Hello packets to the neighbor router. This field normally displays "no".

- **Retrans Queue**

Shows the length of the queue with Hello packets still to be transmitted.

- **Events**

Shows the number of status changes.

### 5.3.9.4 OSPFv2 Virtual Neighbors

#### Overview

This page shows the configured virtual neighbors.

Open Short Path First v2 (OSPFv2) Neighbors

Routing Table	OSPFv2 Interfaces	OSPFv2 Neighbors	OSPFv2 Virtual Neighbors	OSPFv2 LSDB		
IP Address	Router ID	Status	Transit Area ID	Hello Suppr.	Retrans Queue	Events
162.80.1.1	1.1.1.1	full	3.0.0.0	1	0	5
172.80.1.2	3.3.3.3	full	3.0.0.0	1	0	5

Refresh

#### Description of the displayed values

The table has the following columns:

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

**Note**

**Normal status**

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

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

**5.3.9.5 OSPFv2 LSDB**

**Overview**

The link state database is the central database for managing all links within an area. It consists of the link state advertisements (LSAs). The most important data of these LSAs is shown on the this WBM page.

Open Shortest Path First v2 (OSPFv2) Link State Database				
Routing Table	OSPFv2 Interfaces	OSPFv2 Neighbors	OSPFv2 Virtual Neighbors	OSPFv2 LSDB
Area ID	Link State Type	Link State ID	Router ID	Sequence No
0.0.0.0	Router	1.1.1.1	1.1.1.1	-2147483645
0.0.0.0	Router	2.2.2.2	2.2.2.2	-2147483600
0.0.0.0	Router	3.3.3.3	3.3.3.3	-2147483645
3.0.0.0	Network	162.80.1.2	2.2.2.2	-2147483606
3.0.0.0	Network	172.80.1.2	3.3.3.3	-2147483606
3.0.0.0	Summary	120.80.0.0	2.2.2.2	-2147483605
3.0.0.0	Summary	152.80.1.0	1.1.1.1	-2147483606
3.0.0.0	Summary	182.80.1.0	3.3.3.3	-2147483605



## Description of the displayed boxes

The table has the following columns:

- **Area ID**  
Shows the ID of the area to which the LSA belongs. If the LSA is an external connection, '-' is displayed.
- **Link State Type**  
Shows the LSA type. The following values are possible:
  - Unknown  
LSA type is unknown.
  - Router  
The router LSA (Type 1) is sent by the OSPF router within an area. The LSA contains information about the status of all router interfaces.
  - Network  
The network LSA (Type 2) is sent by the designated router within an area. The LSA contains a list of routers connected to the network.
  - NSSA External  
The NSSA external LSA (Type 7) is sent by the NSSA-ASBR within an NSSA. The NSSA-ASBR receives LSAs of Type 5 and converts the information to LSAs of Type 7. The NSSA router can forward these LSAs within an NSSA.
  - Summary  
The summary LSA (Type 3) is sent by the ABR within an area. The LSA contains information about routes to other networks.
  - AS Summary  
The AS summary LSA (Type 4) is sent by the area border router within an area. The LSA contains information about routes to other autonomous systems.
  - AS External  
The AS external LSA (Type 5) is sent by the AS border router within an autonomous system. The LSA contains information about routes from one network to another.
- **Link State ID**  
Shows the ID of the LSA.
- **Router ID**  
Shows the ID of the router that sent this LSA.
- **Sequence No.**  
Shows the sequence number of the LSA. Each time an LSA is renewed, this sequence number is incremented by one.

## 5.4 The "System" menu

### 5.4.1 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.

**System Configuration**

Telnet Server  
 SSH Server  
 HTTPS Server only  
 SMTP Client  
 Syslog Client

DCP Server: Read/Write  
Time: Manual  
SNMP: SNMPv1v2cV3  
 SNMPv1v2 Read-Only  
 SNMPv1 Traps

NFC (Near Field Communication)

Configuration Mode: Trial  
**Write Startup Config**

Set Values Refresh

#### Description of the displayed boxes

The page contains the following boxes:

- **"Telnet Server" check box**  
Enable or disable the "Telnet Server" service for unencrypted access to the CLI.
- **"SSH Server" check box**  
Enable or disable the "SSH Server" service for encrypted access to the CLI.
- **"HTTPS Server only" check box**  
Enable or disable the SIMATIC Time Client.
- **"SMTP Client" check box**  
Enable or disable the SMTP client. You can configure other settings in "System > SMTP Client".

- **"Syslog Client"** check box  
Enable or disable the Syslog client. You can configure other settings in "System > Syslog Client".
- **"DCP Server"** drop-down list  
Specify whether or not the device can be accessed with DCP (Discovery and Configuration Protocol):
  - "-" (disabled)  
DCP is disabled. Device parameters can neither be read nor modified.
  - Read/Write  
With DCP, device parameters can be both read and modified.
  - Read-Only  
With DCP, device parameters can be read but cannot be modified.
- **"Time"** drop-down list  
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 > Time > Manual Setting".
  - 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".
  - SIMATIC Time  
The system time is set using a SIMATIC time transmitter. You can configure other settings in "System > System Time > SIMATIC Time Client".
- **"SNMP" drop-down list:**  
Select the protocol from the drop-down list. The following settings are possible:
  - "-" (SNMP disabled)  
Access to device parameters via 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"** check box  
Enable or disable write access to SNMP variables with SNMPv1/v2c.
- **"SNMPv1 Traps"** check box  
Enable or disable the sending of traps (alarm frames). You can configure other settings in "System > SNMP > Traps".
- **"SINEMA Configuration Interface"** check box  
Enable or disable the SINEMA configuration interface

- **"NFC" check box** (only for SCALANCE XM400)  
Activate or deactivate the "NFC" (Near Field Communication) function.  
You will find further information on NFC in the "SCALANCE XM400" Operating Instructions.
- **"Configuration Mode" drop-down list:**  
Select the mode from the drop-down list. The following modes are possible:
  - Automatic Save  
Automatic save mode. Approximately 1 minute after the last parameter change or when you restart the device, the configuration is automatically saved.
  - Trial  
Trial mode. In Trial mode, although changes are adopted, they are not saved in the configuration file (startup configuration).  
To save changes in the configuration file, use the "Write Startup Config" button. The "Write Startup Config" button is displayed when you set trial mode. The message "Trial Mode Active – Press "Write Startup Config" button to make your settings persistent" is also displayed in the display area as soon as there are unsaved changes. This message can be seen on every WBM page until the changes made have either been saved or the device has been restarted.

### Steps in configuration


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.

## 5.4.2 General

### 5.4.2.1 Device

#### General device information

This page contains the general device information.



The screenshot shows a web interface titled "Device" with two tabs: "Device" and "Coordinates". The "Device" tab is active. Below the tabs, there are several rows of information:

- Current System Time: 02/17/2012 10:15:00
- System Up Time: 1h 8m 5s
- Device Type: SCALANCE XM400 (read-only)
- System Name: sysName Not Set
- System Contact: sysContact Not Set
- System Location: sysLocation Not Set

At the bottom of the form, there are two buttons: "Set Values" and "Refresh".

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

#### Description

The page contains the following boxes:

- **Current System Time**  
Shows the current system time. The system time is either set by the user or by a time-of-day frame: either SINEC H1 time-of-day frame, NTP or SNTP. (readonly)
- **System Up Time**  
Shows the running time of the device since the last restart. (readonly)
- **Device Type**  
Shows the type of the device. (readonly)
- **"System Name" input box**  
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" input box**  
You can enter the name of a contact person responsible for managing the device. A maximum of 255 characters are possible.
- **"System Location" input box**  
You can enter the installation location of the device. 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.

At the start and end of the boxes **"System Name"**, **"System Contact"** and **"System Location"**, the characters "<", ">" and "space" are not permitted.

---

**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.

**5.4.2.2 Coordinates**

**Information on geographic coordinates**

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

**Getting the coordinates**

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

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

Geographic Coordinates

Device | Coordinates

Latitude: e.g. DD°MM'SS"

Longitude: e.g. DDD°MM'SS"

Height: e.g. dddd m

Set Values Refresh

## Description

The page contains the following boxes. These are purely information 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**

Geographical 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"**

Geographical 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 latitude in the "Latitude" input box.
2. Enter the longitude in the "Longitude" input box.
3. Enter the height in the "Height" input box.
4. Click the "Set Values" button.

### 5.4.3 Agent IP

#### Configuration of the IP addresses

Here, you specify the IP configuration for the device. With layer 3 devices, this call references the layer 3 menu "Subnets Configuration"

**Connected Subnets Configuration**

Overview | Configuration

Interface (Name): Out-Band (eth0) ▼

Interface Name: eth0

MAC Address: 00-5e-1d-d2-75-3d

DHCP

IP Address: 192.168.0.30

Subnet Mask: 255.255.255.0

Address Type: Primary

TIA Interface

Set Values Refresh

#### Note

The IP addresses of the in-band interface and the out-band interface must belong to different subnets.

#### Description of the displayed boxes

The page contains the following boxes:

- **"Interface (Name)" drop-down list**  
Select the interface to be configured. Here, you can also select the Out Of Band interface.
- **"Interface Name" input box**  
Enter the name of the interface.
- **"IP Address" input box**  
In "In-Band", you enter the IP address via which the management will be accessible via the switch ports. In "Out-Band", enter the IP address at which the management will be accessible via the out-of-band port.  
If you change the IP address, the Web browser should adjust to the new address automatically. If this does not happen, enter the new address in the Web browser manually.
- **"Subnet Mask" text box**  
In "In-Band", enter the subnet mask of the CPU module and in "Out-Band" the subnet mask of the out-of-band port.



- **"Default Gateway" text box**  
If the device is required to communicate with devices (diagnostics stations, e-mail servers etc.) in another subnet, enter the IP address of the default gateway here. The out-band port it is not accessible from a different subnet.
- **"Agent VLAN ID" drop-down list**  
From the drop-down list, select the VLAN ID for the in-band management. You can only select VLANs that have already been configured.

---

**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.

---

- **Text box "MAC Address"**  
Shows the MAC address of the device. The MAC address is linked to the hardware and cannot be modified.

## Steps in configuration

**Follow the steps below to configure the in-band interface:**

1. In the input boxes under "In Band", enter the IP address, subnet mask and the default gateway.
2. Select the assigned VLAN ID from the "Agent VLAN ID" drop-down list.
3. Click the "Set Values" button.

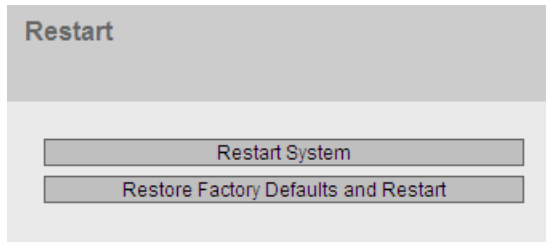
**Follow the steps below to configure the out-of-band interface:**

1. In the input boxes under "Out Band", enter the IP address and subnet mask.
2. Click the "Set Values" button.

### 5.4.4 Restart

#### Resetting to the defaults

In this menu, there is a button with which you can restart the device and the option of resetting to the device defaults.



---

#### Note

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.
  - Any modifications you have made only become active on the device after clicking the "Set Values" button on the relevant WBM page. If the device is in "Trial Mode", configuration modifications must be saved manually before a restart. In "Autosave mode", the last changes are saved automatically before a restart.
- 

#### Description of the displayed boxes

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

- **"Restart System" button**  
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 learned entries in the address table are deleted. You can leave the browser window open while the device restarts. You then need to log in again.
- **"Restore Factory Defaults and Restart" button**  
Click this button to restore the factory defaults for the configuration. The protected defaults are also reset.  
An automatic restart is triggered.

---

#### Note

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

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

---

## 5.4.5 Load & Save

### 5.4.5.1 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 PC to the devices. This means, for example, that you can also load new firmware from a file located on your client PC.

---

**Note****Incompatibility with predecessor versions**

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.

**Incompatibility with previous versions with PLUG inserted**

During the installation of a previous version, the configuration data can be lost. In this case, the device starts up with the factory settings after the firmware has been installed. In this situation, if a PLUG is inserted in the device, following the restart, this has the status "Not Accepted" since the PLUG still has the configuration data of the previous more up-to-date firmware. This allows you to return to the previous, more up-to-date firmware without any loss of configuration data. If the original configuration on the PLUG is no longer required, the PLUG can be deleted or rewritten manually using System > PLUG.

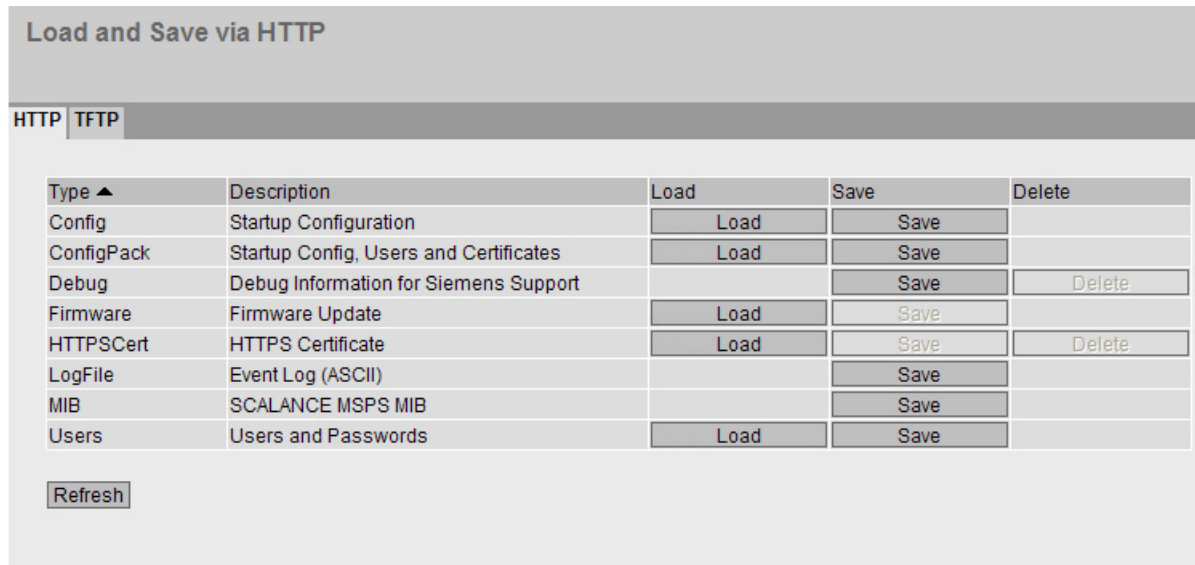
---

**Note****Configuration files and trial mode/Automatic Save mode**

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

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

---



### Description of the displayed boxes

The table has the following columns:

- **Type**  
Shows the file type.
- **Description**  
Shows the short description of the file type.
- **Load**  
With this button, you can upload files to the device. The button can be enabled, if this function is supported by the file type.
- **Save**  
With this button, you can save files from the device. The button can only be enabled if this function is supported by the file type and the file exists on the device.
- **Delete**  
With this button, you can delete files from the device. The button can only be enabled if this function is supported by the file type and the file exists on the device.
- **Yes**  
Start the action
- **No**  
The action is discarded.

---

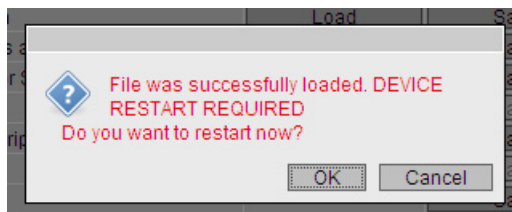
#### Note

Following a firmware update, delete the cache of the Web browser.

---

### Loading new firmware

After successfully downloading the firmware, you will be requested to restart the device.



Restart the device and continue to configure the newly started firmware.

## Steps in configuration

### Loading files using HTTP

1. Start the load function by clicking the one of the "Load" buttons.  
The dialog for uploading a file opens.
2. Go to the file you want to upload.
3. Click the "Open" button in the dialog.  
The file is now uploaded.
4. When the message "restart required" appears, click the "Yes" button to trigger the restart. If you click the "No" button, there is no device restart. The changes only take effect after a restart.

### Saving files using HTTP

1. Start the save function by clicking the one of the "Save" buttons.
2. You will be prompted to select a storage location and a name for the file. Or you accept the proposed file name. To make the selection, use the dialog in your browser. After making your selection, click the "Save" button.

### Deleting files using HTTP

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

### Reusing configuration data

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

Follow the steps below to reuse configuration data:

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

Note that the configuration data is coded when it is saved. This means that you cannot edit the files with a text editor.

### 5.4.5.2 TFTP

#### Loading and saving data via a TFTP server

On this page, you can configure the TFTP server and the file names. The WBM also allows you to store device data in an external file on 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 client PC.

---

#### Note

##### Incompatibility with predecessor versions

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.

##### Incompatibility with previous versions with PLUG inserted

During the installation of a previous version, the configuration data can be lost. In this case, the device starts up with the factory settings after the firmware has been installed. In this situation, if a PLUG is inserted in the device, following the restart, this has the status "Not Accepted" since the PLUG still has the configuration data of the previous more up-to-date firmware. This allows you to return to the previous, more up-to-date firmware without any loss of configuration data. If the original configuration on the PLUG is no longer required, the PLUG can be deleted or rewritten manually using System > PLUG.

---

#### Note

##### Configuration files and trial mode/Automatic Save mode

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

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

---

**Load and Save via TFTP**

HTTP | **TFTP**

TFTP Server IP Address:

TFTP Server Port:

Type	Description	Filename	Actions
Config	Startup Configuration	config_SCALANCE_XR500.conf	Select action ▼
ConfigPack	Startup Config, Users and Certificates	configpack_SCALANCE_XR500.zip	Select action ▼
Debug	Debug Information for Siemens Support	debug_SCALANCE_XR500.bin	Select action ▼
Firmware	Firmware Update	firmware_SCALANCE_XR500.sfw	Select action ▼
GSDML	GSDML Device Description	gsdml_SCALANCE_XR500.zip	Select action ▼
HTTPSCert	HTTPS Certificate	https_cert	Select action ▼
LogFile	Event Log (ASCII)	logfile_SCALANCE_XR500.log	Select action ▼
MIB	SCALANCE X MSPS MIB	scalance_x_mspms.mib	Select action ▼
Script	Script	Script.bt	Select action ▼
StartupInfo	Startup Information	startup_SCALANCE_XR500.log	Select action ▼
Users	Users and Passwords	users.enc	Select action ▼

### Description of the displayed boxes

The page contains the following boxes:

- **"TFTP Server IP Address" input box**  
Here, enter the IP address of the TFTP server with which you exchange data.
- **TFTP Server Port**  
Here, enter the port of the TFTP server over which data exchange will be handled. If necessary, you can change the default value 69 to your own requirements.

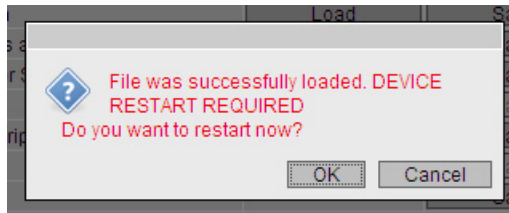
The table has the following columns:

- **Type**  
Shows the file type.
- **Description**  
Shows the short description of the file type.
- **"Filename" input box**  
Enter a file name.
- **"Actions" drop-down list**  
Select the action from the drop-down list. The selection depends on the selected file type, for example the log file can only be saved.  
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.

- **"Yes" button**  
Perform the requested action.
- **"No" button**  
The requested action is not performed

**Loading new firmware**

After successfully downloading the firmware, you will be requested to restart the device.



Restart the device and continue to configure the newly started firmware.

**Steps in configuration**

**Loading or saving data using TFTP**

1. Enter the IP address of the TFTP server in the "TFTP Server IP Address" input box.
2. Enter the server port to be used in the in the "TFTP Server Port" input box.
3. Enter the name of a file in which you want to save the data or take the data from in the "Filename" input box.
4. Select the action you want to execute from the "Actions" drop-down list.
5. Click the "Set Values" button to start the selected actions.
6. When the message "restart required" appears, click the "Yes" button to trigger a restart on the device. Click the "No" button and there is not restart. The changes only take effect after a restart.

**Reusing configuration data**

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

Follow the steps below to reuse configuration data:

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

Note that the configuration data is coded when it is saved. This means that you cannot edit the files with a text editor.



5.4.6 Events

5.4.6.1 Configuration

Selecting system events

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

**Event Configuration**

Configuration | Severity Filters

Signaling Contact Method: aligned ▾  
Signaling Contact Status: open ▾

	E-Mail	Trap	Log Table	Syslog	Fault	Copy To Table
All Events	No Change ▾	No Change ▾	No Change ▾	No Change ▾	No Change ▾	Copy To Table

Event	E-Mail	Trap	Log Table	Syslog	Fault
Cold/Warm Start	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Link Change	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Authentication Failure	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
RMON Alarm	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Power Change	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
RM State Change	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Spanning Tree Change	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Fault State Change	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Standby State Change	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
VRRP State Change	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Loop Detection	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
OSPF State Change	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	

Set Values Refresh

## Description of the displayed boxes

The page contains the following boxes:

- **"Signaling Contact Method" drop-down list**  
Select the reaction of the signaling contact from the drop-down list. The following reactions are possible:
  - conventional  
Default setting for the signaling contact. An error/fault is displayed by the fault LED and the signaling contact is opened. When the error/fault state no longer exists, the fault LED goes off and the signaling contact is closed.
  - aligned  
The way the signaling contact works depends on the error/fault that has occurred. The signaling contact can be opened or closed as required by user actions.
- **"Signaling Contact Status" drop-down list**  
Select the status of the signaling contact from the drop-down list. The following states are possible:
  - close  
Signaling contact is closed.
  - open  
Signaling contact is opened.

The table has the following columns:

- **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

- **Event**

The "Event" column contains the following values:

- Cold/Warm Start  
The device was turned on or restarted by the user.
- Link Change  
This event occurs only when the port status is monitored and has changed, see "System > Fault Monitoring > Link Change".
- Authentication Failure  
This event occurs when attempting access with a bad password.
- Power Change  
This event occurs only when power supply lines 1 and 2 are monitored. It indicates that there was a change to line 1 or line 2. See "System > Fault Monitoring > Power Supply".
- STP/RSTP/MSTP Change  
The STP or RSTP or MSTP topology has changed.
- Fault State Change  
The fault status has changed. The fault status can relate to the activated port monitoring, the response of the signaling contact or the power supply monitoring.
- RMON Alarm  
An alarm or event has occurred relating to the remote monitoring of the system.
- VRRP State Change (only when routing via VRRP)  
The state of the virtual router has changed.
- Loop Detection  
A loop was detected in the network segment.
- OSPF State Change  
The status of OSPF has changed.

### Steps in configuration

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.

### 5.4.6.2 Severity Filters

#### Setting the severity filter

On this page, set the threshold levels for sending system event notifications.

Client Type	Severity
E-Mail	Info
Log Table	Info
Syslog	Info

Buttons: Set Values, Refresh

The first table column shows the client type for which you are making the settings:

- **E-Mail**  
Sending system event messages by e-mail
- **Log Table**  
Entry of system events in the log table
- **Syslog**  
Entry of system events in the Syslog file

Select the required level from the drop-down lists of the second table column.

You can select from the following values:

- **Info**  
System events are processed as of the severity level "Info".
- **Warning**  
System events are processed as of the severity level "Warning".
- **Critical**  
System events are processed as of the severity level "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.

## 5.4.7 SMTP client

### Network monitoring with e-mails

The device provides the option of automatically sending an e-mail if an alarm event occurs (for example to the network administrator). The e-mail contains the identification of the sending device, a description of the cause of the alarm in plain language, and a time stamp. This allows centralized network monitoring to be set up for networks with few nodes based on an E-mail system. When an e-mail event message is received, the WBM can be started by the browser using the identification of the sender to read out further diagnostics information. This is only possible if there is an SMTP server in the internal network.

On this page, you can configure up to three SMTP servers and the corresponding e-mail addresses.

Simple Mail Transfer Protocol (SMTP) Client

SMTP Client

'From'-Field: DEVICE@SCALANCE

Send Test Mail

SMTP Port: 25

SMTP Server IP Address:

SMTP Server IP Address	Receiver Email Address
<input type="checkbox"/> 192.168.10.1	

1 entry.

Create Delete Set Values Refresh

### Description

The page contains the following boxes:

- **"SMTP Client" check box**  
Enable or disable the SMTP client.
- **"'From'-Field" input box**  
Enter the name of the sender that will be included in the e-mail, for example the device name.
- **"SMTP Port" input box**  
Change the port if the SMTP server is not obtainable via port 25.
- **"SMTP Server IP Address" input box**  
Enter the IP address of the SMTP server.
- **"Send Test Mail" button**  
Sends an e-mail for testing.

This table contains the following columns:

- **1st column**  
Select the check box in the row to be deleted.
- **SMTP Server IP Address**  
Shows the SMTP server IP address.
- **Receiver Email Address**  
Enter the e-mail address to which the device sends an e-mail if a fault occurs. The e-mail address can be the address of a single person or a distribution list.

## Procedure

1. Enable the "SMTP Client" option.
2. Enter the IP address of an NTP server in the "SMTP Server IP Address" input box.
3. Click the "Create" button. A new entry is generated in the table.
4. In the "Receiver Email Address" input box, enter the e-mail address to which the device sends an e-mail if a fault occurs.
5. Click the "Set Values" button.

---

### Note

Depending on the properties and configuration of the SMTP server, it may be necessary to adapt the "'From'-Field" box for the e-mails. Check with the administrator of the SMTP server.

---

## 5.4.8 DHCP client

### Setting the DHCP mode

If the DHCP mode is activated, the DHCP client starts a DHCP request to a configured DHCP server and is assigned an IP address as the response. The server manages an address range from which it assigns IP addresses. It is also possible to configure the server so that the client always receives the same IP address in response to its request.

Interface	DHCP
vlan1	<input type="checkbox"/>

### Description

The page contains the following boxes:

- **"DHCP Client Config File Request (Opt.66, 67)" check box**  
Select this option if you want the DHCP client to use options 66 and 67 to download and then enable a configuration file.
- **"DHCP Mode" drop-down list**  
Select the DHCP mode from the drop-down list. The following modes are possible:
  - via MAC Address  
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.
- **"DHCP" check box**  
Enable or disable the DHCP client for the relevant IP interface.

**Procedure**

Follow the steps below to configure the IP address using the DHCP client ID:

1. Enable the "DHCP Client" option.
2. Select the DHCP mode "via DHCP Client ID" from the "DHCP Mode" drop-down list.
3. Enter a character string to identify the device in the enabled "DHCP Client ID" input box. This is then evaluated by the DHCP server.
4. Select the "Client Config File Request (Opt.66, 67)" option, if you want the DHCP client to use options 66 and 67 to download and then enable a configuration file.
5. Click the "Set Values" button.

---

**Note**

If a configuration file is downloaded, this triggers a system restart. Make sure that the option "Client Config File Request (Opt.66, 67)" is no longer set in this configuration file.

---

**5.4.9 SNMP**

**5.4.9.1 General**

**Configuration of SNMP**

On this page, you make the basic settings for SNMP. Enable the check boxes according to the function you want to use.

**Simple Network Management Protocol (SNMP) General**

General | Traps | v3 Groups | v3 Users

SNMP:

SNMPv1v2c Read Only

SNMPv1v2c Read Community String:

SNMPv1v2c Read/Write Community String:

SNMPv1 Traps

SNMPv1v2c Trap Community String:



## Description

The page contains the following boxes:

- **"SNMPv1/v2c/v3" drop-down list**  
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.
  - SNMPv3  
Only SNMPv3 is supported.
- **"SNMPv1/v2c Read Only" check box**  
If you enable this option, SNMPv1/v2c can only read the SNMP variables.

---

### Note

#### Community String

For security reasons, do not use the standard values "public" or "private". Change the community strings following the initial installation.

---

- **"SNMPv1/v2c Read/Write Community String" input box**  
Enter the community string for read and write access of the SNMP protocol.
- **"SNMPv1/v2c Read Community String" input box**  
Enter the community string for access of the SNMP protocol.
- **"SNMPv1 Traps" check box**  
Enable or disable the sending of traps (alarm frames). On the "Trap" tab, specify the IP addresses of the devices to which SNMP traps will be sent.
- **"SNMPv1/v2c Trap Community String" input box**  
Enter the community string for sending SNMPv1/v2 messages.

## Procedure

1. Select the required option from the "SNMP" drop-down list:
  - "-" (disabled)
  - SNMPv1/v2c/v3
  - SNMPv3
2. Enable 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. Click the "Set Values" button.

### 5.4.9.2 Traps

#### SNMP traps for alarm events

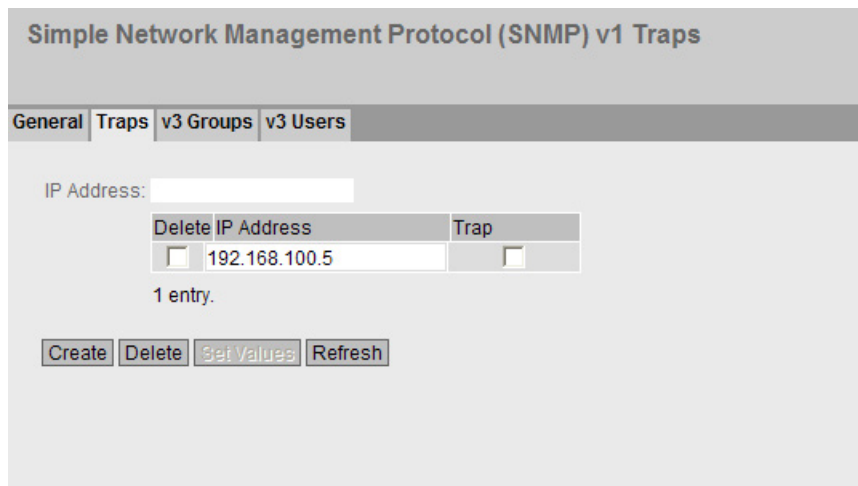
If an alarm event occurs, a device can send SNMP traps (alarm frames) to up to ten different management stations at the same time. Traps are only sent if the events specified in the "Events" menu occur.

---

**Note**

Traps are sent only when the "SNMPv1 Traps" option was selected in the "General" or "System > Configuration" tab.

---



#### Description

- **"IP Address" input box**  
Enter the IP address of the station to which the device sends SNMP traps. You can specify up to ten different IP addresses for various recipients.

The table has the following columns:

- **Delete**  
Select the check box in the row to be deleted.
- **IP Address**  
If necessary, change the IP addresses of the stations.
- **Trap**  
Enable or disable the sending of traps. Stations that are entered but not selected do not receive SNMP traps.

## Procedure

### Creating a trap entry

1. In "IP Address", enter the IP address of the station to which the device sends SNMP traps.
2. Click the "Create" button to create a new trap entry.
3. Select the check box for the corresponding IP address.
4. Click the "Set Values" button.

### Deleting a trap entry

1. Select the check box in the row to be deleted.
2. Click the "Delete" button. The entry is deleted.

## 5.4.9.3 Groups

### Security settings and assigning permissions

SNMP version 3 allows permissions to be assigned, authentication, and encryption at protocol level. The security levels and read/write permissions are assigned according to groups. The settings automatically apply to every member of a group.

### Simple Network Management Protocol (SNMP) v3 Groups

General
Traps
v3 Groups
v3 Users

Group Name:

Security Level: no Auth/no Priv ▼

Delete	Group Name	Security Level	Read	Write
<input type="checkbox"/>	service	Auth/Priv	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

1 entry.

Create
Delete
Set Values
Refresh

## Description

The page contains the following boxes:

- **"Group Name" input box**  
Enter the name of the group. The maximum length is 32 characters.
- **"Security Level" drop-down list**  
Select the security level (authentication, encryption) valid for the selected group. In the security levels, the following options:
  - 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:

- **Delete**  
Select the check box in the row to be deleted.
- **Group Name**  
Shows the defined group names.
- **Security Level**  
Shows the configured security level.
- **Read**  
Enable or disable read access for the required group.
- **Write**  
Enable or disable write access for the required group.

---

### Note

For write access to work, you also need to enable read access.

---

## Procedure

### Creating a new group

1. Enter the required group name in "Group Name".
2. Select the required security level from the "Security Level" drop-down list.
3. Click the "Create" button to create a new entry.
4. Specify the required read rights for the group in "Read".
5. Specify the required write rights for the group in "Write".
6. Click the "Set Values" button.

### Modifying a group

1. Specify the required read rights for the group in " Read".
2. Specify the required write rights for the group in " Write".
3. Click the "Set Values" button.

#### Note

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 recreate it and reconfigure it with the new name.

### Deleting a group

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

## 5.4.9.4 Users

### User-specific security settings

On the WBM page, you can create new SNMPv3 users and modify or delete existing users. The user-based security model works with the concept of the user name; in other words, a user ID is added to every frame. This user name and the applicable security settings are checked by both the sender and recipient.

Simple Network Management Protocol (SNMP) v3 Users

General | Traps | v3 Groups | v3 Users

User Name:

Delete	User Name	Group Name	Authentication Protocol	Privacy Protocol	Authentication Password	Authentication Password Confirmation	Privacy Password	Privacy Password Confirmation
<input type="checkbox"/>	Miller	service	MD5	DES				

1 entry.

### Description

The page contains the following boxes:

- **"User Name" input box**  
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:

- **Delete**  
Select the check box in the row to be deleted.
- **User Name**  
Shows the created users.
- **Group Name**  
Select the group to which the user will be assigned.
- **Authentication Protocol**  
Specify the authentication protocol. Can only be enabled, if this group supports the function.

The following settings are available:

- none
- MD5
- SHA

- **Privacy Protocol**  
Specify whether or not the user uses the DES algorithm. Can only be enabled, if the group supports this function.
- **Authentication Password**  
Enter the authentication password in the first input box. This password must have at least 6 characters, the maximum length is 32 characters.
- **Authentication Password Confirmation**  
Confirm the password by repeating the entry.
- **Privacy Password**  
Enter your encryption password. This password must have at least 6 characters, the maximum length is 32 characters.
- **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. In "Groups", select the group to which the new user will belong.  
If the group has not yet been created, change to the "v3 Groups" page and make the settings for this group.
4. If an authentication is necessary for the selected group, select the authentication algorithm in "Authentication Protocol".  
In the relevant input boxes, enter the authentication password and its confirmation.

5. If encryption was specified for the group, select the algorithm from the "Privacy Protocol" drop-down list. In the relevant input boxes, enter the encryption password and the confirmation.
6. Click the "Set Values" button.

#### Delete user

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

---

#### Note

If you click a different button prior to this step (for example the "Refresh" button), the delete action is canceled. The data of the selected rows is retained. The selections are removed. If you want to repeat the action, you will need to reselect the data records to be deleted.

---

## 5.4.10 System time

There are four 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.

### 5.4.10.1 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".

The screenshot shows the 'Manual System Time Setting' web page. At the top, there is a title bar 'Manual System Time Setting'. Below it is a navigation menu with four tabs: 'Manual Setting', 'SNTP Client', 'NTP Client', and 'SIMATIC Time Client'. The 'Manual Setting' tab is selected. The main content area contains a checked checkbox labeled 'Time Manually'. Below this, the 'System Time' is displayed as '06/27/2013 10:12:40'. There is a button labeled 'Use PC Time'. Below that, the 'Last Synchronization Time' is shown as '06/27/2013 10:12:40' and the 'Last Synchronization Mechanism' is 'Manual'. At the bottom of the form, there are two buttons: 'Set Values' and 'Refresh'.

## Description

The page contains the following boxes:

- **"Time Manually" check box**  
Enable or disable manual setting of the time. If you enable the option, the "System Time" input box can be edited.
- **"System Time" input box**  
Enter the date and time in the format "MM/DD/YYYY HH:MM:SS".  
After a restart, the time of day begins at 01/01/2000 00:00:00
- **"Use PC Time" button**  
Click the button to use the time setting of the PC.
- **Last Synchronization Time**  
This box is read-only and 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**  
This box displays how the last time-of-day synchronization was performed.
  - Not set  
The system 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.

## 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 the "Last Synchronization Mechanism" box.



### 5.4.10.2 SNTP client

#### Time-of-day synchronization in the network

SNTP (**Simple Network Time Protocol**) is used for synchronizing the time in the network. The appropriate frames are sent by an SNTP server in the network.

Simple Network Time Protocol (SNTP) Client

Manual Setting | SNTP Client | NTP Client | SIMATIC Time Client

SNTP Client

Current System Time: 06/27/2013 10:12:50

Last Synchronization Time: 06/27/2013 10:12:40

Last Synchronization Mechanism: Manual

Time Zone: +00:00

SNTP Mode: Poll

SNTP Server IP Address: 0.0.0.0

SNTP Server Port: 123

Poll Interval(s): 64

Set Values Refresh

#### Description

The page contains the following boxes:

- **"SNTP Client" check box**  
Enable or disable automatic time-of-day synchronization using SNTP.
- **Current System Time**  
Shows the values currently set in the system for date and time.
- **Last Synchronization Time**  
This box is read-only and shows when the last time-of-day synchronization took place.

- **Last Synchronization Mechanism**

This box displays how the last time-of-day synchronization was performed. The following methods are possible:

  - Not set  
The system time was not set.
  - Manual  
Manual time setting
  - SNTP  
Automatic time-of-day synchronization with SNTP
  - SIMATIC  
Automatic time-of-day synchronization using the SIMATIC time frame.
  - NTP  
Automatic time-of-day synchronization with NTP
- **"Time Zone" input box**

Enter the time zone you are using in the format "+/- HH:MM". The time zone relates to UTC standard world time. Settings for daylight-saving and standard time are taken into account in this box by specifying the time offset.
- **"SNTP Mode" drop-down list**

Select the synchronization mode from the drop-down list. The following types of synchronization are possible:

  - Poll  
If you select this protocol type, the input boxes "SNTP Server IP Address", "SNTP Server Port" and "Poll Interval(s)" are displayed for further configuration. With this type of synchronization, the device is active and sends a time query to the SNTP server.
  - Listen  
With this type of synchronization, the device is passive and "listens" for SNTP frames that deliver the time of day.
- **"SNTP Server IP Address" input box**

Enter the IP address of the SNTP server.
- **"SNTP Server Port" input box**

Enter the port of the SNTP server.  
The following ports are possible:

  - 123 (standard port)
  - 1025 to 36564
- **"Poll Interval(s)"input box**

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.

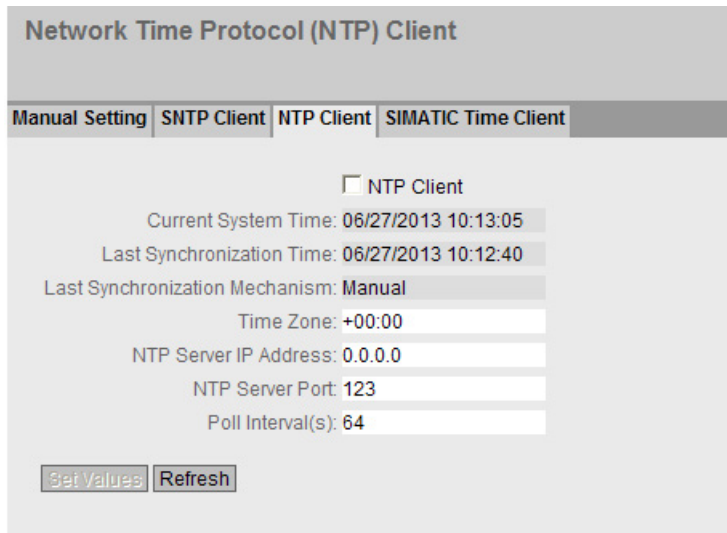
## Procedure

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 and displayed as the local time based on the specified time zone. On the device itself, there is no changeover from the daylight saving to standard time. 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)
    - time server (step 4)
    - Port (step 5)
    - query interval (step 6)
    - complete the configuration with step 7.
  - Listen  
For this mode, you need to configure the following:
    - time difference to the time sent by the server (step 2)
    - complete the configuration with step 7.
4. In the "SNTP Server IP Address" input box, enter the IP address of the SNTP server whose frames will be used to synchronize the time of day.
5. In the "SNTP Server Port" input box, enter the port via which the SNTP server is available. The port can only be modified if the IP address of the SNTP server is entered.
6. In the "Poll Interval(s)" input box, enter the time in seconds after which a new time query is sent to the time server.
7. Click the "Set Values" button to transfer your changes to the device.

### 5.4.10.3 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" check box**  
Select this check box to enable automatic time-of-day synchronization with NTP.
- **Current System Time**  
This box displays the current system time.
- **Last Synchronization Time**  
This box is read-only and shows when the last time-of-day synchronization took place.
- **Last Synchronization Mechanism**  
This box displays how the last time-of-day synchronization was performed. The following methods are possible:
  - Not set  
The system 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.

- **"Time Zone" input box**  
In this box, enter the time zone you are using in the format "+/- HH:MM". The time zone relates to UTC standard world time. Settings for daylight-saving and standard time are taken into account in this box by specifying the time offset.
- **"NTP Server IP Address" input box**  
Enter the IP address of the NTP server.
- **"NTP Server Port" input box**  
Enter the port of the NTP server.  
The following ports are possible:
  - 123 (standard port)
  - 1025 to 36564
- **"Poll Interval(s)" input box**  
Here, enter the interval between two-time queries. In this box, you enter the query interval in seconds. Possible values are 64 to 1024 seconds.

## Procedure

1. Click the "NTP Client" check box to enable the automatic time setting using NTP.
2. Enter the necessary values in the following boxes:
  - Time zone
  - NTP server IP address
  - NTP server port
  - Query interval
3. Click the "Set Values" button.

### 5.4.10.4 SIMATIC time client

#### Time setting via SIMATIC time client



#### Description

The page contains the following boxes:

- **"SIMATIC Time Client" check box**  
Select this check box to enable the device as a SIMATIC time client.
- **Current System Time**  
This box displays the current system time.
- **Last Synchronization Time**  
This box is read-only and shows when the last time-of-day synchronization took place.
- **Last Synchronization Mechanism**  
This box displays how the last time-of-day synchronization was performed. The following methods are possible:
  - Not set  
The system 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.

#### Procedure

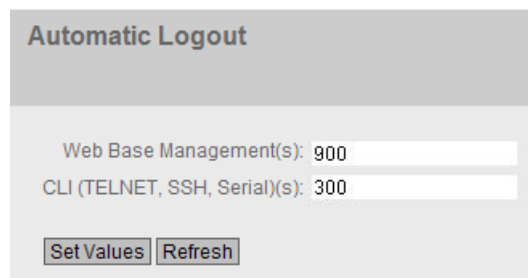
1. Click the "SIMATIC Time Client" check box to enable the SIMATIC Time Client.
2. Click the "Set Values" button.

## 5.4.11 Auto logout

### Setting the automatic logout

On this page, set the times after which there is an automatic logout from WBM or the CLI following user in activity.

If you have been logged out automatically, you will need to log in again.



**Automatic Logout**

Web Base Management(s): 900

CLI (TELNET, SSH, Serial)(s): 300

### Configuration

1. Enter a value of 60-3600 seconds in the "Web Base Management(s)" input box. If you enter the value 0, the 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, the automatic logout is disabled.
3. Click the "Set Values" button.

## 5.4.12 Select/Set button configuration

### Description of the Select/Set button

The "Select/Set" button is used for the following:

- Changing the display mode,
- Resetting to factory defaults,
- Defining the fault mask and the LED display,

You will find a detailed description of the individual functions available with the buttons in the device operating instructions.


On this page, the functionality of the Select/Set button can be restricted or fully disabled.



### Description of the displayed boxes

The following functions are possible:

- **"Restore Factory Defaults" check box**  
Enable or disable the function "Restore Factory Defaults" function with the Select/Set button.

 <b>CAUTION</b>
<b>"Restore Factory Defaults" button function active during startup</b> If you have disabled this function in your configuration, disabling is only valid during operation. When restarting, for example after power down, the function is active until the configuration is loaded so that the device can inadvertently be reset to the factory settings. This may cause unwanted disruption in network operation since the device needs to be reconfigured if this occurs. An inserted PLUG is also deleted and returned to the status as shipped.

- **"Set Fault Mask" check box**  
Enable or disable the function "Define fault mask via the LED display" with the Select/Set button.
- **"Redundancy Manager" check box**  
Enables/disables the redundancy manager function.

### Steps in configuration

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



### 5.4.13 Syslog client

#### System event agent

Syslog according to RFC 3164 is used for transferring short, unencrypted text messages over UDP in the IP network. This requires a Syslog server.

#### Requirements for sending log entries:

- The Syslog function is enabled on the device.
- The Syslog function is enabled for the relevant event.
- There is a Syslog server in your network that receives the log entries. (Since this is a UDP connection, there is no acknowledgment to the sender)
- The IP address of the Syslog server is entered on the device.

**System Logging (Syslog) Client**

Syslog Client

Server IP Address:

Delete	Server IP Address	Server Port
<input type="checkbox"/>	192.168.100.25	514

1 entry.

#### Description

The page contains the following boxes:

- **"Syslog Client" check box**  
Enable or disable the Syslog function.
- **"Server IP Address" input box**  
Enter the IP address of the Syslog server.

This table contains the following columns

- **Delete**  
Select the check box in the row to be deleted.
- **Server IP Address**  
Shows the IP address of the Syslog server.
- **Server Port**  
Enter the port of the Syslog server being used.

## Procedure

### Enabling function

1. Select the "Syslog Client" check box.
2. Click the "Set Values" button.

### Creating a new entry

1. In the "Server IP Address" input box, enter the IP address 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.

## 5.4.14 Ports

### 5.4.14.1 Overview

#### Overview of the port configuration

The page shows the configuration for the data transfer for all ports of the device. You cannot configure anything on this page.

Ports Overview											
Overview Configuration											
Port	Port Name	MAC Address	Mode	Negotiation	Flow Ctrl. Type	Flow Ctrl.	MTU	Port Type	Combo Port Media Type	Status	Link
<a href="#">P1.1</a>		08-00-06-4b-01-05	1G HD	enabled	<input type="checkbox"/>	disabled	1514	Switch-Port	auto	enabled	down
<a href="#">P1.2</a>		08-00-06-4b-01-06	1G HD	enabled	<input type="checkbox"/>	disabled	1514	Switch-Port	rj45	enabled	down
<a href="#">P1.3</a>		08-00-06-4b-01-07	1G HD	enabled	<input type="checkbox"/>	disabled	1514	Switch-Port	auto	enabled	down
<a href="#">P1.4</a>		08-00-06-4b-01-08	1G HD	enabled	<input type="checkbox"/>	disabled	1514	Switch-Port	auto	enabled	down
<a href="#">P1.5</a>		08-00-06-4b-01-09	1G HD	enabled	<input type="checkbox"/>	disabled	1514	Switch-Port	-	enabled	down
<a href="#">P1.6</a>		08-00-06-4b-01-0a	1G HD	enabled	<input type="checkbox"/>	disabled	1514	Switch-Port	-	enabled	down
<a href="#">P1.7</a>		08-00-06-4b-01-0b	1G HD	enabled	<input type="checkbox"/>	disabled	1514	Switch-Port	-	enabled	down
<a href="#">P1.8</a>		08-00-06-4b-01-0c	1G HD	enabled	<input type="checkbox"/>	disabled	1514	Switch-Port	-	enabled	down
<a href="#">P1.9</a>		08-00-06-4b-01-0d	100M FD	enabled	<input type="checkbox"/>	disabled	1514	Switch-Port	-	enabled	up
<a href="#">P1.10</a>		08-00-06-4b-01-0e	1G HD	enabled	<input type="checkbox"/>	disabled	1514	Switch-Port	-	enabled	down
<a href="#">P1.11</a>		08-00-06-4b-01-0f	1G HD	enabled	<input type="checkbox"/>	disabled	1514	Switch-Port	-	enabled	down
<a href="#">P1.12</a>		08-00-06-4b-01-10	1G HD	enabled	<input type="checkbox"/>	disabled	1514	Switch-Port	-	enabled	down
<a href="#">P1.13</a>		08-00-06-4b-01-11	1G HD	enabled	<input type="checkbox"/>	disabled	1514	Switch-Port	-	enabled	down
<a href="#">P1.14</a>		08-00-06-4b-01-12	1G HD	enabled	<input type="checkbox"/>	disabled	1514	Switch-Port	-	enabled	down
<a href="#">P1.15</a>		08-00-06-4b-01-13	1G HD	enabled	<input type="checkbox"/>	disabled	1514	Switch-Port	-	enabled	down
<a href="#">P1.16</a>		08-00-06-4b-01-14	1G HD	enabled	<input type="checkbox"/>	disabled	1514	Switch-Port	-	enabled	down
<a href="#">P2.1</a>		08-00-06-4b-01-15	1G HD	enabled	<input type="checkbox"/>	disabled	1514	Switch-Port	-	enabled	down
<a href="#">P2.2</a>		08-00-06-4b-01-16	1G HD	enabled	<input type="checkbox"/>	disabled	1514	Switch-Port	-	enabled	down
<a href="#">P2.3</a>		08-00-06-4b-01-17	1G HD	enabled	<input type="checkbox"/>	disabled	1514	Switch-Port	-	enabled	down

Refresh

#### Description of the displayed boxes

The table has the following columns:

- **Port**  
Shows the configurable ports. The entry is a link. If you click on the link, 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.
- **MAC Address**  
Shows the MAC address of the port.
- **Mode**  
Shows the transfer 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.
- **MTU (Maximum Transmission Unit)**  
Shows the packet size.
- **Port type** (only with routing)  
Shows the type of the port. The following types are possible:
  - Switch port
  - Router port
- **Combo Port Media Type** (SCALANCE XM400 only)  
This column contains a value only with combo ports.  
Shows the mode of the combo port:
  - auto
  - rj45
  - sfp
- **Status**  
Shows whether the port is on or off. Data traffic is possible only over an enabled port.
- **Link**  
Shows the connection status to the network. With the connection status, the following is possible:
  - Up  
The port has a valid link to the network, a link integrity signal is being received.
  - Down  
The link is down, for example because the connected device is turned off.

## 5.4.14.2 Configuration

### Configuring ports

With this page, you can configure all the ports of the device.

**Ports Configuration**

Overview | Configuration

Port: P1.2

Status: enabled

Port Name:

MAC Address: 08-00-06-4b-01-06

Mode Type: Auto negotiation

Mode: 1G HD

Negotiation: enabled

Flow Ctrl. Type

Flow Ctrl.: disabled

MTU: 1514

Port Type: Switch-Port

Combo Port Media Type: rj45

Link: down

### Description of the displayed boxes

The table has the following rows:

- **"Port" drop-down list**  
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" drop-down list**  
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.
- **"Port Name" input box**  
Here, enter a name for the port.

- **"Mode Type" drop-down list**

From this drop-down list, select the transmission speed and the transmission method of the port. If you set the mode to "Auto negotiation", these parameters are automatically negotiated with the connected end device. This must also be in the "Autonegotiation" mode.

---

**Note**

Before the port and partner port can communicate with each other, the settings must match at both ends.

---

- **"Mode" display box**

Shows the transmission speed and the transmission method of the port. The transmission speed can be 10 Mbps, 100 Mbps, 1000 Mbps or 10 Gbps. As the transmission mode, you can configure full duplex (FD) or half duplex (HD).

- **"Negotiation" display box**

Shows whether the automatic configuration of the connection to the partner port is enabled or disabled.

---

**Note**

**Turning flow control on/off with autonegotiation**

Flow control can only be enabled or disabled if the "autonegotiation" function is turned off. The function cannot be enabled again afterwards.

---

- **"Flow Ctrl. Type" check box**

Enable or disable flow control for the port.

- **Flow Ctrl.**

Shows whether flow control is working on this port.

- **"MTU" input box**

Enter the packet size.

- **"Port Type" drop-down list (only with routing)**

Select the type of port from the drop-down list.

- Switch port
- Router port

- **"Combo Port Media Type" drop-down list**(SCALANCE XM400 only)

Specify the mode of the combo port:

- auto

If you select this mode, the SFP transceiver port has priority.

As soon as an SFP transceiver is plugged in, an existing connection at the fixed RJ-45 port is terminated. If no SFP transceiver is plugged in, a connection can be established via the fixed RJ-45 port.

- rj45

If you select this mode, the fixed RJ-45 port is used regardless of the SFP transceiver port.

If an SFP transceiver is plugged in, it is disabled and the power turned off.

- sfp

If you select this mode, the SFP transceiver port is used regardless of the built-in RJ-45 port.

If an RJ-45 connection is established, it is terminated because the power of the RJ-45 port is turned off.

The factory setting for the combo ports is auto mode.

- **"Link" display box**

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 is being received.

- Down

The link is down, for example because the connected device is turned off.

## Changing the port configuration

Click the appropriate box to change the configuration.

---

### Note

Optical ports only work with the full duplex mode and at maximum transmission rate. As a result, the following settings cannot be made for optical ports:

- Automatic configuration
  - Transmission speed
  - Transmission technique
-

---

**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.

---

**Steps in configuration**

1. Change the settings according to your configuration.
2. Click the "Set Values" button.

**5.4.15 Fault monitoring**

**5.4.15.1 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 (Line 1 / Line 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 one of the monitored lines (line 1 or line 2) or when the voltage is too low.

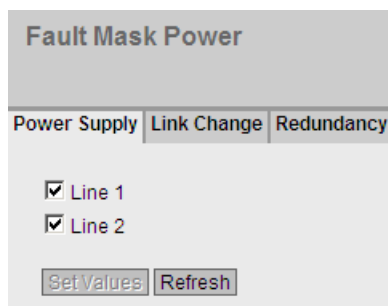
---

**Note**

You will find the permitted operating voltage limits in the compact 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.

**5.4.15.2 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 error is signaled

- when there should be a link on a port and this is missing.
- or when there should not be a link on a port and a link is detected.

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.

Port	Setting
P3.1	-
P3.2	-
P3.3	-
P3.4	Up
P4.1	-
P4.2	-
P4.3	-
P4.4	-
P5.1	-

### 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. You have the following setting options:
  - "-" (disabled)
  - Up
  - Down
  - 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:
  - 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")
  - "-" (disabled)  
The error handling is not triggered.

### Steps in configuration

#### Configure error monitoring for a port

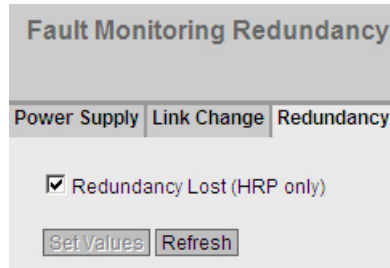
1. From the relevant drop-down list, select the options of the slots / ports whose connection status you want to monitor.
2. Click the "Set Values" button.

#### Configure error monitoring for all ports

1. Select the required setting from the drop-down list of the "Setting" column.
2. Click the "Copy to Table" button. The setting is adopted for all ports of table 2.
3. Click the "Set Values" button.

### 5.4.15.3 Redundancy

On this page, you configure whether or not an error message is triggered if there is a status change on a network connection.



The screenshot shows a web-based configuration interface for 'Fault Monitoring Redundancy'. At the top, there is a title bar 'Fault Monitoring Redundancy'. Below it, there are three tabs: 'Power Supply', 'Link Change', and 'Redundancy'. The 'Redundancy' tab is selected. Underneath the tabs, there is a checkbox labeled 'Redundancy Lost (HRP only)' which is checked. At the bottom of the form, there are two buttons: 'Set Values' and 'Refresh'.

#### Setting

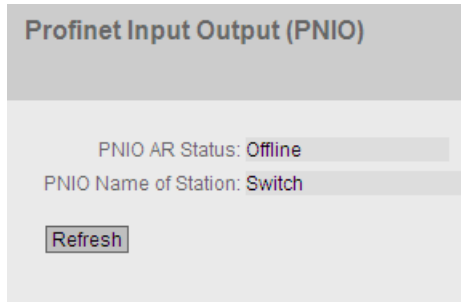
- **Redundancy Lost (HRP only)**

Enable or disable connection monitoring. If the redundancy of the connection is lost, an error is signaled.

## 5.4.16 PNIO

### Settings for PROFINET IO

This page shows the PROFINET IO AR status and the device name.



### Description of the displayed boxes

The page contains the following boxes:

- **PNIO AR Status**  
This box shows the status of the PROFINET IO connection; in other words whether the device is connected to a PROFINET IO controller "Online " or "Offline". Here, online means that a connection to a PROFINET IO controller exists, that this has downloaded its configuration data to the device and that the device can send status data to the PROFINET IO controller. In this status known as "in data exchange", the parameters set with the PROFINET IO controller cannot be configured.
- **PNIO Name of Station**  
This box displays the PROFINET IO device name according to the configuration in HW Config of STEP 7.

## 5.4.17 PLUG configuration

**NOTICE****Do not remove or insert a C-PLUG / KEY-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 it is detected that the PLUG was removed, there is a restart. If a valid KEY-PLUG was inserted in the device, the device changes to a defined error state following the restart.

### Information about the configuration of the C-PLUG / KEY-PLUG

This page provides detailed information about the configuration stored on the C-PLUG or KEY-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.

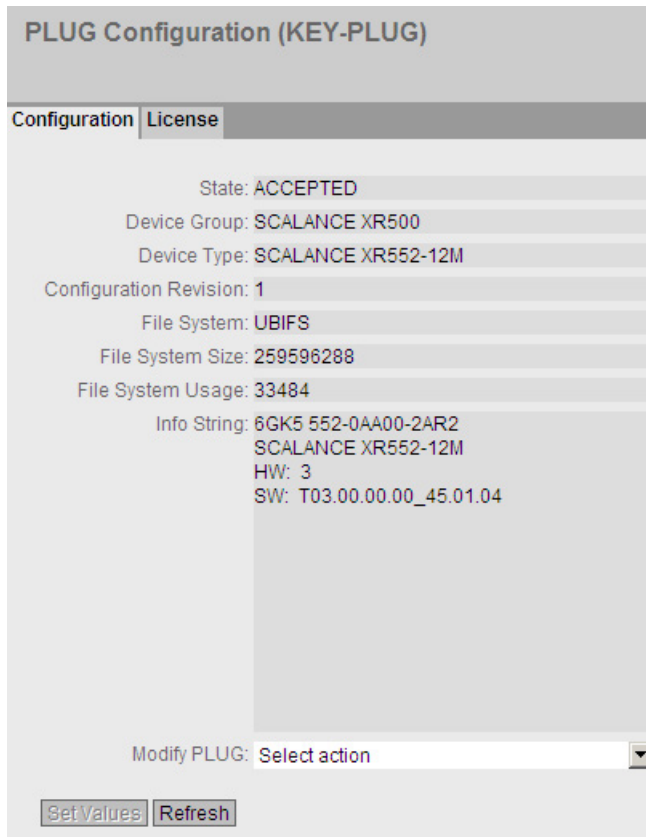
The action cannot be undone.

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 previous versions with PLUG inserted**

During the installation of a previous version, the configuration data can be lost. In this case, the device starts up with the factory settings after the firmware has been installed. In this situation, if a PLUG is inserted in the device, following the restart, this has the status "Not Accepted" since the PLUG still has the configuration data of the previous more up-to-date firmware. This allows you to return to the previous, more up-to-date firmware without any loss of configuration data.

If the original configuration on the PLUG is no longer required, the PLUG can be deleted or rewritten manually using "System > PLUG".



### Description of the displayed boxes

The table has the following rows:

- **State**  
Shows the status of the PLUG. The following are possible:
  - ACCEPTED  
There is a PLUG with a valid and suitable configuration in the device.
  - NOT ACCEPTED  
Invalid or incompatible configuration on the inserted PLUG.
  - NOT PRESENT  
There is no C-PLUG or KEY-PLUG 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.
  - MISSING  
There is no PLUG inserted. Functions are configured on the device for which a license is required.
- **Device Group**  
Shows the SIMATIC NET product line that used the C-PLUG or KEY-PLUG previously.

- **Device Type**  
Shows the device type within the product line that used the C-PLUG or KEY-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.

**NOTICE****New file system UBI**

As of firmware version 3.0, UBI is the standard file system for the C-PLUG or KEY-PLUG. If a C-PLUG with the previous file system IECP is detected in such a device, this C-PLUG will be formatted for the UBI file system and the data will be rewritten to the C-PLUG.

The file system is also changed following a firmware update to V3.0. A downgrade to the previous version of the corresponding software is then a problem. The firmware can neither read nor write the C-PLUG or KEY-PLUG and it is not even possible to "Erase PLUG to Factory Default".

- **File System Size [byte]**  
Displays the maximum storage space of the file system on the PLUG.
- **File System Usage [byte]**  
Shows the storage space being utilized in the PLUG file system.
- **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.
- **"Modify PLUG" drop-down list**  
Select the setting from the drop-down list. You have the following options for changing the configuration on the C-PLUG or KEY-PLUG:
  - Write current configuration to PLUG  
This option is available only if the status of the PLUG is "NOT ACCEPTED" or "FACTORY".  
The configuration in the internal flash memory of the device is copied to the PLUG.
  - Erase PLUG to factory default  
Deletes all data from the C-PLUG and triggers low-level formatting.

### Steps in configuration

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. Select the required option from the "Modify PLUG" drop-down list.
3. Click the "Set Values" button.

### 5.4.18 PLUG license

<b>NOTICE</b>
<b>Do not remove or insert a C-PLUG / KEY-PLUG during operation!</b>
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 it is detected that the PLUG was removed, there is a restart. If a valid KEY-PLUG was inserted in the device, the device changes to a defined error state following the restart.
If the device was configured at some time with a PLUG, the device can no longer be used without this PLUG. To be able to use the device again, reset the device to the factory settings.

---

#### Note

##### Incompatibility with previous versions with PLUG inserted

During the installation of a previous version, the configuration data can be lost. In this case, the device starts up with the factory settings after the firmware has been installed. In this situation, if a PLUG is inserted in the device, following the restart, this has the status "Not Accepted" since the PLUG still has the configuration data of the previous more up-to-date firmware. This allows you to return to the previous, more up-to-date firmware without any loss of configuration data.

If the original configuration on the PLUG is no longer required, the PLUG can be deleted or rewritten manually using "System > PLUG".

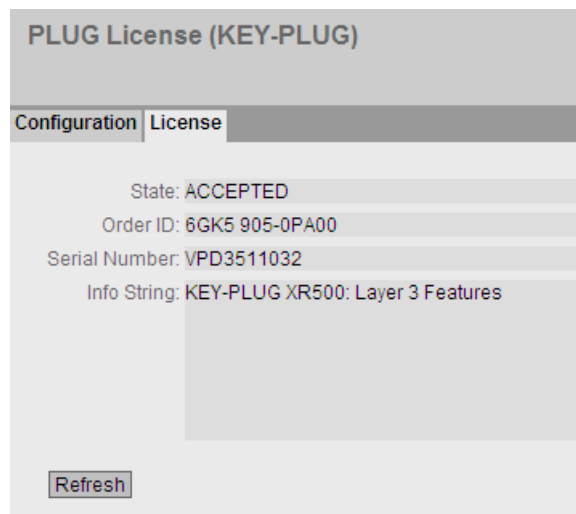
---

### Information about the license of the KEY-PLUG

A C-PLUG can only store the configuration of a device. In addition to the configuration, a KEY-PLUG also contains a license that enables certain functions of your SIMATIC NET device.

This page provides detailed information about the license on the KEY-PLUG. In this example, the KEY-PLUG contains the data for enabling the layer 3 functions of the device.





### Description of the displayed boxes

- **State**

Shows the status of the KEY-PLUG. The following are possible:

  - ACCEPTED  
The KEY-PLUG in the device contains a suitable and valid license.
  - NOT ACCEPTED  
The license of the inserted KEY-PLUG is not valid.
  - NOT PRESENT  
No KEY-PLUG is inserted in the device.
  - MISSING  
There is no KEY-PLUG or a C-PLUG with the status "FACTORY" inserted in the device. Functions are configured on the device for which a license is required.
  - WRONG  
The inserted KEY-PLUG is not suitable for the device.
  - UNKNOWN  
Unknown content of the KEY-PLUG.
  - DEFECTIVE  
The content of the KEY-PLUG contains errors.
- **Order ID**

Shows the order number of the KEY-PLUG. The KEY-PLUG is available for various functional enhancements and for various target systems.
- **Serial Number**

Shows the serial number of the KEY-PLUG.
- **Info String**

Shows additional information about the device that used the KEY-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.

---

**Note**

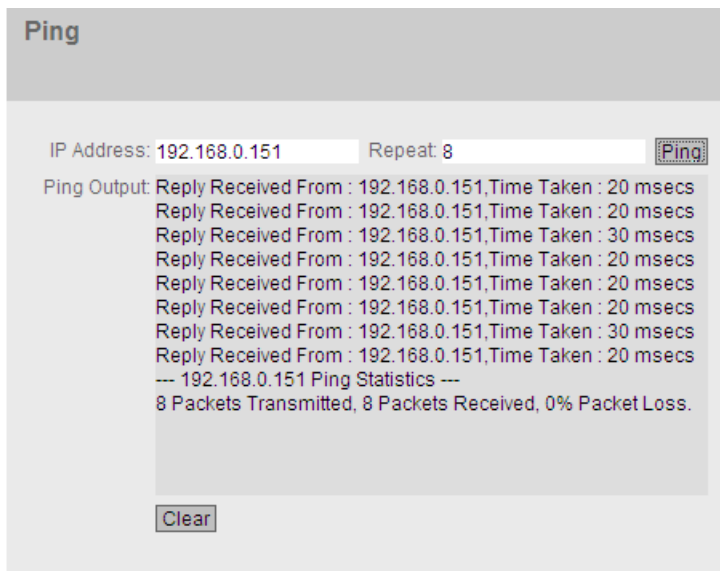
When you save the configuration, the information about whether or not a KEY-PLUG was inserted in the device at the time is also saved. This configuration can then only work if a KEY-PLUG with the same order number / license is inserted.

---

### 5.4.19 Ping

#### Reachability of an address in an IP network

With the ping function, you can check whether a certain IP address is reachable in the network.



#### Description

The table has the following columns:

- **"IP Address" input box**  
Enter the IP address of the device.
- **"Repeat" input box**  
Enter the number of ping requests.
- **"Ping" button**  
Click this button to start the ping function.
- **Ping Output**  
This box shows the output of the ping function.

## 5.4.20 PoE

### 5.4.20.1 General

#### Settings for Power over Ethernet (PoE)

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

The SCALANCE X-500 represents a PSE (Power Sourcing Equipment). With the SCALANCE XM400, each group of four ports with PoE capability is known as a PSE. The displayed value applies only to the corresponding PSE.

PSE	Maximum Power(W)	Allocated Power(W)	Power In Use(W)	Usage Threshold(%)
1	189	0	0	80

#### Description of the displayed boxes

##### Maximum Power [W] (read-only)

Maximum power that a PSE provides to supply PoE devices.

##### 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.

### 5.4.20.2 Port

#### Settings for the ports

For each individual PoE port, you can specify whether or not the power will be supplied via Ethernet. You can also set a priority for each connected powered device (PD). 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.

**Power over Ethernet (PoE) Port**

---

**General** | **Port**

Port	Setting	Priority	Type	Copy to Table
All ports	No Change <input type="checkbox"/>	No Change <input type="checkbox"/>	No Change	Copy to Table

Port	Setting	Priority	Type	Classification	Status	Power(mW)	Voltage(V)	Current(mA)
P3.1	<input checked="" type="checkbox"/>	low <input type="checkbox"/>	Wlan AP 1	Class 3	delivering	4644	54	86
P3.2	<input checked="" type="checkbox"/>	critical <input type="checkbox"/>	Webcam	Class 3	delivering	3240	54	60
P3.3	<input checked="" type="checkbox"/>	low <input type="checkbox"/>		Class 4	delivering	4320	54	80
P3.4	<input type="checkbox"/>	low <input type="checkbox"/>		-	disabled	0	0	0

#### 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 setting from the drop-down list. You have the following setting options:
  - enabled  
Enables the function
  - disabled  
Disables the function
  - No Change  
The setting in table 2 remains unchanged

- **Priority**

Select the priority of the ports from the drop-down list. If you set the priority in table 1 and copy the values to table 2, all ports will have the same priority.

The following settings are possible, in ascending order of relevance:

- low  
low priority
- high  
medium priority
- critical  
high priority
- No Change

The setting 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.

- **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 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 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.

- **Classification (read-only)**

The classification specifies the class of the device. From this, it is possible to recognize the maximum power of the device.

- **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 Power

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 for 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.

## 5.4.21 Port Diagnostics

### 5.4.21.1 Cable tester

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

---

#### Note

Please note that this test is permitted only when no data connection is established on the port to be tested.

If, however, there is a data connection to the port to be tested, this is briefly interrupted.

Automatic re-establishment of the connection can fail and then needs to be done manually.

---

Pair	Status	Distance
1-2	open	0
3-6	open	0
4-5	open	0
7-8	open	0

#### Description

The page contains the following boxes:

- **"Port" drop-down list**  
Select the port to be configured from the drop-down list.
- **"Run Test" button**  
Activates error diagnostics. The result is shown in the table.

This table contains the following columns:

- **Pair**  
Shows the wire pair in the cable.

---

**Note**

**Wire pairs**

Wire pairs 4-5 and 7-8 of 10/100 Mbps network cables are not used.

1000 Mbps or gigabit Ethernet uses all 4 wire pairs.

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

Pair 1 = pin 4-5

Pair 2 = pin 1-2

Pair 3 = pin 3-6

Pair 4 = pin 7-8

---

- **Status**  
Displays the status of the cable.
- **Distance [m]**  
Displays the distance to the cable end, cable break, or short-circuit.



### 5.4.21.2 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

Please note that this test is permitted only when no data connection is established on the port to be tested.

If, however, there is a data connection to the port to be tested, this is briefly interrupted.

Automatic re-establishment of the connection can fail and then needs to be done manually.

#### Small Form-factor Pluggable (SFP) Transceiver Diagnostics

Cable Tester
SFP Diagnostics

Port: P0.2 ▼

Name: CORETEK

Model: SFP993-1

Revision: 000A

Serial: NM0001J81S0005

Nominal Bit Rate(MBit/s): 10300

Max. Link (50.0/125um)(m): 80

Max. Link (62.5/125um)(m): 30

	Current	Low	High
Temperature(°C):	27.30	-5.00	75.00
Voltage(V):	3.20	3.00	3.55
Current(mA):	5.68	3.00	12.00
Rx Power(mW):	0.00	1.00	100.00
Tx Power(mW):	56.11	30.00	70.00

Refresh

#### Description

The page contains the following boxes:

- **"Port" drop-down list**  
Select the port to be configured from the drop-down list.
- **"Refresh" button**  
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 [MBit/s]**  
Shows the nominal bit rate of the interface.
- **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:

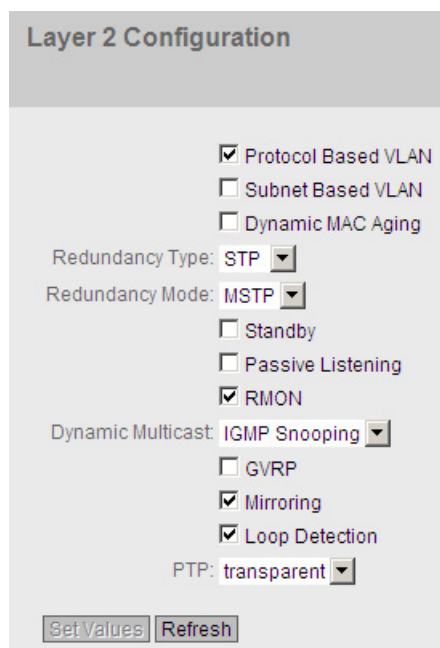
- **Temperature [°C]**  
Shows the temperature of the interface.
- **Voltage [V]**  
Shows the voltage applied to the interface [V].
- **Current [mA]**  
Shows the current consumption of the interface [mA].
- **Rx Power(mW)**  
Shows the receive power of the interface [mW].
- **Tx Power(mW)**  
Shows the transmit power of the interface [mW].
- **Current column**  
Shows the current value.
- **Low column**  
Shows the lowest value.
- **High column**  
Shows the highest value.

## 5.5 The "Layer 2" menu

### 5.5.1 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 detailed settings. You can also check the settings on the configuration pages.



The screenshot shows the "Layer 2 Configuration" web interface. It features a title bar "Layer 2 Configuration" and a list of configuration options:

- Protocol Based VLAN
- Subnet Based VLAN
- Dynamic MAC Aging
- Redundancy Type: STP (dropdown)
- Redundancy Mode: MSTP (dropdown)
- Standby
- Passive Listening
- RMON
- Dynamic Multicast: IGMP Snooping (dropdown)
- GVRP
- Mirroring
- Loop Detection
- PTP: transparent (dropdown)

At the bottom, there are two buttons: "Set Values" and "Refresh".

#### Description of the displayed boxes

- **"Protocol Based VLAN"** check box  
Enable or disable protocol-based VLAN. Other settings in "Layer 2 > VLAN".
- **"Subnet Based VLAN"** check box  
Enable or disable subnet-based VLAN. Other settings in "Layer 2 > VLAN".
- **"Dynamic MAC Aging"** check box  
Enable or disable the "aging" mechanism. You can configure other settings in "Layer 2 > Dynamic MAC Aging".

- **"Redundancy Type" drop-down list**

The following settings are available

- **"-" (disabled)**

The redundancy function is disabled.

- **STP**

If you select this option, you specify the required redundancy mode in the "Redundancy Mode" drop-down list.

- **Ring**

If you select this option, specify the required redundancy mode in the "Redundancy Mode" drop-down list.

- **"Redundancy Mode" drop-down list**

If you select "Ring" in the "Redundancy Type" drop-down list, the following options are then available:

- -

None

- Automatic Redundancy Detection

Select this setting to configure the redundant mode automatically.

In "Automatic Redundancy Detection" mode, the IE Switch automatically detects whether or not there is a device with the role of "HRP Manager" 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 "MRP Manager". The other devices automatically set themselves to "MRP Client" mode.

- MRP Auto-Manager

Automatic media redundancy manager

- MRP Client

Media redundancy client

- HRP Client

High Speed Redundancy Protocol client

- HRP Manager

High Speed Redundancy Protocol manager

If you select "STP" in the "Redundancy Type" drop-down list, the following options are then available:

- **STP**  
Enables Spanning Tree Protocol. Typical reconfiguration times with spanning tree are between 20 and 30 seconds. You can configure other settings in "Layer 2 > MSTP".
- **RSTP**  
Enables 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 > MSTP".

---

**Note**

When using RSTP (Rapid Spanning Tree Protocol), loops involving duplication of frames or frames being overtaken may occur briefly. If this is not acceptable in your particular application, use the slower standard spanning tree mechanism.

---

- **MSTP**  
Enables Multiple Spanning Tree Protocol (MSTP). You can configure other settings in "Layer 2 > MSTP".
- **"Standby" check box**  
Enable or disable the standby redundancy function. You will find other settings in "Layer 2 > Ring Redundancy".
- **"Passive Listening" check box**  
Enable or disable the passive listening function.
- **"RMON" check box**  
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" drop-down list**  
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 operate at the same time.

---

- **"GVRP" check box**  
Enable or disable "GVRP" (GARP VLAN Registration Protocol). You can configure other settings in "Layer 2 > VLAN > GVRP".
- **"Mirroring" check box**  
Enable or disable port mirroring. You can configure other settings in "Layer 2 > Mirroring".
- **"Loop detection" check box**  
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 for the Precision Time Protocol:
  - **off**  
The device does not process any PTP messages. PTP messages are, however, forwarded according to the rules of the device
  - **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.

## 5.5.2 Qos

### 5.5.2.1 CoS queue mapping

#### COS Queue Mapping

Here, CoS priorities are assigned to certain queues (Traffic Queues).

COS	Queue
0	1
1	2
2	3
3	4
4	5
5	6
6	7
7	8

#### Description of the displayed boxes

The table has the following columns:

- **COS**  
Shows the CoS priority of the incoming packets.
- **Queue**  
From the drop-down list, select the forwarding queue (send priority) that is assigned to the CoS priority.  
The higher the number of the queue, the higher the send priority.

#### Steps in configuration

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

### 5.5.2.2 DSCP mapping

#### DSCP queue

On this page, DSCP settings are assigned to various queues (Traffic Queues).

DSCP	Queue
0	1
1	1
2	1
3	1
4	1
5	1
6	1
7	1
8	2
9	2
10	2
11	2
12	2
13	2
14	2
15	2
16	3
17	3
18	3

#### Description of the displayed values

The table has the following columns:

- **DSCP**  
Shows the DSCP priority of the incoming packets.
- **Queue**  
From the drop-down list, select the forwarding queue (send priority) that is assigned to the DSCP value.  
The higher the queue number, the higher the send priority.

#### Steps in configuration

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



### 5.5.3 Rate control

#### Limiting the transfer rate of incoming and outgoing data

On this page, you configure the load limitation (maximum number of data packets per second) for the individual ports. You can specify the category of frame for which these limit values will apply.

#### Rate Control

	Limit Ingress Unicast(DLF)	Limit Ingress Broadcast	Limit Ingress Multicast	Total Ingress Rate pkts/s	Egress Rate kb/s	Copy to Table
All ports	No Change <input type="button" value="v"/>	No Change <input type="button" value="v"/>	No Change <input type="button" value="v"/>	No Change	No Change	<input type="button" value="Copy to Table"/>

Port	Limit Ingress Unicast(DLF)	Limit Ingress Broadcast	Limit Ingress Multicast	Total Ingress Rate pkts/s	Egress Rate kb/s
P0.1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	0	0
P0.2	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	0	0
P0.3	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	0	0
P0.4	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	0	0
P1.1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	0	0
P1.2	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	0	0
P1.3	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	0	0
P1.4	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	0	0
P2.1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	0	0
P2.2	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	0	0
P2.3	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	0	0
P2.4	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	0	0
P3.1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	0	0
P3.2	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	0	0
P3.3	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	0	0

#### Description of the displayed values

Table 1 has the following columns:

- **1st column**  
Shows that the settings are valid for all ports.
- **Limit Ingress Unicast (DLF) / Limit Ingress Broadcast / Limit Ingress Multicast**  
Select the required setting in the drop-down list.
  - enabled: Enables the function.
  - disabled: Disables the function
  - No Change: The setting in table 2 remains unchanged

- **Total Ingress Rate pkts/s**  
Specify the maximum number of incoming packets processed by the device. If "No Change is entered, the entry in the table remains unchanged.
- **Egress Rate kb/s**  
Specify the data rate for all outgoing frames. If "No Change is entered, the entry in the table remains unchanged
- **Copy to Table**  
If you click the button, the settings are adopted for all ports of table 2.

Table 2 has the following columns:

- **Port**  
Shows the slot and the port to which the other information relates. This field cannot be configured. The port is made up of the module number and the port number, for example port 0.1 is module 0, port 1.
- **Limit Ingress Unicast (DLF)**  
Enable or disable the data rate for limiting incoming unicast frames with an unresolvable address (Destination Lookup Failure).
- **Limit Ingress Broadcast**  
Enable or disable the data rate for limiting incoming broadcast frames.
- **Limit Ingress Multicast**  
Enable or disable the data rate for limiting incoming multicast frames.
- **Total Ingress Rate pkts/s**  
Specify the maximum number of incoming packets processed by the device.
- **Egress Rate kb/s**  
Specify the data rate for all outgoing frames.

---

**Note**

**Rounding of the values, deviation from desired value**

When you input the rate values, note that the WBM rounds to correct values.

If values are configured for Total Ingress Rate and Egress Rate, the actual values in operation can exceed or fall below the set values by 10%.

---

### 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.

## 5.5.4 VLAN

### 5.5.4.1 General

#### VLAN configuration page

On this page, you define the VLAN and specify the use of the ports.

#### 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.

**Virtual Local Area Network (VLAN) General**

General | GVRP | Port Based VLAN | Protocol Based VLAN Group | Protocol Based VLAN Port | IPv4 Subnet Based VLAN

VLAN ID:

	VLAN ID	Name	Status	P0.1	P0.2	P0.3	P0.4	P1.1	P1.2	P
<input type="checkbox"/>	1	<input type="text"/>	Static	U	U	U	U	U	U	
<input type="checkbox"/>	2	<input type="text"/>	Static	-	-	-	-	-	-	
<input type="checkbox"/>	3	<input type="text"/>	Static	-	-	-	-	-	-	

3 entries.

#### 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 IE switches, the VLAN ID "1" is the default on all ports.

If an end node is connected to a port, outgoing frames should be sent without a tag (static access port). If, however, there is a further switch at this port, the frame should have a tag added (trunk port).

### Description of the displayed boxes

The page contains the following boxes:

- **"VLAN ID" input box**  
Enter the VLAN ID in the input box.  
Range of values: 1 ... 4094

The table has the following columns:

- **1st column**  
Select the check box in the row to be deleted.
- **VLAN ID**  
Shows the VLAN ID. The VLAN ID (a number between 1 and 4094) can only be assigned once when creating a new data record and can then no longer be changed. To make a change, the entire data record must be deleted and created again. Up to 257 VLANs can be defined.
- **Name**  
Enter a name for the VLAN. The name only provides information and has no effect on the configuration. The length is a maximum of 32 characters.
- **Status**  
Shows the status type of the entry in the port filter table. Here, static means that the address was entered as a static address by the user. The entry GVRP means that the configuration was registered by a GVRP frame. This is, however, only possible if GVRP was enabled for the device.

- **List of ports**

Specify the use of the port. The following options are available:

- "-"  
The port is not a member of the 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 it is not possible for the VLAN to be registered dynamically at this port using GVRP. If a port in a VLAN has this option, it cannot become a member of this VLAN even if it is configured as a trunk port.  
You can configure further settings in "Layer 2 > VLAN > Port Based VLAN".
- 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.  
You configure this function in the CLI (Command Line Interface) using the "`switchport mode trunk`" command.

### Steps in configuration

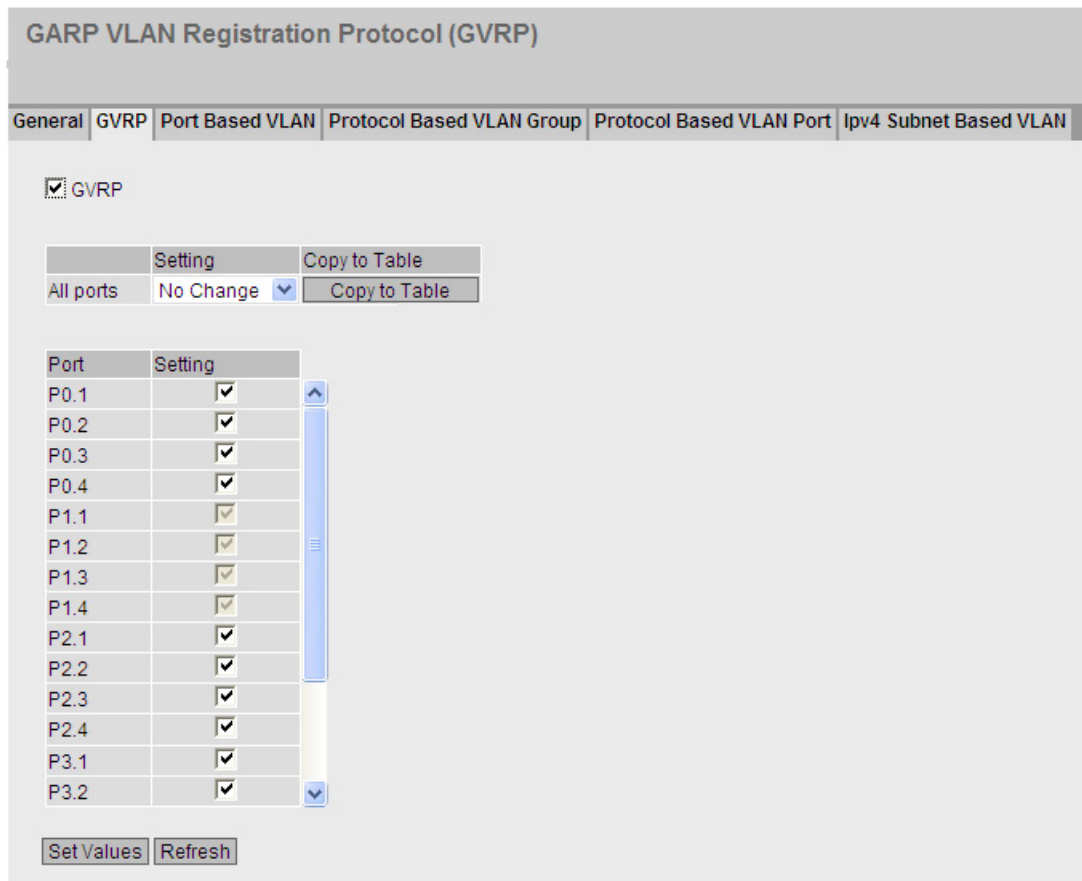
1. Enter an ID in the "VLAN ID" input box.
2. Click the "Create" button. A new entry is generated in the table. As default, the boxes have "-" entered.
3. Enter a name for the VLAN under Name.
4. Specify the use of the port in the VLAN. If, for example you select M, the port is a member of the VLAN. The frame sent in this VLAN is forwarded with the corresponding VLAN tag.
5. Click the "Set Values" button.

### 5.5.4.2 GVRP

#### Configuration of GVRP functionality

Using GVRP frame, a different device can register at the port of the device for a specific VID. A different device, can, for example be an end device or a switch. The device can also send GVRP frames via this port.

On this page, you can enable each port for GVRP functionality.



#### Description of the displayed boxes

The page contains the following box:

- **"GVRP" check box**  
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 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 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.

### 5.5.4.3 Port-based VLAN

#### Processing received frames

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

#### Port Based Virtual Local Area Network (VLAN) Configuration

General
GVRP
Port Based VLAN
Protocol Based VLAN Group
Protocol Based VLAN Port
Ipv4 Subnet Based VLAN

	Priority	Port VID	Acceptable Frames	Ingress Filtering	Copy to Table
All ports	No Change	No Change	No Change	No Change	Copy to Table

Port	Priority	Port VID	Acceptable Frames	Ingress Filtering	
P0.1	0	VLAN1	All	<input type="checkbox"/>	
P0.2	0	VLAN1	All	<input type="checkbox"/>	
P0.3	0	VLAN1	All	<input type="checkbox"/>	
P0.4	0	VLAN1	All	<input type="checkbox"/>	
P2.1	0	VLAN1	All	<input type="checkbox"/>	
P2.2	0	VLAN1	All	<input type="checkbox"/>	
P2.3	0	VLAN1	All	<input type="checkbox"/>	
P2.4	0	VLAN1	All	<input type="checkbox"/>	
P3.1	0	VLAN1	All	<input type="checkbox"/>	
P3.2	0	VLAN1	All	<input type="checkbox"/>	
P3.3	0	VLAN1	All	<input type="checkbox"/>	
P3.4	0	VLAN1	All	<input type="checkbox"/>	
P4.1	0	VLAN1	All	<input type="checkbox"/>	
P4.2	0	VLAN1	All	<input type="checkbox"/>	
P4.3	0	VLAN1	All	<input type="checkbox"/>	
P4.4	0	VLAN1	All	<input type="checkbox"/>	

Set Values
Refresh

#### Description of the displayed boxes

Table 1 has the following columns:

- **Port**  
Shows that the settings are valid for all ports.
- **Priority / Port VID / Acceptable Frames / Ingress Filtering**  
Select the setting in the drop-down list. If "No Change is selected, the entry in table 2 remains unchanged.
- **Copy to Table**  
If you click the button, the setting is adopted for all ports of table 2.



Table 2 has the following columns:

- **Port**  
Shows the available ports and link aggregations. The port is made up of the module number and the port number, for example port 0.1 is module 0, port 1.
- **Priority**  
From the drop-down list, select the priority given to untagged frames.  
  
The CoS priority (Class of Service) used in the VLAN tag. If a frame is received without a tag, it will be assigned this priority. This priority specifies how the frame is further processed compared with other frames.  
There are a total of eight priorities with values 0 to 7, where 7 represents the highest priority (IEEE 802.1p Port Priority).
- **Port VID**  
Select the VLAN ID from the drop-down list. Only VLAN IDs defined on the "VLAN > General" page can be selected.  
If a received frame does not have a VLAN tag, it has a tag with the VLAN ID specified here added to it and is sent according to the rules at the port.
- **Acceptable Frames**  
Specify which types of frames will be accepted. The following alternatives are possible:
  - Tagged Frames Only  
The device discards all untagged frames. Otherwise, the forwarding rules apply according to the configuration.
  - All  
The device forwards all frames.
- **Ingress Filtering**  
Specify whether the VID of received frames is evaluated  
You have the following options:
  - Enabled  
The VLAN ID of received frames decides whether they are forwarded: To forward a VLAN tagged frame, the receiving port must be a member in the same VLAN. Frames from unknown VLANs are discarded at the receiving port.
  - Disabled  
All frames are forwarded.

### 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.

### 5.5.4.4 Protocol Based VLAN Group

#### Introduction

On this page, you specify groups and assign a protocol to them.

Protocol based Virtual Local Area Network (VLAN) - Group					
General	GVRP	Port Based VLAN	Protocol Based VLAN Group	Protocol Based VLAN Port	Ipv4 Subnet Based VLAN
<input checked="" type="checkbox"/> Protocol Based VLAN					
Protocol Value: <input type="text"/>					
Group Identifier: <input type="text"/>					
	<input type="checkbox"/>	00:80	1		
	<input type="checkbox"/>	00:90	2		
<input type="button" value="Create"/> <input type="button" value="Delete"/> <input type="button" value="Set Values"/> <input type="button" value="Refresh"/>					

#### Description of the displayed boxes

The page contains the following boxes:

- **"Protocol Based VLAN" check box**  
Enable or disable the protocol-based VLAN assignment.
- **"Protocol Value" input box**  
Enter the hexadecimal protocol value.  
A few examples are shown below:
  - PROFINET: 88:92
  - IP: 08:00
  - Novell: 81:37
  - netbios: f0:f0
  - appletalk: 80:9b
- **"Group Identifier" input box**  
Enter the ID of the group.

The table has the following columns:

- **1st column**  
Select the check box in the row to be deleted.
- **Protocol Value**  
Shows the protocol value.
- **Group Identifier**  
Shows the group ID.

## Steps in configuration

### Adding an entry

1. Enter the protocol value in the "Protocol Value" input box.
2. Enter the ID for the group in the Group Identifier input box.
3. Click the "Create" button. A new entry is generated in the table.
4. Click the "Set Values" button.

### Deleting an entry

1. On the "Protocol Based VLAN Port" tab check that the protocol group is not used at any port.
2. Select the check box in the row to be deleted.
3. Click the "Delete" button.
4. Click the "Set Values" button.

## 5.5.4.5 Protocol Based VLAN Port

### Introduction

On this page, you specify which protocol and which VLAN is assigned to the individual port.

**Protocol based Virtual Local Area Network (VLAN) - Port**

General | GVRP | Port Based VLAN | Protocol Based VLAN Group | Protocol Based VLAN Port | Ipv4 Subnet Based VLAN

Port: P0.1 ▾

Group Identifier: 1 ▾

	Port	Group Identifier	VLAN ID
<input type="checkbox"/>	P0.1	1	VLAN1
<input type="checkbox"/>	P0.2	2	VLAN1

Create Delete Set Values Refresh

### Description of the displayed boxes

The page contains the following boxes:

- **Drop-down list "Port"**  
Select the port in the drop-down list. All All available ports and the link aggregations can be selected.
- **Drop-down list "Group Identifier"**  
Select the group ID in the drop-down list. You specify the ID the WBM page "Protocol Based VLAN Group".

The table has the following columns:

- **1st column**  
Select the check box in the row to be deleted.
- **Port**  
All available ports and the link aggregations are shown.
- **Group Identifier**  
Shows the group ID assigned to the port.
- **VLAN ID**  
From the drop-down list, select the VLAN ID you want to assign to the port.

### Steps in configuration

1. Select the port from the "Port" drop-down list.
2. Select the group ID from the "Group Identifier" drop-down list.
3. Click the "Create" button. A new entry is generated in the table.
4. Specify the VLAN ID in "VLAN ID".
5. Click the "Set Values" button.

#### 5.5.4.6 Ipv4 Subnet Based VLAN

### Introduction

On this page, you specify which VLAN ID is assigned to the subnet.

**IPV4 Subnet based Virtual Local Area Network (VLAN)**

General | GVRP | Port Based VLAN | Protocol Based VLAN Group | Protocol Based VLAN Port | **Ipv4 Subnet Based VLAN**

Subnet Based VLAN

Port: P1.1

Subnet Address:

Subnet Mask:

	Port	Subnet Address	Subnet Mask	VLAN ID
<input type="checkbox"/>	P1.1	192.168.16.10	255.0.0.0	VLAN1

1 entry.

Create Delete Set Values Refresh

## Description of the displayed boxes

The page contains the following boxes:

- **"Subnet Based VLAN" check box**  
Enable or disable the subnet-based VLAN assignment.
- **Drop-down list "Port"**  
Select the port in the drop-down list. All available ports and the link aggregations can be selected.
- **Subnet Address**  
Enter the IP address of the subnet.  
Example: 192.168.10.0 for the network 192.168.10.x with nodes 192.168.10.1 to 192.168.10.254.
- **Subnet Mask**  
Enter the subnet mask.

The table has the following columns:

- **1st column**  
Select the check box in the row to be deleted.
- **Port**  
All available ports and the link aggregations are shown.
- **Subnet** Shows the subnet assigned to the port.
- **Drop-down list "VLAN ID"**  
Select the VLAN ID you want to assign to the port or the subnet.

## Steps in configuration

1. Select a port from the "Port" drop-down list.
2. In "Subnet", enter the subnet mask.
3. Click the "Create" button. A new entry is generated in the table.
4. Select the VLAN ID from the VLAN ID drop-down list.
5. Click the "Set Values" button.

## 5.5.5 Mirroring

### Mirroring

The device provides the option of diverting incoming or outgoing data streams at the same time to other interfaces for analysis or monitoring without having any repercussions on the data streams themselves. This procedure is known as mirroring. In this menu section, you enable or disable mirroring and set the parameters.

#### 5.5.5.1 General

### Mirroring General

This tab contains the main switches of mirroring and the basic settings.

**Mirroring General**

General | Port | VLAN | MAC Flow | IP Flow

Mirroring  
 Monitor Barrier

	Session ID	Session Type	Status	Dest. Port
<input type="checkbox"/>	1	VLAN	active	P3.3

1 entry.

Create Delete Set Values Refresh

Click the "Create" button to create a further entry in the table. The session ID is assigned automatically. Depending on the session type selected, you can create one or more mirroring sessions.

## Settings

Select the settings.

- "Mirroring" check box  
Click this check box to enable or disable mirroring
- Monitor Barrier check box  
Click this check box to enable or disable Monitor Barrier

---

### Note

#### Monitor Barrier

If you enable the monitor barrier, other traffic on the destination port is automatically blocked (broadcast, multicast, unicast, DCP forwarding, LLDP) so that only the mirrored traffic is present here.

If you want to allow other traffic again, you will need to reconfigure this manually.

The previous statuses of these options are not restored after stopping the monitor barrier and must be reconfigured.

---

The table for the basic settings has the following boxes:

- Click the check box in the first column to select the row.  
Then click the "Delete" button to delete the selected rows.
- Session ID  
The Session ID is assigned automatically when a new entry is created.
- Session Type  
Select the required entry from the drop-down list:
  - -  
None
  - Port Based  
Port based
  - VLAN  
VLAN-based mirroring
  - MAC ACL  
Mirroring of the MAC Access Control List
  - IP ACL  
Mirroring of the IP Access Control List

- 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.

Click the Set Values button to save and activate the selected settings.

You can make further detailed settings for the relevant session ID in the following tabs.

### 5.5.5.2 Port

#### 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

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.

Mirroring a port does not work beyond switch core boundaries.

Disable port mirroring if you want to connect a normal end device to the monitor port.

---

You can only configure the settings on this page if you have already generated a session ID with the session type "Prot Based" on the "General" tab.



**Port Mirroring Sources**

General | **Port** | VLAN | MAC Flow | IP Flow

Session ID: 1

Port	Ingress Mirroring	Egress Mirroring
P0.1	<input type="checkbox"/>	<input type="checkbox"/>
P0.2	<input type="checkbox"/>	<input type="checkbox"/>
P0.3	<input type="checkbox"/>	<input type="checkbox"/>
P0.4	<input type="checkbox"/>	<input type="checkbox"/>
P1.1	<input type="checkbox"/>	<input type="checkbox"/>
P1.2	<input type="checkbox"/>	<input type="checkbox"/>
P1.3	<input type="checkbox"/>	<input type="checkbox"/>
P1.4	<input type="checkbox"/>	<input type="checkbox"/>
P2.1	<input type="checkbox"/>	<input type="checkbox"/>
P2.2	<input type="checkbox"/>	<input type="checkbox"/>
P2.3	<input type="checkbox"/>	<input type="checkbox"/>

Set Values Refresh

### Description of the displayed boxes

- **"Session ID"**  
Select the session you want to monitor.
- **"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.

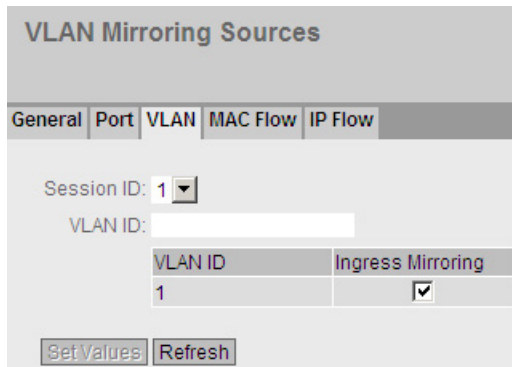
### Steps in configuration

1. In the "Session ID" drop-down list, select the session you created earlier on the General tab.
2. In the table, click the check box of the row after the port to be mirrored.  
Select whether you want to monitor incoming or outgoing packets.  
To monitor the entire data traffic of the port, select both check boxes.
3. Click the "Set Values" button.

### 5.5.5.3 VLAN

#### VLAN sources of the port mirroring function

On this page, you specify the VLAN whose incoming data traffic will be mirrored to the monitor port.



#### Description of the displayed boxes

The page contains the following boxes:

- **Session ID drop-down list**  
Select the session ID. Range of values 1 to 20.
- **"VLAN-ID" input box**  
Enter the VLAN-ID in the input box.  
Range of values: 1 ... 4094

---

#### Note

The VLAN ID 500 is reserved for future use and is already configured

---

The table has the following columns:

- **VLAN-ID**  
Shows the VLAN ID. The VLAN ID (a number between 1 and 4094) can only be assigned once when creating a new data record and can then no longer be changed. To make a change, the entire data record must be deleted and created again. Up to 257 VLANs can be defined.
- **Ingress mirroring**  
Enable or disable mirroring of incoming frames.

### 5.5.5.4 MAC Flow

#### 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.

The ACL filter decides which data is available at the monitor port. The Ingress monitoring and Egress monitoring boxes decide whether incoming or also outgoing frames are available at the monitor port.

#### Description of the displayed boxes

- **Session ID**  
Select the session number of the port mirroring. Range of values 1 to 20.
- **ACL Filter Number**  
Shows the number of the ACL filter.
- **Ingress Mirroring**  
Shows whether incoming packets are mirrored.

---

#### Note

##### Rules

A rule selected for ingress mirroring only becomes active if it was configured as a port ingress rule on at least one port. See section "Port Ingress Rules (Page 253)"

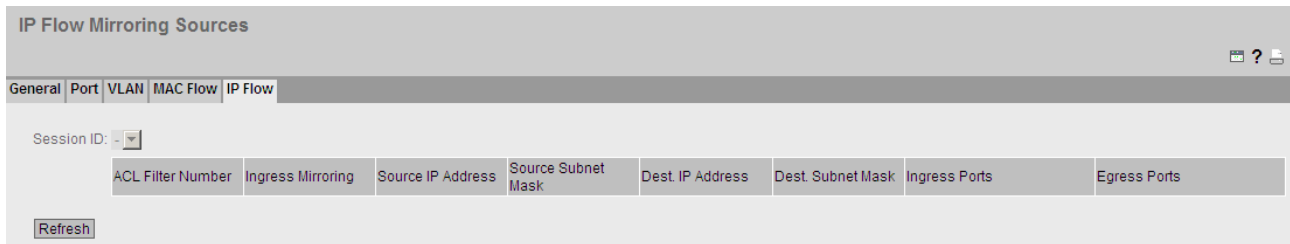
---

- **Egress mirroring**  
Shows whether outgoing packets are mirrored.
- **Source MAC Address**  
Shows the MAC address of the sender.
- **Dest. MAC Address**  
Shows the MAC address of the recipient.

### 5.5.5.5 IP Flow

#### 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.

The ACL filter decides which data is available at the monitor port.

In this list, IP data is output at the monitor port.

#### Description of the displayed boxes

- **Session ID**  
Select the session number of the port mirroring. Range of values 1 to 20.
- **ACL Filter Number**  
Shows the number of the ACL filter.
- **Ingress Mirroring**  
Shows whether incoming packets are mirrored.

---

#### Note

##### Rules

A rule selected for ingress mirroring only becomes active if it was configured as a port ingress rule on at least one port. See section "Port Ingress Rules (Page 259)"

---

- **Egress mirroring**  
Shows whether outgoing packets are mirrored.
- **Source IP Address**  
Shows the IP address of the sender.
- **Source Subnet Mask**  
Shows the subnet mask of the sender.
- **Dest. IP Address**  
Shows the IP address of the recipient.
- **Dest. Subnet Mask**  
Shows the subnet mask of the recipient.

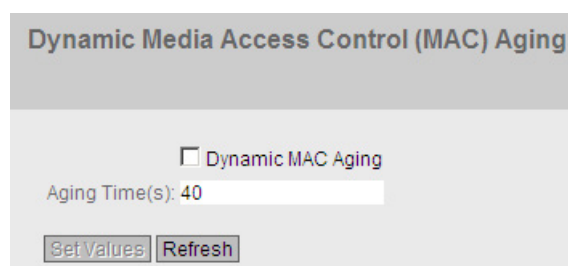
## 5.5.6 Dynamic MAC aging

### 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 (for example a programming 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" check box**  
Enable or disable the function for automatic aging of learned MAC addresses:
- **"Aging Time (s)" input box**  
Enter the time in seconds. After this time, a learned address is deleted if the device does not receive any further frames from this sender address. The range of values is from 10 seconds to 630 seconds

### 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.

## 5.5.7 Ring redundancy

### 5.5.7.1 Ring redundancy

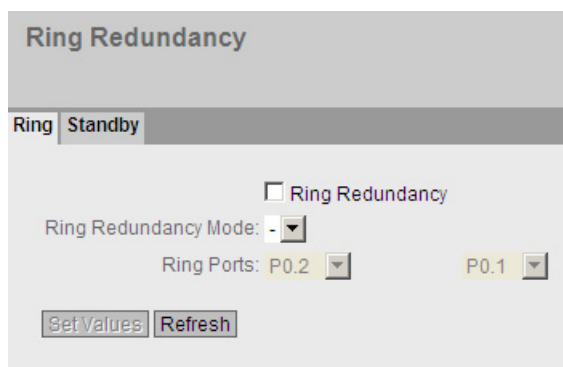
#### Configuration of ring redundancy

---

#### Note

The ring redundancy cannot be enabled if MSTP is enabled on the device.

---



- **Ring Redundancy**  
If you enable the "Ring Redundancy" check box, you turn ring redundancy on. The ring ports set on this page are used.
- **Ring Redundancy Mode**  
Here, you set the mode of the ring redundancy.  
The following modes are available:
  - -  
None
  - Automatic Redundancy Detection  
Select this setting to configure the redundant mode automatically.  
In "Automatic Redundancy Detection" mode, the IE Switch automatically detects whether or not there is a device with the role of "HRP Manager" 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 "MRP Manager". The other devices automatically set themselves to "MRP Client" mode.
  - MRP Auto-Manager  
Automatic media redundancy manager

- MRP Client  
Media redundancy client
- HRP Client  
High Speed Redundancy Protocol client
- HRP Manager  
High Speed Redundancy Protocol manager
- **Ring Ports**  
Here, you set the ports to be used as ring ports in ring redundancy.

---

**Note**

**Ring ports of SCALANCE XM400**

With SCALANCE XM400, the redundancy function is restricted to the basic devices.

Only use the following ports as ring ports:

- with SCALANCE XM416-4C only ports P1.1 to P1.16
  - with SCALANCE XM408-8C only ports P1.1 to P1.8
- 

## Restoring factory settings

If you have restored the factory defaults, ring redundancy is disabled and ports 0.1 and 0.2 are used as the ring ports. This can lead to circulating frames and failure of the data traffic if other settings were used in a previous configuration.

## Changing the status of the ring ports with the redundancy manager

If you configure a redundancy manager, set the status of the ring ports. The first ring port changes to the "forwarding" status and the second ring port to the "blocking" status. As long as ring redundancy is enabled, you cannot change the status of these ring ports.

To change the status of the two ring ports with the redundancy manager, follow the steps below:

1. Open the ring so that there are no circulating frames.
2. Disable ring redundancy.
3. Click the "Set Values" button.
4. Enable ring redundancy.
5. For "Ring Redundancy Mode", select the "HRP Manager" mode.
6. Replace the ring ports.
7. Click the "Set Values" button.

---

**Note**

If ring redundancy is enabled, you can specify other ring ports. To do this, you do not need to disable ring redundancy first.

Make sure that you first open the ring so that there are no circulating frames.

---



## 5.5.7.2 Standby

### Standby manager

The standby manager allows the redundant linking of two HRP rings. To do this, two neighboring devices within a ring must be configured as standby partners.

Enable the standby manager for both standby partners and select the port via which the device is connected to the ring 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 devices as standby partners that belong together.

---

#### Note

To be able to use the function, HRP must be activated.

---

### Menu entries

Devices already being used as HRP managers cannot be configured as standby partners at the same time.

Port	Setting
P0.1	<input type="checkbox"/>
P0.2	<input type="checkbox"/>
P0.3	<input type="checkbox"/>
P0.4	<input type="checkbox"/>
P1.1	<input type="checkbox"/>
P1.3	<input type="checkbox"/>
P1.4	<input type="checkbox"/>
P2.1	<input checked="" type="checkbox"/>
P2.2	<input type="checkbox"/>
P2.3	<input type="checkbox"/>

---

#### Note

The standby manager always requires an activated HRP client.

---

### Standby Manager

Click the check box to enable or disable the function.

### Standby Port

Select a port for the link to the second ring.

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 (link) of one of the standby ports 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.

---

### Note

#### Standby ports of SCALANCE XM400

With SCALANCE XM400, the standby function is restricted to the basic devices.

Only use the following ports as standby ports:

- with SCALANCE XM416-4C only ports P1.1 to P1.16
  - with SCALANCE XM408-8C only ports P1.1 to P1.8
- 

### 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 two devices are linked by the standby function, the "Standby" function must be enabled on both devices.

---

## 5.5.8 MSTP

### 5.5.8.1 General

#### General settings of MSTP

This is the basic page for MSTP. Select the compatibility mode from the drop-down list. As default, Multiple Spanning Tree is enabled.

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.

Multiple Spanning Tree Protocol (MSTP) General

General CIST General CIST Port MST General MST Port Enhanced Passive Listening Compatibility

MSTP Protocol Compatibility: MSTP

Set Values Refresh

#### Description of the displayed boxes

The page contains the following boxes:

- **"MSTP" check box**  
Enable or disable MSTP.
- **"Protocol Compatibility" drop-down list**  
Select the compatibility mode of MSTP, for example if you select RSTP, MSTP behaves like RSTP.

The following settings are available:

- STP
- RSTP
- MSTP

#### Steps in configuration

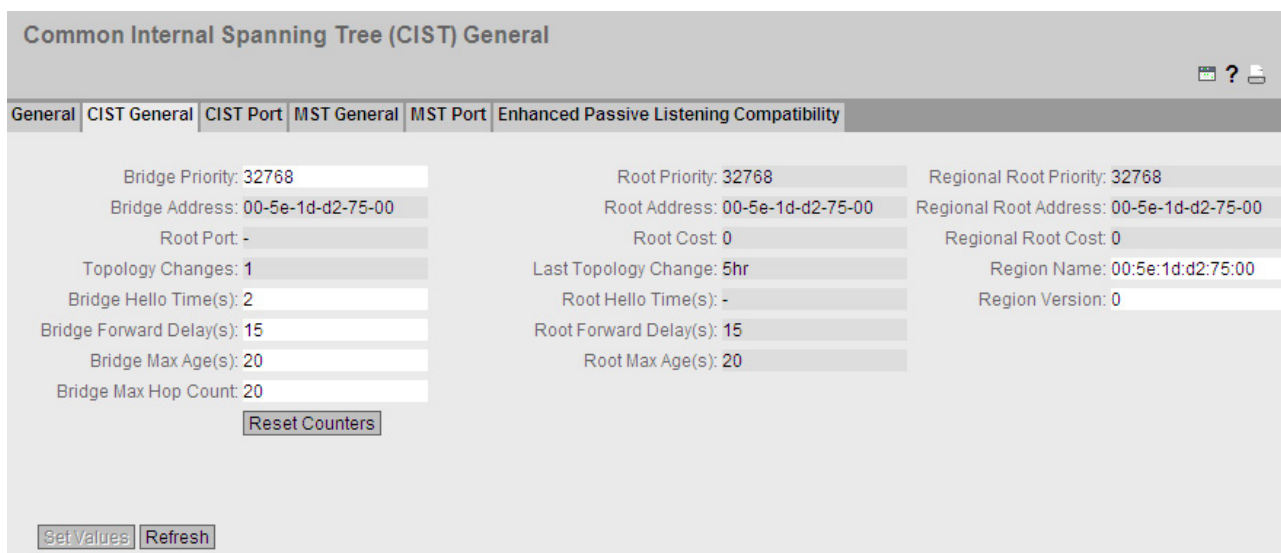
1. Select the "MSTP" check box.
2. From the "Protocol Compatibility" drop-down list, select the type of compatibility.
3. Click the "Set Values" button.

### 5.5.8.2 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 received by an device. The displayed data is only visible if you have enabled "MSTP" on the "General" page and when "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 of the displayed boxes

The page contains the following boxes:

- **"Bridge Priority" input box / Root Priority**  
The Bridge Priority specifies which device becomes 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. 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 through 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 over 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: sec unit after the number
  - Minutes: min unit after the number
  - Hour: hr unit after the number
- **Bridge Hello Time(s) / Root Hello Time(s)**  
Each bridge sends configuration frames (BPDUs) regularly. The interval between two such frames is the Hello time. The default for this parameter is 2 seconds.
- **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. The default for this parameter is 15 seconds.
- **Bridge Max Age / Root Max Age**  
Bridge Max Age defines the maximum "age" of a received BPDU for it to be accepted as valid by the switch. The default for this parameter is 20.
- **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.
- **"Reset Counters" button**  
Click this button to reset the counters on this page.
- **"Region Name" input box**  
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" input box**  
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

Steps in configuration

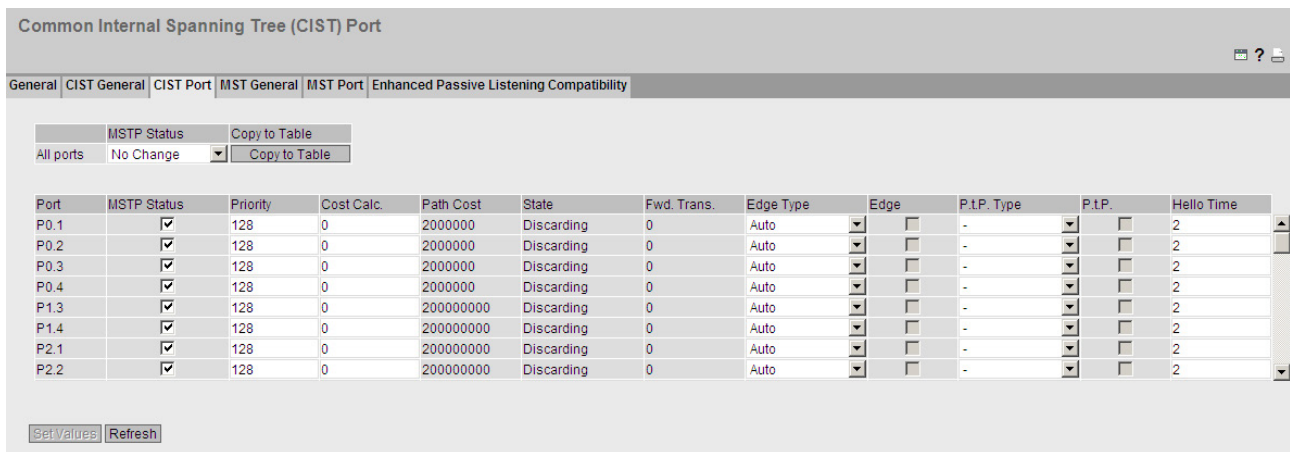
1. Enter the data required for the configuration in the input boxes.
2. Click the "Set Values" button.

5.5.8.3 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.



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.
- **MSTP 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.
- **MSTP Status**  
Specify whether the port is integrated in the spanning tree or not.

---

**Note**

If you disable the "MSTP 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", the automatically calculated value is displayed in the "Path Cost" 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" field is "0", the automatically calculated value is displayed. Otherwise, the value of the "Cost Calc" field 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 = 2,000,000The 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 is possible for status:

  - 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 EdgePort".
  - 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 for switches.



- **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.

---

- **Hello Time**

Enter the interval after which the bridge sends configuration 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 in MSTP compatible mode.

---

## 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.

### 5.5.8.4 MST general

#### Multiple Spanning Tree configuration

With MSTP, in addition to RSTP, several VLANs can be managed in a LAN with separate RSTP trees.

MSTP Instance ID:

<input type="checkbox"/>	MSTP Instance ID	Root Address	Root Priority	Bridge Priority	VLAN ID
<input type="checkbox"/>	10	00-1b-1b-39-85-38	32768	32768	

1 entry.

#### Description

The page contains the following box:

- **Input box "MSTP Instance ID"**  
Enter the number of the MSTP instance.  
Permitted values: 0 - 64

The table has the following columns:

- **1st column**  
Select the check box in the row to be deleted.
- **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 identifier of the virtual LAN in the "VLAN ID" input box.
4. Enter the priority of the bridge in the "Bridge Priority" input 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.

## 5.5.8.5 MST port

### Configuration of the Multiple Spanning Tree port parameters

On this page, you set the parameters for the ports of the configured multiple spanning tree instances.

**Multiple Spanning Tree (MST) Port**

General	CIST General	CIST Port	MST General	MST Port	Enhanced Passive Listening Compatibility																
MSTP Instance ID: <input type="text" value="-"/>																					
<table border="1" style="width: 100%; border-collapse: collapse; background-color: #d0d0d0;"> <thead> <tr> <th style="background-color: #c0c0c0;">Port</th> <th style="background-color: #c0c0c0;">MSTP Instance ID</th> <th style="background-color: #c0c0c0;">MSTP Status</th> <th style="background-color: #c0c0c0;">Priority</th> <th style="background-color: #c0c0c0;">Cost Calc.</th> <th style="background-color: #c0c0c0;">Path Cost</th> <th style="background-color: #c0c0c0;">State</th> <th style="background-color: #c0c0c0;">Fwd. Trans.</th> </tr> </thead> <tbody> <tr> <td colspan="8" style="text-align: center; padding: 5px;"> <input type="button" value="Refresh"/> </td> </tr> </tbody> </table>						Port	MSTP Instance ID	MSTP Status	Priority	Cost Calc.	Path Cost	State	Fwd. Trans.	<input type="button" value="Refresh"/>							
Port	MSTP Instance ID	MSTP Status	Priority	Cost Calc.	Path Cost	State	Fwd. Trans.														
<input type="button" value="Refresh"/>																					

### Description of the displayed boxes

The page contains the following box:

- Drop-down list "**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**  
Click the check box to enable or disable this option.
- **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 in the input box. If you enter the value "0" here, the automatically calculated value is displayed in the next box "Path Cost".
- **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 is selected.  
If the value in the "Cost Calc" field is "0", the automatically calculated value is displayed. Otherwise, the value of the "Cost Calc" field 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:
  - 1000 Mbps = 20,000
  - 100 Mbps = 200,000
  - 10 Mbps = 2,000,000The values can, however, also be set individually.

- **State**  
 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.

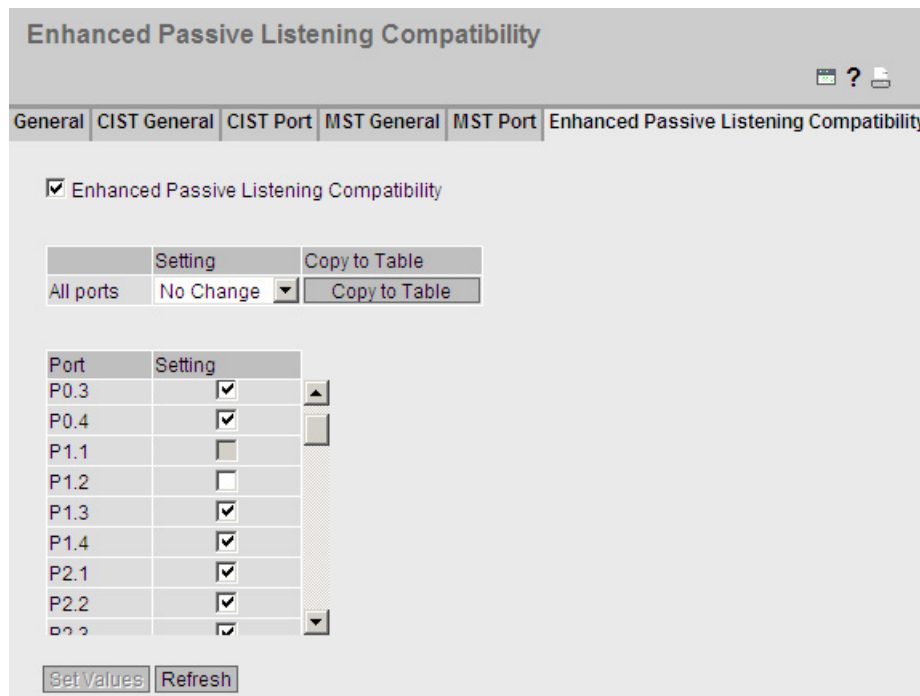
**Steps in configuration**

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.

**5.5.8.6 Enhanced Passive Listening Compatibility**

**Enabling the function**

On this page, you can enable passive listening compatibility.



### Description of the displayed boxes

The page contains the following boxes:

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

- **Setting drop-down list**

- enabled

- Enable the function for all ports of the device

- disabled

- Disable the function for all ports of the device

- No Change

- No Change

- **"Copy to Table" button**

- Writes the setting made in "Setting" to the following table

#### Port-specific table:

If the function is enabled for the entire device, enable or disable this function on individual ports.

- **Port**

- Displays the port of the device.

- **"Setting" check box**

- Enable or disable the function for this port

### Steps in configuration

#### Enable the function for the entire device

1. Enable or disable "Enhanced Passive Listening Compatibility"
2. Click the "Set Values" button

#### For all ports of the device:

1. From the drop-down list, select whether the function should be enabled or disabled or adopted unchanged.
2. Click the "Copy to Table" button
3. Click the "Set Values" button.

#### For individual ports of the device:

1. Click the check box after the required port in the port table to enable or disable the function.
2. Click the "Set Values" button

### 5.5.9 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 "remote loop" involving other network components.

**Loop Detection** ? 📄

Loop Detection

VLAN Loop Detection

	Threshold	Remote Reaction	Local Reaction	Copy to Table
All ports	No Change	No Change	No Change	Copy to Table

Port	Setting	Threshold	Remote Reaction	Local Reaction	Status	Source Port	Source VLAN	Reset
P0.1	forwarder	2	disable	disable	active	-	-	Reset
P0.2	forwarder	2	disable	disable	active	-	-	Reset
P0.3	forwarder	2	disable	disable	active	-	-	Reset
P0.4	forwarder	2	disable	disable	active	-	-	Reset
P1.1	forwarder	2	disable	disable	active	-	-	Reset
P1.2	forwarder	2	disable	disable	active	-	-	Reset

---

#### 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 only possible at ports that were not configured as ring ports or standby ports.

---

#### Description

- **"Loop detection" option button**  
Enable or disable the loop detection.
- **"VLAN loop detection" option button**  
Enable or disable the VLAN loop detection.

Table 1 contains the following columns:

- **1st column**  
Shows that the settings are valid for all ports of table 2
- **Threshold Value / 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".

---

- **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.
- **Threshold**  
By entering a number, specify the number of received loop detection frames as of which a loop is assumed.
- **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 output 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 is only possible if "VLAN Support Enabled" was selected earlier on the "Loop Detection Configuration" page.
- **Reset**  
After a loop in the network has been eliminated, click this button "Reset counters to reset the port again."

### 5.5.10 Link aggregation

#### Bundling network connections for redundancy and higher bandwidth

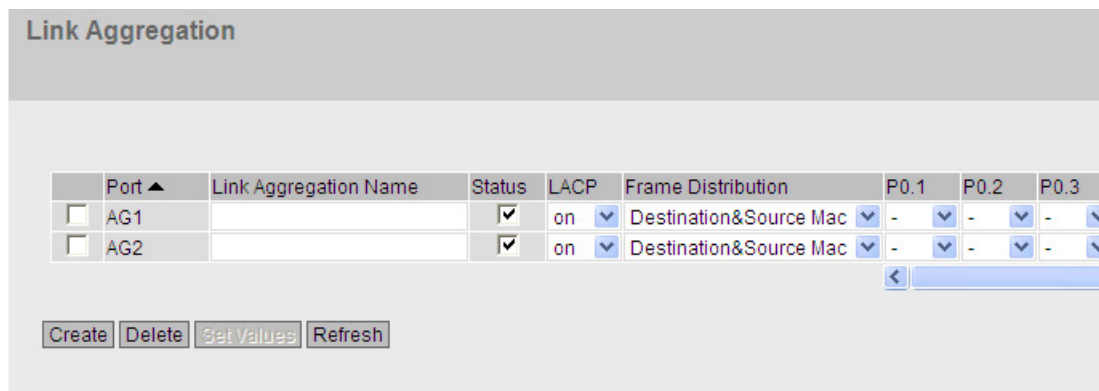
Link aggregations according to IEEE 802.3ad allow several connections between neighboring devices to be bundled to achieve higher bandwidths and protection against failure.

Ports on both partner devices are included in link aggregations and the devices are then connected via these ports. To assign ports (in other words links) correctly to a partner device, the Link Aggregation Control Protocol (LACP) from the IEEE 802.3ad standard is used.

Up to 8 link aggregations can be defined. A maximum of 8 ports can be assigned to each link aggregation.

#### Display of the configured aggregation

The menu displays all the configured link aggregations.



#### Description of the displayed boxes

The table has the following columns:

- **1st column**  
Select the check box in the row to be deleted.
- **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.

- **LACP**
  - On  
Enables the sending of LACP frames.
  - Off  
Disables the sending of LACP frames.
- **Status**  
Enable or disable link aggregation.
- **Frame Distribution**  
Set the type of distribution of packets on the individual links of an aggregation.
  - Destination&Source MAC  
The distribution is based on a combination of the destination and source MAC address.
  - Destination&Source IP MAC  
The distribution is based on a combination of the destination and source IP and MAC address.
- **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 put together to form a link aggregation between the devices.
2. Configure the link aggregation on the devices.
3. Adopt the configuration for all devices.
4. Perform the last step, the cabling.

---

### Note

If you cable aggregated links prior to configuration, it is possible that you will create loops in the network! The network involved may deteriorate badly due to this or complete disruption may occur.

---

### Creating a new link aggregation

1. Click the "Create" button to create a new link aggregation.  
This creates a new row.
2. Select the ports that will belong to this link aggregation.
3. Click the "Set Values" button.

### Deleting an aggregation

1. Using the check box at the beginning of a row, select the link aggregation you want to delete.
2. Click the "Delete" button.

### Changing an aggregation

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

### 5.5.11 DCP forwarding

#### Applications

The DCP protocol is used by STEP 7 and the PST Tool 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 sending of these frames for individual ports, for example to prevent individual parts of the network from being configured with the PST Tool or to divide the full network into smaller parts for configuration and diagnostics.

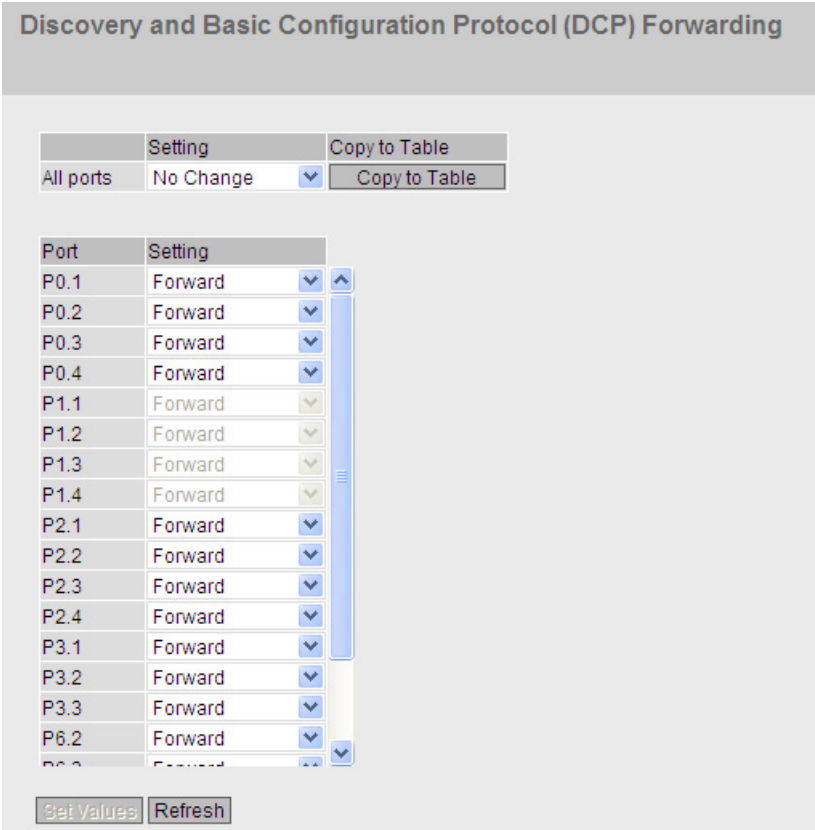
---

#### Note PNIO configuration

Since DCP is a PROFINET protocol, the configuration created here is only effective with 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.

### Steps in configuration

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.

## 5.5.12 LLDP

### Applications

PROFINET uses the LLDP protocol 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.

Setting	Copy to Table
All ports No Change	Copy to Table

Port	Setting
P0.1	Rx & Tx
P0.2	Rx & Tx
P0.3	Rx & Tx
P0.4	Rx & Tx
P1.1	Rx & Tx
P1.2	Rx & Tx
P1.3	Rx & Tx
P1.4	Rx & Tx
P2.1	Rx & Tx
P2.2	Rx & Tx
P2.3	Rx & Tx
P2.4	Rx & Tx
P3.1	Rx & Tx
P3.2	Rx & Tx
P6.2	Rx & Tx

Set Values Refresh

### Description of the displayed boxes

Table 1 has the following columns:

- **1st column**  
Shows that the settings are valid for all ports.
- **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 port.
- **Setting**  
From the drop-down list, select whether or not the port will send or receive LLDP frames. You have the following options available:
  - Rx  
This port can only receive LLDP frames.
  - Tx  
This port can only send LLDP frames.
  - Rx & Tx  
This port can receive and send LLDP frames.
  - "-" (disabled)  
This port can neither receive nor send LLDP frames.

### Steps in configuration

1. From the drop-down list in the row of the port you want to configure, select the LLDP functionality.
2. Click the "Set Values" button.



## 5.5.13 Unicast

### 5.5.13.1 Filtering

#### Address filtering

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.

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

### Filtering

Filtering
Locked Ports
Learning
Blocking

VLAN ID: VLAN1 ▼

MAC Address:

	VLAN ID	MAC Address	Status	Port
<input type="checkbox"/>	1	08-00-06-01-00-00	Learnt	P11.1
<input type="checkbox"/>	1	08-00-06-4b-67-04	Learnt	P0.1
<input type="checkbox"/>	1	08-00-06-4b-67-3f	Learnt	P0.1
<input type="checkbox"/>	1	08-00-06-4b-8f-09	Learnt	P11.1
<input type="checkbox"/>	1	6c-62-6d-6f-38-31	Learnt	P11.1

5 entries.

Create
Delete
Set Values
Refresh

#### Description of the displayed boxes

The page contains the following boxes:

- **Drop-down list "VLAN ID"**  
Select the VLAN ID in which you configure a new static MAC address. If nothing is set, "VLAN1" is set as the basic setting.
- **Input box "MAC Address"**  
Enter the MAC address.

This table contains the following columns:

- **1st column**  
Select the check box in the row to be deleted.
- **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.
  - **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.
  - **Invalid**  
These values are not evaluated.
- **Port** Shows the port over which the node with the specified address can be reached. Frames received by the device whose destination address matches this address will be forwarded to this port.

---

**Note**

You can only specify **one** port for unicast addresses.

---

### Steps in configuration

To edit the entries, follow the steps below. Note that automatically learned entries (status = "Learnt") cannot be modified.

#### Creating a new entry

1. Select the relevant VLAN ID.
2. Enter the MAC address in the "MAC Address" input box.
3. Click the "Create" button to create a new entry in the table.
4. Select the relevant port from the drop-down list.
5. Click the "Set Values" button.

#### Changing the entry

1. Select the relevant port.
2. Click the "Set Values" button.

#### Deleting an entry

1. Select the check box in the row to be deleted.  
Repeat this for all entries you want to delete.
2. Click the "Delete" button to delete the selected entries from the filter table.

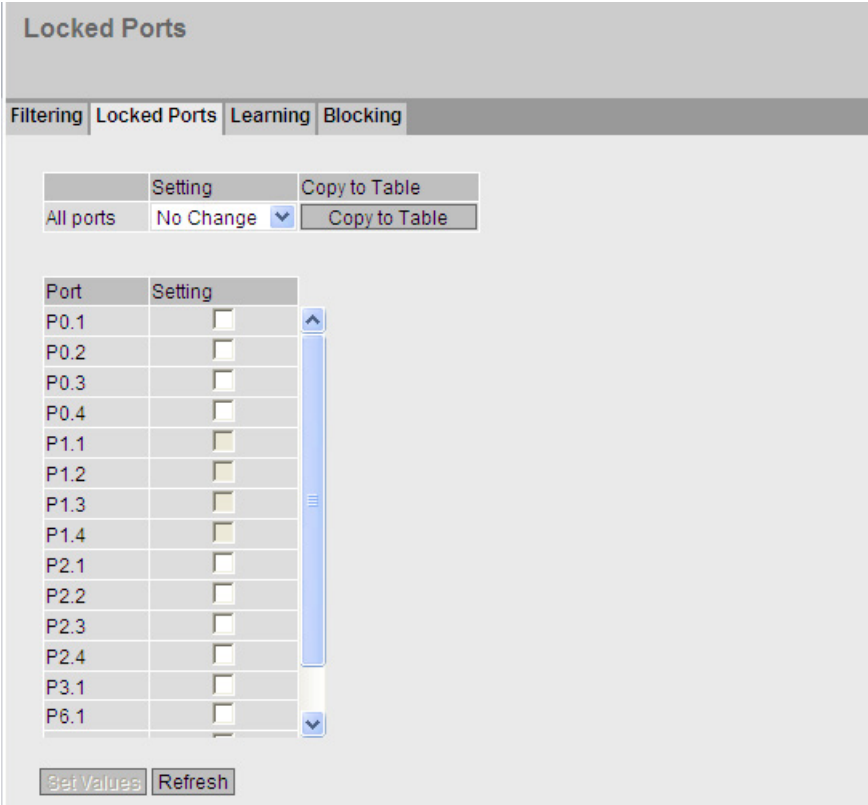
5.5.13.2 Locked ports

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. Since ports with the Port Lock function enabled cannot learn any MAC addresses, learned addresses on these ports are automatically deleted after the Port Lock function is enabled. 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.
- **Check box "Setting"**  
Enable or disable access control for the port.

### Steps in configuration

#### 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.

### 5.5.13.3 Learning

#### Starting/stopping learning

With the automatic learning function, all connected devices are automatically entered in the unicast filter table. As long as the "Start learning" function is enabled, all learned unicast addresses are created immediately as static unicast entries.

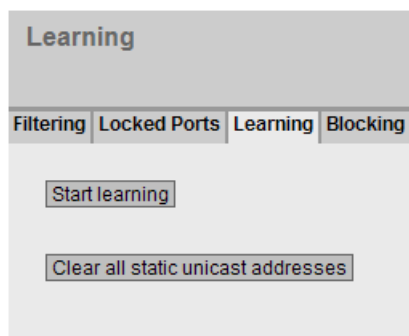
The learning process is ended only after clicking the "Stop learning" button. With this method, learning can take a few minutes or several hours in larger networks before all nodes have really been learned. Only nodes that send packets during the learning phase are found. By subsequently enabling the 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.

**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**

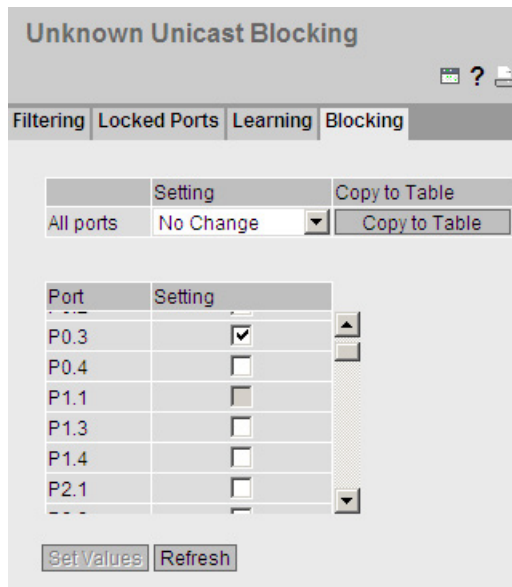
Depending on the number of entries involved, deleting may take some time.

---

**5.5.13.4 Unicast blocking**

**Blocking the 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**  
All available ports are listed in this column. Unavailable ports are not displayed.
- **Setting**  
Enable or disable the blocking of unicast frames.

---

### Note

#### Ring redundancy / standby

If ring redundancy or standby is enabled, the ports configured for this are not included in the unicast blocking.

---

## 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.

## 5.5.14 Multicast

### 5.5.14.1 Groups

#### Multicast applications

In the majority of cases, a frame is sent with a unicast address to a particular recipient. If an application sends the same data to several recipients, the amount of data can be reduced by sending the data using one multicast address. For some applications, there are fixed multicast addresses (NTP, IETF1 Audio, IETF1 Video etc.).

#### Reducing network load

In contrast to unicast frames, multicast frames represent a higher load for the device. Generally, multicast frames are sent to all ports. There are three ways of reducing the load caused by multicast frames:

- Static entry of the addresses in the multicast filter table.
- Dynamic entry of the addresses by listening in on IGMP 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. The entries can be dynamic (the device has learned them) or static (the user has set them).

#### Configuring multicast addresses

**Multicast Configuration**

Groups | **IGMP** | GMRP | Blocking

VLAN ID: VLAN1

MAC Address:

VLAN ID	MAC Address	Status
0 entries.		

Create Delete Refresh



## Description of the displayed boxes

The page contains the following boxes:

- **Check box "Block Unknown Multicasts"**  
If this check box is enabled, the IE switch does not forward any multicast packets to an unknown destination address. To be forwarded, the multicast addresses must be make known.
- **Drop-down list "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.
- **Text box "MAC Address"**  
Here you enter a new MAC multicast address you want to configure.

The table has the following columns:

- **1st column**  
Select the check box in the row to be deleted.
- **VLAN ID**  
Here, the VLAN ID of the VLAN is displayed to which the MAC multicast address of this row is assigned.
- **MAC Address**  
Here, the multicast address is displayed that the device has learned or the user has configured.
- **Status**  
Shows the status of each address entry. The following information is possible:
  - **Static**  
The address was entered statically by the user. Static addresses are stored permanently; in other words, they are not deleted when the aging time expires or when the device is restarted. These must be deleted by the user.
  - **IGMP**  
The destination port for this address was obtained by IGMP configuration.
  - **GMRP**  
The destination port for this address was registered by a received GMRP frame.

- **Port List**

There is a column for each slot. Within a column, the multicast group to which the port belongs is shown. 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.
- –  
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 must also not be an address learned dynamically with GMRP or IGMP.

## Steps in configuration

### Creating a new entry

1. Specify the required ID in the "VLAN ID" text box.
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.  
The row is deleted from the display and from the memory of the device.

## 5.5.14.2 IGMP

### Specifying the 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; a port-specific configuration is not possible.

IE switches support not only "IGMP snooping" but also the IGMP querier function. If "IGMP snooping" is enabled, IGMP frames are evaluated and the multicast filter table is updated with this information. If IGMP Query is also enabled, IE switches also send IGMP queries that trigger responses from IGMP-compliant nodes.

Internet Group Management Protocol (IGMP) Snooping & Querier

Groups | IGMP | GMRP | Blocking

IGMP Snooping

IGMP Snooping Aging Time(s): 300

IGMP Querier

Set Values Refresh

### Description of the displayed boxes

The page contains the following boxes:

- **Check box "IGMP Snooping"**  
Enable or disable IGMP (Internet Group Management Protocol). The function allows the assignment of IP addresses to multicast groups. If the check box is selected, IGMP entries are included in the table and IGMP frames are forwarded.
- **Input box "IGMP Snooping Aging Time"**  
In this box, enter the value for the aging time in seconds. As default, 300 seconds is set. Valid values: 130 - 300 (seconds)
- **Check box "IGMP Querier"**  
Enable or disable "IGMP Querier". The device sends IGMP queries.

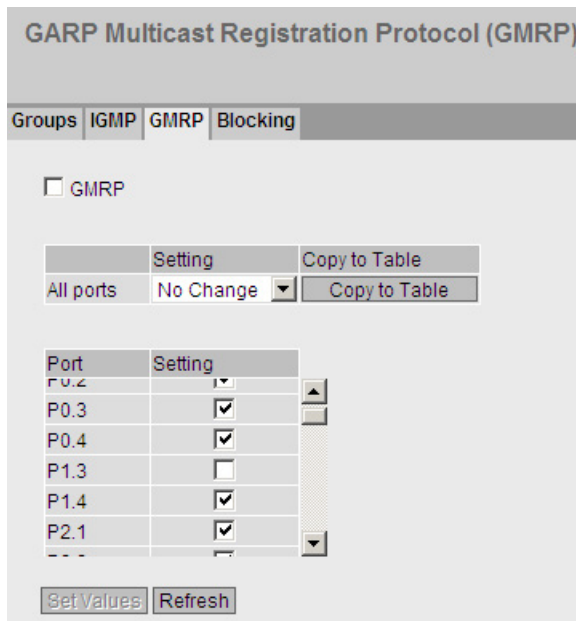
### Steps in configuration

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. Click the "Set Values" button.

### 5.5.14.3 GMRP

#### Activating GMRP

By selecting the check box, 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.



#### Description of the displayed boxes

The page contains the following box:

- **Check 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 GRMP frames.
  - disabled  
Disables the sending of GRMP 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 each individual port or link aggregation.

### Steps in configuration

#### Enabling the sending of GMRP frames for an individual port

1. Select the "GRMP" check box.
2. Select the check box in the relevant row in table 2.
3. To apply the changes, click the "Set Values" button.

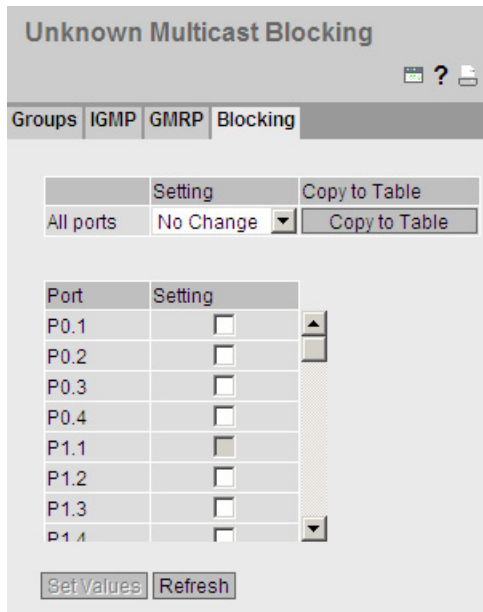
#### Enabling the sending of GMRP frames for all ports

1. Select the "GRMP" 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.

### 5.5.14.4 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.

### 5.5.15 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.

---

**Broadcast Blocking**

	Setting	Copy to Table
All ports	No Change	Copy to Table

Port	Setting
P0.1	<input type="checkbox"/>
P0.2	<input type="checkbox"/>
P0.3	<input type="checkbox"/>
P0.4	<input type="checkbox"/>
P1.1	<input type="checkbox"/>
P1.2	<input type="checkbox"/>
P1.3	<input type="checkbox"/>
P1.4	<input type="checkbox"/>
P2.1	<input type="checkbox"/>
P2.2	<input type="checkbox"/>
P2.3	<input type="checkbox"/>
P2.4	<input type="checkbox"/>
P3.1	<input type="checkbox"/>
P3.2	<input type="checkbox"/>
P3.3	<input type="checkbox"/>
P3.4	<input type="checkbox"/>
P4.1	<input type="checkbox"/>
P4.2	<input type="checkbox"/>

Set Values Refresh



## Description of the displayed boxes

Table 1 has the following columns:

- **1st column**  
Shows that the settings are valid for all ports of table 2.
- **Setting**  
Select the setting from the drop-down list. You have the following setting options:
  - enabled  
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 and the link aggregations are shown.
- **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, 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.

## 5.6 The "Layer 3" menu

### 5.6.1 Configuration

#### Introduction

The page contains the overview of the layer 3 functions of the device. On this page, you enable or disable the required layer 3 function.

The functions "Routing", "VRRP" and "OSPF" are only available with layer 3.



#### Description of the displayed boxes

The page contains the following boxes:

- **"Routing" check box**(only available with KEY-PLUG inserted)  
Enable or disable the routing function.
- **"DHCP Relay Agent" check box**  
Enable or disable the DHCP relay agent. You can configure other settings in "Layer 3 > DHCP Relay Agent".
- **"VRRP" check box**(only available with KEY-PLUG inserted, when Routing was enabled)  
Enable or disable routing using VRRP. To use VRRP, first enable the routing function. You can configure other settings in "Layer 3 > VRRP".
- **"OSPF" check box**(only available with KEY-PLUG inserted, when routing was enabled)  
Enable or disable routing using OSPF. You can configure other settings in "Layer 3 > OSPF".

#### Steps in configuration

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

## 5.6.2 Subnets

### 5.6.2.1 Overview

#### Creating subnets

The page shows the subnets for the selected interface. If more than one subnet is available on an interface, in the first entry of this interface is of the address type "Primary".

The first subnet of an interface corresponds to the agent IP configuration. You configure the first subnet of the management VLAN and the subnet of the out-of-band interface in "SYSTEM > AGENT IP".

All other subnets are created on this page. A subnet always relates to an interface. The interface is created on the "Configuration" tab.

Connected Subnets Overview

Overview | Configuration

Interface: P1.2

	Interface	TIA Interface	Interface Name	MAC Address	IP Address	Subnet Mask	Address Type	IP Assgn. Method
	P1.2	-	Slot1/2	00-5e-1d-d2-75-00	0.0.0.0	0.0.0.0	Primary	Static
	P3.1	-	Slot3/1	00-5e-1d-d2-75-00	192.168.5.10	0.0.0.0	Primary	Static
	Out-Band	-	eth0	00-5e-1d-d2-75-3d	192.168.0.30	255.255.255.0	Primary	Static
<input type="checkbox"/>	vlan1	-	vlan1	00-5e-1d-d2-75-00	192.168.10.11	255.255.255.0	Primary	Static
	vlan2	yes	vlan2	00-5e-1d-d2-75-00	192.168.2.10	255.255.255.0	Primary	Static
	loopback0	-	loopback0	00-00-00-00-00-00	127.0.0.1	255.0.0.0	Primary	Static
<input type="checkbox"/>	vlan2	-	vlan2-1	00-5e-1d-d2-75-00	0.0.0.0	0.0.0.0	Secondary	Static

7 entries.

Create Delete Refresh

#### Description of the displayed values

The page contains the following boxes:

- **"Interface" drop-down list**  
In the "Interface" drop-down list, select the interface on which you want to configure a further subnet.

The table has the following columns:

- **1st column**  
Select the check box in the row to be deleted.
- **Interface**  
Shows the interface.
- **TIA Interface**  
Shows the selected TIA interface.

- **Interface Name**  
Shows the name of the interface.
- **IP Address**  
Shows the IP address of the subnet.
- **Subnet Mask**  
Shows the subnet mask.
- **Address Type**  
Displays the address type. The following values are possible:
  - Primary  
The first IP address that was configured on an IP interface.
  - Secondary  
All other IP addresses that were configured on an IP interface.

**Steps in configuration**

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. Configure the subnet on the "Configuration" tab.

**5.6.2.2 Configuration**

On this page, you specify the name of the interface.

**Connected Subnets Configuration**

Overview | Configuration

Interface (Name): vlan1 (vlan1) ▼

Interface Name: vlan1

MAC Address: 00-5e-1d-d2-75-00

DHCP

IP Address: 192.168.10.11

Subnet Mask: 255.255.255.0

Address Type: Primary

TIA Interface

Set Values Refresh

## Description of the displayed values

The page contains the following boxes:

- **"Interface (Name)" drop-down list**  
Select the interface from the drop-down list.
- **"Interface Name" input box**  
Enter the name of the interface.
- **"MAC Address"**  
Shows the MAC address of the selected interface.
- **"DHCP" check box**  
Enable or disable the DHCP client for this IP interface.
- **"IP Address" input box**  
Enter the IP address of the interface. IP addresses must not be used more than once.
- **"Subnet Mask" input box**  
Enter the subnet mask of the subnet you are creating. Subnets on different interfaces must not overlap.
- **Address Type**  
Shows the address type. The following values are possible:
  - Primary  
The first subnet of the management VLAN and the subnet of the out-of-band interface. You can only change the subnet with the agent IP.
  - Secondary  
All further subnets of the interface.
- **"TIA Interface" check box**  
Specify whether or not this interface will become the TIA Interface.

## Steps in configuration

1. Select the Interface from the "Interface (Name)" drop-down list.
2. Enter a name for the Interface in "Interface Name".
3. Enter the IP address of the subnet in the "IP Address" column.
4. Enter the subnet mask belonging to the IP address in the "Subnet Mask" column
5. Click the "Set Values" button.

### 5.6.3 Static routes

#### Static route

On this page, you create the static routes.

**Routes**

Destination Network:

Subnet Mask:

Gateway:

	Destination Network	Subnet Mask	Gateway	Interface	Metric	Status
<input type="checkbox"/>	192.168.0.0	255.255.0.0	192.152.0.1		Not used	inactive

#### Description of the displayed values

The page contains the following boxes:

- **"Destination Network" input box**  
Enter the network address of the destination.
- **"Subnet Mask" input box**  
Enter the corresponding subnet mask.
- **"Gateway" input box**  
Enter the IP address of the next gateway.

The table has the following columns:

- **1st column**  
Select the check box in the row to be deleted.
- **Destination Network**  
Shows the network address of the destination.
- **Subnet Mask**  
Shows the corresponding subnet mask.
- **Gateway**  
Shows the IP address of the next gateway.
- **Interface**  
Shows the Interface of the route.

- **Metric**  
Enter the metric for the route. When creating the route, "not used" is entered automatically. The metric corresponds to the quality of a connection, for example speed, costs. If there are several equal routes, the route with the lowest metric value is used.  
Range of values: 1 - 254
- **Status**  
Shows whether or not the route is active.

### Steps in configuration

1. Enter the network address of the destination in the "Destination Network" input box.
2. Enter the corresponding subnet mask in the "Subnet Mask" input box.
3. Enter the gateway in the "Gateway" input box.
4. Click the "Create" button. A new entry is generated in the table.
5. Enter the weighting of the route in "Metric".
6. Click the "Set Values" button.

## 5.6.4 DHCP Relay Agent

### 5.6.4.1 General

#### DHCP Relay Agent

If the DHCP server is in a different network, the device cannot reach the DHCP server. The DHCP relay agent intercedes between a DHCP server and the device. The DHCP relay agent forwards the port number of the device with the DHCP query to the DHCP server.

You can specify up to 4 DHCP server IP addresses for the DHCP relay agent. If a DHCP server is unreachable, the device can switch to a different DHCP server.

Dynamic Host Configuration Protocol (DHCP) Relay Agent General

General Option

DHCP Relay Agent (Opt. 82)

Server IP Address:

Server IP Address
<input type="checkbox"/> 192.168.0.1

Create Delete Set Values Refresh

#### Description of the displayed values

The page contains the following boxes:

- **"DHCP Relay Agent (Opt. 82)" check box**  
Enable or disable the DHCP relay agent.
- **"Server IP Address" input box**  
Enter the IP address of the DHCP server.

The table has the following columns:

- **1st column**  
Select the check box in the row to be deleted.
- **Server IP Address**  
Shows the IP address of the DHCP server.

#### Steps in configuration

1. Enter the IP 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 (Opt. 82)" check box.
4. Click the "Set Values" button.



## 5.6.4.2 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 on the "General" tab.

### Dynamic Host Configuration Protocol (DHCP) Relay Agent Option

General
Option

**Global Configuration**

Circuit ID Router Index

Circuit ID Receive VLAN ID

Circuit ID Receive Port

Remote ID:

**Interface specific configuration**

Interface:

Interface	Remote ID Type	Remote ID	Circuit ID Type	Circuit ID
<input type="checkbox"/> vlan1	MAC Address	08-00-06-4b-69-3f	Predefined	-

### Description of the displayed values

The page contains the following boxes:

- **Check box "Circuit ID Router Index"**  
Enable or disable the check box. If you enable the check box, the generated circuit ID of the has the router index added to it.
- **Check box "Circuit ID Receive VLAN ID"**  
Enable or disable the check box. If you enable the check box, the generated circuit ID has the VLAN ID added to it.
- **Check box "Circuit ID Receive Port"**  
Enable or disable the check box. If you enable the check box, the generated circuit ID has the receiving port added to it.

---

#### Note

You need to select a least one option.

---

- **Remote ID**  
Shows the device ID.
- Select the interface from the "**Interface**" drop-down list.

The table has the following columns:

- **1st column**  
Select the check box in the row to be deleted.
- **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 IP 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 ID 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".  
Range of values: 1- 188

## Steps in configuration

Follow the steps below to specify automatic assignment of the parameters:

1. Select the "Circuit ID Router Index" check box.
2. Select the interface from the "Interface" drop-down list.
3. Click the "Create" button. A new row is inserted in the table
4. Select the entry "IP Address" in the "Remote ID Type" drop-down list. The IP address is used as the device ID.
5. Select the "Predefined" entry in the "Circuit ID Type" drop-down list. The router index is added to the generated Circuit ID.
6. Click the "Set Values" button.

Follow the steps below to specify the parameters manually:

1. Select the "Circuit ID Router Index" check box.
2. Select the interface from the "Interface" drop-down list.
3. Click the "Create" button. A new row is inserted in the table
4. Select the entry "Free Text" in the "Remote ID Type" drop-down list. Enter the device ID in "Remote ID".
5. Select the entry "Free Number" in the "Circuit ID Type" drop-down list. Enter the ID in "Circuit ID".
6. Click the "Set Values" button.

## 5.6.5 VRRP

### 5.6.5.1 Router

#### Introduction

Using the "Create" button, you can create new virtual routers. A maximum of 52 Virtual routers can be configured. You can configure other parameters on the "Configuration" tab.

---

#### Note

- This tab is available only with layer 3.
  - Select the "VRRP" check box to configure VRRP.
  - You can only use VRRP in conjunction with VLAN interfaces. Router ports are not supported.
-

Virtual Router Redundancy Protocol (VRRP) Router

Router Configuration Addresses Overview Addresses Configuration

VRRP  
 Reply to pings on virtual interfaces

Interface:

VRID:

	Interface	VRID	Virtual MAC Address	Primary IP Address	Router State	Master IP Address	Priority	Advert. Interval	Preempt
<input type="checkbox"/>	vlan1	1	00-00-5e-00-01-01	192.168.10.11	Master	192.168.10.11	255	1	yes
<input type="checkbox"/>	vlan1	2	00-00-5e-00-01-02	0.0.0.0	Initialize	0.0.0.0	100	1	yes
<input type="checkbox"/>	vlan2	1	00-00-5e-00-01-01	0.0.0.0	Initialize	0.0.0.0	100	1	yes

3 entries.

**Description of the displayed values**

The page contains the following boxes:

- **"VRRP" check box**  
Enable or disable routing using VRRP.
- **"Reply to pings on virtual interfaces" check box**  
Allow virtual IP addresses to reply to pings as well.
- **"Interface" drop-down list**  
Select the Interface that functions as the virtual router from the drop-down list.
- **"VRID" input box**  
Enter the ID of the virtual router in the input box. This ID defines the group of routers that form a virtual router (VR). In the group, this is the same. It can no longer be used for other groups.  
Valid values are 1.. 255.

The table has the following columns:

- **1st column**  
Select the check box in the row to be deleted.
- **Interface**  
Shows the Interface that functions as the virtual router.
- **VRID**  
Shows the ID of the virtual router.
- **Virtual MAC Address**  
Shows the Virtual MAC address of the virtual router.
- **Primary IP Address**  
Shows the primary IP address on this VLAN. The entry 0.0.0.0 means that the "Primary" address on this VLAN is used. Otherwise all IP addresses configured on this VLAN in the "Subnets" menu are valid addresses.

- **Router State**  
Shows the current status of the virtual router. Possible values are:
  - Master  
The router is the Master router and handles the routing functionality for all assigned IP addresses.
  - Backup  
The router is the backup router. If the master router fails, the backup router takes over the tasks of the master router.
  - Initialize  
The virtual router has just been turned on. It will soon change to the "Master" or "Backup" state.
- **Master IP Address**  
Shows the IP address of the master router.
- **Priority**  
Shows the priority of the virtual router.  
Valid values are 1-254.  
The current master router is given 255 automatically. All other priorities can be distributed freely among the VRRP routers. The higher the priority, the earlier the VRRP router becomes "Master".
- **Advert. Interval**  
Shows the interval at which the master router sends VRRP packets.
- **Preempt**  
Shows the precedence of a router when changing roles between backup and master.
  - yes  
This router has precedence when changing roles.
  - no  
This router does not have precedence when changing roles.
- **"Reply to pings on virtual interfaces"**  
Shows whether this virtual IP address replies to pings.

### Steps in configuration

1. Select the "VRRP" check box.
2. Select the interface from the "Interface" drop-down list.
3. Enter the ID of the virtual router in the "VRID" input box.
4. Select the "Reply to pings on virtual interfaces" check box so that virtual IP addresses reply to pings as well.
5. Click the "Create" button. A new row is inserted in the table.
6. Click the "Set Values" button. To configure the virtual router, click on the "Configuration" tab.

### 5.6.5.2 Configuration

#### Introduction

On this page, you configure the virtual router.

---

#### Note

This tab is available only with layer 3.

---

Virtual Router Redundancy Protocol (VRRP) Configuration

Router Configuration Addresses Overview Addresses Configuration

Interface / VRID: vlan1 / 1

Status

Primary IP Address: 192.168.10.11

Master

Priority: 255

Advertisement Interval(s): 1

Preempt lower priority Master

Set Values Refresh

#### Description of the displayed values

The page contains the following boxes:

- **"Interface / VRID" drop-down list**  
Select the ID of the virtual router you are configuring from the drop-down list.
- **"Status" check box**  
Enable or disable the "Status" function.
- **"Primary IP Address" drop-down list**  
Select the primary IP address from the drop-down list. If the router becomes master router, the router uses this IP address.

---

#### Note

If you only configure one subnet on this VLAN, no entry is necessary. The entry is then 0.0.0.0.

If you configure more than one subnet on the VLAN and you want a specific IP address to be used as the source address for VRRP packets, select the IP address from the drop-down list. Otherwise, the IP address with priority will be used.

---

- **"Master" check box**  
If this option is enabled, the highest priority IP address is entered for "Associated IP Address". This means that the highest priority IP address of the VRRP router is used as the virtual IP address of the virtual master router. The option must be disabled for the backup routers in this group and the IP address of the router in "Associated IP Address" must be used.
- **"Priority" input box**  
Enter the priority of this virtual router. Valid values are 1-254.  
The current Master router is always given 255. All other priorities can be distributed freely among the redundant routers. The higher the priority, the earlier the router becomes "Master".
- **"Advertisement Interval" input box**  
Enter the interval in seconds after which a master router sends a VRRP packet again.
- **"Preempt lower priority master" check box**  
Allow precedence when changing roles between backup and master based on the selection process.

### Steps in configuration

To configure a virtual router as the master router, follow the steps below:

1. Select the ID of the virtual router you want to configure from the "Interface /VRID" drop-down list.
2. Select the "Status" check box.
3. Select the source address from the "Primary IP Address" drop-down list.
4. From the "Priority" drop-down list, enter the priority of this virtual router.
5. Select the "Master" check box.
6. Enter the interval in "Advertisement Interval".
7. Select the "Preempt lower priority Master" check box.
8. Click the "Set Values" button.

### 5.6.5.3 Addresses Overview

#### Overview

This page shows which IP addresses the virtual router monitors. Each virtual router can monitor a maximum of 10 IP addresses.

---

**Note**

This tab is available only with layer 3.

---

**Virtual Router Redundancy Protocol (VRRP) Associated IP Addresses Overview**

Router	Configuration	Addresses Overview	Addresses Configuration				
Interface	VRID	Number of Addresses	Associated IP Address (1)	Associated IP Address (2)	Associated IP Address (3)	Associated IP Address (4)	
vlan1	1	2	192.168.10.11	192.168.10.12			
vlan1	2	0					
vlan2	1	0					

#### Description of the displayed boxes:

The table has the following columns:

- **Interface**  
Shows the Interface that functions as the virtual router.
- **VR ID**  
Shows the ID of this virtual router.
- **Number of Addresses**  
Shows the number of IP addresses.
- **Associated IP Address (1) ... Associated IP Address (10)**  
Shows the router IP addresses monitored by this virtual router. If a router takes over the role of master, the routing function is taken over by this router for all these IP addresses.



### 5.6.5.4 Addresses Configuration

#### Creating or changing the monitored IP addresses

On this page, you can create, modify or delete the IP addresses to be monitored. A maximum of 10 IP addresses can be monitored by a virtual router.

---

#### Note

This tab is available only with layer 3.

---

Virtual Router Redundancy Protocol (VRRP) Associated IP Addresses Configuration

Router Configuration Addresses Overview Addresses Configuration

Interface / VRID:

Associated IP Address:

	Associated IP Address
<input type="checkbox"/>	192.168.10.11
<input type="checkbox"/>	192.168.10.12

2 entries.

#### Description of the displayed values

The page contains the following boxes:

- **"Interface / VRID" drop-down list**  
Select the virtual router from the drop-down list.
- **"Associated IP Address" input box**  
Enter the IP address that the virtual router will monitor.  
A maximum of 10 IP addresses are possible.

The table has the following columns:

- **1st column**  
Select the check box in the row to be deleted.
- **Associated IP Address**  
Shows the IP addresses that the virtual router monitors.

#### Steps in configuration

1. Select the ID of the virtual router from the "Interface / VRID" drop-down list.
2. Enter the IP address that the virtual router will monitor.
3. Click the "Create" button. A new entry is generated in the table.

## 5.6.6 OSPFv2

### 5.6.6.1 Configuration

#### Introduction

On this page, you configure routing with OSPF.

#### Note

This tab is available only with layer 3.

**Open Shortest Path First v2 (OSPFv2) Configuration**

Configuration | Areas | Area Range | Interfaces | Virtual Links

OSPFv2

Router ID: 0.0.0.0

Border Router: Not Area Border Router

New LSA Received: 0

External LSA Maximum: -

Exit Interval(s): -

New LSA Configured: 0

OSPFv2 RFC1583 Compatibility

AS Border Router

Redistribute Routes

Default

Connected

Static

RIP

Set Values Refresh

#### Description of the displayed values

The page contains the following boxes

- **"OSPFv2" check box**  
Enable or disable routing using OSPF.
- **"Router ID" input box**  
Enter the name of one of the OSPF interfaces. The name is entered in the IP address format and does not need to match the local IP address. The router ID must be unique in the network.
- **"OSPFv2 RFC 1583 Compatibility" check box**  
Enable the option if you still have old OSPF routers in operation that are not compatible with RFC 2328.

- **Border Router**  
Shows the status of the OSPF router. If the local system is an active member in at least 2 areas, this is an area border router.
- **"AS Border Router" check box**  
Specify whether or not the router is an AS border router. An AS border router intercedes between multiple autonomous systems, for example if you have an additional RIP network. An AS border router is also necessary to add and to distribute static routes.
- **New LSA Received**  
Shows the number of received LSAs.  
Updates and local LSAs are not counted.
- **New LSA Configured**  
Number of different LSAs sent by this local system.
- **External LSA Maximum**  
To limit the number of entries of external LSAs in the database, enter the maximum number of external LSAs.
- **Exit Interval (s)**  
Enter the interval after which the OSPF router once again attempts to come out of the overflow status. A 0 means that the OSPF router attempts to exit the overflow status only following a restart.
- **Redistribute Routes (Default/Connected/Static)**  
Specify which known routes are distributed using OSPF. You can make different decisions for the route types Default, Connected and Static.

---

**Note**

The options can only be enabled on an AS border router. Enabling the Default and Static options, in particular, can cause problems if they are enabled at too many points in the network, for example, forwarding loops.

---

### Steps in configuration

1. Select the "OSPFv2" check box.
2. Enter the ID of the router in the "Router ID" input box.
3. Select the "AS Border Router" check box.
4. Click the "Set Values" button.

### 5.6.6.2 Areas

#### Overview

An autonomous system can be divided into smaller areas.

On this page, you can view, create, modify or delete the areas of the router.

---

#### Note

This tab is available only with layer 3.

---

Open Shortest Path First v2 (OSPF v2) Areas

Configuration Areas Area Range Interfaces Interface Authentication Virtual Links Virtual Link Authentication

Area ID:

	Area ID	Area Type	Summary	Metric	Updates	LSA Count	Area BR	AS BR
<input type="checkbox"/>	0.0.0.0	Backbone	No Summary	0	4	1	0	0
<input type="checkbox"/>	1.0.0.0	Normal	Summary	0	3	1	0	0
<input type="checkbox"/>	2.0.0.0	NSSA	Summary	1	3	1	0	0

3 entries.

#### Description of the displayed values

The page contains the following boxes:

- **"Area ID" input box**

Enter the identifier of the area. The database is synchronized for all routers of an area. The area identifier must be unique in the network.

The area identifier is a 32-bit number with the following format: x.x.x.x where x = 0 ... 255. The area identifier 0.0.0.0 is reserved for the backbone area.

This table contains the following columns:

- **1st column**

Select the check box in the row to be deleted.

- **Area ID**

Shows the identifier of the area.

- **Area Type**  
Select the area type in the drop-down list.
  - Standard
  - Stub
  - NSSA
  - Backbone
- **Summary**  
Specify whether summary LSAs are generated for this area.
  - Summary: Summary LSAs are generated and sent to the area.
  - No Summary: Summary LSAs are not generated and sent to the area.
- **Updates**  
Shows the number of recalculations of the routing tables.
- **LSA Count**  
Shows the number of LSAs in the database.
- **Area BR**  
Shows the number of reachable area border routers (ABR) within this area.
- **AS BR**  
Shows the number of reachable autonomous system border routers (ASBR) in this area.

### Steps in configuration

1. Enter the ID for the area in the "Area ID" input box.
2. Click the "Create" button. A new entry is generated in the table.
3. Select the type of area, for example Stub in the "Area Type" drop-down list.
4. Select the "Summary LSA" entry in the "Summary" drop-down list.
5. Click the "Set Values" button.

### 5.6.6.3 Area Range

#### Creating a new OSPFv2 area range

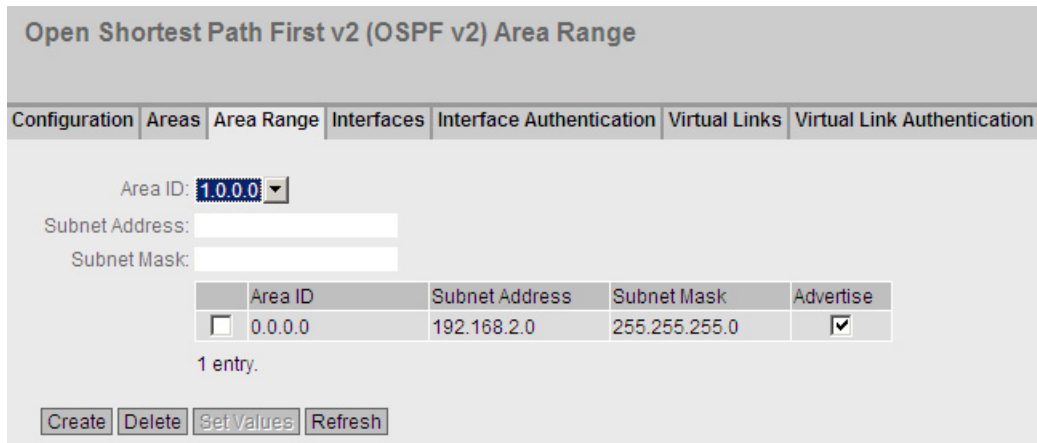
Using the "New Entry" button in the "OSPFv2 Area Ranges" menu, up to four networks can be grouped together under one area ID. The method is used only with area border routers. This means that an area border router only advertises one route for each address area to the outside.

---

**Note**

This tab is available only with layer 3.

---



### Description of the displayed boxes

The page contains the following boxes:

- **"Area ID" drop-down list**  
Select the ID of the area from the drop-down list. You specify the ID on the "Areas" tab.
- **"Subnet Address" input box**  
Enter the IP address of the network that will be grouped.
- **"Subnet Mask" input box**  
Enter the subnet mask of the network that will be grouped.

This table contains the following columns:

- **1st column**  
Select the check box in the row to be deleted.
- **Area ID**  
Shows the ID of the area.
- **Subnet Addr.**  
Shows the IP address of the network that will be grouped.
- **Subnet Mask**  
Shows the subnet mask of the network that will be grouped.
- **Advertise**  
Enable this option to advertise the grouped network.

### Steps in configuration

1. Select the ID of the area from the drop-down list.
2. Enter the IP address of the network that will be grouped.
3. Enter the subnet mask of the network that will be grouped.
4. Click the "Create" button. A new entry is generated in the table.
5. Enable the "Advertise" option to advertise the grouped network.
6. Click the "Set Values" button.

## 5.6.6.4 Interfaces

### Overview

On this page, you can configure OSPF interfaces.

#### Note

This tab is available only with layer 3.

Open Shortest Path First v2 (OSPFv2) Interfaces

Configuration Areas Area Range Interfaces Interface Authentication Virtual Links Virtual Link Authentication

IP Address: - ▾

	IP Address	Area ID	OSPF Status	Metric	Priority	Trans. Delay	Retrans. Delay	Hello Interval	Dead Interval
<input type="checkbox"/>	192.168.2.10	2.0.0.0 ▾	<input checked="" type="checkbox"/>	1	1	1	5	10	40
<input type="checkbox"/>	192.168.5.10	1.0.0.0 ▾	<input checked="" type="checkbox"/>	1	1	1	5	10	40
<input type="checkbox"/>	192.168.10.11	0.0.0.0 ▾	<input checked="" type="checkbox"/>	1	1	1	5	10	40

3 entries.

Create Delete Set Values Refresh

### Description of the displayed boxes

The page contains the following boxes:

- **"IP Address" drop-down list**  
Select the IP address of the OSPF interface from the drop-down list.

This table contains the following columns:

- **1st column**  
Select the check box in the row to be deleted.
- **IP Address**  
Shows the IP address of the OSPF interface.
- **Area ID**  
Select the ID of the area that is connected to the OSPF interface from the drop-down list.

#### Note

For the secondary interfaces, select the same Area ID as for the corresponding primary interface.

The information whether an interface is primary or secondary can be found in the "Address Type" column on the "Subnets" > "Overview (Page 219)" page.

- **OSPF Status**  
Specify whether OSPF is active on the Interface.
  - Enabled: OSPF is enabled on the interface.
  - Disabled: OSPF is disabled on the interface
- **Metric**  
Enter the costs for the OSPF interface.
- **Priority**  
Enter the router priority. The priority is only relevant for selecting the designated router or designated border router. This parameter can be selected differently on routers within the same subnet.  
Range of values: 0 to 255  
Default: 1.
- **Transit Delay**  
Enter the expected delay when sending a connection update.  
Range of values: 1 s to 3600 s  
Default: 1 s
- **Retrans. Interval**  
Enter the time after which an OSPF packet is transferred again if no confirmation was received.  
Range of values: 1 s to 3600 s  
Default: 5 s
- **Hello Interval**  
Enter the interval between two Hello packets.  
Range of values: 1 s to 65,535 s  
Default: 10 s
- **Dead Interval**  
Enter the interval after which the neighbor router is marked as "failed" if no more Hello packets are received from it during this time.  
Default: 40 s

### Steps in configuration

1. Select the IP address of the OSPF interface from the "IP Address" drop-down list.
2. Click the "Create" button. A new entry is generated in the table.
3. Select the ID of the area with which the OSPF interface is connected from the "Area ID" drop-down list.
4. Select the check box beside "OSPF Status".
5. Enter suitable values or use the default settings for "Transit Delay", "Retrans. Delay" and "Dead Interval".
6. Click the "Set Values" button.



### 5.6.6.5 Interface authentication

#### Configuring interface authentication

On this page, you define the authentication of the interface.

Open Shortest Path First v2 (OSPFv2) Interface Authentication

Configuration | Areas | Area Range | Interfaces | **Interface Authentication** | Virtual Links | Virtual Link Authentication

OSPF Interface: 192.168.2.10  
Authentication Type: MD5

**Simple Authentication**

Password:   
Confirmation:

**MD5 Authentication**

Authentication Key ID:

Authentication Key ID	MD5 Key	MD5 Key Confirmation	Youngest Key ID
<input type="checkbox"/> 100	<input type="text"/>	<input type="text"/>	yes

1 entry.

Create Delete Set Values Refresh

#### Description of the displayed boxes

The page contains the following boxes:

- **OSPF Interface**  
Select the OSPF interface for which you want to configure authentication.
- **Authentication Type**  
Select the type of authentication.
- **Simple Authentication**
  - Password  
Enter a password.
  - Confirmation  
Confirm the entered password.
- **MD5 authentication**  
Enter the identifier of the authentication key.

The table has the following columns:

- Authentication Key ID
- MD5 Key

- MD5 Key Confirmation
- Youngest Key ID

**Steps in configuration**

1. Select the OSPF interface and the authentication method from the drop-down lists.
2. Enter the following data in the relevant input box:
  - Password
  - Confirmation of the password
  - Identifier of the MD5 authentication key
3. Click the "Create" button.

**5.6.6.6 Virtual Links**

**Overview**

Due to the protocol, each area border router must have access to the backbone area. If a router is not connected directly to the backbone area, a virtual link to it is created.

**Note**

This tab is available only with layer 3.

**Note**

Note that when creating a virtual link both the transit area and the backbone area must already be configured.

A virtual link must be configured identically at both ends.

Open Shortest Path First v2 (OSPFv2) Virtual Links

Configuration Areas Area Range Interfaces Interface Authentication **Virtual Links** Virtual Link Authentication

Neighbor Router ID:

Transit Area ID: 1.0.0.0

Transit Area ID	Neighbor Router ID	Virt. Link Status	Trans. Delay	Retrans. Delay	Hello Interval	Dead Interval
0 entries.						

Create Delete Refresh

## Description of the displayed boxes

The page contains the following boxes:

- **"Neighbor Router ID" input box**  
Enter the ID of the neighbor router at the other end of the virtual connection.
- **"Transit Area ID" drop-down list**  
Select the ID of the area that connects both routers from the drop-down list.

This table contains the following columns:

- **1st column**  
Select the check box in the row to be deleted.
- **Transit Area ID**  
Shows the ID via which the two routers are connected.
- **Neighbor Router ID**  
Shows the ID of the neighbor router at the other end of the virtual link.
- **Virt. Link Status**  
Specify the status of the virtual link. The following states are possible:
  - down: The virtual link is inactive.
  - point-to-point: The virtual link is active.
- **Transmit Delay**  
Enter the expected delay when sending a link update packet.  
Range of values: 1 s to 3600 s  
Default: 1 s
- **Retrans. Interval**  
Enter the time after which a packet is transferred again if no confirmation was received.  
Range of values: 1 s to 3600 s  
Default: 5 s
- **Hello Interval**  
Enter the interval between two Hello packets.  
Range of values: 1 s to 65,535 s  
Default: 10 s
- **Dead Interval**  
Enter the interval after which the neighbor router counts as "failed" if no more Hello packets are received from it during this time.  
Default setting: 40 s

## Steps in configuration

1. Enter the ID of the neighbor router at the other end of the virtual link in "Neighbor Router ID".
2. Select the area ID that connects the two routers from the "Transit Area ID" drop-down list.
3. Click the "Create" button. A new entry is generated in the table.
4. Enter suitable values for "Transit Delay", "Retrans. Delay" and "Dead Interval".
5. Click the "Set Values" button.

### 5.6.6.7 Virtual link authentication

#### Configuring the interface login

On this page, you define the authentication of the interface.

Open Shortest Path First v2 (OSPFv2) Virtual Link Authentication

Configuration | Areas | Area Range | Interfaces | Interface Authentication | Virtual Links | Virtual Link Authentication

Virtual Link (Area/Neighbor): -  
Authentication Type: none

Simple Authentication

Password:  
Confirmation:

MD5 Authentication

Authentication Key ID:

Authentication Key ID	MD5 Key	MD5 Key Confirmation	Youngest Key ID
0 entries.			

Create Delete Set Values Refresh

#### Description of the displayed boxes

The page contains the following boxes:

- **Virtual Link (Area/Neighbor)**  
Select the interface for which you want to set up authentication.
- **Authentication Type**  
Select the type of authentication.
- **Simple Authentication**
  - Password  
Enter a password.
  - Confirmation  
Confirm the entered password.
- **MD5 Authentication**  
Enter the identifier of the MD5 authentication key.

The table has the following columns:

- Authentication Key ID
- MD5 Key
- MD5 Key Confirmation
- Youngest Key ID

### **Steps in configuration**

Follow these steps:

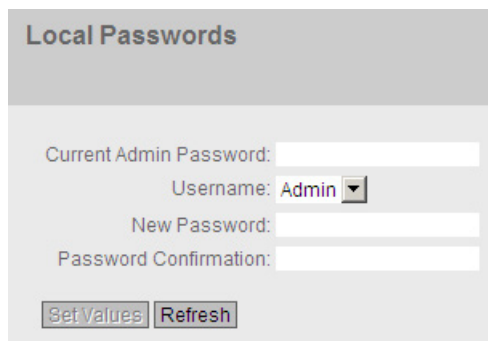
1. Select the virtual connection and the authentication method from the drop-down lists.
2. Enter the following data in the relevant input box:
  - Password
  - Confirmation of the password
  - Identifier of the MD5 authentication key
3. Click the "Set Values" button.

## 5.7 The "Security" menu

### 5.7.1 Passwords

#### Configuration of the device passwords

Changes to the device passwords for administrator and users can only be made locally by the administrator.



#### Procedure

1. From the "Username" drop-down list, select the user whose password you want to change.  
Select between "Admin" and "User".
2. Enter the valid administrator password in the "Current Admin Password" input box.
3. Enter the new password for the selected user in the "New Password" input box. The new password must be at least 6 characters long.
4. Repeat the new password in the "Password Confirmation" input box.
5. Click the "Set Values" button.

---

#### Note

The factory settings for the passwords when the devices ship are as follows:

- admin: admin
- user: user

If you log on the first time or log on after a "Restore Factory Defaults and Restart", you will be prompted to change the password.

---

#### Note

##### Changing the password in Trial mode

Even if you change the password in Trial mode, this change is saved immediately.

---

## 5.7.2 AAA

### 5.7.2.1 General

#### Description of the displayed boxes

The page contains the following boxes:

- **"Login Authentication" drop-down list**  
Specify how the login is made:
  - Local  
Login with local user name and password.
  - Radius  
Login using a Radius server.
- **"802.1x Reauthentication" check box**  
If you select this check box, an authenticated 802.1X supplicant is forced to reauthenticate cyclically. As default, one hour (3,600 s) is set.

#### Steps in configuration

1. Select the "802.1x Reauthentication" check box if you want to enable the forced reauthentication.
2. Click the "Set Values" button.

### 5.7.2.2 Radius client

#### Authentication over an external server

The concept of RADIUS is based on an external authentication server. An end device can only access the network after the device has verified the logon data of the device with the authentication server. Both the end device and the authentication server must support the EAP protocol (Extensive Authentication Protocol).

Each column 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. The client has no access to the network although a link is indicated at the port.

	Server IP Address	Server Port	Shared Secret	Shared Secret Conf.	Max. Retrans.	Primary Server	Status
<input type="checkbox"/>	0.0.0.0	1812			3	no	<input checked="" type="checkbox"/>

1 entry.

### Description of the displayed boxes

The table has the following columns:

- **Check box of the relevant row**  
Click this check box to select the entry in this row for the delete function.
- **Input box "Server IP Address"**  
Enter the IP address of the server.
- **Input box "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.
- **Input box "Shared Secret"**  
Enter your access ID here.
- **Input box "Shared Secret Conf."**  
Enter your access ID again as confirmation.
- **Input box "Max. Retrans."**  
Here, enter the maximum number of query attempts before another configured RADIUS server is queried or the logon counts as having failed. As default, 3 is set. The range of values is 1 to 254.
- **Drop-down list "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".
- **Check box "Status"**  
With this check box, you can enable or disable the RADIUS server.

---

#### Note

You can configure a maximum of two servers on this page.

---



## Steps in configuration

### 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:
  - Server IP address: 0.0.0.0
  - Port number: 1812
  - Maximum number of transmission retries: 3
  - Primary server: No
2. In the relevant row, enter the following data in the input boxes:
  - Server IP address
  - Port number of the destination
  - Secret access ID
  - Repetition of the secret access ID
  - Maximum number of transmission retries
  - Primary server
3. Click the "Set Values" button.

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:
  - IP address
  - Port number of the destination
  - Secret access ID
  - Repetition of the secret access ID
  - Maximum number of transmission retries
  - Primary server
2. Click the "Set Values" button.

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.

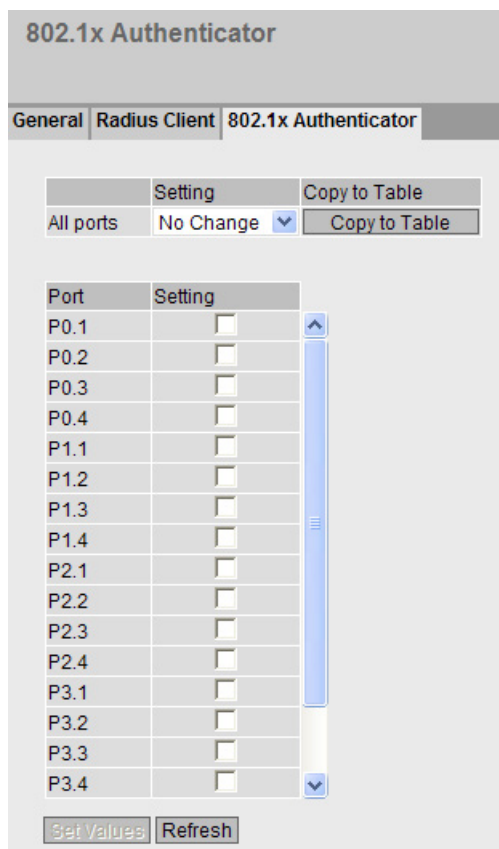
**Note**

If you click the "Refresh" button before you have transferred your configuration changes with the "Set Values" or "Delete" button, your changes will be canceled and the previous configuration is loaded from the memory of the device and displayed.

**5.7.2.3 802.1x authenticator**

**Enabling authentication for individual ports**

By selecting the check box, you specify whether or not network access protection according to IEEE 802.1x is enabled on this 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  
Access protection is enabled.
  - disabled  
Access protection is disabled.
  - 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 lists all the ports available on this device.
- **Check box "Setting"**  
In this column, select the check boxes for the authentication enabled for this port. An empty check box means that the authentication is not enabled for the port in question. If this configuration is not possible for a port, it is displayed grayed out and you cannot modify the settings.

## Steps in configuration

### Enabling authentication 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 authentication for all ports

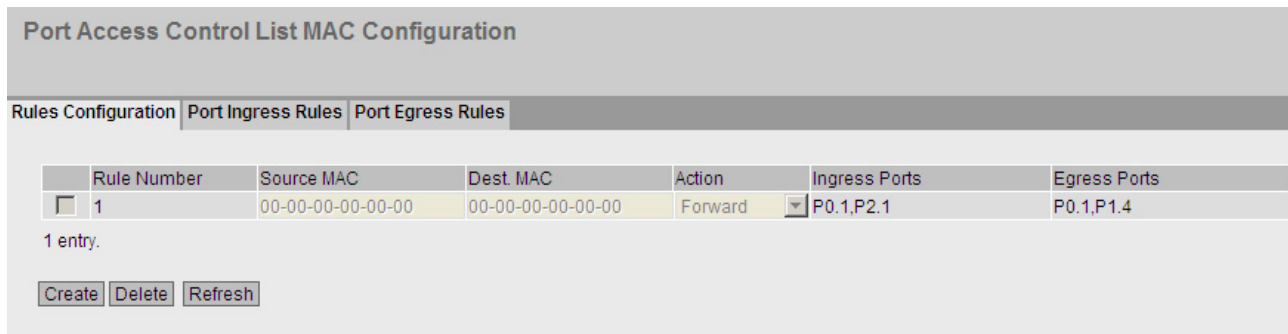
1. In the "Setting" drop-down list, select the "enabled" entry.
2. Click the "Copy to Table" button. The check box is enabled for all ports in table 2.
3. To apply the changes, click the "Set Values" button.

### 5.7.3 Port ACL MAC

#### 5.7.3.1 Rules Configuration

##### Introduction

On this page, you specify the ACL rules for the MAC-based ACL.



##### Description of the displayed boxes

The table has the following columns:

- **Rule Number**  
Shows the number of the ACL rule. If you click the "Create" button, a new row with a unique number is created.
- **Source MAC**  
Enter the unicast MAC address of the source.
- **Dest. MAC**  
Enter the unicast MAC address of the destination.
- **Action**  
Select the action from the drop-down list. The following is possible:
  - Forward  
If the frame complies with the ACL rule, the frame is forwarded.
  - Discard  
If the frame complies with the ACL rule, the frame is not forwarded.
- **Ingress Ports**  
Shows a list of all ingress ports to which this rule applies
- **Egress Ports**  
Shows a list of all egress ports to which this rule applies

**Note**

**Entering the MAC addresses**

If you enter the address "00:00:00:00:00:00" for the source and/or destination MAC address, the rule created in this way applies to all source or destination MAC addresses.

**Steps in configuration**

1. Click the "Create" button. A new row with a unique number (rule number) is created in the table.
2. Enter the MAC address of the source in "Source Mac".
3. Enter the MAC address of the destination in "Dest. MAC".
4. For "Action", specify whether the frame is forwarded or denied if the frame complies with the ACL rule.

**5.7.3.2 Port Ingress Rules**

**Introduction**

On this page, you specify the ACL rule according to which incoming frames are handled by the port.

**Port ACL MAC Port Ingress Rules**

Rules Configuration	Port Ingress Rules	Port Egress Rules
---------------------	--------------------	-------------------

Ports: P0.1

Add Rule: -

Remove Rule: Rule 1

Rule Order	Rule Number	Source MAC	Dest. MAC	Action
1	1	00-00-00-00-00-00	00-00-00-00-00-00	Forward <input type="button" value="v"/>

## Description of the displayed boxes

The page contains the following boxes

- **"Ports" drop-down list**  
Select the required port from the drop-down list.
- **"Add Rules" drop-down list**  
From the drop-down list, select the ACL rule that will be assigned to the port. You specify the ACL rule on the "Rules Configuration" tab.
- **"Add" button**  
To permanently assign the ACL rule to the port, click the "Add" button. The configuration is shown in the table.
- **"Remove Rule" drop-down list**  
From the "Remove Rule" drop-down list, select the ACL rule to be deleted.
- **"Remove" button**  
To remove the ACL rule from the port, click the "Remove" button.

The table has the following columns:

- **Rule Order**  
Shows the order of the ACL rules.
- **Rule Number**  
Shows the number of the ACL rule.
- **Source MAC**  
Shows the unicast MAC address of the source.
- **Dest. MAC**  
Shows the unicast MAC address of the destination.
- **Action**  
Shows the action.
  - Forward  
If the frame complies with the ACL rule, the frame is forwarded.
  - Discard  
If the frame complies with the ACL rule, the frame is not forwarded.

## Steps in configuration

Follow the steps below to assign an ACL rule to a port:

1. Select the port in the "Ports" drop-down list.
2. Select the ACL rule in the "Rules" drop-down list.
3. Click the "Add" button. A new entry is generated in the table.

Follow the steps below to remove an ACL rule from a port:

1. Select the port in the "Ports" drop-down list.
2. Select the ACL rule in the "Rules" drop-down list.
3. Click the "Remove" button. The corresponding entry is removed in the table.

### 5.7.3.3 Port Egress Rules

#### Introduction

On this page, you specify the ACL rule according to which outgoing frames are handled by the port.

Port ACL MAC Port Egress Rules

Rules Configuration | Port Ingress Rules | Port Egress Rules

Ports: P0.1

Add Rule: -

Add

Remove Rule: Rule 1

Remove

Rule Order	Rule Number	Source MAC	Dest. MAC	Action
1	1	00-00-00-00-00-00	00-00-00-00-00-00	Forward

Set Values Refresh

#### Description of the displayed boxes

- **"Ports" drop-down list**  
Select the required port from the drop-down list.
- **"Add Rules" drop-down list**  
From the drop-down list, select the ACL rule that will be assigned to the port. You specify the ACL rule on the "Rules Configuration" tab.
- **"Add" button**  
To permanently assign the ACL rule to the port, click the "Add" button. The configuration is shown in the table.
- **"Remove Rule" drop-down list**  
From the "Remove Rule" drop-down list, select the ACL rule to be deleted.
- **"Remove" button**  
To remove the ACL rule from the port, click the "Remove" button.

The table has the following columns:

- **Rule Order**  
Shows the order of the ACL rules.
- **Rule Number**  
Shows the number of the ACL rule.
- **Source MAC**  
Shows the unicast MAC address of the source.

- **Dest. MAC**  
Shows the unicast MAC address of the destination.
- **Action**  
Shows the action.
  - Forward  
If the frame complies with the ACL rule, the frame is forwarded.
  - Discard.  
If the frame complies with the ACL rule, the frame is not forwarded.

### Steps in configuration

Follow the steps below to assign an ACL rule to a port:

1. Select the port in the "Ports" drop-down list.
2. Select the ACL rule in the "Rules" drop-down list.
3. Click the "Add" button. A new entry is generated in the table.

Follow the steps below to remove an ACL rule from a port:

1. Select the port in the "Ports" drop-down list.
2. Select the ACL rule in the "Rules" drop-down list.
3. Click the "Remove" button. The corresponding entry is removed in the table.



## 5.7.4 Port ACL IP

### 5.7.4.1 Rules Configuration

#### Introduction

On this page, you specify the rules for the IP-based ACL.

Port Access Control List IP Configuration

Rules Configuration | Port Ingress Rules | Port Egress Rules

	Rule Number	Source IP	Source Subnet Mask	Dest. IP	Dest. Subnet Mask	Action	Ingress Ports	Egress Ports
<input type="checkbox"/>	1	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	Forward		

1 entry.

#### Description of the displayed boxes

The table has the following columns:

- **Rule Number**  
Shows the number of the ACL rule. If you click the "Create" button, a new row with a unique number is created.
- **Source IP**  
Enter the IP address of the source.
- **Source Subnet Mask**  
Enter the subnet mask in which the source is located.
- **Dest. IP**  
Enter the IP address of the destination.
- **Source Dest. Mask**  
Enter the subnet mask in which the destination is located.
- **Action**  
Select the action from the drop-down list. The following is possible:
  - Forward  
If the frame complies with the ACL rule, the frame is forwarded.
  - Discard  
If the frame complies with the ACL rule, the frame is not forwarded.
- **Ingress Ports**  
Shows a list of all ingress ports to which this rule applies
- **Egress Ports**  
Shows a list of all egress ports to which this rule applies

---

**Note**

**Subnet mask for individual hosts**

If you create the rule for a single system (one IP address), you will need to specify a 32-Bit long subnet mask. This is then "255.255.255.255".

---

**Steps in configuration**

1. Click the "Create" button. A new row with a unique number (rule number) is created in the table.
2. Enter the data of the source in "Source IP" and in "Source Subnet Mask".
3. Enter the data of the destination in "Source IP" and in "Source Dest Mask".
4. For the action, specify whether the frame will be forwarded or denied if the frame complies with the ACL rule.

## 5.7.4.2 Port Ingress Rules

### Introduction

On this page, you specify the ACL rule according to which incoming frames are handled by the port.

Port ACL IP Port Ingress Rules

Rules Configuration | Port Ingress Rules | Port Egress Rules

Ports: P0.1

Add Rule: -

Add

Remove Rule: Rule 1

Remove

Rule Order	Rule Number	Source IP	Source Subnet Mask	Dest. IP	Dest. Subnet Mask	Action
1	1	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	Forward

Set Values Refresh

### Description of the displayed boxes

The page contains the following boxes

- **Drop-down list "Ports"**  
Select the required port from the drop-down list.
- **Drop-down list "Add Rules"**  
From the drop-down list, select the ACL rule that will be assigned to the port. You specify the ACL rule on the "Rules Configuration" tab.
- **"Add" button**  
To permanently assign the ACL rule to the port, click the "Add" button. The configuration is shown in the table.
- **Drop-down list "Remove Rule"**  
From the "Remove Rule" drop-down list, select the ACL rule to be deleted.
- **"Remove" button**  
To remove the ACL rule from the port, click the "Remove" button.

The table has the following columns:

- **Rule Order**  
Shows the order of the ACL rules. In
- **Rule Number**  
Shows the number of the ACL rule. If you click the "Create" button, a new row with a unique number is created.

- **Source IP**  
Shows the IP address of the source.
- **Source Subnet Mask**  
Shows the subnet mask in which the source is located.
- **Dest. IP**  
Shows the IP address of the destination.
- **Source Dest. Mask**  
Shows the subnet mask in which the destination is located.
- **Action**  
Select the action from the drop-down list. The following reactions are possible:
  - Forward  
If the frame complies with the ACL rule, the frame is forwarded.
  - Discard  
If the frame complies with the ACL rule, the frame is not forwarded.

### Steps in configuration

Follow the steps below to assign an ACL rule to a port:

1. Select the port in the "Ports" drop-down list.
2. Select the ACL rule in the "Rules" drop-down list.
3. Click the "Add" button. A new entry is generated in the table.

Follow the steps below to remove an ACL rule from a port:

1. Select the port in the "Ports" drop-down list.
2. Select the ACL rule in the "Rules" drop-down list.
3. Click the "Remove" button. The corresponding entry is removed in the table.

### 5.7.4.3 Port Egress Rules

#### Introduction

On this page, you specify the ACL rule according to which outgoing frames are handled by the port.

Port ACL IP Port Egress Rules

Rules Configuration | Port Ingress Rules | Port Egress Rules

Ports: P0.1

Add Rule: -

Add

Remove Rule: Rule 1

Remove

Rule Order	Rule Number	Source IP	Source Subnet Mask	Dest. IP	Dest. Subnet Mask	Action
1	1	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	Forward

Set Values Refresh

#### Description of the displayed boxes

The page contains the following boxes

- **Drop-down list "Ports"**  
Select the required port from the drop-down list.
- **Drop-down list "Add Rules"**  
From the drop-down list, select the ACL rule that will be assigned to the port. You specify the ACL rule on the "Rules Configuration" tab.
- **"Add" button**  
To permanently assign the ACL rule to the port, click the "Add" button. The configuration is shown in the table.
- **Drop-down list "Remove Rule"**  
From the "Remove Rule" drop-down list, select the ACL rule to be deleted.
- **"Remove" button**  
To remove the ACL rule from the port, click the "Remove" button.

The table has the following columns:

- **Rule Order**  
Shows the order of the ACL rules. In
- **Rule Number**  
Shows the number of the ACL rule. If you click the "Create" button, a new row with a unique number is created.

- **Source IP**  
Shows the IP address of the source.
- **Source Subnet Mask**  
Shows the subnet mask in which the source is located.
- **Dest. IP**  
Shows the IP address of the destination.
- **Source Dest. Mask**  
Shows the subnet mask in which the destination is located.
- **Action**  
Select the action from the drop-down list. The following reactions are possible:
  - Forward  
If the frame complies with the ACL rule, the frame is forwarded.
  - Discard  
If the frame complies with the ACL rule, the frame is not forwarded.

### Steps in configuration

Follow the steps below to assign an ACL rule to a port:

1. Select the port in the "Ports" drop-down list.
2. Select the ACL rule in the "Rules" drop-down list.
3. Click the "Add" button. A new entry is generated in the table.

Follow the steps below to remove an ACL rule from a port:

1. Select the port in the "Ports" drop-down list.
2. Select the ACL rule in the "Rules" drop-down list.
3. Click the "Remove" button. The corresponding entry is removed in the table.

## 5.7.5 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. You define the VLAN in which the station may be located. This ensures that only certain stations within a VLAN have access to the device.

**Management Access Control List**

Management ACL

IP Address:

Subnet Mask:

Rule Order	IP Address	Subnet Mask	VLANs Allowed	Out-Band	SNMP	TELNET	HTTP	HTTPS	SSH	P0.1	P0.2
<input type="checkbox"/> 1	192.168.10.10	255.255.255.255	1-4094	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

1 entry.

### Description of the displayed boxes

The page contains the following boxes:

- **"IP Address" input box**  
Enter the IP address or the network address to which the rule will apply. If you use the IP address 0.0.0.0, the settings apply to all IP addresses.
- **Subnet Mask**  
Enter the subnet mask. The subnet mask 255.255.255.255 is for a specific IP address. If you want to allow a subnet, for example a C subnet, enter 255.255.255.0. The subnet mask 0.0.0.0 applies to all subnets.

The table has the following columns:

- **1st column**  
Select the check box in the row to be deleted.
- **IP Address**  
Shows the IP address.
- **Subnet Mask**  
Shows the subnet mask.
- **VLANs Allowed**  
Enter the number of the VLAN in which the device is located. The station can only access the device if it is located in this configured VLAN. If this input box remains empty, there is no restriction relating to the VLANs.
- **Out-Band**  
Specify whether or not the IP address can access the switch via the out-band port.

- **SNMP**  
Specify whether the station (or the IP address) can access the device using the SNMP protocol.
- **TELNET**  
Specify whether the station (or the IP address) can access the device using the TELNET protocol.
- **HTTP**  
Specify whether the station (or the IP address) can access the device using the HTTP protocol.
- **HTTPS**  
Specify whether the station (or the IP address) can access the device using the HTTPS protocol.
- **SSH**  
Specify whether the station (or the IP address) can access the device using the SSH protocol.
- **Px.y**  
Specify whether the station (or the IP address) can access this device via this port (slot.port).

## Steps in configuration

### Changing the entry

1. Configure the data of the entry you want to modify.
2. Click the "Set Values" button to transfer the changes to the device.

### Creating a new entry

1. In the "IP Address" input box, enter the IP address of the device and in the "Subnet Mask" input box the corresponding subnet mask.
2. Click the "Create" button to create a new row in the table.
3. Configure the entries of the new row.
4. Click the "Set Values" button to transfer the new entry to the device.

### Deleting entries

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 entries are deleted and the page is updated.

---

### Note

Note that 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.

---



## Troubleshooting/FAQ

### 6.1 Firmware update via WBM or CLI not possible

#### Cause

If there is a power failure during the firmware update, it is possible that the IE switch is no longer accessible using Web Based Management or the Command Line Interface.

#### Solution

If the IE switch cannot be reached using WBM or CLI, you can download the firmware to your IE switch using TFTP.

Follow the steps below to load new firmware using TFTP:

1. Turn off the power to the IE switch.
2. Press the Reset button and reconnect the power to the IE switch while holding down the button.
3. Hold down the button until the red fault LED (F) starts to flash after approximately 30 seconds.
4. Release the button.

The bootloader waits in this state for a new firmware file that you can download by TFTP.

5. Connect a PC via the Ethernet interface with the out-band interface of the IE switch.
6. Assign an IP address to the IE switch with the Primary Setup Tool.
7. In the command prompt, change to the directory where the file with the new firmware is located and then execute the command "tftp -i <ip address> PUT <firmware>". As an alternative, you can use a different TFTP client.

#### Result

The firmware is transferred to the IE switch.

---

#### Note

Please note that the transfer of the firmware can take several minutes. During the transmission, the red error LED (F) flashes.

---

Once the firmware has been transferred completely to the IE switch, the IE switch is restarted automatically.

*6.1 Firmware update via WBM or CLI not possible*

# Index

## A

- Access control, 203, 205
  - Automatic learning, 205
- ACL, 205, 263
- Aging
  - Dynamic MAC Aging, 173
- Aging time, 211
- Alarm events, 101
- Authentication, 110, 250

## B

- Bridge, 180
  - Bridge priority, 180
  - Root bridge, 180
- Bridge Max Age, 181
- Bridge Max Hop Count, 181
- Broadcast, 216

## C

- Cable test, 143
- Class of Service, 151
- Collisions, 74
- Combo Port Media Type, 124
- Configuration mode, 84
- CoS, 151
  - Traffic queue, 151
- CoS (Class of Service), 24
- C-PLUG
  - Formatting, 135
  - Saving the configuration, 135
- C-PLUG / KEY-PLUG, 13
- CRC, 73

## D

- DCP server, 83, 197
- DHCP
  - Client, 103
- DSCP, 152

## E

- E-Mail function, 101
  - Alarm events, 101
  - Line monitoring, 101
- Error status, 60
- Ethernet
  - Packet Error, 73
  - Packet size, 70
  - Packet type, 72
- Event log table, 58
- Events
  - Log table, 58

## F

- Fault monitoring
  - Connection status change, 129
  - Redundancy, 131
- Filter
  - Filter configuration,
- Forward Delay, 181
- Fragments, 73

## G

- Geographic coordinates, 86
- Glossary, 8
- GMRP, 212
- GVRP, 158

## H

- Hardware version, 56
- Hello time, 181
- HRP, 177
- HTTP
  - Load/save, 91
- HTTPS
  - Server, 82

## I

- IGMP, 211
- Information

- ARP table, 57
- Log table, 58
- Ring redundancy, 66, 68
- Spanning Tree, 61
- Start page, 49
- Versions, 54

IP address, 88

## J

Jabbers, 73

## K

KEY-PLUG, 133, 136

- Formatting, 135

## L

LACP, 194

Layer 2, 147

Layer 3, 136, 218

- Configuration, 218

Line monitoring, 101

Location, 86

Logging on

- via HTTP, 47
- via HTTPS, 47

Logout

- Automatic, 119

Loop, 191

Loop detection, 191

## M

MAC ACL, 252, 253

- Configuration, 253, 255

Maintenance data, 55

Management ACL, 263

Manufacturer, 55

Mirroring, 166

- General, 166
- IP Flow, 172
- MAC Flow, 171
- Port, 168
- VLAN, 170

MSTP, 179, 186

- Port, 182
- Port parameters, 187

MSTP instance, 187, 188

Multicast, 208

Multiple Spanning Tree, 182, 186

## N

Near Field Communication, 84

Negotiation, 124

NFC, 84

NTP, 208

- Client, 116

## O

Order number, 55

OSPF

- Area range, 237
- Areas, 31, 236
- Configuration, 234
- Link State Advertisement, 31
- OSPFv2 Interfaces, 75, 239
- OSPFv2 LSDB (information), 80
- OSPFv2 Neighbors, 77
- OSPFv2 Virtual Neighbors, 79
- Router, 31
- Router status, 31
- Virtual Links, 242

Oversize, 73

## P

Packet error statistics, 73

Password, 246

Ping, 138

PLUG, 136

- C-PLUG,
- KEY-PLUG,

PNIO, 132

PoE, 139, 140

- Port, 140

point-to-point, 29

Port, 125

- Port configuration, 123, 127

Port configuration, 125, 127

Port diagnostics

- Cable test, 143
- SFP diagnostics, 145

Power over Ethernet, 14, 139

- Port, 140

Power supply

- Monitoring, 128

Priority, 181

PROFINET IO, 132  
PST tool, 197

## R

RADIUS, 247  
Rate control, 153  
Reboot, 90  
Redundancy, 174, 177  
Redundancy methods  
  HRP, 35  
Redundant networks, 180  
Reset, 90  
RFC  
  RFC 1518, 17  
Ring redundancy, 174  
  HRP, 148, 175  
  MRP, 148, 174  
  Ring ports, 175  
  Standby, 177  
Root Max Age, 181  
Routing, 30, 222  
  Routing table, 74  
  Static routes, 30, 222  
  VRRP, 30  
RSTP, 179  
Rule, 252, 253, 257  
  Configuration, 257  
  Egress, 255, 257  
  Ingress, 253, 257  
  IP ACL, 257

## S

Scope of the manual, 7  
Security settings, 107  
Select/Set button, 119  
Serial number, 56  
SFP diagnostics, 145  
SHA algorithm, 108  
SIMATIC NET glossary, 8  
SMTP  
  Client, 82  
SNMP, 26, 83, 104, 107  
  Groups, 107  
  SNMPv1, 26  
  SNMPv2c, 26  
  SNMPv3, 26  
  Trap, 106  
  Users, 109  
Software version, 56

Spanning tree, 179  
  MSTP, 179  
  Passive listening, 189  
  RSTP, 179  
Spanning Tree  
  Information, 61  
  Rapid Spanning Tree, 29  
SSH  
  Server, 82  
Standby, 177  
Standby redundancy, 42  
Start page, 49  
STEP 7, 197  
STP, 179  
Subnet  
  Configuration, 220  
  Overview, 219  
Subnet mask, 17  
Syslog, 121  
  Client, 83  
System  
  Configuration, 82  
  General information, 85  
System event log  
  Agent, 121  
System events  
  Configuration, 97  
  Severity filter, 100

## T

Telnet  
  Server, 82  
TFTP  
  Load/save, 94  
Time, 83  
Time of day  
  Manual setting, 112  
  SIMATIC Time Client, 118  
  SNTP (Simple Network Time Protocol), 113  
  System time, 111  
  Time zone, 115  
  Time-of-day synchronization, 113  
  UTC time, 115  
Time setting, 83

## U

Undersize, 73

## **V**

- Vendor ID, 55
- VLAN, 22, 162
  - Group, 162
  - Port VID, 161
  - Priority, 161
  - Tag, 161
  - VLAN ID, 25
  - VLAN tag, 23
- VRRP
  - Addresses Configuration, 233
  - Addresses Overview, 232
  - Backup router, 30
  - Configuration, 230
  - Master router, 30
  - Router, 227
  - Virtual router, 30
  - VRRP router, 30
  - VRRP Statistics, 64

## **W**

- Web Based Management, 45
  - Requirement, 45