SIEMENS

SIMATIC NET

Industrial Ethernet Switches SCALANCE X-300 / X-400

Configuration Manual

02/2012

C79000-G8976-C187-18

Legal information

Warning notice system

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

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

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

⚠CAUTION
with a safety alert symbol, indicates that minor personal injury can result if proper precautions are not taken.

CAUTION
without a safety alert symbol, indicates that property damage can result if proper precautions are not taken.

NOTICE
indicates that an unintended result or situation can occur if the relevant information is not taken into account.

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

Qualified Personnel

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

Proper use of Siemens products

Note the following:

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

Trademarks

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

Disclaimer of Liability

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

Siemens AG
Industry Sector
Postfach 48 48
90026 NÜRNBERG
GERMANY

Order number: C79000-G8976-C187-18
℗ 02/2012 Technical data subject to change

Preface

Purpose of the manual

This manual supports you when configuring the SCALANCE X-300 and X-400 Industrial Ethernet switches. It outlines the technical options provided by a SCALANCE X-300/X-400 and describes how to configure with Web Based Management and the Command Line Interface.

Validity of this manual

This manual is valid for the following software versions:

- SCALANCE X-300/X-400 firmware version 3.7.0
- Primary Setup Tool as of version 3.1.0
- SNMP/OPC server as of version 6.2.1

- This manual is valid for the following products lines:
- SCALANCE X-300
- SCALANCE X-400

Within the SCALANCE X-300 product line, there are product groups (see also the product overview in the "Operating Instructions Industrial Ethernet Switches SCALANCE X-300").

Names of the devices in this configuration manual

The descriptions in this configuration manual always apply to the devices of the SCALANCE X-300 and SCALANCE X-400 product lines listed under "Validity of the manual" in this configuration manual unless the description relates to a specific device of the product line. In the remainder of the description, the devices are called "IE switches".

IT security

NOTICE
For its automation and drives product portfolio, Siemens provides IT security mechanisms to support secure operation of the plant/machine. For the secure operation of a plant/machine, it is also necessary to integrate the automation components in a full IT security concept for the entire plant/machine. You will find information about this on the Internet at the following address: (http://www.siemens.com/industrialsecurity)

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 DVD

  The DVD ships with most SIMATIC NET products.
- On the Internet under the following entry ID:

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

Table of contents

1 Introduction

1.1 Technical documentation for SCALANCE X-300/X-400

Content of the Configuration Manual

This manual describes the configuration of IE switches.

You will need to configure IE switches if you want to use functions such as SNMP, Rapid Spanning Tree, VLAN, routing (SCALANCE X414-3E) or E-mail. The manual also covers the question of firmware updates and the C-PLUG.

Before configuration, the device must be installed and connected up. You will find a description of the necessary steps for this in the Operating Instructions.

The following table shows you which information you will find in which chapter.

Topic	Chapter
You would like an overview of the documentation of an IE switch.	Chapter 1
You would like to know which functions and configuration options are available with an IE switch.	Chapter 2
You would like to know how an IP address is structured and which options you have for assigning an IP address to an IE switch.	Chapter 3
You would like to configure an IE switch and require information on the relevant CLI commands or want to know which pages of Web Based Management you need to edit.	Chapter 4
You want to know how to manage an IE switch with SNMP.	Chapter 5
You want to know how you can use the options of PROFINET IO for a connected IE switch.	Chapter 6
You would like to know about the options available with the configuration plug C-PLUG.	Chapter 7
You want to update the firmware.	Chapter 8

Content of the Operating Instructions

The "Operating Instructions Industrial Ethernet Switches SCALANCE X-400" and the "Operating Instructions Industrial Ethernet Switches SCALANCE X-300" contain not only basic information on the topic of switches but also product descriptions of IE switches, media modules and extender modules. The instructions also describe commissioning of IE switches (installation, wiring, using modules etc.).

Overview of the technical documentation of the IE Switches X-300 and X-400

The technical documentation of the X-300 product line is divided into hardware and software and can be found in the following documents:

- PH - Configuration Manual (PDF)

  The software is described in the configuration manual (PH) for both product lines X-300 and X-400.
- BAK - Compact operating instructions on paper

  The hardware of each product group is described in the Compact operating instructions (BAK).
- BA - Operating Instructions (PDF)

  The hardware for all product groups and general information can be found in the Operating Instructions (BA).

Contents	Product group	Type of document	Document identification number
Software description	All devices of the X-300 and X-400 product lines	PH X-300/X-400	C79000-G89000-C187
Hardware description	All devices of the X-300 product line	BA X-300	A5E01113043
	X-300	BAK X-300	A5E00982643A
	X-300M	BAK X-300M	A5E02630801A
	XR-300M	BAK XR-300M	A5E02661171A
	X-300 EEC	BAK X-300 EEC	A5E02630809
	XR-300M EEC	BAK XR-300M EEC	A5E02661176A
	MM900 (media modules)	BAK MM900	A5E02630805A
	SFP (transceivers)	BAK SFP Notices leaflet	A5E02630804A A5E02648904A
	All devices of the X-400 product line	BA X-400	C79000-G8900-C186-07
	X-400	BAK X-400	C79000-G8900-C186-07
	X-400EM (extender module)	BAK X-400EM	A5E00367421
	X-400 media modules	BAK X-400 media modules	A5E00367420

2 Network management for industrial networks

2.1 Configuration options with a SCALANCE X-300/X-400

Ethernet port

The IE switches can be configured over the switch ports (in-band ports) if an IP address has already been assigned (see section "Assignment of an IP address").

Over the Ethernet interface, you can use the following protocols or services:

- Web Based Management (HTTP- and HTTPS-based)
- TELNET
- SSH
- SNMP
- Traps
- FTP
- TFTP
- E-mail
- Syslog

Note

With the SCALANCE X414-3E, there is also a Fast Ethernet interface available (out-band port) on the CPU module.

RS-232 interface

The IE switches X-400/XR-300 have an RS-232 interface. You can connect a PC or PG to this port with a null modem cable and a terminal program (for example HyperTerminal in Windows, See also Appendix A). You use this port for the manual assignment of an IP address for the out-band port (SCALANCE X414-3E only) or the in-band port (refer to the Section "Assignment of an IP address over the serial port"). The entire set of CLI commands is also available.

Note

Access to the IE switch management over the serial port or the Ethernet port of the CPU module is also possible when the network is disrupted (out-of-band management).

2.2 Functionality and properties of a SCALANCE X-300/X-400

Integration of existing subnets with 10 Mbps and 100 Mbps

An IE switch automatically detects the following at its twisted pair ports:

- Send and receive wire pairs (autocrossover)
- Data rate (10 Mbps or 100 Mbps)
- Mode (full or half duplex)

This allows you to integrate subnets easily with IE switches over twisted pair.

NOTICE
Even when using straight cables, an illegal loop can occur in the Ethernet network, for example by connecting two ports to an IE switch. Such a loop can lead to network overload and network failures.

Note

If an IE switch port operating in autonegotiation mode is connected to a partner device that is not operating in autonegotiation mode, the partner device must be set permanently to half duplex mode.

Gigabit Ethernet ports

These ports are particularly suitable for a high-performance connection between switches and have the following properties:

- Automatic detection of the send and receive cable pairs (autocrossover)
- Data rates 10 Mbps, 100 Mbps, or 1000 Mbps
- Full duplex

Note

For data transmission at 1 Gbps, at least a Cat 5e twisted-pair cable with 4 x 2 wires is necessary. With a four-wire cable (2 x 2 wires), a maximum data transmission rate of 100 Mbps is possible.

Fast redundancy in the ring

As of firmware version V3.0.0, the IE switches can handle the following redundancy procedures:

- MRP in the ring with a maximum reconfiguration time of 200 ms
- HSR with a maximum reconfiguration time of 300 ms

An IE switch can adopt the function of a redundancy manager when it is part of a ring topology. If the transmission links are intact, an IE switch behaves as though it was the start or end point of a linear topology and prevents circulating frames. If an IE switch acting as redundancy manager detects the failure of a link in the ring, it closes the connection between its ring ports in a maximum of 200 ms. This restores a connection between all components of the ring.

Rings made up of IE switch devices can be operated at 1000 Mbps. In rings with SCALANCE X-200 or OSMs/ESMs, it is possible to integrate IE switches as redundancy manager or as simple nodes in the ring at 100 Mbps.

Redundant coupling of network segments

Rings or linear bus structures made up of IE switches (SCALANCE X-200 or X-300/X-400 or OSM/ESM) can be linked redundantly with suitable cabling and appropriate configuration. (See also section "X-400 Standby Mask menu item".)
The maximum failover time is 300 ms.

For more detailed information on redundant coupling of network segments and media redundancy in ring topologies, refer to the operating instructions "Industrial Ethernet Switches SCALANCE X-400" or "Industrial Ethernet Switches SCALANCE X-300".

Store and Forward

An IE switch calculates the CRC sum of incoming data packets and only forwards data with a valid checksum (store and forward). Bad packets are not forwarded by the switch. Store and forward also allows operation in a network on different links with different transmission rates.

Support of virtual networks (VLAN port-based)

There is no physical difference between a virtual network (VLAN) and a normal LAN. The particular feature of a VLAN is that devices can be assigned to a device group during configuration. Several of these device groups use a network infrastructure that exists only once physically. Several "virtual networks" result on the one physical network. Data exchange and even the transmission of broadcasts takes place only within a VLAN.

The assignment to VLANs is achieved by expanding the frames. Four bytes of additional information are inserted after the destination and source address. For more detailed information on frame tagging, refer to Appendix C.

To be able to integrate end devices and subnets that do not support VLAN in virtual networks, switches can also handle the addition and removal of the VLAN additional information. IE switches support assignment based on the port over which the devices are connected (port-based VLAN).

- X-400
  Up to 62 port-based VLANs and the two predefined VLANs can be configured. VLANs are defined in the IEEE 802.1Q standard.
- X-300
  Up to 253 port-based VLANs and the two predefined VLANs can be configured. VLANs are defined in the IEEE 802.1Q standard.

Rapid Spanning Tree

Using the rapid spanning tree algorithm, networks with several paths between two stations can be operated. Rapid spanning tree (RSTP) prevents loops being formed in the network by allowing only one path and deactivating the other (redundant) ports for data traffic.
IE switches support both rapid spanning tree and spanning tree.

Spanning tree is defined in the IEEE 802.1D-1998 standard and rapid spanning tree in the IEEE 802.1D-2004 standard.

C-PLUG

The C-PLUG is an exchangeable storage medium on which all configuration information of an IE switch is stored. When you replace an IE switch, you simply need to insert the C-PLUG of the previous device in the new device. The new IE switch then starts up with the configuration of the previous device.

Address table

The address table of an IE switch contains information about the port or ports to which a received frame should be forwarded. This table can contain both static entries (inserted by the user) as well as dynamic entries (learned based on the frames received by the IE switch).

Access Control

Note

In the firmware versions prior to 2.2.0, this property is called "Locked Ports".

If this function is activated for a port, an IE switch only forwards frames received at this port if their source address exists in the address table.

It is possible to have all connected nodes entered in the access control list automatically.

Note

The ring ports cannot be configured with access control *enabled*.

Network access protection complying with the standard IEEE 802.1x

Ports can be configured for end devices that support authentication according to IEEE 802.1x. The authentication is made via a RADIUS server that must be reachable over the network.

Mirroring

Mirroring allows the data traffic of a port to be mirrored at another port. The data traffic can then be analyzed at this monitor port without any effects on operation.

E-Mail function

An IE switch can be configured so that it sends an E-mail when certain events occur.

Event log table

The event log table logs events that occur during operation with an IE switch. The user can specify which events cause an entry in the table.

Time-of-day synchronization

IE switches allow the system time to be synchronized with external time transmitters. To use this functionality, there must be a SICLOCK time transmitter, for example, or an SNTP server whose frames the IE switch can evaluate. Entries in the event log table then have a time stamp that is uniform throughout the system. This allows events to be sorted according to the time of their occurrence throughout the system speeding up the identification of the causes of problems.

Flow control

IE switches support flow control in half and full duplex mode.

BOOTP/DHCP

IE switches can obtain their IP addresses dynamically from a BOOTP or DHCP server.

As of firmware version 2.0, the DHCP mode can be selected if DHCP is enabled. In the previous firmware versions, DHCP is operated over the MAC address.

Note

If routing functions (SCALANCE X414-3E only) are enabled, DHCP and BOOTP are not in effect.

Note

DHCP and BOOTP only influence the in-band agent IP configuration; the out-band agent IP configuration of the SCALANCE X414-3E can only be set manually.

PROFINET IO

As of firmware version 2.0, operation of the switch as a PROFINET IO device is supported.

TELNET

The command line interface of an IE switch can be controlled with TELNET over a LAN or the Internet.

Note

A maximum of three simultaneous CLI connections (serial (only with an IE Switch X-400) and LAN) are possible.

SSH

The command line interface of an IE switch can be controlled with SSH over a LAN or the Internet.

Note

A maximum of three simultaneous CLI connections (serial (only with an IE Switch X-400) and LAN) are possible.

SNMPv3

IE switches support SNMPv1, SNMPv2c, and SNMPv3. Among other things, SNMPv3 provides user management at protocol level as well as security functions (for example authentication). The configuration of users and groups for SNMPv3 is possible using Web Based Management, the Command Line Interface or by direct access to the MIB objects (only recommended for experts).

Syslog

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

DHCP Option 82

The DHCP relay function allows the IP address initialization of an end device depending on the connected switch port. DHCP Option 82 is supported with this function.

IGMP Snooping and IGMP Querier

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.

Only for SCALANCE X414-3E: Layer 3 functionality (routing)

You can also configure the SCALANCE X414-3E as a router. This allows various IP subnets to be interconnected. You can enter static routes and/or enable RIP/OSPF and VRRP router protocols. Using these standardized protocols, SCALANCE X414-3E can synchronize the configuration with other routers in the network.

3 Assignment of an IP address

Introduction

An IE switch provides a wide range of functions for settings and diagnostics. To access these functions over the network, the Internet protocol is used.

The Internet protocol has its own address mechanism using IP addresses. As the protocol of layer 3 of the ISO/OSI reference model, the IP protocol is independent of hardware allowing flexible address assignment. In contrast to layer 2 communication (where the MAC address is permanently assigned to a device), this makes it necessary to assign an address to a device explicitly.

This section describes the structure of an IP address and the various options for assigning the address with an IE switch.

IP address types of IE switches

IE switches can have several IP addresses:

- The out-band IP address (SCALANCE X414-3E only) is used for administration.
- The in-band agent IP address is used for administration.
- Further IP addresses
  These IP addresses can only be set for routing purposes (SCALANCE X414-3E only). They cannot be configured over DHCP but must be assigned using WBM, CLI or SNMP.

3.1 Structure of an IP address

Address classes to RFC 1518 and RFC 1519

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
Multicast groups			D	
Reserved for experiments			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 3rd byte of the subnet address must be set to 11110000 (binary notation). In this case, this results in the subnet mask 255.255.240.0.

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

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

Note

In the bit representation of the subnet mask, the "ones" must be set left-justified (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 or the Command Line Interface over Telnet or SSH because these configuration tools require that an IP address already exists.

The following options are available to assign an IP address to an unconfigured device currently without an IP address:

- CLI over the serial port (IE Switch X-400 only)
- DHCP
- BOOTP
- STEP 7
- NCM PC
- the Primary Setup Tool (only over in-band port)

Note

DHCP is set as default when the module ships or following *Reset to Factory Defaults*. If a DHCP server is available in the local area network, and this responds to the DHCP request of the IE switch, the IP address, subnet mask and gateway are assigned automatically when the module first starts up. DHCP and BOOTP, just like permanently set IP addresses are not deleted by a *Reset to Memory Defaults*.

NOTICE
With the SCALANCE X414-3E, the IP addresses of the out-band port and the in-band port must belong to different subnets. Example: IP address (out-band port): 140.90.45.66 IP address (in-band port): 140.91.23.66 Subnet mask (out-band port/in band port): 255.255.0.0

With the routing function, the SCALANCE X414-3E can have more than one in-band address. When using the Primary Setup Tool (PST), only one in-band address (the agent IP address) can be assigned. The other addresses must be assigned with WBM, CLI, or SNMP.

Note

The routing function is available only with the SCALANCE X414-3E.

Note

If routing functionality is enabled, no address can be set with DHCP/BOOTP.

3.3 Assigning an IP address over the serial interface of the SCALANCE X-400

Connection over null modem cable and login

Follow the steps outlined below to specify the IP address of an IE Switch X-400 over the serial interface:

1. Connect the serial port of the IE Switch X-400 to a PC over a null modem cable.
2. Start a program for terminal emulation, for example the HyperTerminal program available in Windows (settings see Appendix A).
3. Once the connection is established, the message "Login": appears. Enter "admin" (for administrator) assuming you have this access permission and press Return.
4. When prompted for the "Password:" enter your password. Make sure you read the notes below.
5. Enter "AGENT" when the message CLI> appears; you then change to the required submenu. Following this, you can enter the commands for configuring the IP address. You will find a description of these commands in the next section.

Note

If no new passwords have been assigned (default factory setting), the valid password is "admin" for the administrator login and "user" for the user login with restricted permissions.

After a successful login over the serial interface, you can enter commands until you log off with the "exit" command. The session is closed automatically if there is no further activity for 5 minutes.

Note

If you lose the password, you can reset an IE Switch X-300/X-400 to the factory settings with the SET/SEL button on the CPU module. To do this, press the SET/SEL button in the basic status display mode A (the LEDs D1 and D2 are off) for 12 seconds. You can cancel the reset procedure by releasing the button before the 12 seconds have elapsed. All settings you made previously are overwritten by the factory defaults. The passwords "admin" and "user" are then valid again.

Commands for the Command Line Interface

The commands provided for the configuration of the IP address by the CLI in the submenu AGENT are described in the section "Agent Configuration menu item".

For general information on the Command Line Interface, refer to the section "Command Line Interface (CLI)".

3.4 Assigning addresses with the BOOTP client

How address assignment works

BOOTP (Bootstrap Protocol) is a protocol for the automatic assignment of IP addresses. This type of address assignment is possible only when there is a BOOTP server in the network.

A node without an IP address (BOOTP client) sends its MAC address with a BOOTP query to all devices (MAC broadcast address FF-FF-FF-FF-FF-FF) on the network. The reply from the server is also sent as a broadcast and contains not only the IP address but also the MAC address of the client. A client that receives such a reply can recognize whether or not the IP address is intended for it based on the MAC address.

BOOTP is based on the UDP protocol and uses UDP port 67 for the BOOTP server and port 68 for the client.

BOOTP with an IE switch

When shipped, DCP (and therefore access over the Primary Setup Tool or NCM) and DHCP are enabled; BOOTP is disabled.

3.5 Assigning addresses with the DHCP client

Properties of DHCP

DHCP (Dynamic Host Configuration Protocol) is an expansion of BOOTP; however, there are several important differences compared with BOOTP:

- The use of DHCP is not restricted to the boot phase; DHCP can also be used during normal operation.
- The assigned IP address remains valid only for a particular 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, however possible, to configure the DHCP server so that it assigns a fixed address.

Note

As soon as the IP address has been assigned once by a PROFINET IO controller, DHCP automatically deactivates itself and must be reactivated if required.

Note

DHCP uses a mechanism with which the IP address is assigned for only a short time (lease time). If the IE switch does not reach the DHCP server for a new request on expiry of the lease time, the assigned IP address, the subnet mask and the gateway are changed to static entries.

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 either

- change the IP address of the IE switch 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.

3.6 Address assignment with the Primary Setup Tool

Introduction

The PST (Primary Setup Tool) is capable of assigning such an address to unconfigured devices without an IP address.

Prerequisite

This is only possible when the devices can be reached over 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

Configuration using Web Based Management and Command Line Interface 4

Introduction

To make the best possible use of the technical possibilities of the IE switches, you can adapt the configuration of the device to the concrete situation in which it is used. There are two ways of configuring an IE switch:

- With the Command Line Interface, you can reach the IE switches over Telnet (assuming there is an Ethernet connection) or over the serial interface (IE Switch X-400 only).
- Web Based Management accesses the configuration of an IE switch using a Web browser. An Ethernet connection to the IE switch is necessary.

NOTICE
Depending on the selected configuration method, the following mechanisms are integrated to prevent unauthorized access to an IE switch: • CLI over the serial interface (IE Switch X-400 only), TELNET or SSH • Web Based Management There is an automatic logout after 5 minutes (CLI) or 15 minutes (WBM) or depending on the time configured in the Agent Timeout Configuration menu. A manual logout is also possible with the appropriate button in the user interface. Exiting the browser does does not close the session. If the browser is started again within the timeout, the session continues to be used.

Note

All the configuration changes are adopted in the flash memory after approximately 1 minute or after a warm restart. You should therefore run the "Restart" command in the command line interface or in Web Based Management before turning off the device. You can then be certain that all the configuration changes have been saved.

Note

To use SNMP Management, RMON, and traps, you require a network management station. This does not ship with IE switches.

4.1 General information on Web Based Management and Command Line Interface

4.1.1 Introduction

Note

The screens described in this section apply to both the SCALANCE X-300 and the SCALANCE X-400. The screens shown here are based on those of the SCALANCE X-400. Deviations are possible depending on the configuration and device.

Principle of Web Based Management

IE switches have an integrated HTTP server for Web Based Management. If an IE switch is addressed using a Web browser, it returns HTML pages to the client computer depending on the user input.

The user enters the configuration data in the HTML pages sent by the IE switch. The IE switch evaluates this information and generates reply pages dynamically. The great advantage of this method is that apart from a Web browser, no special software is required on the client.

Requirements for Web Based Management

- An IE switch must have an IP address before you can use Web Based Management.
- To use Web Based Management, there must be an Ethernet connection between the IE switch and the client computer.
- Use of a Microsoft Internet Explorer, version 5.5 or higher is recommended.
- All the pages of Web Based Management require JavaScript. You should therefore make sure that Java Script is enabled in your browser settings.

Note

The 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 *Temporary Internet Files* with the Settings button.

Below the text *Check for newer versions of stored pages*, the *Automatically* check box must be selected.

- Web Based Management is HTTP- or HTTPS-based, so you must also enable access to port 80 or 443 if you have a firewall installed.

Starting Web Based Management and logging on

Note

For security reasons, make sure that you change the original factory-set passwords:

- User name "admin" = password "admin"
- User name "user" = password "user".

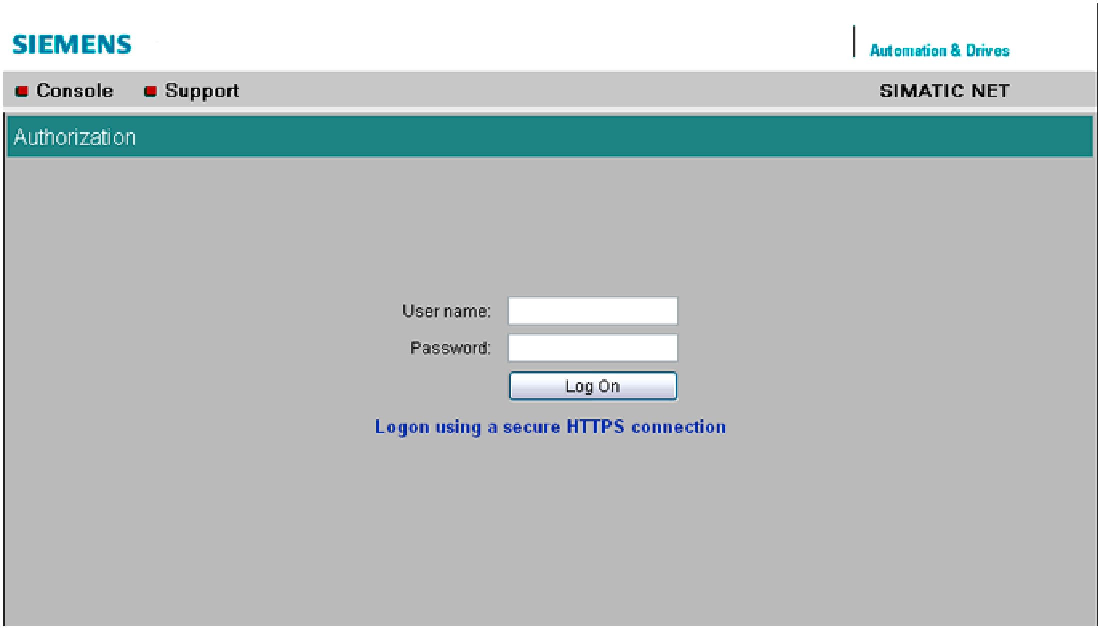


Figure 4-1 Logon dialog

1. Enter the IP address or the URL of the IE switch in the address box of the Web browser. If there is a problem-free connection to the IE switch, the logon dialog of Web Based Management appears as shown above.
2. Enter a user name in the "User name" input box. The following entries are possible:
   - admin: With this user name, you have read and write access.
   - user: With this user name, you only have read access.
   - The user name stored on a RADIUS server: See sections System Passwords & Login Mode (Page 47) and 802.1x RADIUS Configuration (Page 137).
3. Enter your password.
4. Click the "Log On" button to start the logon.

4.1.2 The LED simulation of Web Based Management (WBM)

Display of the operating state

Each component of an IE switch has one or more LEDs that provide information on the operating state of the device. Depending on its location, direct access to the IE switch may not always be possible. Web Based Management therefore displays simulated LEDs.

The upper quarter of the screen displays a schematic representation of the IE Switch X-300 or the IE Switch X-400 with the existing modules and corresponding LEDs. The traffic display is not represented realistically (the LEDs do not flash). The meaning of the LED displays is described in the operating instructions "Industrial Ethernet Switches SCALANCE X-300" or operating instructions "Industrial Ethernet Switches SCALANCE X-400".

If you click on the labels above the symbolically displayed modules, you can change the display mode (LEDs DM or D1/D2) of the display in the simulation just as with the button on the device.

Note

The media module extender of the SCALANCE X414-3E is displayed in the simulation only if it has at least one module inserted.

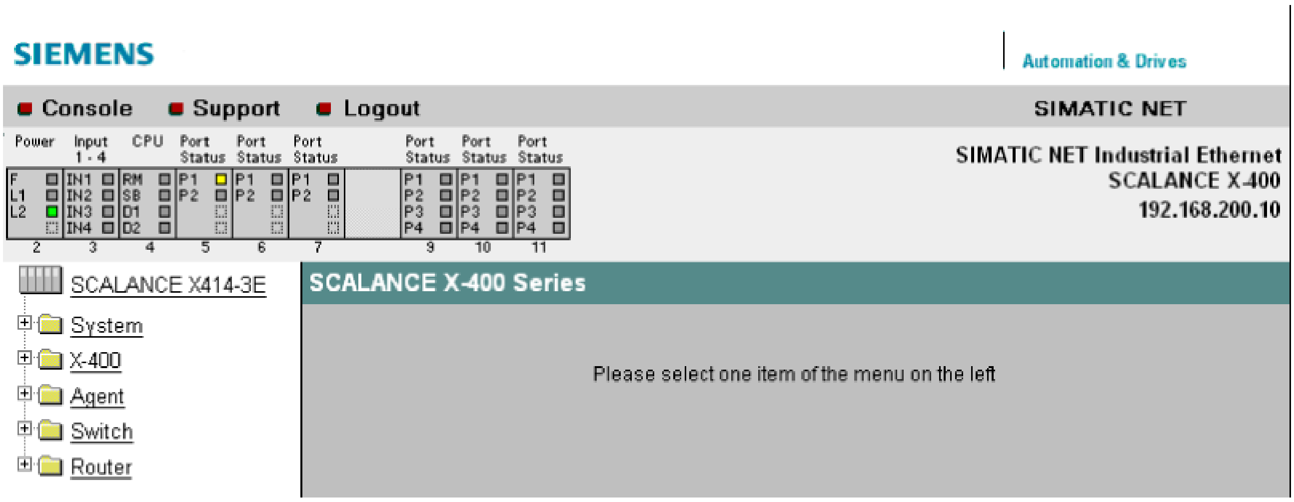


Figure 4-2 SCALANCE X414-3E LED simulation

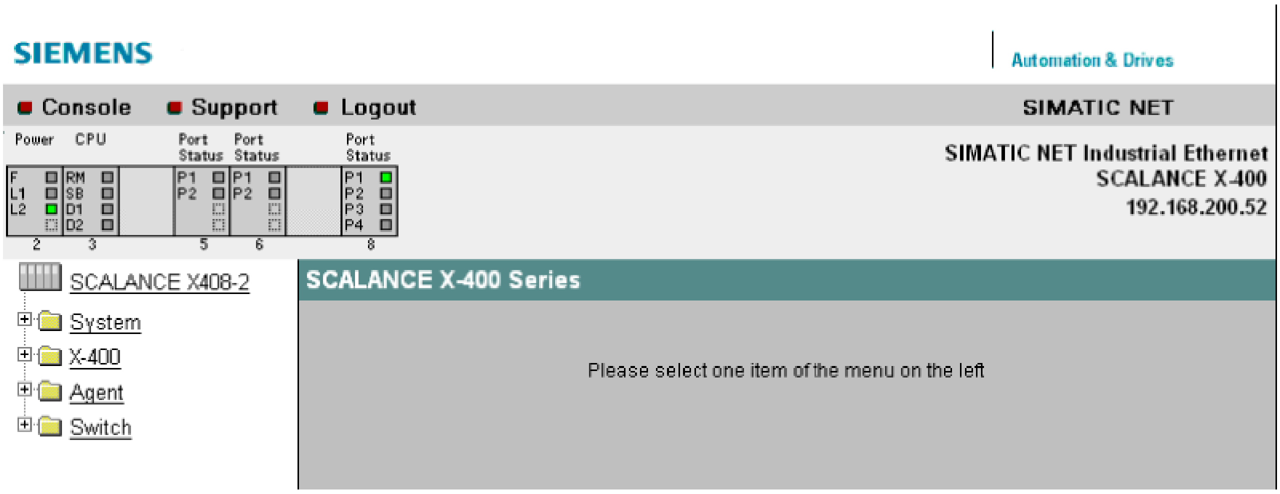


Figure 4-3 SCALANCE X408-2 LED simulation

Figure 4-4 SCALANCE X308-2 LED simulation

4.1.3 Working with Web Based Management

Navigation bar

The upper menu bar of WBM contains the following links:

- Console
  This link opens a console window in which you can enter CLI commands. You are then connected to the switch over a TELNET connection.
- Support
  When you click this link, you open a SIEMENS AG support page. SIEMENS Support is, however, only accessible when your PC has a connection to the Internet.
- Logout
  By clicking on this link, you log out from the device.

Updating the display with "Refresh"

Web Based Management pages have a "Refresh" button at the lower edge of the page. Click this button to request up-to-date information from the IE switch for the current page.

Storing entries with "Set Values"

Pages in which you can make configuration settings have a "Set Values" button at the lower edge. Click this button to save the configuration data you have entered on the IE switch.

Note

Changing configuration data is possible only with the "Administrator" login.

4.1.4 Command Line Interface (CLI)

Starting the CLI in a Windows console

Follow the steps outlined below to start the Command Line Interface in a Windows console:

1. Open a Windows console and type in the command telnet followed by the IP address of the IE switch: *C:\>telnet <IP address>*
2. Enter your login and password.

Starting the CLI in Web Based Management

Click on the "Console" entry in the upper menu bar of Web Based Management. A Telnet connection opens automatically in which you can log on with your user name and password.

Shortcuts for commands

As an alternative, instead of entering full CLI commands, you can simply enter the first letter or the first few letters and then press the Tab key. The Command Line Interface then displays a command starting with the letter or letters you typed in. If the command displayed is not the command you require, press the Tab key again to display the next command.

Directory structure

Before you can enter a command in the Command Line Interface, you must first open the required menu or submenu. This section lists the commands of each menu in a separate table. The table lists only the commands themselves.

Addressing scheme for the ports of an IE Switch X-400

The following addressing scheme applies to the port labeling of an IE Switch X-400:

- The first number indicates the slot.
- The second number is separated by a period and specifies the port.

For example, the identifier 6.2 means the second port on the sixth slot.

Addressing scheme for the ports of an IE Switch X-300

The following addressing scheme applies to the port labeling of an IE Switch X-300:

- The number relates directly to the port.

The label 2 stands for the second port on the IE Switch X-300.

Symbols for representing CLI commands

CLI commands generally have one or more parameters that are represented in the syntax description as follows:

<table>
<tr><th colspan="2">CLI command syntax</th><th>Use of parameter</th><th>Description</th><th colspan="2">Example</th></tr>
<tr><td>< ></td><td>Angle brackets</td><td>necessary</td><td>Mandatory parameters are shown in angle brackets.
Note: If mandatory parameters are omitted, most commands output the current value.</td><td colspan="2"><ip address></td></tr>
<tr><td>[ ]</td><td>Square brackets</td><td>optional</td><td>Optional parameters are shown in square brackets.</td><td colspan="2">[D|A]</td></tr>
<tr><td>|</td><td>Pipe character</td><td>alternative</td><td>Alternative parameters are shown by the pipe character.
Enter either a or b
or value range 1 or value range 2</td><td><a | b>
<... | ....></td><td>[a | b]
[.... | ...]</td></tr>
<tr><td>...</td><td>Periods</td><td>Value range</td><td>Value ranges of parameters are indicated by three periods.</td><td><0...255></td><td>[0...255]</td></tr>
<tr><td colspan="2">string</td><td>text</td><td>Text is identified as string. (see example)</td><td colspan="2">• File name
• Geographic coordinates
• Names and designations
• Passwords</td></tr>
<tr><td colspan="2">Port</td><td>Port name</td><td>Port name</td><td colspan="2">5.1 for X-400
or 7 for X-300</td></tr>
<tr><td colspan="2">Number</td><td>Numeric value</td><td>Numeric value</td><td colspan="2">1</td></tr>
<tr><td colspan="2">MAC</td><td>MAC address</td><td>MAC address</td><td colspan="2">80:fe:11:f3:4d:d6</td></tr>
<tr><td colspan="2">IP</td><td>IP address</td><td>IP address</td><td colspan="2">192.168.1.1</td></tr>
<tr><td colspan="2">mode</td><td>Modes of a function</td><td>If there is more than one operating mode for a function, this is indicated by the mode parameter.
All available modes can be displayed using the "?" parameter</td><td colspan="2">• D
disables the function</td></tr>
</table>

Cross-menu commands

You can use the commands in the following table in any menu or submenu.

Table 4- 1 Command Line Interface - CLI\ … >

Command	Description	Comment
/	Changes to the highest menu level.	Administrator and User
..	Moves you one menu level higher.	Administrator and User
?	Displays the commands available in the menu.	Administrator and User
exit	Closes the CLI session.	Administrator and User
restart	Restarts the IE switch	Administrator only
About	Displays information on the current menu item.	Administrator and User

Help on CLI commands

- You can call up further information with the "?" parameter (if this is necessary and available for a command).
- If no further information is available, the command syntax from the menu overview is displayed.

4.2 The System menu

4.2.1 System Configuration

General device information

This screen appears if you click the *System* folder icon:

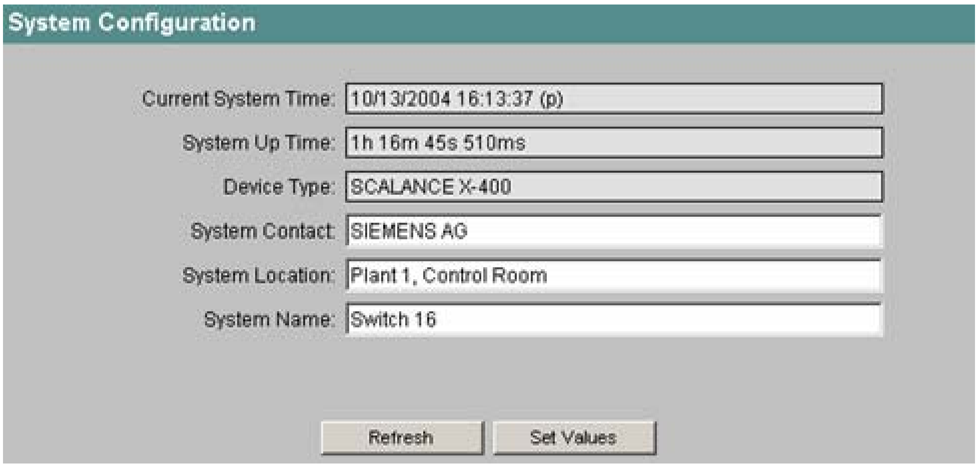


Figure 4-5 System Configuration

Current System Time(read-only)
The system time is set either by the user or is synchronized by a time-of-day frame (either SINEC H1 time frame or SNTP). You can also see when and how it was set:

- (m) The setting was made manually.
- (t) The setting was made by SIMATIC time-of-day frame, however, it is not synchronized with the time transmitter.
- (s) The setting was made by SIMATIC time-of-day frame and it is synchronized with the time transmitter.
- (p) The setting was made by the SNTP protocol.

System Up Time (read-only)
The time since the last reboot.

Device Type (read-only)
The type designation of the device.

System Contact
Enter the name of a contact person responsible for managing the device in this box.

System Location
In this box, you enter a location for the device, for example a room number.

System Name
Enter a description of the device in this box.

Syntax of the Command Line Interface

Table 4- 2 System Configuration - CLI\SYSTEM>

Command	Description	Comment
syscon [string]	Sets/displays the syscontact MIB variable.	Administrator only.
sysloc [string]	Sets/displays the syslocation MIB variable.	Administrator only.
sysname [string]	Sets/displays the sysname MIB variable.	Administrator only.

4.2.2 System Identification & Maintenance (I&M)

System Identification & Maintenance

The following screen contains information on device-specific vendor and maintenance data such as the order number, serial number, version numbers etc.

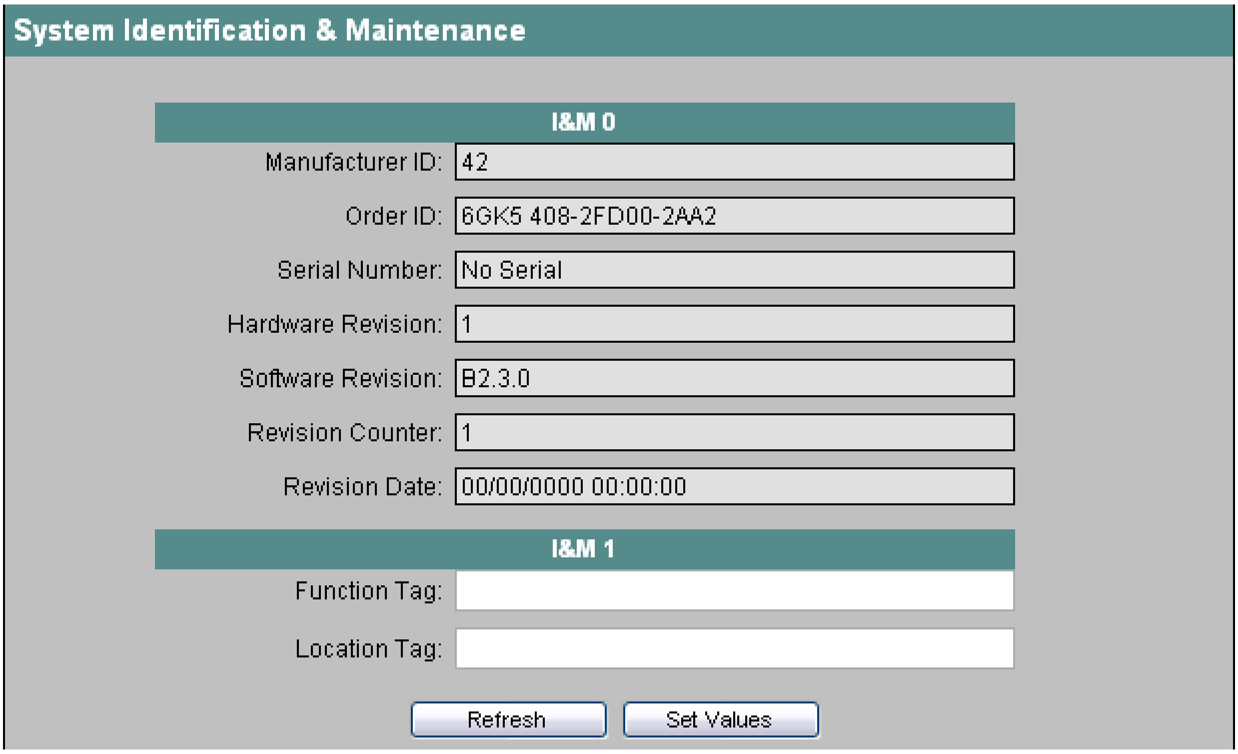


Figure 4-6 System Identification & Maintenance

I&M 0
Here, you can see the individual parameters for Identification & Maintenance.

I&M 1
Function Tag
Here, you can enter the function tag (plant designation).

Location Tag
Here, you can enter the location tag (location identifier).

Syntax of the Command Line Interface

Table 4- 3 System Identification & Maintenance - CLI\SYSTEM\IM>

Command	Description	Comment
info	Displays information on the "Identification & Maintenance" menu item.	-
function [string]	Specifies the plant designation (max. 32 characters).	Administrator only.
location [string]	Specifies the location identifier (max. 32 characters).	Administrator only.

4.2.3 System Restart & Defaults

Resetting to the defaults

In this screen, there is a button with which you can restart the IE switch and various options for resetting to the IE switch defaults.

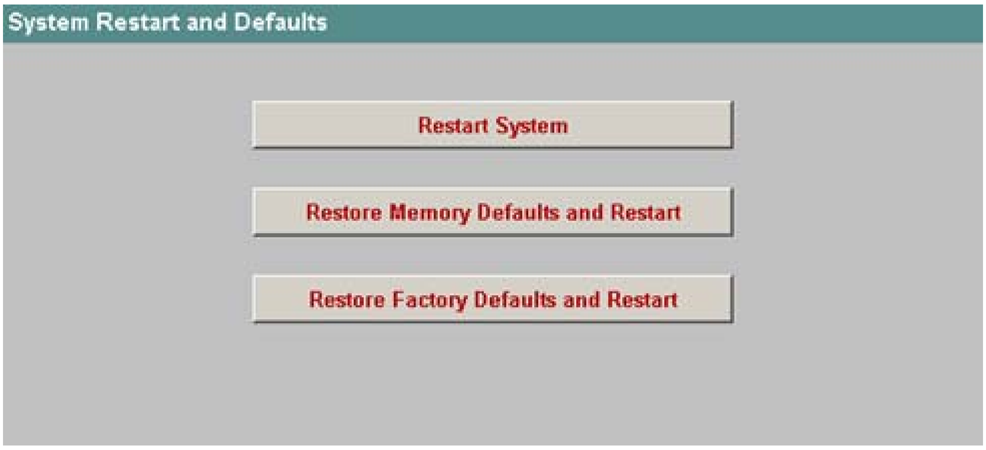


Figure 4-7 System Restart and Defaults

Note

Note the following points about restarting an IE switch:

- You can only restart the IE switch with administrator privileges.
- An IE switch 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 changes you make are only saved on the device after clicking the "Set Value" button on the relevant page of the WBM, saving the configuration data prior to a restart is neither necessary nor possible.
- The 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 *Temporary Internet Files* with the Settings button.
- Below the text *Checkfor newer versions of stored pages*, the *Automatically* check box must be selected.

Restart System

Click this button to restart the IE Switch. You must confirm the restart in a dialog box. During a restart, the IE switch 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 IE switch restarts.

Restore Memory Defaults and Restart

Click on this button to restore the factory configuration settings with the exception of the following parameters:

- IP addresses (in-band and out-band)
- Subnet masks (in-band and out-band)
- IP address of the default gateway
- DHCP/BOOTP flag
- System name
- System location
- System contact
- Ring redundancy
- Standby functionality
- (R)STP
- PNIO device name (name of station)

An automatic restart is triggered.

Restore Factory Defaults and Restart

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, the IP address is also lost. An IE switch is then only accessible using the Primary Setup Tool or the serial interface (IE Switch X-400 only).

Syntax of the Command Line Interface

Table 4- 4 System Restart & Defaults - CLI>

Command	Description	Comment
restart	Restarts the IE switch	Administrator only. This command can be executed from within all menus.

Table 4- 5 System Restart & Defaults - CLI\SYSTEM>

Command	Description	Comment
defaults	Restores the factory defaults. The protected settings are also reset. The device is restarted.	Administrator only. This command has the same effect as clicking the *Restore Factory Defaults and Restart* button in WBM.
memreset	Restores the factory defaults. The protected settings are retained. The device is automatically restarted.	Administrator only. This command has the same effect as clicking the *Restore Memory Defaults and Restart* button in WBM.

4.2.4 System Save & Load via HTTP

System Save & Load HTTP

The WBM allows you to store configuration information in an external file on your client PC or to load such data from an external file from the PC to IE switches. You can also load new firmware from a file located on your client PC.

Note

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

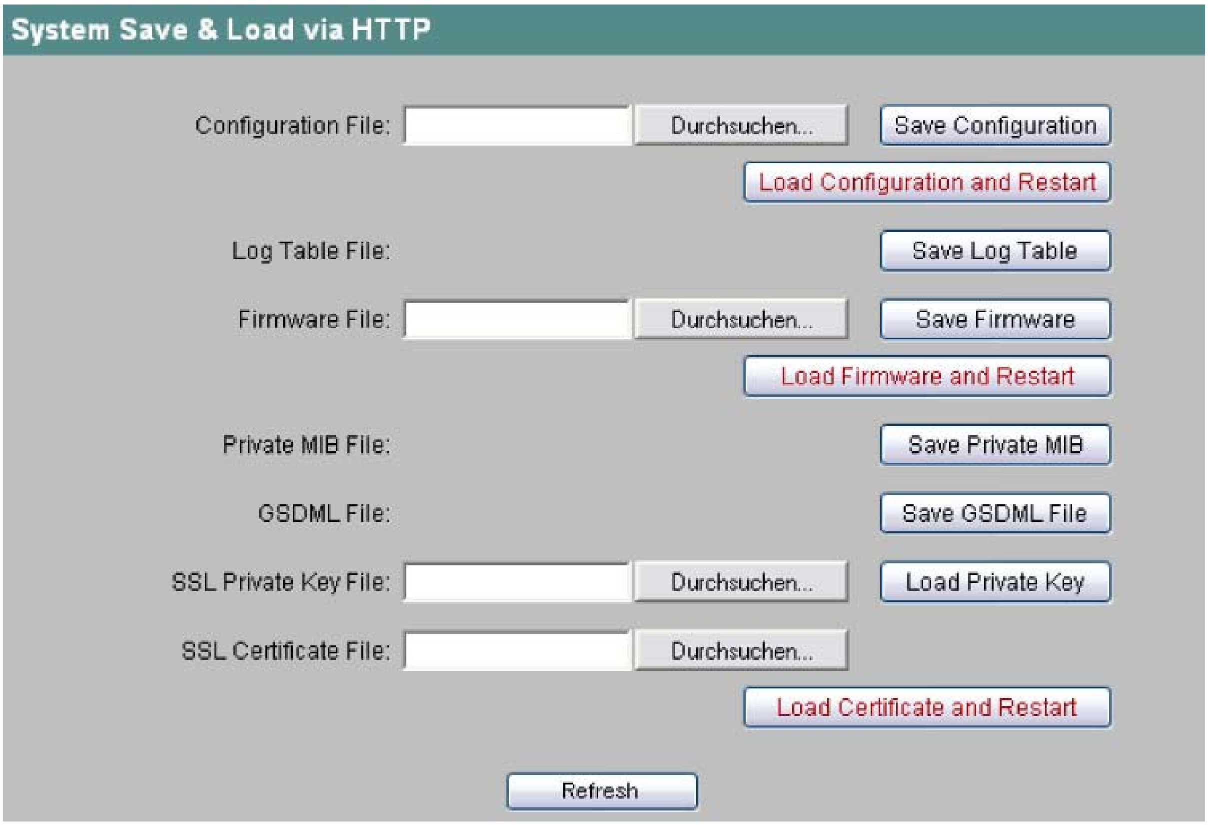


Figure 4-8 System Save & Load via HTTP

Configuration File
Name and directory path of the configuration file you want to load to the IE Switch.

Firmware File
Name and directory path of the file from which you want to load the new firmware.

SSL Private Key File
Name and directory path of the file from which you want to load the private SSL key to the device.

SSL Certificate File
Name and directory path of the file from which you want to load the SSL certificate to the device.

Note

Since the private key and certificate belong together, files are saved only after both the key and certificate have been downloaded. When you load the certificate, it is checked to make sure it matches the loaded key. A restart is required before the new SSL files are adopted.

Only private RSA keys with a maximum length of 128 bytes are accepted, private keys must not be password protected.

An SSL certificate must be PEM coded, its length must not exceed 256 bytes.

How to load data over HTTP / HTTPS

1. In the relevant text box, enter a name and directory path for the file from which you want to take the data.
2. Start loading the relevant file by clicking one of the buttons "Load Firmware and Restart", "Load Configuration and Restart", "Load Private Key" or "Load Certificate and Restart". There is an automatic restart after downloading except following "Load Private Key" and the device starts up again with the new data.

How to save data over HTTP / HTTPS

1. Start the save by clicking one of the buttons "Save Configuration", "Save Log Table", "Save Firmware", "Save Private MIB" or "Save GSDML File".
2. You will be prompted to select a storage location and a name for the file or to accept the proposed file name.

Reusing configuration data

Saving and reading in configuration data reduces the effort if several IE switches have the same configuration and when IP addresses are obtained over DHCP.

Save the configuration data on your computer after you have configured an IE switch. As an alternative, you can save the data on a TFTP server (Page 43).

Download this file to all other IE switches you want to configure.

If individual settings are necessary for specific devices, these must be made online.

The stored configuration data is coded and, as a result, these files cannot be edited with a text editor.

4.2.5 System Save & Load via TFTP

Data exchange with a TFTP server

WBM allows you to save configuration information in an external file and to load this information on the IE switch from an external file. You can also save the log information in a file or load new firmware from a file. You can make the entries required for this in the Save & Load menu.

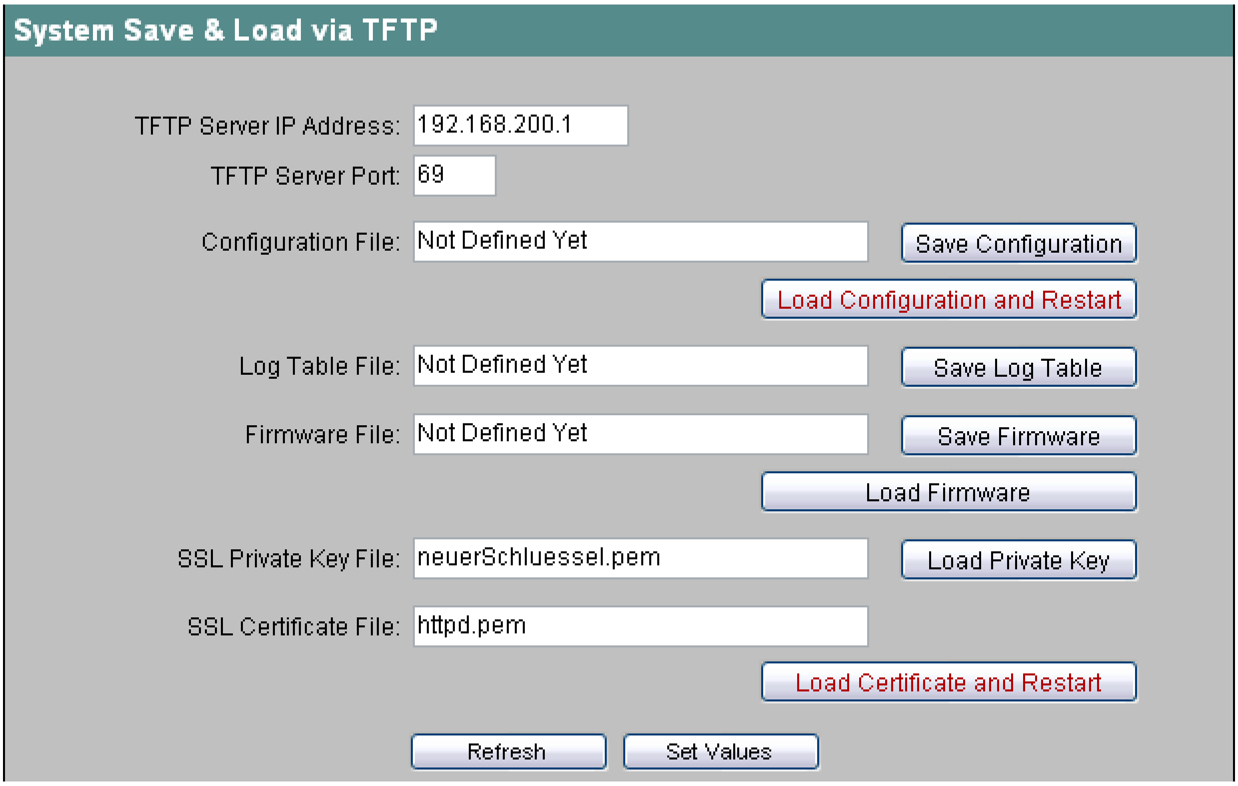


Figure 4-9 System Save & Load

TFTP Server IP Address
The IP address of the TFTP server with which you want to exchange data.

TFTP Server Port
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.

Configuration File
Name and, if necessary, folder path of the configuration file (maximum 32 characters) that you want to load on the IE switch or where you want to store the current configuration information.

Log Table File
Name and, if necessary, path of the file (maximum of 32 characters) in which you want to save the content of the log table.

Firmware File
Name and, if necessary, directory path of the file (maximum 32 characters) from which you want to load the new firmware or in which you want to save the current firmware.

SSL Private Key File
Name and directory path of the file from which you want to load the private SSL key to the device. The entry in this box is restricted to a maximum of 32 characters.

SSL Certificate File
Name and directory path of the file from which you want to load the SSL certificate to the device.
The entry in this box is restricted to a maximum of 32 characters.

Note

Since the private key and certificate belong together, files are saved only after both the key and certificate have been downloaded. When you load the certificate, it is checked to make sure it matches the loaded key. A restart is required before the new SSL files are adopted.

Only private RSA keys with a maximum length of 1280 bytes are accepted, private keys must not be password protected.

An SSL certificate must be PEM coded, its length must not exceed 2560 bytes.

How to load or save data over TFTP

1. Enter the IP address of the TFTP server in the "TFTP Server IP Address" text box.
2. Enter a name (maximum of 32 characters) for the file in which you want to save the data or take the data from in the text box.
3. Click on the "Set Values" button before you make any further entries for saving or loading the data.
4. Start the save / load function by clicking the relevant button "Save" or "Load".

After you load the configuration and the SSL certificate, the device restarts with the new data.

Reusing configuration data

Saving and reading in configuration data reduces the effort if several IE switches have the same configuration and when IP addresses are obtained over DHCP.

Save the configuration data on a TFTP server after you have configured an IE switch. As an alternative, you can save the data on your computer (Page 41).

Download this file to all other IE switches you want to configure.

If individual settings are necessary for specific devices, these must be made online.

The stored configuration data is coded and, as a result, these files cannot be edited with a text editor.

Syntax of the Command Line Interface

Table 4- 6 System Save & Load - CLI\SYSTEM\SAVELOAD>

Command	Description	Comment
server [<ip>[:port]]	Specifies the IP address and, as an option, the port of the TFTP server with which data will be exchanged.	Administrator only. Default value: 0.0.0.0
cfgname <string>	Specifies the name of a file (maximum 32 characters) from which the configuration data will be loaded or in which the configuration data will be saved.	Administrator only.
cfgsave	Saves the configuration data in a file on the TFTP server.	Administrator only.
cfgload	Loads the configuration data from a file on the TFTP server.	Administrator only.
logname <string>	Specifies the name of a file (maximum 32 characters) in which the log table is stored.	Administrator only.
logsave	Saves the log table in a file on the TFTP server.	Administrator only.
fwname <string>	Specifies the name of a file (maximum 32 characters) from which the firmware is loaded.	Administrator only. Default value: Not defined.
fwload	Loads the firmware from a file.	Administrator only.
fwsave	Saves the firmware in a file on the TFTP server.	Administrator only.
keyload	Loads the private SSL key from a file.	Administrator only.
certload	Loads an SSL certificate from a file.	Administrator only.

4.2.6 System Version Numbers

Versions of hardware and software

This page shows the versions of the hardware and software with which the IE switch is being operated:

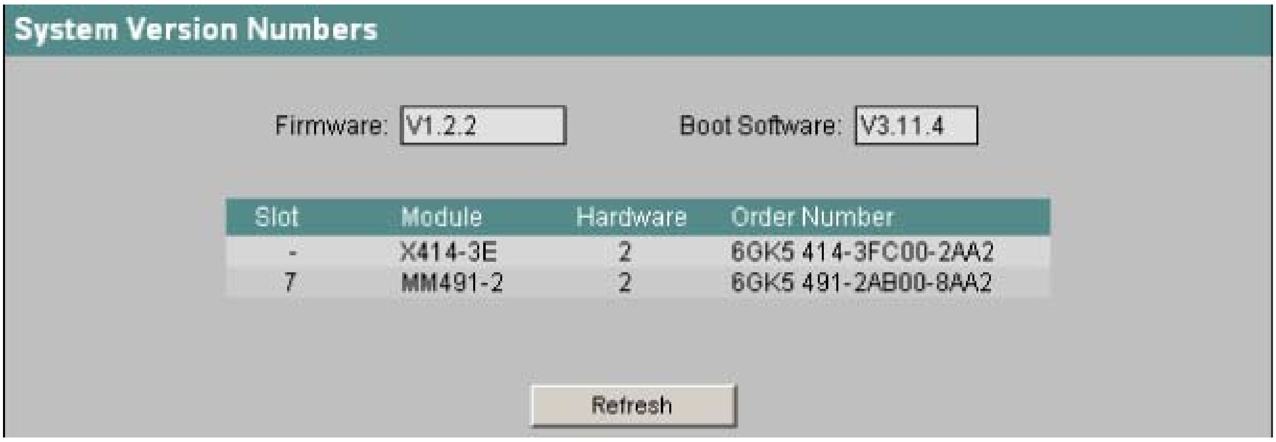


Figure 4-10 System Version Numbers

Boot Software
The version of the boot software is displayed here. The boot software is stored permanently on the IE switch.

Firmware
The version of the firmware running on the IE switch.

Table with entries for the basic device and the modules
The first row of the table indicates the version of the IE switch. The slot column shows the slot on the basic device. If the information relates to the basic device itself, "-" is entered in this column. The Hardware column displays the version and the Order Number column the order number of the IE switch or module.

Syntax of the Command Line Interface

Table 4- 7 System Version Numbers - CLI>

Command	Description	Comment
info	Along with other information, this command displays the versions of software with which the IE switch is operated.	-

Table 4- 8 System Version Numbers - CLI\SYSTEM>

Command	Description	Comment
version	Displays the firmware, hardware and boot software version of the IE Switch and provides more detailed information on the basic device and any modules.	-

4.2.7 System Passwords & Login Mode

Passwords and login mode

Note

Default for the passwords when supplied

Admin password: admin
User password: user

In this dialog, if you are the administrator, you can change the passwords for Admin and User. The password can be up to a maximum of 16 characters (7-bit ASCII) long.

By selecting a login mode, you also specify which user names can be used for the login.

Note

RADIUS

To be able to use the login mode "RADIUS" or "RADIUS and Local", a RADIUS server must be stored and configured for user authentication. You configure this information in the "Switch" menu on the "802.1x RADIUS Configuration" page.

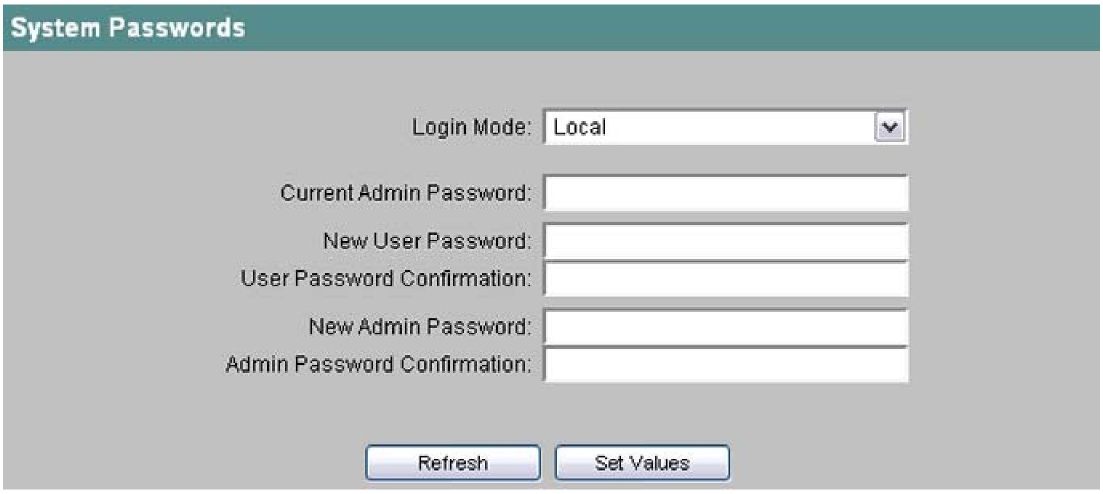


Figure 4-11 System passwords

"Login Mode" list box

The login mode provides the following options:

Local:	The login is only possible with the users that exist in the firmware (user and admin).
RADIUS and Local:	The login is possible both with the users that exist in the firmware (user and admin) and via a RADIUS server. The local user names have priority.
RADIUS:	The login is only possible using the login data stored on a RADIUS server. The local user names are disabled.

Save

Save your entries by clicking the "Set Values" button.

Note

RADIUS authentication fails

If the RADIUS server configured as the primary server fails, authentication will initially fail. The request is only sent to the backup server with the next login attempt.

Syntax of the Command Line Interface

Table 4- 9 System Passwords - CLI\SYSTEM>

Command	Description	Comment
passwd <admin|user>	Sets a new password for "admin" or "user".	Administrator only.
loginmod [L|B|R]	Specifies the login mode: • L Only user names that exist in the firmware. • B Both the user names in the firmware and those stored on a RADIUS server (local names have priority). • R Only user names that are stored on a RADIUS server.	Administrator only.

4.2.8 System Select/Set Button

Disabling the Select/Set button

On the IE Switch, the SELECT/SET button is used to

- Change the display mode
- Reset to the factory defaults
- Define the fault mask and the LED display
- Enable/disable the redundancy manager.

You will find a detailed description of the individual functions available with the buttons in the SCALANCE X-400 operating instructions.

On this page, the functionality of the Select/Set button can be restricted or fully disabled. This is possible for the following three functionalities:

- Restore Factory Defaults
- Enable/Disable Redundancy Manager
- Set Fault Mask

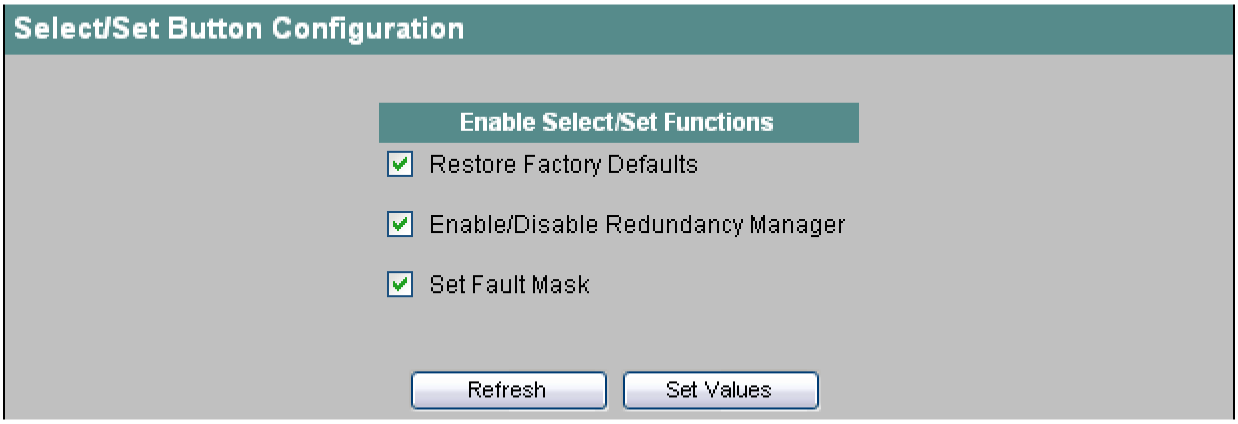


Figure 4-12 Select/Set Button Configuration

Enable Select/Set Functions

You can enable or disable the individual functions of the button by checking or unchecking the relevant box.

System Command Line Interface

Table 4- 10 System Configuration - CLI\SYSTEM\SELSET>

Command	Description	Comment
info	Displays the functionality of the button.	-
defaults	Enables/disables the "Restore Factory Defaults" function of the button.	Administrator only.
rm	Enables/disables the "Enable/Disable Redundancy Manager" function of the button.	Administrator only.
faultmsk	Enables/disables the "Set Fault Mask" function of the button.	Administrator only.

4.2.9 System Event Log Table

Logging events

An IE switch allows you to log events and to display them on the page of the "Log Table" menu. This, for example, allows you to record when an SNMP authentication attempt failed or when the connection status of a port has changed. You can specify which events are logged in the "Agent Event Configuration" menu item. The content of the log table is retained even when the IE switch is turned off.

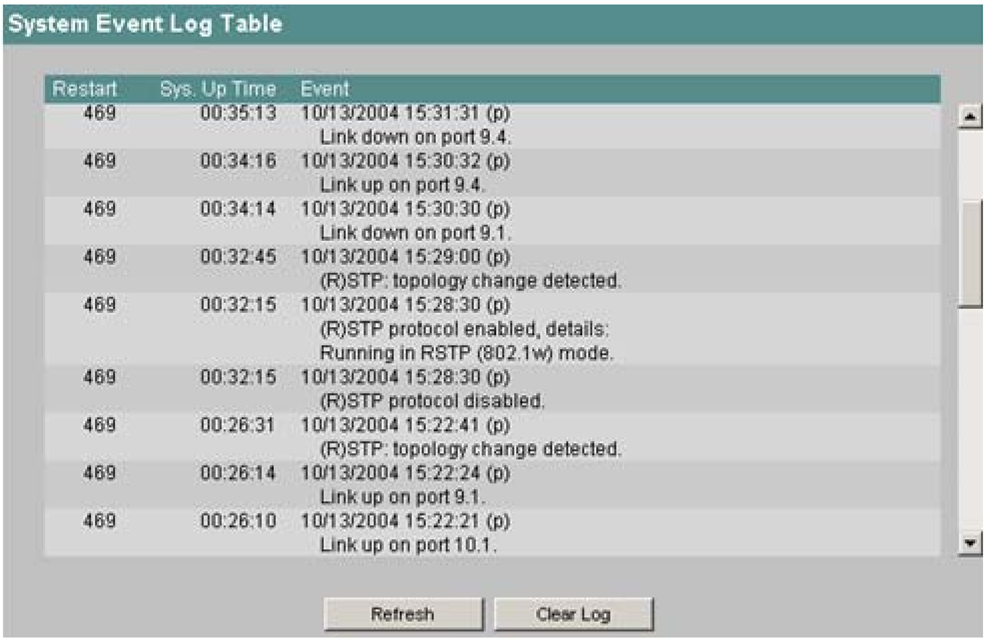


Figure 4-13 System Event Log Table

The "Restart" column indicates the device restart after which the corresponding event occurred.

The "Sys.Up Time" column shows the time since the IE switch was last restarted in the format HH:MM:SS.

Refresh
Click on this button to refresh the display.

Clear Log
With this button, you can delete the content of the log table.

Syntax of the Command Line Interface

Table 4- 11 System Event Log Table - CLI\SYSTEM>

Command	Description	Comment
events <clear>	Shows the content of the log table. The content of the log table can be deleted with the [clear] parameter.	Only the administrator can delete the log table. The content of the log table is retained even when the IE switch is turned off.
addlog <string>	Inserts a text in the log table. Blanks in the string are also included.	Administrator only.

4.2.10 C-PLUG Information

Information on the content of the C-PLUG

This menu provides you with detailed information on the C-PLUG. You can also format the C-PLUG or provide it with new content.

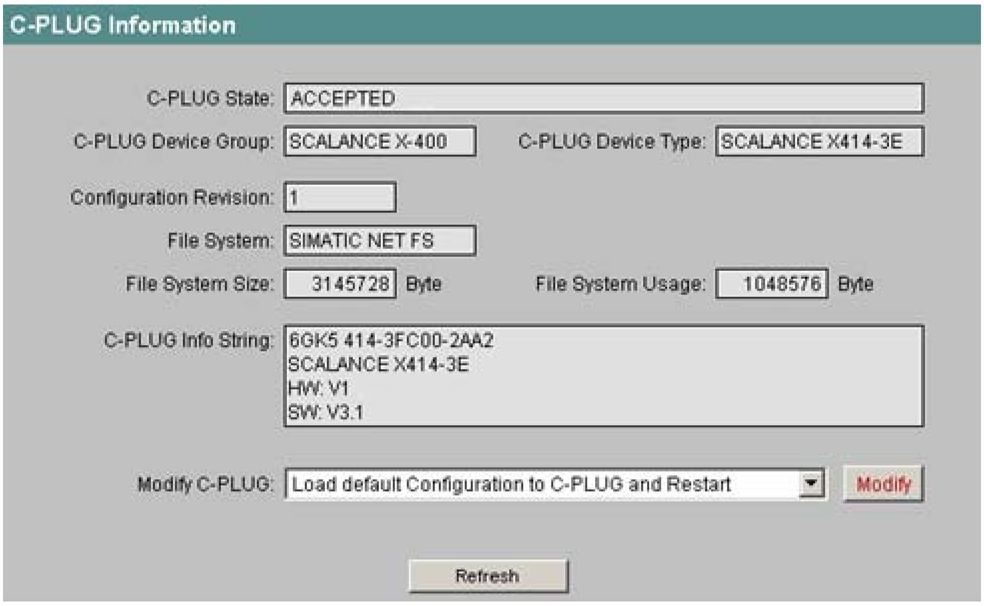


Figure 4-14 C-PLUG Information

The text boxes of this menu are all read-only.

C-PLUG State
The status of the C-PLUG is displayed here. The following are possible:

- ACCEPTED
  There is a C-PLUG with a valid and matching content inserted in the IE switch.
- NOT ACCEPTED
  Invalid or incompatible content of an inserted C-PLUG. This status is also displayed when the C-PLUG was formatted during operation.
- NOT ACCEPTED, HEADER CRC ERROR
  A C-PLUG with bad content is inserted.
- NOT PRESENT
  There is no C-PLUG inserted in the IE switch.

C-PLUG Device Group
Indicates the SIMATIC NET product line that previously operated with the C-PLUG.

C-PLUG Device Type
Indicates the device type within the product line that previously operated with the C-PLUG.

Configuration Revision
The version of the configuration structure. This information relates to the configuration options supported by the IE switch and has nothing to do with the concrete hardware configuration. This revision information does not therefore change if you add or remove modules or extenders, it can, however, change if you update the firmware.

File System
Displays the type of file system on the C-PLUG.

File System Size
Displays the maximum storage space of the file system on the C-PLUG.

File System Usage
Shows the storage space being utilized in the C-PLUG file system.

C-PLUG Info String
Here, you will see all the additional information about the device that used the C-PLUG during previous operation, for example, order number, type designation, and the versions of the hardware and software.

Modify C-PLUG, Modify
You can only make settings in this box if you are logged in as "Administrator". Here, you decide how you want to change the content of the C-PLUG. The following alternatives are possible:

- Copy internal Configuration to C-PLUG and Restart
  The configuration in the internal flash memory of the IE switch is copied to the C-PLUG; this is followed by a restart.
  This function is required in the following important use case: The IE switch has started up with a C-PLUG containing a bad configuration or a configuration different from the IE switch. If you have not yet made any configuration changes after starting up the device, you can use this function to overwrite the content of the C-PLUG with the original device configuration.
- Copy default Configuration to C-PLUG and Restart
  A configuration with all the factory default values is stored on the C-PLUG. This is followed by a restart in which the IE switch starts up with these default values.
- Clean C-PLUG (Low Level Format, Configuration lost)
  Deletes all data on the C-PLUG and starts a low-level formatting function. This is not followed by an automatic restart and the IE switch displays an error. You can clear this error status by restarting or removing the C-PLUG.

Select the necessary entry in the drop-down list and click "Modify, to change the C-PLUG as required.

Syntax of the Command Line Interface

Table 4- 12 C-PLUG Information - CLI\SYSTEM\C-PLUG>

Command	Description	Comment
info	Displays the current status of the C-PLUG.	The same information is displayed as on the "X-400 C-PLUG Information page" of the WBM.
copyint	Overwrites the C-PLUG with the content of main memory.	Administrator only. Same function as the "Copy internal Configuration to C-PLUG and Restart" command in WBM.
copydef	Initializes the C-PLUG with default parameters.	Administrator only. Same function as the "Copy default Configuration to C-PLUG and Restart" command in WBM.
clean	Deletes all the data from the C-PLUG and runs a low-level formatting function.	Administrator only. Same function as the "Clean C-PLUG" command in WBM.

4.2.11 Geographic coordinates

Information on geographic coordinates

In the "Geographic Coordinates" window, you can enter or read out information on the geographic coordinates. To be able to read out the geographic coordinates, the geographic location of the device must be entered correctly once in 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 "Geographic Coordinates" window.

The geographic coordinates can, for example, be calculated by a GPS receiver. Generally, the geographic coordinates are displayed by these devices directly. Following configuration, the SCALANCE device provides you with this geographic data for management purposes using SNMP private MIBs, Telnet or WEB.

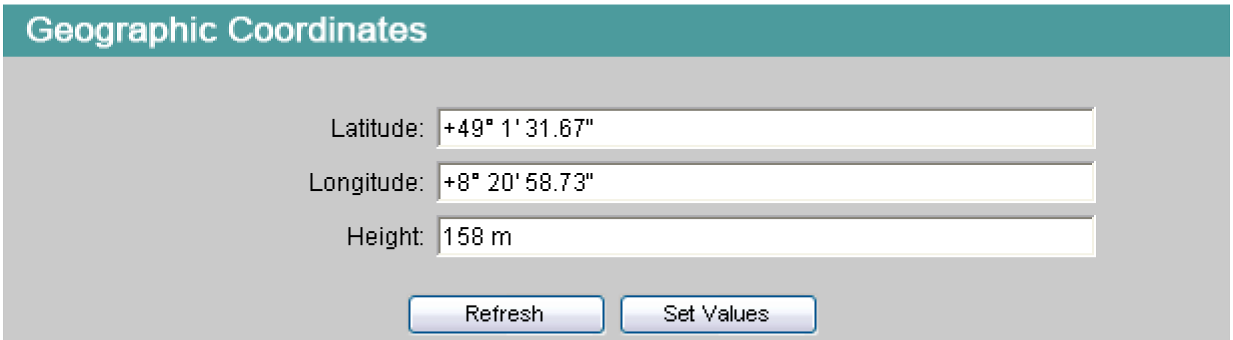


Figure 4-15 Geographic coordinates

Latitude
Here, you enter the value of the northern or southern latitude of the location of the device. For example, +49° 1´ 31.67" means that the device is located at 49 degrees, 1 minute and 31.67 seconds north.
A southern latitude is indicated by a preceding minus sign.

You can also append the letters N' (north) or S' (south) after the numbers (49° 1´ 31.67" N).

Longitude
Here, you enter the value of the eastern or western longitude of the location of the device. For example, +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 append the letters O' or E' (east) or W' (west) after the numbers (8° 20´ 58.73" E).

Height (geographic height)
Here, you enter the value of the geographic height above seal 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 are indicated by a preceding minus sign.

Entering the geographic coordinates

The values for the geographic coordinates can be entered in the text boxes, for example

- as degrees with minutes and seconds in the formats:
  DD°MM.MMM´, DD°MM´SS, DD°MM´SS.SSS
- in degrees in decimal format: DD.DDD°
- with or without a sign or with the letter S; N, E (or O) and W appended

Syntax of the Command Line Interface for the geographic coordinates

Table 4- 13 Geographic coordinates - CLI\SYSTEM\GEO>

Command	Description	Comment
info	Displays the current status of the geographic coordinates.	-
lat [string]	Shows/sets the geographical latitude coordinate.	Administrator only.
long [string]	Shows/sets the geographical longitude coordinate.	Administrator only.
height [string]	Shows/sets the geographical height coordinate.	Administrator only.

4.3 The X-300/X-400 menu

4.3.1 X-300/X-400 Status

Information on the operating status

This screen appears if you click the "X-400" or "X-300" folder icon.

The screen shows whether or not the IE switch is operating as redundancy manager and whether it has opened or closed the ring in this role. The status of a device related to the standby function is also displayed in this menu. Here, you will also find information about the power supply and error/fault status. The text boxes on this page are read-only.

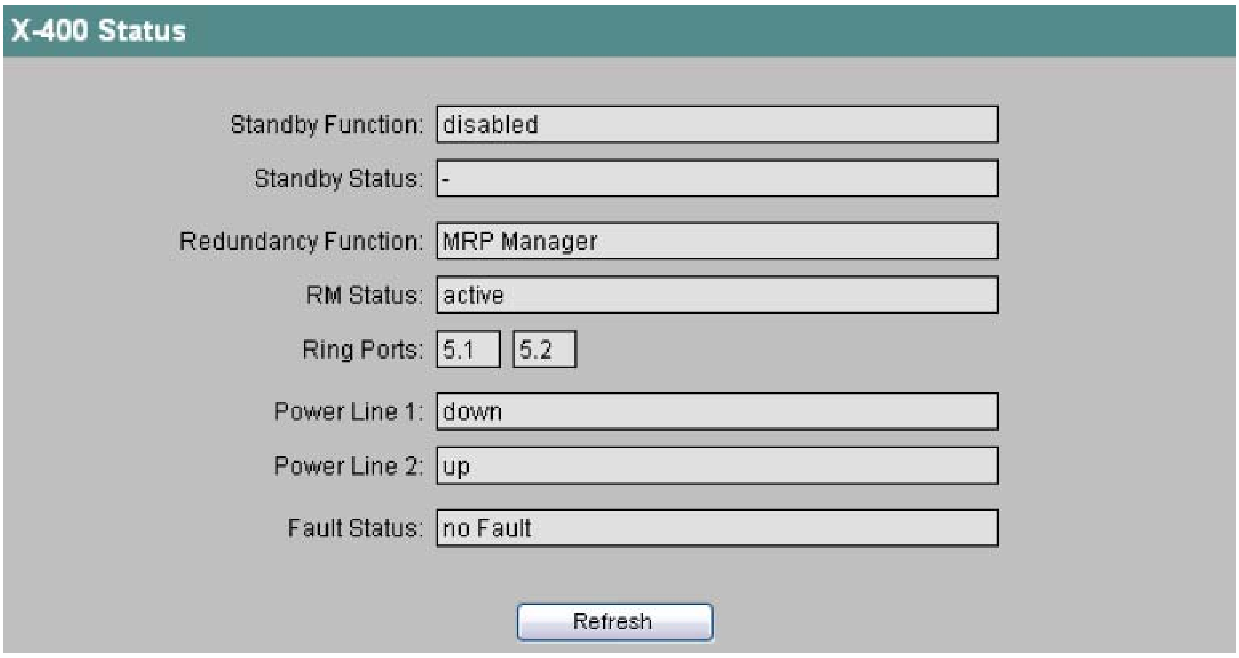


Figure 4-16 X-400 Status

Standby Function

Note

Device with the higher MAC address becomes master

When linking HSR rings redundantly, two devices are always configured as a master/slave pair. This also applies to interrupted HSR 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.

- Master:
  The device has a connection to the partner device and is operating as master. In normal operation, the standby ports of this device are active.
- Slave:
  The device has a connection to the partner device and is operating as slave. In normal operation, the standby ports of this device are inactive.
- Disabled:
  Standby link is disabled. The device is operating neither as master nor slave. The standby ports are working as normal ports without standby function.
- Waiting for Connection
  No connection has yet been established to the partner device. The standby ports are 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).

For information on configuring, enabling and disabling

- Standby link: Refer to the section "X-300/X-400 Standby Mask".
- Media redundancy in ring topologies: Refer to the section "X-300/X-400 Ring Configuration".

Only the status information is described here.

Standby Status

- Active:
  The standby ports of this device are active; in other words are enabled for frame traffic.
- Passive:
  The standby ports of this device are inactive; in other words are disabled for frame traffic.
  .

Redundancy Function

- no Ring Redundancy
  The IE switch works without redundancy functionality.
- HSR Client
  The IE switch operates as an HSR client.
- HSR Manager
  The IE switch operates as an HSR manager.
- MRP Client
  The IE switch operates as an MRP client.
- MRP Manager
  The IE switch operates as an MRP manager.

RM Status

- 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.
- Ringports
  These boxes display the ports operating as ring ports.

Note

If media redundancy in ring topologies is completely disabled, no ring ports are displayed and the text "Ring Redundancy disabled" is displayed.

Power Line 1

- Up:
  Power supply 1 (line 1) is applied.
- Down:
  Power supply 1 is not applied or is below the permitted voltage.

Power Line 2

- Up:
  Power supply 2 (line 2) is applied.
- Down:
  Power supply 2 is not applied or is below the permitted voltage.

Fault Status
The fault status of the IE switch is shown here. The following table contains examples of possible error messages. If more than one problem has occurred, they are listed in the text box one above the other. You will find a complete list of the error messages in the section "Error messages of the SCALANCE X300 / X400 (Page 335)".

Error messages	Meaning
Redundant power line down	The redundant power supply has failed.
Link down on monitored port	The connection to a monitored port is interrupted.
More than one RM in ring	More than one device in the ring has adopted the function of redundancy manager.
Non-recoverable ring error	These errors cannot be resolved by the redundancy manager. There can, for example, be a loss of redundancy frames sent by the redundancy manager at one end, without there being a link down. An incorrectly configured second redundancy manager in the ring also causes this error message. In the first case, check the configuration of the ring ports: • Suitable setting for the operating mode (full duplex/half duplex)? • With fiber-optic cables: Send and receive cables correctly plugged in? In the second case: Reconfigure the second redundancy manager in the ring so that this adopts the suitable client role or remove the device from the ring.
No Fault	The switch has not detected a fault (the signaling contacts have not responded and the fault LED is not lit).

Syntax of the Command Line Interface

Table 4- 14 X-400 Status - CLI\X-400> or X-300 Status - CLI\X-300>

Command	Description	Comment
info	Displays the status information for the IE switch.	-

4.3.2 X-300/X-400 observer

Observer in the HSR ring

The observer function provides additional options for error diagnostics and protection from errors for HSR. This allows malfunctions of the redundancy manager or incorrect configurations of an HSR ring to be monitored. If the observer is enabled (Protection Mode), it is capable of interrupting the connected ring if errors are detected. To do this, the observer changes its status from passive to active and changes a ring port (observer port) to the "blocking" status. When the error is resolved, the observer enables the port again.

If too many errors occur to quickly one after the other within a certain time, the observer no longer enables its port automatically and it remains permanently in the "active" status. This is signaled by the error LED and the following message text: "Observer stopped recovering because of too many (<number or errors>) repeated errors". From this status, the observer must be reactivated by the user after the errors have been eliminated (Restart Observer).

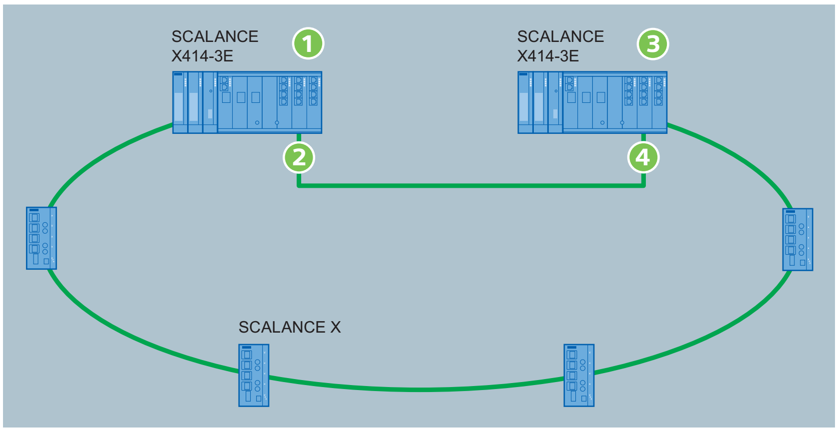
When setting up a ring with an observer, note the following points:

- The first configured ring port of the HSR manager (blocked port) must be connected directly to the first configured ring port of the observer (observer port).
- On an IE switch, the observer function can be enabled using the Command Line Interface (CLI) or Web Based Management (WBM).
- The observer and redundancy manager must both have firmware version V2.2 or higher.

Note

To be able to use the observer function, HSR must be activated.

Example of a configuration



① SCALANCE X414-3E configured as redundancy manager
② Blocked port of the redundancy manager
③ SCALANCE X414-3E configured as observer
④ First configured observer port

Figure 4-17 Redundant ring with monitoring of the redundancy manager by an observer

Activate or deactivate

The observer function is optional. It is enabled or disabled on the "Ring Configuration" page. As default, it is disabled.

Error messages

Errors detected by the observer are signaled by an error LED, signaling contact and corresponding message text. This uses the message method configured for the alarm event "Fault State Change", see section "Agent Event Configuration".

The possible message methods are e-mail, trap and/or event log table entry.

You will find a list with the message texts in Appendix D "Error messages of the SCALANCE X-300 / X-400".

Standby observer

The standby observer is an expansion of the simple redundant ring link. This is a second, independent standby link to master and slave. The full standby-observer link consists of two interconnected master-slave pairs as shown in the following figure:

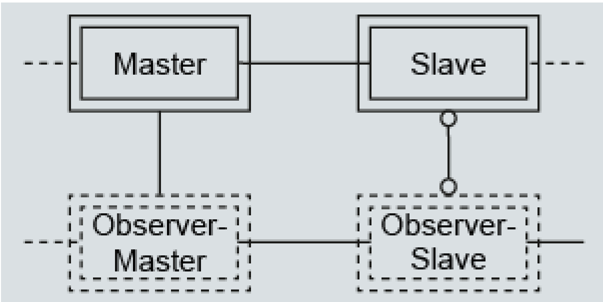


Figure 4-18 Standby observer link in the HSR ring

Both master-slave pairs make sure independently that only one of the two link paths is enabled at any one time. This prevents circulating frames.

Malfunctions are detected by each device comparing its current status with that of the linked device.

To check whether a link is active, you must, however, query the statuses of both devices of a link; in other words, slave and observer slave.

Activate or deactivate

The standby observer function is enabled in different ways:

- By device configuration on the "Standby Mask" page of the master or slave.
  When the connection is established to the linked device, the observer function starts automatically. This means that it is adequate for the function to be activated on one of the two linked devices.
- On the linked devices "Observer Master" or "Observer Slave", the function is enabled automatically when an observer frame is received.

CAUTION
If the standby observer function is enabled, you can only select a single standby port on the "Standby Mask" page.

Note

Restrictions with a linear bus topology

Note the following about the redundant linking of linear buses with an active standby observer function:
The redundancy is restricted solely to the link paths between the buses. If the bus between the standby master and standby slave or observer master and observer slave is interrupted, the relevant slave remains passive. This means that the communication to the slave and to all devices connected to the slave is interrupted.

The messages relating to the standby observer function

In the event and error messages, "Partner" indicates the device that is located in the same ring. This means that in the figure shown above, the master and slave are partners and the observer master and observer slave are partners. The "Observer" is the linked device in the other ring.

The following messages can occur:

- "Standby is waiting for <partner / observer>."

  The standby observer function was enabled and up to this point in time there was no contact with the partner or observer.

- "Standby <partner / observer> connected to <master / slave> <MAC address> <port number>."

  The connection to the partner or observer was established.

- "Standby <partner / observer> lost connection to <master / slave> <MAC address> <port number>."

  An existing connection to the partner or observer was interrupted.

- "Standby <partner / observer> conflicts with <active / passive> state."

  The state signaled by the partner or observer conflicts with the modules own current active/passive status. The integrity of the network is retained. In extreme situations (multiple errors), there may be an interruption of the standby link. This error indicates, for example, a connection abort between standby partners or a device failure.

- "Standby <partner's / observer's> state conflict resolved."

  The status described above has been resolved, for example after eliminating a fault.

- "Standby <partner / observer> conflicts with <master / slave> role."

  The function signaled by the partner or observer conflicts with the local master/slave role.

  This is the case when both standby devices adopt the same master/slave role in a ring on or when both connected observers adopt roles that are not master/slave roles. The integrity of the network is retained. In extreme situations (multiple errors), there may be an interruption of the standby link. This error indicates, for example, a connection abort between standby partners or a device failure.

- "Standby <partner / observer> conflicts with <master / slave> role resolved."

  The status described above has been resolved, for example after eliminating a fault.

4.3.3 X-300/X-400 Ring Configuration

The Media Redundancy Protocol (MRP) is available as of firmware V 3.0.0. Automatic Redundancy Detection (ARD) is the default when the IE switches X-300/X-400 are supplied. If you want to use the previous High Speed Redundancy method (HSR), HSR must be configured.

- Reconfiguration time of the frame traffic following a failover in MRP: 200 ms
- Reconfiguration time of the frame traffic following a failover in HSR: 300 ms

---

Note

For more detailed information, refer to the X-300 or X-400 operating instructions.

Ring configuration of the IE switch

Note

Media redundancy in ring topologies and the ring ports are set on the SCALANCE X-300 and SCALANCE X408-2 via the CLI or WBM, with the SCALANCE X414-3E, this is also possible with DIL switches.

NOTICE
With the SCALANCE X414-3E, configuration using software (CLI or WBM) is possible only when both the DIL switches, R1 and R2, are set to "ON". Otherwise the settings are as described in the "Operating Instructions Industrial Ethernet Switches SCALANCE X-400, section DIL switches of the SCALANCE X414-3E".

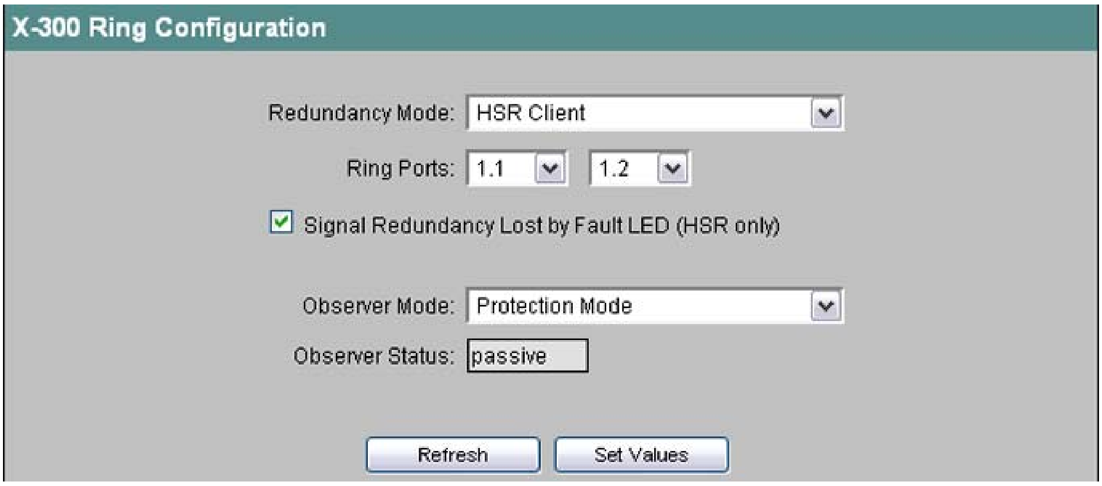


Figure 4-19 X-300 Ring Configuration

Redundancy Mode

In this list box, you can select from the following values:

- Disabled
- 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 "HSR Manager" in the ring. If this is the case, the device adopts the role of "HSR Client".
  If no HSR 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 device automatically set themselves to "MRP Client" mode.
- MRP Auto Manager
  Devices with the setting "Automatic Redundancy Manager" or "MRP Auto Manager" negotiate among themselves which device will adopt the "MRP Manager" role. The device with the lowest MAC address will always become "MRP Manager". In contrast to the setting "Automatic Redundancy Detection", the devices are not capable of detecting whether or not an HSR manager is in the ring. This means that they never adopt the role of "HSR client".
- MRP Client
  Here, you can select the "MRP Client" role.
  In a ring in which the devices are configured with MRP, at least one device must be set to one of the modes "Automatic Redundancy Detection" or "MRP Auto Manager". You also have the option of setting the "MRP Client" role for all other devices. If all except one device in the ring is configured as "MRP Client", this one device automatically adopts the role of "MRP Manager".
  Select "MRP Client" mode if you want to operate the device along with components that do not originate from Siemens in the ring.

- HSR Client
  Here, you can select the role "HSR Client".
- HSR Manager
  Here, you can select the role "HSR Manager". When you configure an HSR ring, one device must be set as HSR manager. All other devices must be configured as HSR clients.

NOTICE
When there is a reset to factory defaults, the redundancy mode Automatic Redundancy Detection (ARD) is enabled. The configuration of the ring ports is also reset to the factory-set ports: • X-300: Port 9 and port 10 • X-300 EEC: Port 8 and port 9 • X304-2: Ports 5 and 6 • X308-2M: Port 1 and port 2 • XR324-4M: Port 1 and port 2 • XR324-12M: Port 1.1 and port 1.2 • X-400: Ports 5.1 and 5.2 If other ports were used previously as ring ports, with the appropriate attachment, a previously correctly configured device can cause circulating frames and therefore the failure of the data traffic.

Ring Ports

Here, you set the ports to be used as ring ports in media redundancy in ring topologies.

Signal Redundancy Lost by Fault LED (HSR only)

If the check box is selected, a loss of HSR redundancy is indicated by the fault LED of the redundancy manager and signaled by the fault signaling contact. The loss of redundancy of a standby link is indicated by the standby slave with the fault LED and the fault signaling contact. In the factory settings, this function is enabled.

Observer Mode

The observer monitors malfunctions of the redundancy manager or incorrect configurations of an HSR ring. It is also capable of opening the connected ring if problems are detected (protection mode). Set the functionality of the observer in the "Observer Mode" list box. The following options are available:

- Disable
  The observer function is disabled.
- Protection Mode
  The observer function operates in protection mode
- Restart Observer
  The observer function is reset and the protection mode is enabled again.

Observer Status

This display box informs you about the current status of the observer:

- If the observer has not detected a problem, "passive" appears in the display.
- If the observer has detected a problem, "active" appears in the display.
- If the observer function is disabled, a small dash appears in the display.

You will find more information on the observer function in the section "X-300/X-400 observer (Page 61)".

Syntax of the Command Line Interface

Table 4- 15 X-400 Ring Configuration - CLI\X-400\RING> or
X-300 Ring Configuration - CLI\X-300\RING>

Command	Description	Comment
info	Displays the current ring configuration of the IE switch.	-
red [mode]	Enables/disables media redundancy in ring topologies. The following modes are possible: • D Disables media redundancy in ring topologies. • HSR The IE switch is an HSR client. • HSRMGR The IE switch is an HSR manager. • MRPCL The IE switch is an MRP client. • MRP The IE switch operates with MRP and can become redundancy manager automatically. • ARD Automatic Redundancy Detection.	Administrator only.
ports [<port1> <port2>]	Specifies the ring ports. Both ports must be specified.	Administrator only.
hsrfled[E|D]	Enables/disables the indication of a loss of HSR redundancy by the fault LED and signaling by the fault signaling contact.	Administrator only.
observer [D|R|P]	Specifies the observer function: • D Disables the observer function • R Restarts the observer function. • P Enables the observer function.	Administrator only.

4.3.4 X-300/X-400 Fault Mask

Function of the fault mask

With the fault mask, you specify the fault/error states to be monitored by the IE switch and that will trigger the signaling contact. Possible fault/error states are the absence of the power supply, power supply too low, or an interrupted connection or an unexpected connection established to a partner device. If the signaling contact is triggered, this causes the fault LED on the device to light up and, depending on the configuration of the event table, can trigger a trap, an E-mail, or an entry in the log table.

Device-related link monitoring of the ports

An IE switch provides device-related link monitoring. A link-up or link-down also affects the message system if the IE switch was appropriately configured.

Setting the fault mask on the device

The fault mask can also be set by the using the SET/SEL button on the front panel of the IE switch; for more detailed information, refer to the "Operating Instructions SCALANCE X-400 Industrial Ethernet Switches".

Settings in WBM

In WBM, you can set the monitoring of the power supply and the device-related link monitoring. The settings are made in three separate masks:

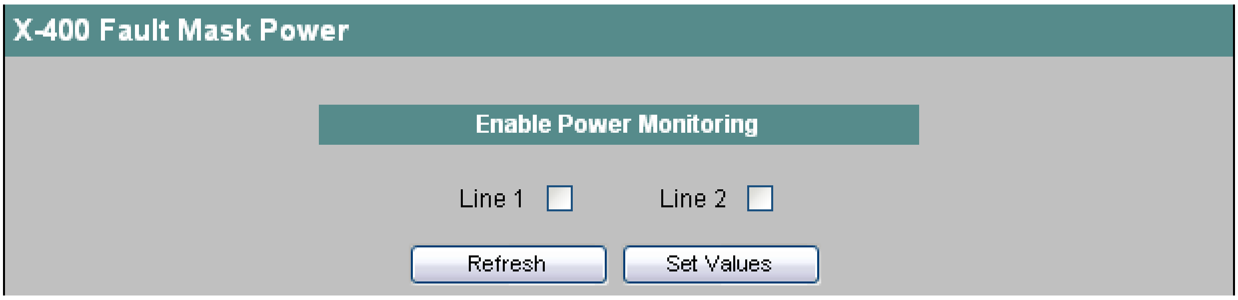


Figure 4-20 X-400 Fault Mask Power Monitoring

Enable Power Monitoring
Here, you specify which of the two power supply lines 1 and 2 is monitored. A fault is then indicated 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 (less than 14 V).

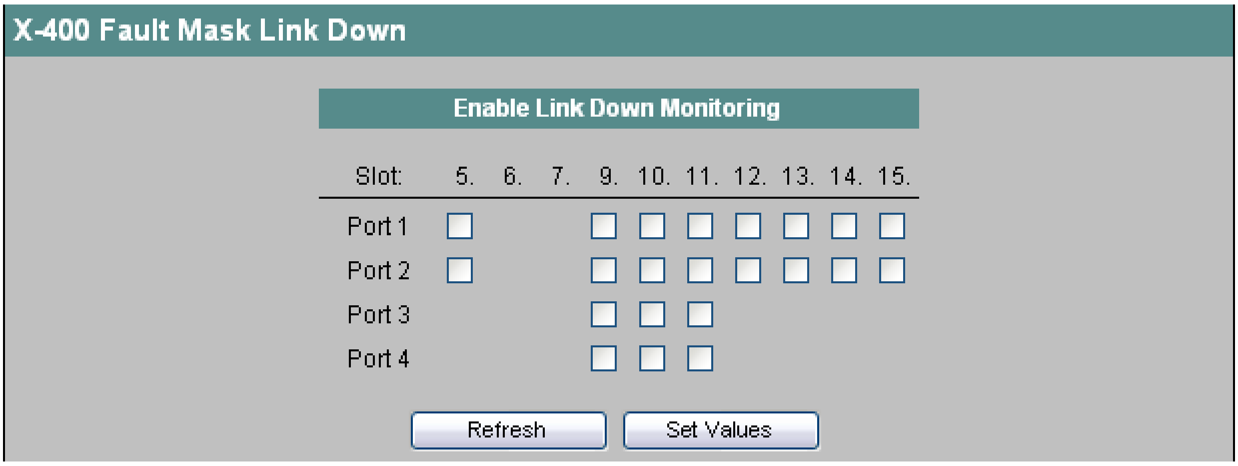


Figure 4-21 X-400 Fault Mask Link Down Monitoring

Enable Link Down Monitoring
Select the check boxes of the slots / ports whose connection status you want to monitor. If link monitoring is activated, an error is signaled when there is no valid link at this port because, for example, the cable is not plugged in or the connected device is turned off.

An error/fault can be signaled in the following ways depending on the configuration of the IE switch: Signaling contact, fault LED, SNMP trap, E-mail, entry in the log table, syslog.

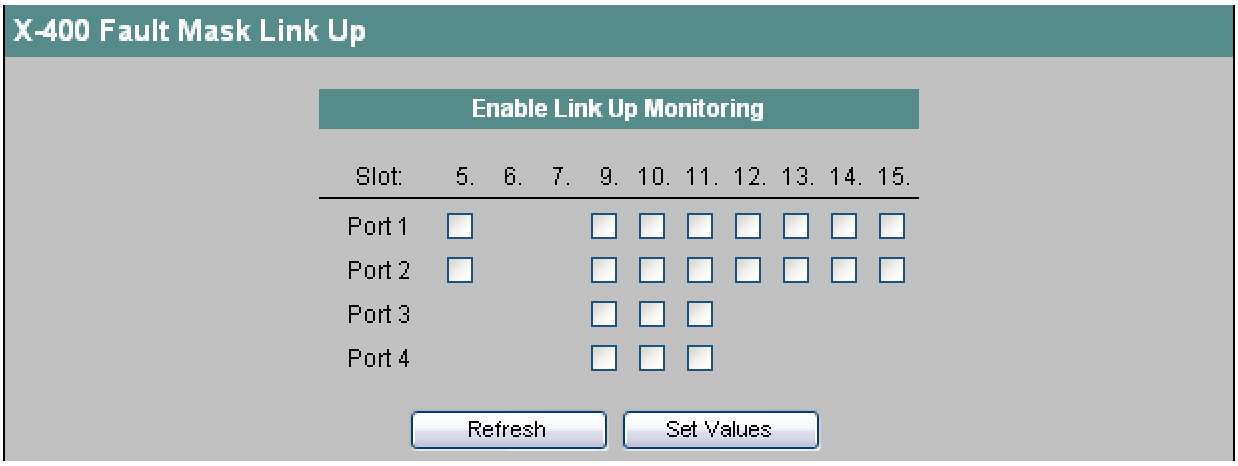


Figure 4-22 X-400 Fault Mask Link Up Monitoring

Enable Link Up Monitoring
Select the check boxes of the slots / ports whose connection status you want to monitor. If link monitoring is activated, an error is signaled when there is a valid link at this port because, for example, the cable should not be plugged in.

An error/fault can be signaled in the following ways depending on the configuration of the IE switch: Signaling contact, fault LED, SNMP trap, E-mail, entry in the log table, syslog.

Syntax of the Command Line Interface

Table 4- 16 X-400 Fault Mask - CLI\X-400> or X-300 Fault Mask - CLI\X-300>

Command	Description	Comment
linkdown [<E|D> [ports]]	Enables / disables link monitoring for the selected ports. If you do not specify any ports, all ports are enabled/disabled.	Administrator only. If you specify more than one port as parameter, each port must the separated by a blank.
linkup [<E|D> [ports]]	Enables / disables link monitoring for the selected ports. If you do not specify any ports, all ports are enabled/disabled.	Administrator only. If you specify more than one port as parameter, each port must the separated by a blank.
power [<E|D> [<1|2|1,2>]]	Enables / disables monitoring of the power supply connectors L1 and L2.	Administrator only.

4.3.5 X-300/X-400 Standby Mask

Redundant linking of rings

Apart from media redundancy in ring topologies, as of firmware version 1.2, the IE switches also support the redundant linking of HSR rings (including interrupted HSR rings = linear topology). In the redundant link, two HSR 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 over the ring ports and, in the event of a fault, redirect the data traffic from one Ethernet connection (standby port of the master) to another Ethernet connection (standby port of the slave).

For more detailed information on Ethernet cabling and the topological location of master and slave, refer to the "Operating Instructions SCALANCE X-400 Industrial Ethernet Switches".

Note

To use the redundant ring linking function, HSR must be enabled.

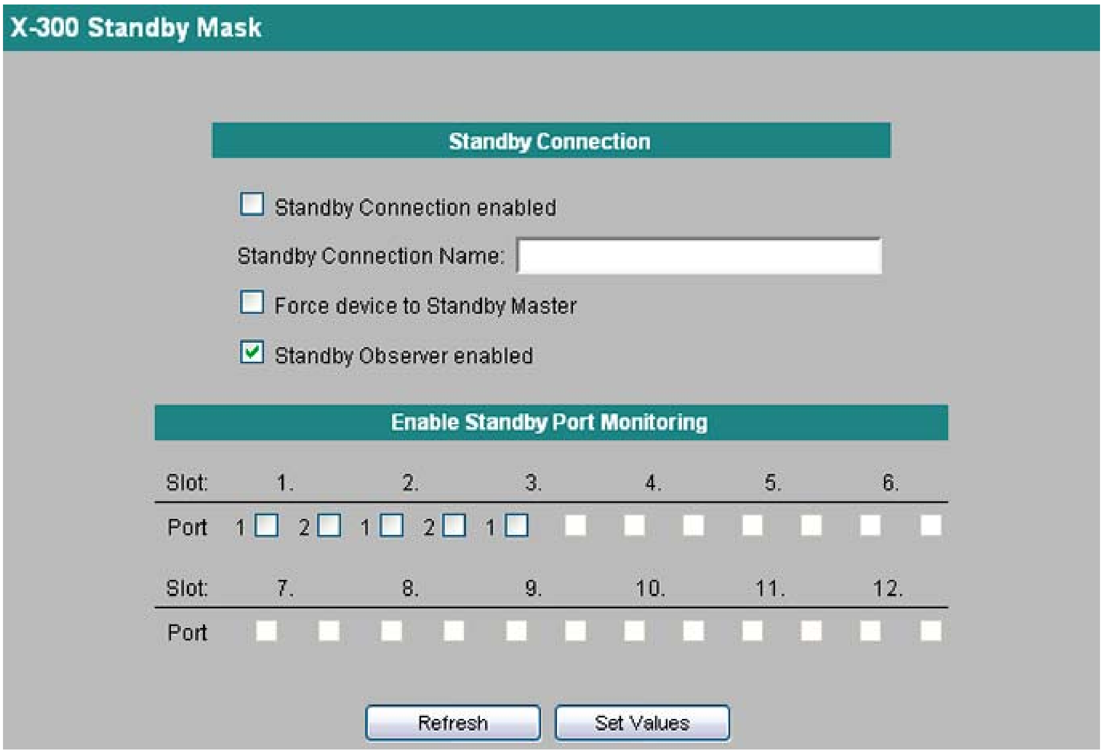


Figure 4-23 X-400 Standby Mask

Standby Connection enabled

Here, you decide whether or not the standby function is enabled.

Standby Connection Name

Here, enter the name for the standby connection. The master/slave device pair is defined by this name (both must be in the same ring). This is achieved by entering the same name on two devices in the ring. 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 function 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.

Standby Observer enabled

Enable or disable the function by selecting the check box.

You will find more information on this function in the section X-300/X-400 observer (Page 61).

Enable Standby Port Monitoring

CAUTION
If the standby observer function is enabled, you can only select one single standby port.

Here, you specify which ports are standby ports. Standby ports are involved in the redirection of data traffic. In there are no problems, only the standby ports of the master are enabled and handle to the data traffic into the connected HSR rings or HSR buses. If the master or the Ethernet connection (link) of one of the standby ports of the master fails, all standby ports of the master will be disabled and the standby ports of the slave enabled. As a result, a functioning Ethernet connection to the connected network segments (HSR rings or HSR linear buses) is restored.

NOTICE
If there are links to several rings (more than one port is enabled in "Standby Port Monitoring"), the standby master and standby slave may only have one Ethernet connection each to one ring. Otherwise circulating frames will result and lead to a loss of data traffic.

Syntax of the Command Line Interface

Table 4- 17 X-400 Standby Mask - CLI\X-400\STANDBY> or
X-300 Standby Mask - CLI\X-300\STANDBY>

<table>
<tr><th>Command</th><th>Description</th><th>Comment</th></tr>
<tr><td>info</td><td>Displays information on the standby configuration.</td><td>-</td></tr>
<tr><td>standby [E|D]</td><td>Enable/disable standby functionality.</td><td>Administrator only.</td></tr>
<tr><td>conname [string]</td><td>Display/specify the standby connection name.</td><td>Administrator only.</td></tr>
<tr><td>stbports [E|D> [ports]]</td><td>Enable/disable standby port monitoring.</td><td>Administrator only.</td></tr>
<tr><td>observer [E|D]</td><td>Enable/disable standby observer monitoring.</td><td>Administrator only.</td></tr>
</table>

Configuring a redundant link between rings

Follow the steps below to configure redundant linking of HSR rings:

1. Plan which devices of the ring adopt the role of "Standby Master" and which adopt the role of "Standby Slave". You should also plan the ports of the standby Master and standby slave to which the Ethernet connections to the other rings are connected.
   With the factory defaults, the device with the highest MAC address adopts the role of "standby master". If both devices support the "Force Device to Standby Master" function, you can configure a device as the standby Master regardless of its MAC address.

   Note

   Make sure that the redundant Ethernet connections are not plugged in until configuration is complete. Otherwise circulating frames will result and lead to a loss of data traffic. The same applies to disabling the redundant link.

2. Specify a name for the standby connection and enter this both for the standby master device and standby slave device.

   Note

   Make sure that the standby connection name (for one pair of devices) is used only once in the network.

3. By selecting the relevant check box under "Enable Standby Port Monitoring", you specify which ports are standby ports both for the standby master and the standby slave.
4. Enable the "Standby Connection enabled" option.
5. Confirm the configuration with "Set Values".
6. Now, you can plug in the redundant Ethernet connections.

   Note

   Make sure that the redundant Ethernet connections are plugged into the correct ports, in other words, into the configured standby ports. Otherwise circulating frames will result and lead to a loss of data traffic.

4.3.6 X-300/X-400 Counters

Response of the signaling contact and redundancy circuit

Using the counters, you monitor whether and how often problems occurred during operation (for example how often the signaling contact responded).

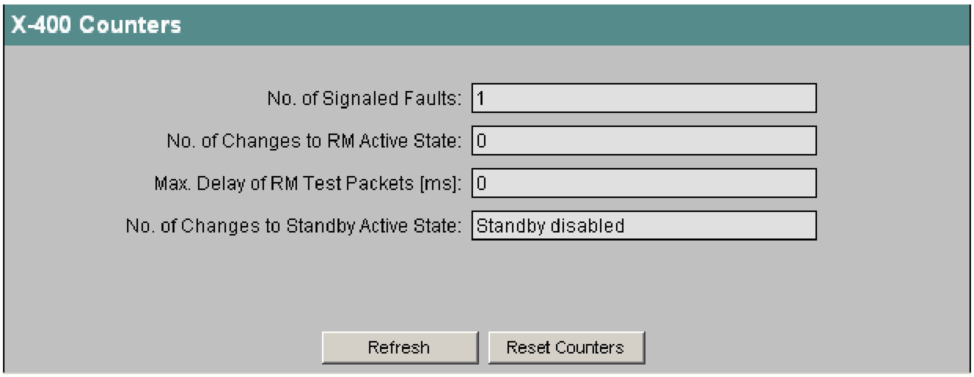


Figure 4-24 X-400 Counters

No. of Signaled Faults
Indicates how often the signaling contact of the IE switch responded.

The counter is reset each time the device is restarted.

No. of Changes to RM Active State
A value is displayed here only when the IE switch operates as HSR manager (see section "X-300/X-400 ring configuration").

The value indicates how often the HSR manager changed to the active state. This state is adopted when the redundancy manager detects an interruption on the line connected to the ring ports.

The counter is reset each time the device is restarted.

Max. Delay of RM Test Packets[ms]
Here, a value is displayed only when the IE switch operates as HSR manager ("Redundancy Manager enabled" check box selected).

In redundancy manager mode, an IE switch sends test frames over the ring ports to the connected line of switches and measures the delay of these test frames. The maximum delay that occurs with these test packets is displayed.

No. of Changes to Standby Active State
A value is displayed here when the standby function is enabled (see section "X-300/X-400 Standby Mask").

The value specifies how often the IE switch has changed the standby status from passive to active. This status is adopted when the connection of a standby port of the standby master fails.

The counter is reset each time the device is restarted.

Reset Counters
Click this button to reset the counters of the IE switch. A restart, for example due to an interruption of the power supply to the IE switch, causes the counters to be reset.

Syntax of the Command Line Interface

Table 4- 18 X-400 Counters - CLI\X-400> or X-300 Counters - CLI\X-300>

Command	Description	Comment
counters	Displays the following counter readings: • Changes to RM active state Indicates how often the IE switch operating as redundancy manager closed the ring. • Max. delay of RM Test Telegrams Indicates the maximum delay of test frames sent by the redundancy manager.	-
resetc	Resets the IE switch counters.	Administrator only.

4.4 The Agent menu

4.4.1 Agent Configuration

Introduction

The "Agent Configuration" screen appears if you click the "Agent" folder icon. This screen provides options for setting the IP address. You can specify whether a IE switch obtains the IP address dynamically or you can assign a fixed address. You can also activate the options for accessing the IE switch, such as TELNET or RMON.

IP configuration for the SCALANCE X414-3E

Here, you specify the IP configuration for the SCALANCE X414-3E. A distinction is made between the switch ports (In-band column) and the Ethernet port of the switch CPU (Out-band column).

Note

The IP addresses of the CPU and the switch ports must belong to different subnets.

IP Address

IP address of the SCALANCE X414-3E or the CPU module. If you change the IP address, you should be automatically guided to the new address. If this does not happen, please enter the new address in the Web browser manually.

Subnet Mask

Here, you enter the subnet mask of the SCALANCE X414-3E or the CPU module.

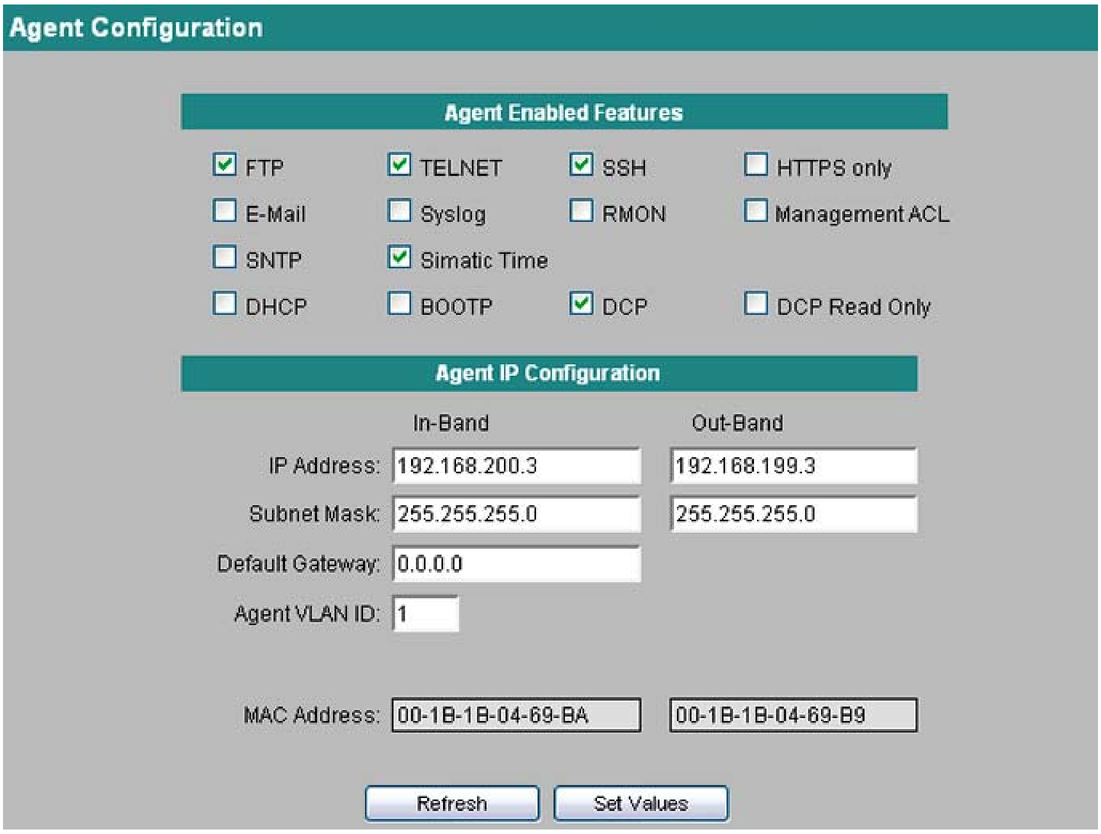


Figure 4-25 SCALANCE X414-3E agent configuration

IP configuration for the SCALANCE X-300/X408-2

Here, you specify the IP configuration for the SCALANCE X-300/X408-2.

Note

On the SCALANCE X-300/X408-2, no CPU Ethernet port (out-band port) can be configured. You can only configure the switch ports.

Subnet Mask

Enter the subnet mask here.

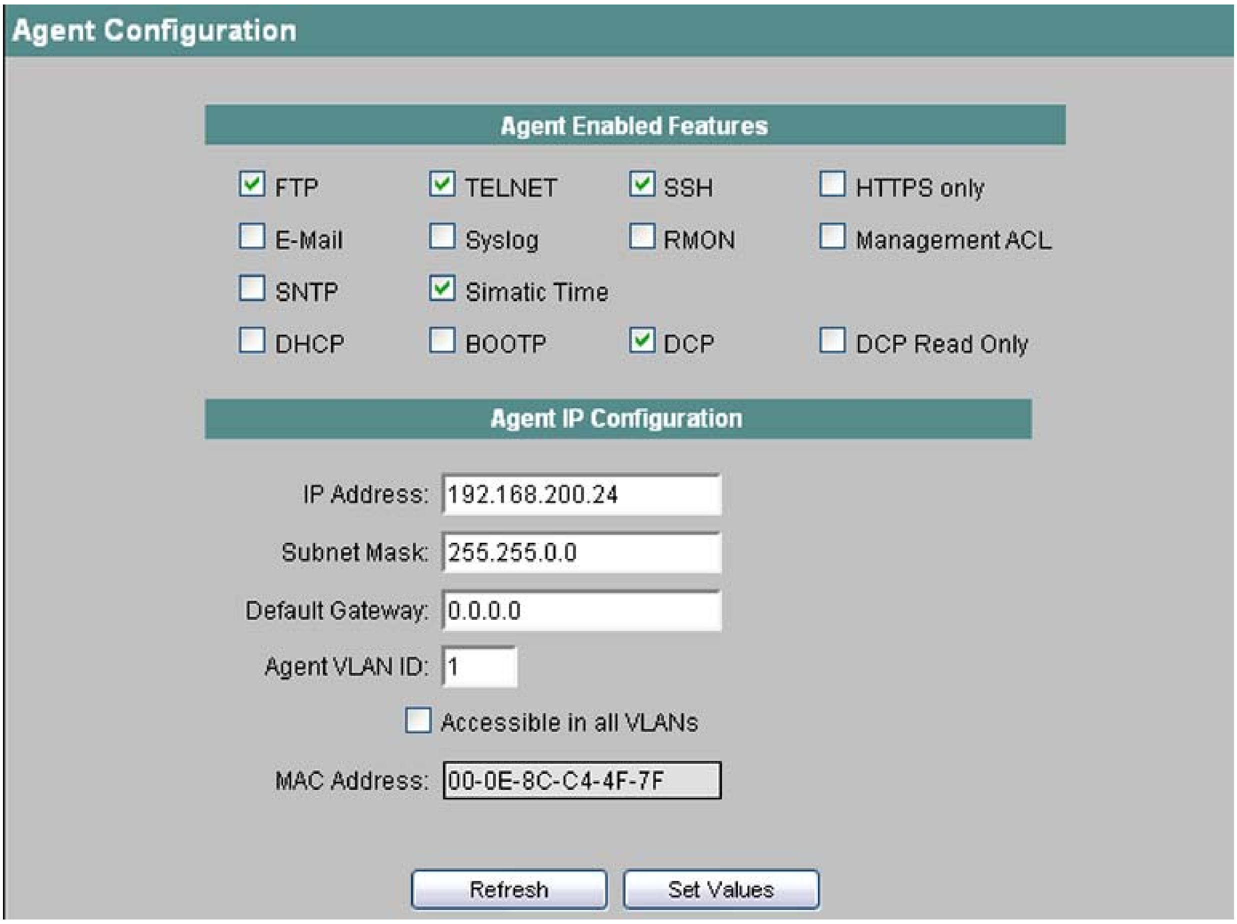


Figure 4-26 Agent Configuration SCALANCE X300

Settings for the IE switch

FTP

Enables / disables the FTP server. FTP can be used to download the firmware. You will find more detailed information on this topic in the section "Firmware update". You can also download or back up the configuration data via FTP.

If an IE switch has an IP address and there is an Ethernet connection to a PC or PG, follow the steps below to download configuration data:

1. Open a console window and type in the command ftp followed by the IP address of the IE switch. Example:
   ftp 192.168.20.54
2. For the login and password enter the same values as you use for WBM and CLI.
3. Enter the "put" command followed by the name of the firmware file.
   Example:
   put cfgdata.txt
4. Once the file has been loaded, the IE switch closes the FTP connection and restarts.

TELNET

Here, you specify whether or not the IE switch is accessible over TELNET.

SSH

Here, you specify whether or not the IE switch is accessible over SSH.

HTTPS only

Here, you specify whether or not the IE Switch is reachable only over HTTPS. If you do not select this option, it can also be reached with HTTP.

E-mail

This enables / disables the e-mail function of the IE switch. For detailed information on this functionality, refer to the section "Agent E-Mail Configuration menu item".

Syslog

Here, you specify whether or not the IE switch stores log entries on a Syslog server. For detailed information on this functionality, refer to the section "Agent Syslog Configuration menu item".

RMON

An IE switch supports remote monitoring (RMON). Remote Monitoring allows diagnostic data to be collected on the IE switch, 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. The setting for RMON does not influence the statistics functions (see section "Statistics menu").

Management ACL

NOTICE
Note the following when enabling this function: A bad configuration on the "Management ACL Configuration" page can result in you being unable to access the device. You should therefore configure an access rule that allows access to the management before you enable the function.

By clicking the check box, enable or disable access control to the management of the IE switch.

As default, the function is disabled.

The access rules are managed on the "Management ACL Configuration" page, see section Management Access Control List (Page 114)

Note

If the function is disabled, there is unrestricted access to the management of the IE switch. The configured access rules are only taken into account when the function is enabled.

SNTP

Enables / disables synchronization of the IE switch system time over an SNTP server in the network.

SIMATIC Time

Enables / disables synchronization of the IE switch system time using the SIMATIC time protocol.

In this case, synchronization makes use of multicast frames sent to the addresses 09-00-06-01-FF-EF.

An IE switch also evaluates SIMATIC time frames when it is logged on at an SNTP server.

Note

To avoid time jumps, you should make sure that there are either only SICLOCK transmitters or only SNTP servers in the network.

DHCP

If you enable this check box, the IE switch browses the network for a DHCP server and configures its IP parameters according to the data supplied by this server. For detailed information on this functionality, refer to the section "Assigning addresses with the DHCP client of the IE switch".

Note

As soon as the IP address has been assigned once by a PROFINET IO controller, DHCP automatically deactivates itself and must be reactivated if required.

BOOTP

If you enable this check box, the IE switch browses the network for a BOOTP server and configures its IP parameters according to the data supplied by this server. For detailed information on this functionality, refer to the section "Assigning addresses with the BOOTP client of the IE switch".

DCP

If you select this option, the device can be accessed and configured via DCP (PST Tool and STEP 7).

DCP Read Only

If you select this option, the configuration data can only be read via DCP (PST Tool and STEP 7).

Default Gateway

If you require the IE switch to communicate with devices (diagnostics stations, e-mail servers, etc.) in a different subnet, you will need to enter the IP address of the default gateway here.

Agent VLAN ID

Enter the VLAN-ID of the agent here.

Accessible in all VLANs

If this option is enabled, all agent functions (ping, Telnet, Web interface etc.) are accessible via all VLANs; if it is disabled, the functions are accessible only via the agent VLAN.

MAC Address

The MAC address of the IE switch or CPU module.

Syntax of the Command Line Interface

Table 4- 19 Agent Configuration - CLI\AGENT>

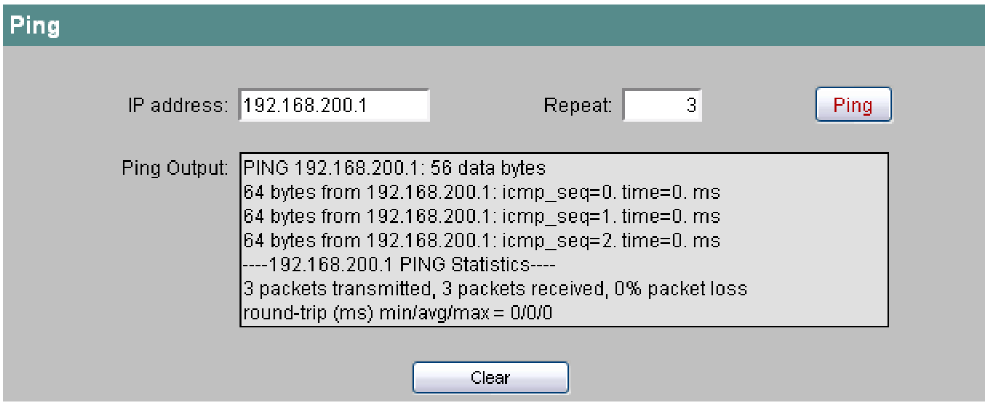
Command	Description	Comment
ip <IP address>	This specifies in-band IP address for the IE switch. You enter four decimal numbers separated by dots. Displays the currently set in-band IP address if no parameter is specified.	Administrator only. The IP address must be entered if you want to access an IE switch using a Web browser, TELNET, or SNMP. The IP address can also be assigned automatically by BOOTP/DHCP.
subnet <subnet mask>	Specifies the subnet mask for the in-band ports of the IE switch. You enter four decimal numbers separated by dots.	Administrator only. The subnet mask must be entered if you want to access an IE switch using a Web browser, TELNET, or SNMP. The IP address can also be assigned automatically by BOOTP/DHCP.
gateway <IP address>	Specifies the IP address of the default IP gateway. You enter four decimal numbers separated by dots.	Administrator only. The IP address must be entered if you want to access a router on the IE switch and the communication partner does not belong to the same subnet as the IE switch. The gateway must either be in the subnet of the in-band IP address or the out-band IP address. The IP address can also be assigned automatically by BOOTP/DHCP.
vid	Specifies the agent VLAN ID.	Administrator only. Default value: 1
allvlans	Specifies whether or not the agent functionalities are available via all VLANs or only via the agent VLAN.	Administrator only. Default value: disabled

Command	Description	Comment
bootp [E|D]	Enables / disables BOOTP.	Administrator only. Default value: disabled
dhcp [E|D]	Enables / disables DHCP.	Administrator only. Default value: Enabled.
mail [E|D]	Enables/disables E-mail functionality.	Administrator only. Default value: Disabled.
ftp [E|D]	Enables / disables FTP.	Administrator only. Default value: Enabled
dcp [D|RO|RW]	Enables / disables DCP • D Disabled • RO Read-only • RW Read-write	Administrator only. Default value: Read Write
telnet [E|D]	Enables / disables TELNET.	Administrator only. Default value: Enabled.
rmon [E|D]	Enables / disables remote monitoring.	Administrator only. Default value: disabled
macl [E|D]	Enables/disables Management Access Control List.	Administrator only.
sntp [E|D]	Enables / disables SNTP.	Administrator only. Default value: disabled
siclock	Enables/disables time synchronization with the SIMATIC time protocol.	Administrator only. Default value: Enabled
ping [-c number] [-s length] <IP address>	Sends a number of packets to the specified IP address. If the parameters for number and length are omitted, an IE switch sends ten packets each with a length of 128 bytes. Example: ping -c 5 -s 256 192.168.1.1 Five packets with a length of 256 bytes are sent to IP address 192.168.1.1.	-
ssh [E|D]	Enables / disables SSH.	Administrator only. Default value: Enabled
httpso [E|D]	Specifies whether or no the IE switch is reachable only over HTTPS (disabled means it is also reachable over HTTP).	Administrator only. Default value: Disabled.
slog [E|D]	Enables / disables Syslog.	Administrator only.

4.4.2 Ping

Reachability of an address in an IP network

The ping function in Web Based Management has exactly the same function as the terminal function of the same name. It checks whether an address exists in an IP network.



IP address
Enter the IP address of the network device you want to ping to test whether it can be reached.

Repeat
Here, enter the number of data packets to be sent.

Ping
Click this button to start sending the data packets.

Ping Output
This box shows the output of the ping function.

4.4.3 Agent SNMP Configuration

How SNMP works

Using SNMP (Simple Network Management Protocol), a Network Management Station can configure and monitor SNMP-compliant nodes, such as an IE switch. To allow this, a management agent is installed in the IE switch with which the management station exchanges data. There are three frame types:

- Read (management station fetches values from an IE switch)
- Write (management station writes values to an IE switch)
- Send events to registered nodes (traps). The agent sends messages to registered management stations.

SNMPv3 (and SNMPv2) enhancements compared with SNMPv1

SNMPv3 (and SNMPv2) has the following enhancements compared with the original SNMPv1:

- Management stations can communicate with each other.
- Multi-level security concept (encryption of data, authentication of users).
- User-defined security settings.

Access permissions with SNMP

When using the SNMP protocol, you specify access permissions by means of the community string. A community string contains information about the user name and password in a string. Different community strings are defined for read and write permissions. More complex and more secure authentications are possible only in some SNMPv2 variants and in SNMPv3.

Note

To preserve security, you should not use the default values public or private.

Configuration of SNMP with an IE switch

The "Agent SNMP Configuration" screen appears if you click the "SNMP" folder icon.

In the SNMP Configuration screen, you make the basic settings for SNMP. Enable the check boxes according to the SNMP functionality you want to use. For detailed settings (traps, groups, users), there are separate menu items in WBM. Here, you can also make the entries even if you have not selected the SNMPv3 enabled option, however the entries do not take effect.

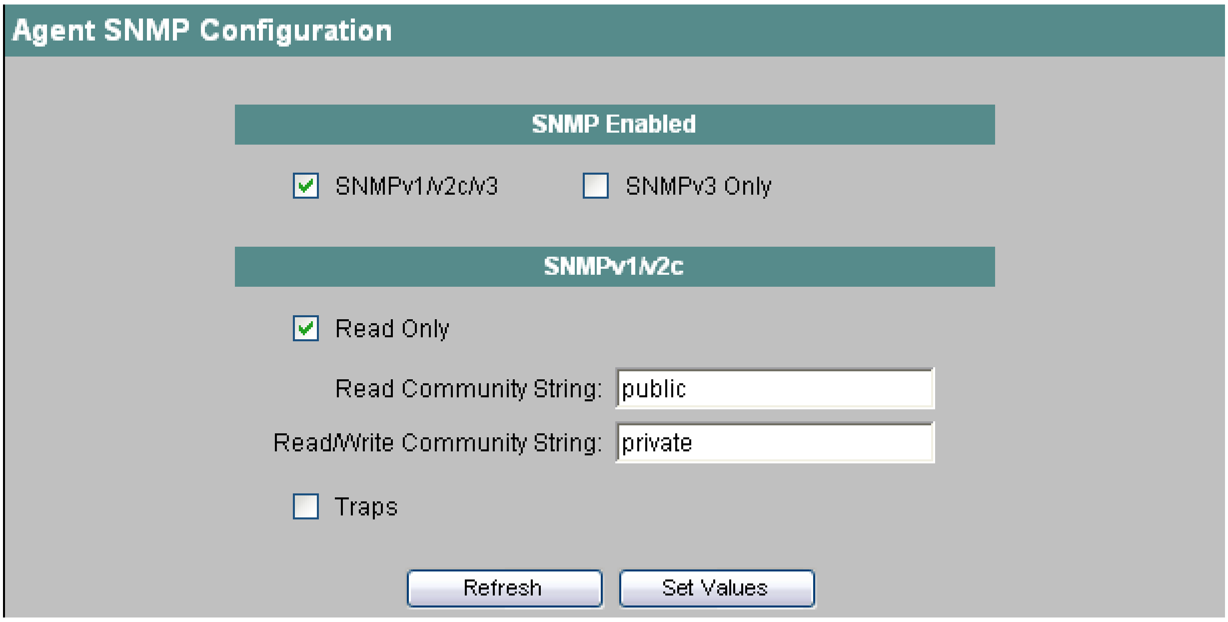


Figure 4-27 Agent SNMP Configuration

SNMPv1/v2/v3
Here, you enable / disable SNMPv1, SNMPv2 and SNMPv3 for an IE switch.

SNMPv3 only
If you select this check box, you enable SNMPv3 only; the functionality of SNMPv1 and SNMPv2 is not available.

Read Only
When this check box is selected, you can only read SNMP variables with SNMPv1/v2c.

Read Community String
Here, you enter the read community string (maximum of 20 characters) for the SNMP protocol.

Read/Write Community String
Here, you enter the write community string (maximum of 20 characters) for the SNMP protocol.

Traps
This enables / disables the sending of SNMPv1/v2c traps.

Syntax of the Command Line Interface

Table 4- 20 Agent SNMP Configuration - CLI\AGENT\SNMP>

Command	Description	Comment
snmp [D|3|A]	Disables / enables SNMP. The meaning of the parameters is as follows: • D Disables SNMP. • 3 Enables only SNMPv3. • A Activates SNMPv1, SNMPv2 and SNMPv3.	Administrator only. Default value: SNMPv1, v2 and v3 are enabled.
getcomm [string]	Specifies the read community string (maximum length 20 characters). The default is "public".	Administrator only.
setcomm [string]	Specifies the read/write community string (maximum length 20 characters). The default is "private".	Administrator only.
traps [E|D]	Enables / disables SNMPv1 traps.	Administrator only.

4.4.4 SNMPv1 Trap Configuration

SNMP traps for alarm events

If an alarm event occurs, an IE switch can send traps (alarm frames) to up to ten different (network management) stations at the same time. Traps are only sent when events as specified in the Agent Event Configuration menu occur (see Section "Agent Event Configuration").

Note

Traps are sent only when the "Traps" option was selected in "SNMP Configuration".

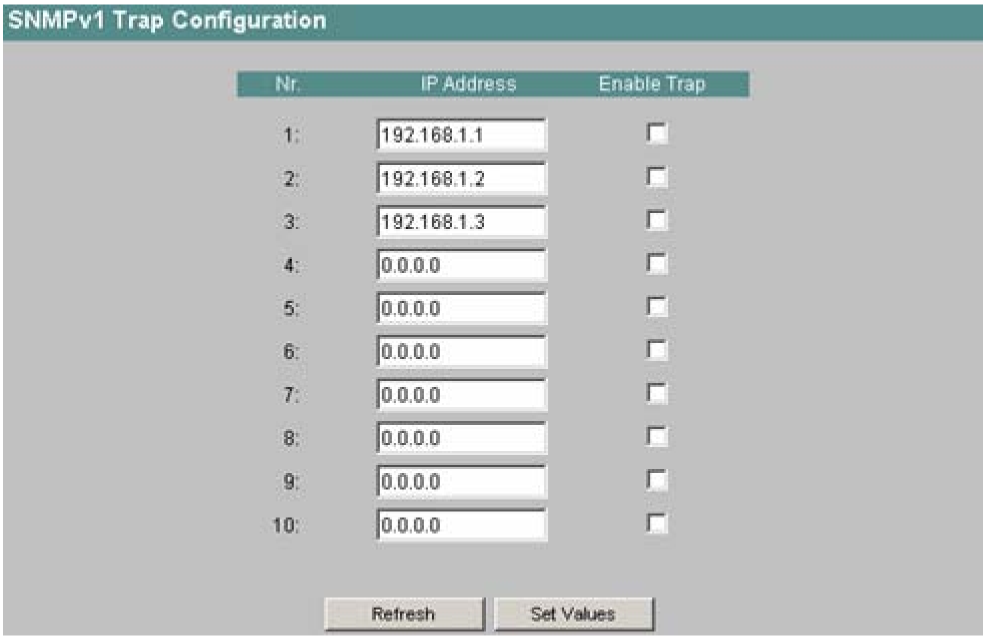


Figure 4-28 SNMPv1 Trap Configuration

IP Address
Here, you enter the addresses of the stations to which an IE switch will send traps.

Enable Trap
Click on the check box next to the IP addresses to enable the sending of traps to the corresponding stations.

Syntax of the Command Line Interface

Table 4- 21 SNMPv1 Trap Configuration - CLI\AGENT\SNMP\TRAPCONF>

Command	Description	Comment
Info	Shows the current trap configuration.	-
ip <entry> <ip>	Specifies the IP address of the trap recipient entry (entry between 1 and 10).	Administrator only. Default value: 0.0.0.0
state <entry><E|D>	Enables/disables the sending of traps to the recipient entry (entry between 1 and 10)	Administrator only. Default value: D

4.4.5 SNMPv3 Group Configuration

Security settings and assigning permissions

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

Figure 4-29 SNMPv3 Groups

Group Name

This lists all previously defined group names. When you click on a group name, a new window opens in which you can change the parameter settings of a group.

Auth
A cross in this column indicates that the authentication is enabled for the corresponding group.

Priv
A cross in this column indicates that encryption is enabled for the corresponding group.

Read
A cross in this column indicates that read access is enabled for the corresponding group.

Write
A cross in this column indicates that write access is enabled for the corresponding group.

New Entry
Click on this button to create a new group.

Configuration of the SNMPv3 groups

When you click on a group name, you open the page for configuring the group properties:

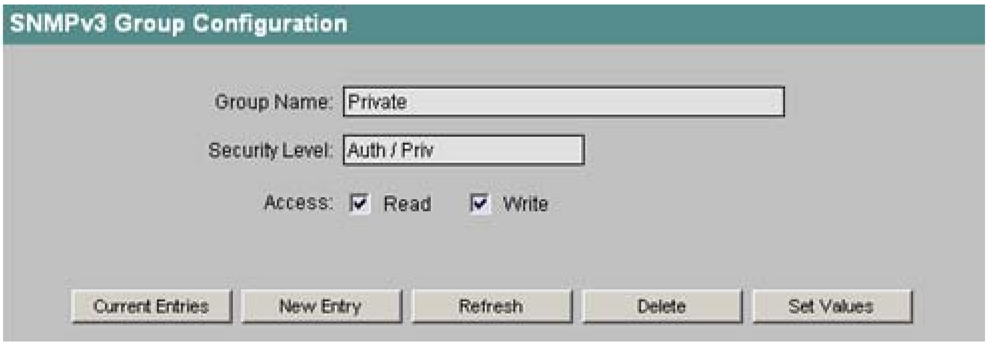


Figure 4-30 SNMPv3 Group Configuration

Group Name

The group name is displayed here. This text box is read-only, you can only assign the group name when creating a group and you cannot modify it later.

Security Level

This text box displays the authentication and the encryption. You have the following three options for the security levels:

Security level	Special features	Comment
no Auth / no Priv	No authentication, no encryption.	-
Auth	Authentication with the MD5 or SHA algorithm, no encryption.	-
Auth / Priv	Authentication with the MD5 or SHA algorithm, encryption with the DES3 algorithm.	-

Read and Write

Here, you enable or disable write access, read access and notification.

Current Entries

By clicking this button, you return to the list of SNMPv3 groups.

New Entry

After clicking this button, the page for creating a new group opens.

Delete

Click on this button to delete a group. If members are already entered in the group, you cannot delete the group nor is it possible to change the security level for the group.

Creating a new group

After clicking the "New Entry" button in the "SNMPv3 Group Configuration" window, the window for creating a new group opens:

Figure 4-31 SNMPv3 Group Configuration II

Group Name
Enter the name of the group here. This name must have at least two characters, the maximum length is 32 characters.

Security Level
Here, you select the security level that will apply to the group.

Read and **Write**
Here, you specify whether members of the group have read access, write access, or both.

Syntax of the Command Line Interface

Table 4- 22 SNMPv3 Groups - CLI\AGENT\SNMP\GROUP>

Command	Description	Comment
info	Displays a list of all SNMPv3 groups.	-
add <groupname> [securitylevel]	Adds a new SNMPv3 group. You specify the security level with the following parameter settings: • NOAUTH No authentication, no encryption. • AUTH Authentication with the MD5 or SHA algorithm, no encryption. • PRIV Authentication with the MD5 or SHA algorithm, encryption with the DES3 algorithm.	Administrator only.
edit <groupname> <accessrights>	Sets the access permissions. The following parameter settings are available for defining write and read access: • - Permit neither write nor read access. • RO Permit read access only. • RW Permit read and write access.	Administrator only.
delete <groupname>	Deletes the SNMPv3 group with the specified name.	Administrator only.
clearall	Deletes all SNMPv3 groups from the list.	Administrator only.

4.4.6 SNMPv3 Users Configuration

User-specific security settings

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. A user is defined by the following settings:

- User name:
  A freely selectable name.
- Security name:
  Name corresponding to the authentication protocol.
- Authentication Protocol:
  Type of authentication protocol.
- Authentication Key:
  The private key of the authentication protocol.
- Privacy Protocol:
  Type of encryption.
- Privacy Key:
  The private password for the encryption.

This page displays the SNMPv3 users. The user name is displayed in the "User Name" column, the name of the group to which the user is assigned is displayed in the "Group" column:


SNMPv3 Users

User Name	Group	Auth	Priv
PrivateMD5	Private	MD5	DES
PrivateSHA	Private	SHA	DES
ProtectedMD5	Protected	MD5	none
ProtectedSHA	Protected	SHA	none
Public	Public	none	none

New Entry Refresh

Figure 4-32 SNMPv3 Users

User Name
This lists all previously defined user names. When you click on a user name, a new window opens in which you can change the passwords of a user.

Group
The entries in this column show the group to which a user belongs.

Auth
This column shows the authentication algorithm used for the user.

Priv
This column displays the encryption method used for the user.

New Entry
Click on this button to create a new user.

Configuration of the SNMPv3 users

When you click on a user name, you open the page for user configuration:

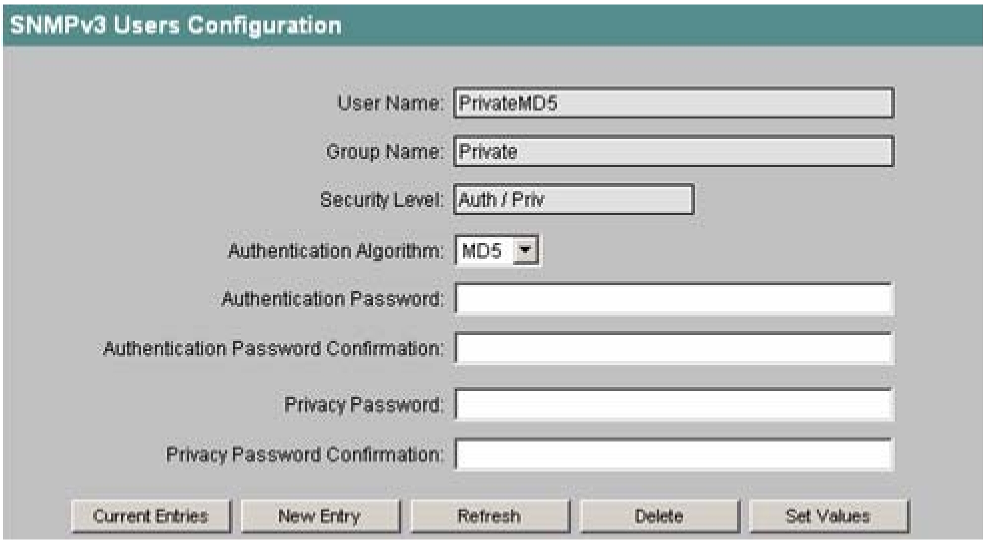


Figure 4-33 SNMPv3 Users Configuration

User Name
The user name is displayed here. This box is read-only because the name of a user can no longer be modified once it has been created.

Group Name
This box displays the group to which the user was assigned.

If authentication is necessary for the selected group, select an authentication algorithm and enter the authentication password. If encryption was also selected for the group, enter the encryption password.

Security Level
This box displays the security level (authentication, encryption) that applies to the group. The various security levels are described on page 70.

Authentication Algorithm
You can choose between the MD5 and the SHA algorithm.

Authentication password / Authentication password confirmation
Enter the authentication password in these boxes. The password can be up to a maximum of 32 characters long. You can use all available characters.

Privacy password / Privacy password confirmation
Enter the encryption password in these boxes. The password can be up to a maximum of 32 characters long.

Current Entries
By clicking this button, you return to the list of MAC SNMPv3 users.

New Entry
You can create a new user by clicking the New Entry button and specifying the group name and the group to which the user will belong.

Delete
Click on this button to delete a user.

Creating a new user

After clicking the "New Entry" button in the "SNMPv3 Users Configuration" window, the window for creating a new user opens:

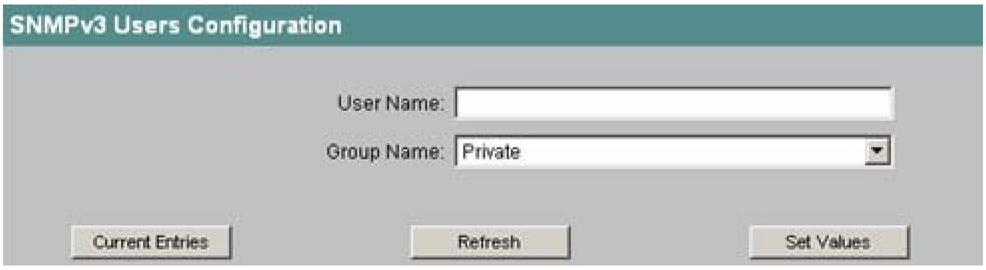


Figure 4-34 SNMPv3 Users Configuration II

User Name
Enter the name of the new user here.

Group Name
Here, you select the group to which the new user will belong.

Syntax of the Command Line Interface

Table 4- 23 SNMPv3 Users - CLI\AGENT\SNMP\USER>

Command	Description	Comment
info	Displays a list of all SNMPv3 users.	-
add <username> <groupname>	Adds a new SNMPv3 user to a group. If authentication is necessary for the group, MD5 is selected as the default algorithm.	Administrator only.
auth <username><MD5|SHA>	Changes the authentication algorithm (MD5 or SHA) or an SNMPv3 user. This command can only be used for members of a group for which this authentication is necessary.	Administrator only.
pass <username><authentpassword> [encr.password]	Changes the passwords of an SNMPv3 user (maximum length 32 characters). This command can only be used for members of a group for which this authentication is necessary. The encryption password can only be specified if it is necessary.	Administrator only.
delete <username>	Deletes the SNMPv3 user with the specified name.	Administrator only.
clearall	Deletes all SNMPv3 users from the list.	Administrator only.

4.4.7 Agent Timeout Configuration

Setting the timeout

Here, you can set the times after which there is an automatic logout in WBM or CLI.

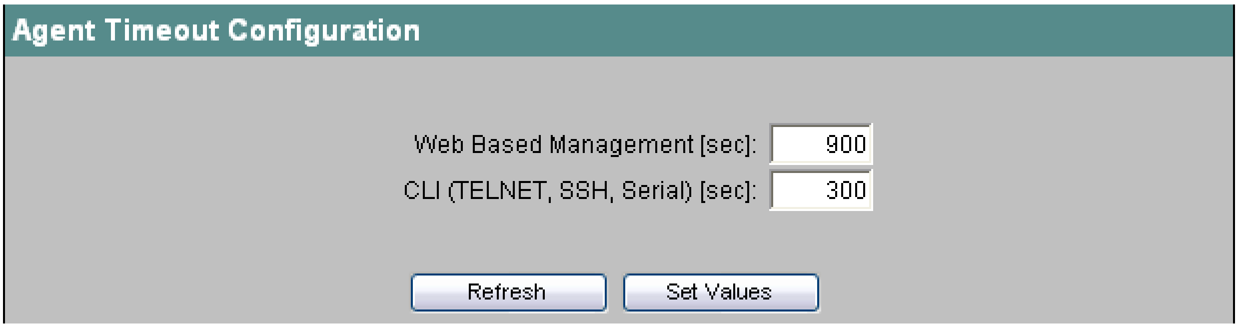


Figure 4-35 Agent Timeout Configuration

Web Based Management (sec)
Here, you specify the WBM timeout.
Permitted values for the WBM timeout: 60-3600 (seconds)

0 means: There is no automatic logout.

CLI (TELNET, SSH, Serial) (sec)
Here, you specify the CLI timeout.
Permitted values for the CLI timeout: 60-600 seconds

0 means: There is no automatic logout.

Syntax of the Command Line Interface

Table 4- 24 CLI\AGENT\TIMEOUT>

Command	Description	Comment
info	Displays the current timeout settings.	-
wbmtime	Sets the WBM timeout (in seconds).	Administrator only. Default value: 900
clitime	Sets the CLI timeout (in seconds).	Administrator only. Default value 300

4.4.8 Agent Event Configuration

System events of the IE switch

On this page, you specify how an IE switch reacts to system events. By enabling the appropriate check boxes, you specify which events trigger which reactions on the IE switch. The following options are available:

- The IE switch sends an E-mail.
- The IE switch triggers an SNMP trap.
- The IE switch writes an entry in the log file.
- The IE switch writes an entry to the Syslog server.

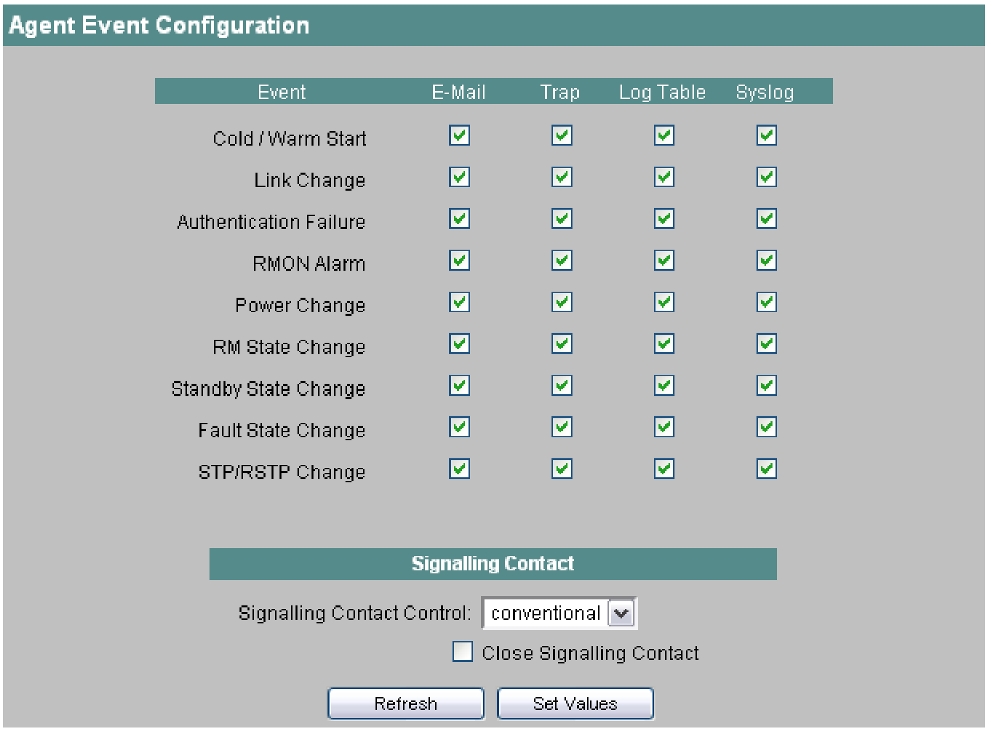


Figure 4-36 Agent Event Configuration

You can configure the reaction of the IE switch to the following events:

Cold/Warm Start
The IE Switch was turned on or restarted by the user.

Link Change
A port has failed or data traffic is being handled again over a port that had previously failed.

Authentication Failure
There was an SNMP access with a bad password or inadequate access rights.

RMON Alarm
An alarm or event has occurred relating to remote monitoring.

Power Change
This event occurs only when the power supply line 1 and line 2 is monitored. It indicates that there was a change to line 1 or line 2.

RM State Change
The redundancy manager has detected an interruption or re-establishment of the ring and has switched the line over or back. To allow an IE switch to operate as redundancy manager, you will need to configure the device appropriately (see section "X-400 Ring Configuration menu item" or "X-300 Ring Configuration menu item).

Standby State Change
A device with an established standby connection (master or slave) has activated or deactivated the link to the other ring (standby port). The data traffic was redirected from one Ethernet connection (standby port of the master) to another Ethernet connection (standby port of the slave) (see section "X-400 Standby Mask menu item" or "X-300 Standby Mask menu item").

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.

STP/RSTP Change
The STP or RSTP topology has changed.

VRRP State Change (SCALANCE X414 only)
The state of the virtual router has changed.

Signaling Contact Control
With this drop-down list, you can specify how the signaling contact works:

- **conventional**
  Default setting for the signaling contact. An error/fault is displayed by the fault LED and the signaling contact opens. When the error/fault state no longer exists, the fault LED goes off and the signaling contact closes.
- **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.

Close Signaling Contact
Select this check box if you want to close the signaling contact.

Note

The setting of the "Close Signaling Contact" check box is only effective if the "aligned" setting was selected in the "Signaling Contact Control" drop-down list.

Syntax of the Command Line Interface

Table 4- 25 Agent Event Configuration - CLI\AGENT\EVENT>

Command	Description	Comment
info	Shows the current event configuration.	-
setec [event] <E|D> <E|D> <E|D> <E|D>	Specifies how an IE switch reacts to system events. The following abbreviations are available for the event parameter: • CW Cold/Warm start • LC Link Change • AF Authentication Failure • RA RMON Alarm • PC Power Change • RC RM State Change • SC Standby State Change • FC Fault State Change • RS STP/RSTP Change • VE VRRP State Change (X414 only) If an event is specified, the configured actions are formed for each event. The four parameters that follow <E> or <D> configure the reactions of the IE switch in the order: • E-mail • Trap • Entry in the log table • Entry on the Syslog server Example: • setec LC E D D D Only sends an E-mail if there is a Link Change.	Administrator only.

Command	Description	Comment
scontrol [C|A]	Selects how the signaling contact works: conventional An error/fault is displayed by the LED and the signaling contact opens. aligned The signaling contact can be opened or closed as required regardless of a fault/error.	Administrator only.
sclose [yes|no]	Switches the signaling contact: Yes The contact is closed. No The contact is opened	Administrator only.

4.4.9 Agent Digital Input Configuration (SCALANCE X414-3E)

Note

Digital inputs and their associated functions are available only on the SCALANCE X414-3E.

Examples of applications for digital inputs

A SCALANCE X414-3E has eight digital inputs that can be used in a wide variety of ways:

- Example 1, monitoring an OLM in process control without I/O
  It is assumed that you have an S7-400 controller without central I/O module, the I/O is connected optically over PROFIBUS OLM. The signaling contact of the OLM can be applied to a digital input of the SCALANCE X414-3E and is available for diagnostics.
  If the signaling contacts of an existing OLM are applied to the digital inputs of the SCALANCE X414-3E, the OLM can be monitored without additional components.
- Example 2, door contact
  The door contact of a cabinet is connected with digital inputs of a SCALANCE X414-3E. By suitably configuring events, it is then possible to monitor any interventions in the cabinet.

Events for changes and the digital inputs

For each individual digital input, you can specify which event is triggered if there is a status change at the input (both rising and falling edges). The following options are available:

- The SCALANCE X414-3E sends an E-mail.
- The SCALANCE X414-3E triggers an SNMP trap.
- The SCALANCE X414-3E writes an entry in the log file.
- The SCALANCE X414-3E writes an entry to the Syslog server.

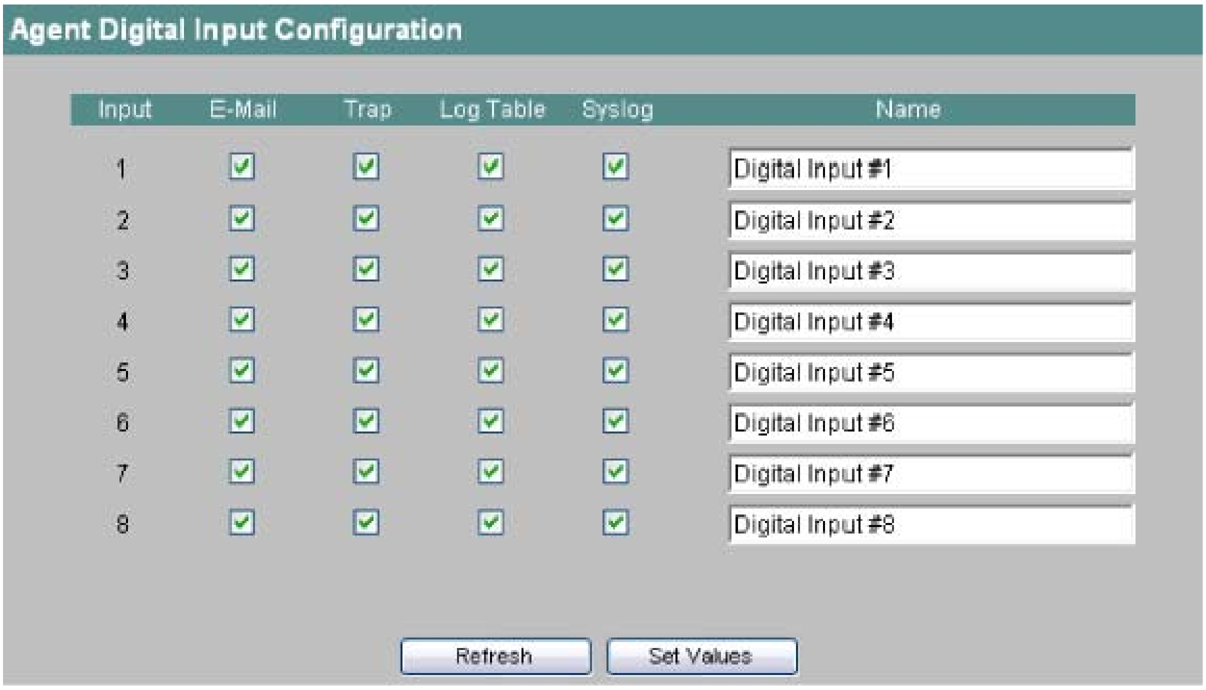


Figure 4-37 Agent Digital Input Configuration

Name

Here, you can assign a meaningful name for each digital input.

Syntax of the Command Line Interface

Table 4- 26 Agent Digital Input Configuration - CLI\AGENT\DIGIN>

Command	Description	Comment
info	Shows the state of the digital inputs of the SCALANCE X414-3E.	-
showdic	Shows the configuration of the digital inputs of the SCALANCE X414-3E.	-
setdic [input] <E|D> <E|D> <E|D> <E|D>	Sets the event configuration for the digital inputs in the order: E-mail, trap, log table entry, entry on the Syslog server. If no input is specified, the specified configuration relates to all inputs. Example: • setdic 5 E D E D If input 5 is set, the SCALANCE X414-3E sends an E-mail and makes an entry in the log table. No trap is sent and no entry is made on the Syslog server.	Administrator only.
name <1 ... 8> <string>	Assigns a symbolic name to a digital input. This name can be a maximum of 64 characters long.	Administrator only.

4.4.10 Agent E-Mail Configuration

Network monitoring with E-mails

An IE switch 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 diagnostic information.

E-mails can only be sent when

- The E-mail function is activated on the IE switch and the E-mail address of the recipient is configured (see "Agent Configuration menu item").
- The E-mail function is enabled for the relevant event (see "Agent Event Configuration" menu item).
- There is an SMTP server in your network that can be reached by the IE switch.
- The IP address of the SMTP server is entered on the IE switch.

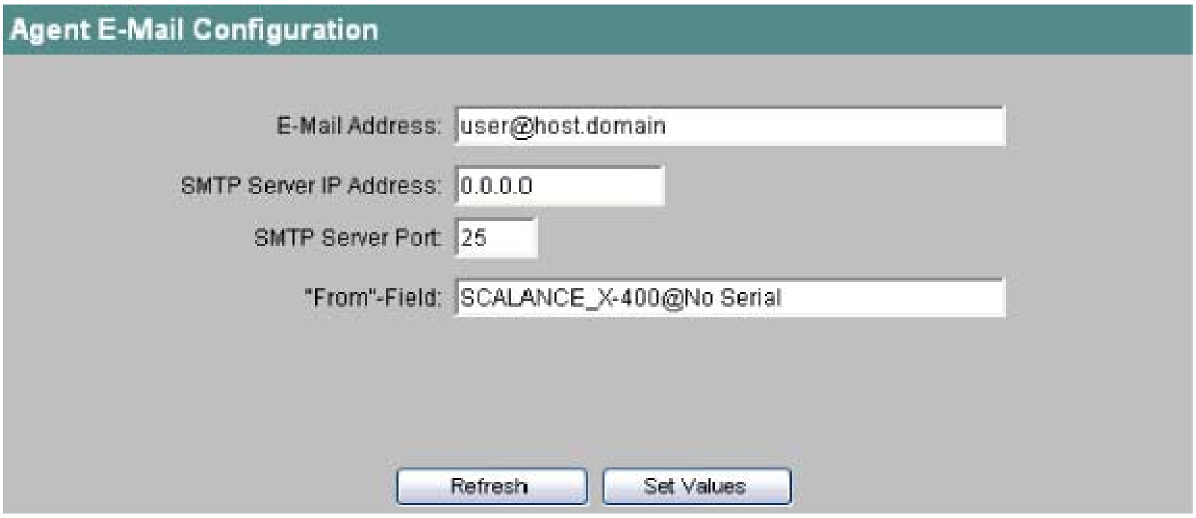


Figure 4-38 Agent E-Mail Configuration

E-Mail Address
Here, you enter the E-mail address to which the IE switch sends an E-mail if a fault occurs.

SMTP Server IP Address
Here, you enter the IP address of the SMTP server over which the E-mail is sent.

SMTP Server Port
The IP port over which the mail is sent. If necessary, you can change the default value 25 to your own requirements.

"From" Field
Address of the sender of the E-mail.

Note

Depending on the properties and configuration of the SMTP server, it may be necessary to adapt the "From” box for the E-mails. Check with the administrator of the SMTP server. You can set the "From” box over WBM, CLI, or direct SNMP access.

Syntax of the Command Line Interface

Table 4- 27 Agent E-Mail Configuration - CLI\AGENT\EMAIL>

Command	Description	Comment
info	Shows the current E-mail configuration.	-
server [<ip>[:port]]	Specifies the IP address and the port number of the SMTP server.	Administrator only. Default value: 0.0.0.0:25
email <E-mail address>	Specifies the address to which an IE switch sends an E-mail. This address can be up to a maximum of 50 characters long.	Administrator only. Default value: Disabled. Default address: user@host.domain
from [E-mail address]	Specifies the sender of E-mails from the IE switch. This address can be up to a maximum of 50 characters long.	Administrator only.

4.4.11 Agent Syslog Configuration

Application

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

Log book entries can only be sent when

- The Syslog function is enabled on the IE Switch (see section "Agent Configuration")
- The Syslog function is enabled for the relevant event (see Agent Event Configuration menu item)
- There is a Syslog server in your network that receives the log entries from the IE switch. (Since this is a UDP connection, there is no acknowledgment to the IE Switch)
- The IP address of the Syslog server is entered on the IE switch.

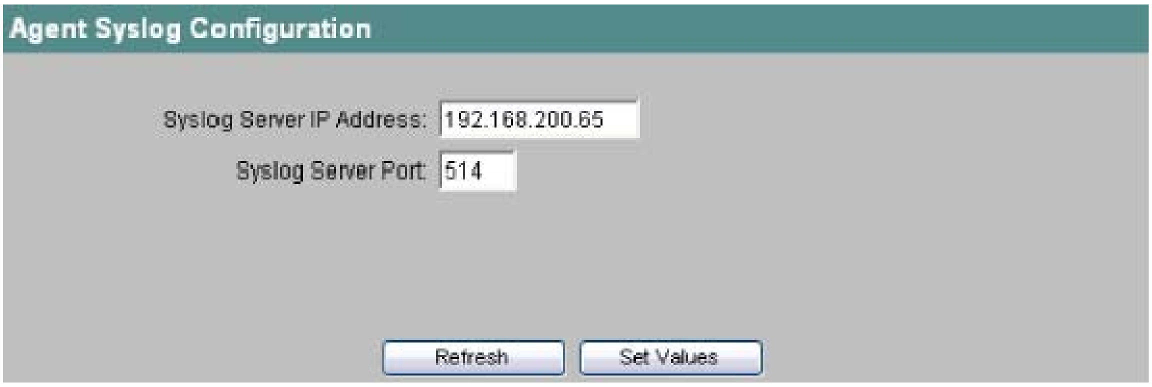


Figure 4-39 Agent Syslog Configuration

Syslog Server IP Address
Here, you enter the IP address of the Syslog server on which the log entries will be stored.

Syslog Server Port
The UDP port via which the log entries will be stored on the server.

Syntax of the Command Line Interface

Table 4- 28 Agent Syslog Configuration - CLI\AGENT\SYSLOG>

Command	Description	Comment
info	Shows the current Syslog configuration.	-
server [<ip>[:port]]	Specifies the IP address and the port number of the Syslog server.	Administrator only. Default value: 0.0.0.0:514

4.4.12 Agent DHCP Configuration

Setting the DHCP mode

There are several ways of identifying the SCALANCE X408-2 in the configuration of the DHCP server:

- with the MAC address
- with a freely defined client ID
- with the system name
- with the PROFINET IO device name

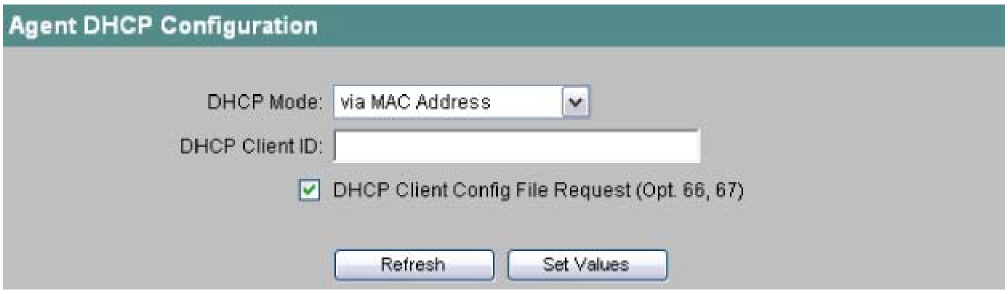


Figure 4-40 Agent DHCP Configuration

DHCP Mode
Here, you set the DHCP mode.

Note

If DHCP is not enabled in the Agent Configuration menu item, no mode can be selected and the text "disabled" is displayed.

DHCP Client ID
For the DHCP mode "via Client ID", you can assign an identification string here that is assigned to an IE switch and will be evaluated by the DHCP server.

DHCP Client Config File Request (Op. 66, 67)
Select this option if you want the DHCP client to use options 66 and 67 to download and then enable a configuration file.

NOTICE
If a configuration file is downloaded, this triggers a system restart. Make sure that the option "DHCP Client Config File Request" is no longer set in this configuration file.

Syntax of the Command Line Interface

Table 4- 29 Agent DHCP Configuration - CLI\AGENT\DHCPCONF>

Command	Description	Comment
info	Shows the current DHCP configuration	-
dhcpmode [mode]	Sets the DHCP mode. The possible modes are as follows: • MAC MAC address • CLID Client ID • SYSN device name • DEVN PNIO device name	Administrator only.
clientid [ClientID]	Specifies the DHCP client ID. This value is used when DHCP via client ID is set. The client ID can be freely defined.	Administrator only.
cfgreq [E|D]	Enables/disables Config File Request (Opt. 66, 67)	Administrator only.

4.4.13 Agent Time Configuration

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. An IE switch logs on as client with this server as receiver of time-of-day frames.

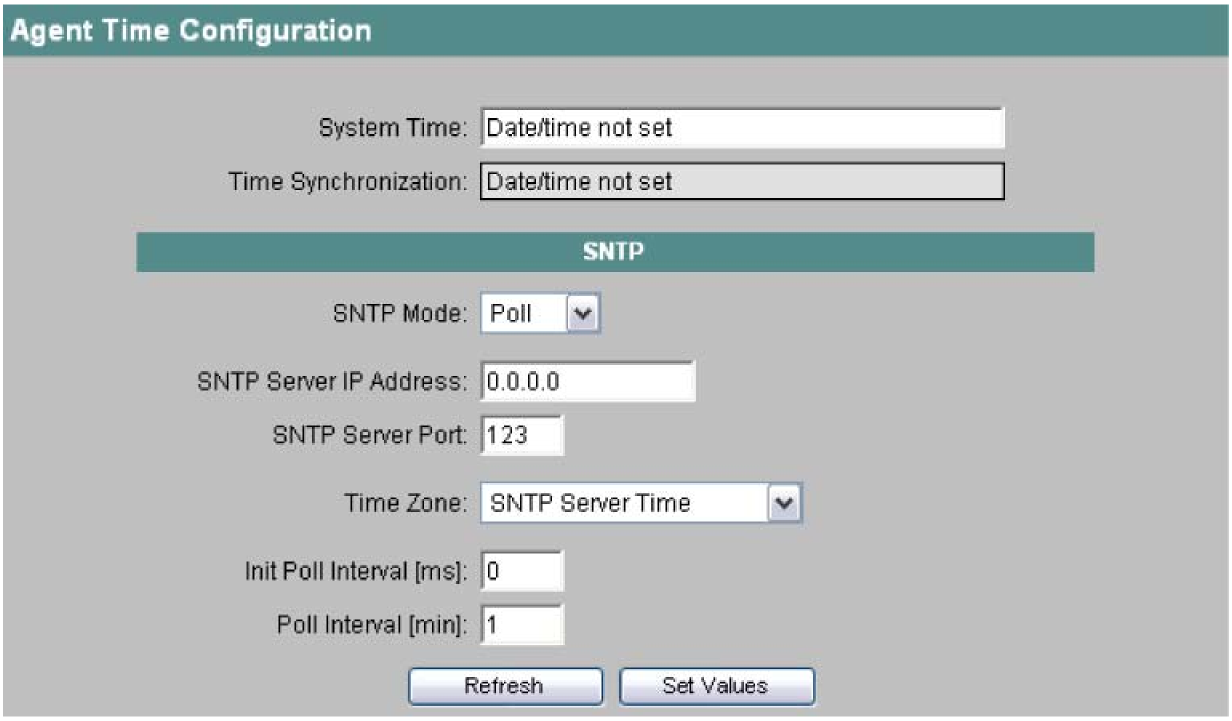


Figure 4-41 Agent Time Configuration

System Time
This box displays the current system time. If no time-of-day synchronization was possible, the box displays "Date/time not set".

You can also set the date and time manually, the required input format is MM/DD/YYYY HH:MM:SS. In this case, the text box displays the data and time along with the suffix (m). If the system time was set as a result of synchronization with a server, the suffix is (p).

Time Synchronization
This box is read-only and shows when the last time-of-day synchronization took place.

SNTP Mode
You can choose from four different protocol types here:

- Poll
  If you choose this protocol type, you have to define further settings:
  Time zone offset, Time server, Init poll interval, Poll interval.
- Listen
  In this mode, you can also select an offset to the time received from the server. Other settings are not possible.

SNTP Server IP Address
Here, you enter the IP address of the SNTP server whose frames will be used by an IE switch to synchronize the time of day.

SNTP Server Port
Here, enter the port over which the SNTP server is available.

Time Zone
In this box, select the time zone for the location of the IE switch because the SNTP server always sends UTC time. This time is then recalculated and displayed as the local time based on the time zone. There is no standard/daylight-saving time switchover on the IE switch.

Init poll interval
Here, you can enter the interval at which an IE Switch repeats the initial poll for the system time if this was not successful the first time.

Poll interval
Once the system time has been adopted the first time from the time server, it is updated cyclically with renewed polls to the time server. Here, you specify how often the updates take place.

Syntax of the Command Line Interface

Table 4- 30 Agent Time Configuration - CLI\AGENT\TIME>

Command	Description	Comment
time [date][time]	Displays or sets the time on the IE switch. When the date and time are displayed, you can also see when and how the time was set: • m The setting was made manually. • t The setting was made by SIMATIC time-of-day frame, however, it is not synchronized with the time transmitter. • s The setting was made by SIMATIC time-of-day frame and it is synchronized with the time transmitter. • p The setting was made by the SNTP protocol.	Administrator only. Input format: MM/DD/YYYY HH:MM:SS
server [<ip>[:port]]	Sets the IP address and optionally the port of the SNTP server.	Administrator only.
timezone [-12 ... 13]	Sets the time difference in hours between the SNTP server and system time.	Administrator only.
sntpmode [mode]	Specifies the SNTP mode. The possible modes are as follows: • POLL IE switch queries the time on the SNTP server • LISTEN IE switch waits for SNTP time-of-day frames	Administrator only.
initint [1...1000]	Specifies the polling interval in the range from 1 - 10000 ms	Administrator only.
Interval [1...1440]	Specifies the polling interval in the range from 1 - 1440 s	Administrator only.

4.4.14 Agent PNIO Configuration

Settings for PROFINET IO

Here, the PROFINET IO device name is set as it was assigned for the IE switch during PROFINET IO hardware configuration with NCM.

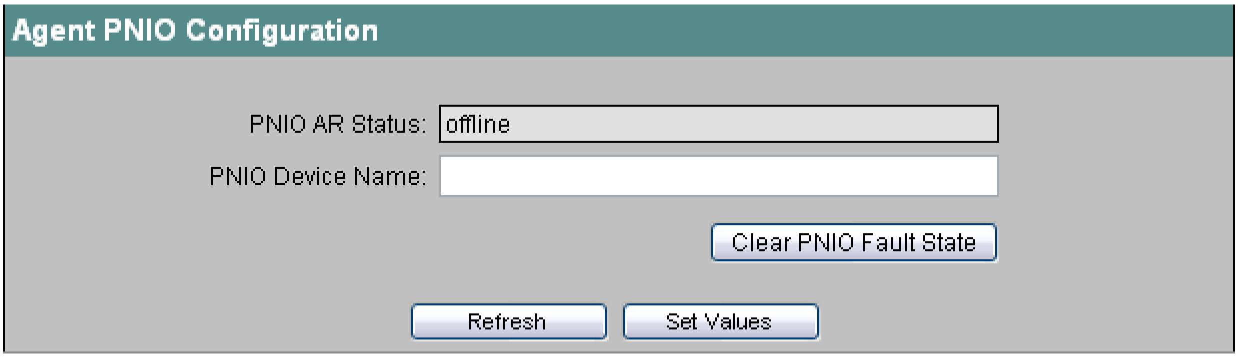


Figure 4-42 Agent PROFINET IO Configuration

PNIO AR Status
This box shows the PROFINET IO application relation status; in other words, whether or not the IE switch is connected "online" or "offline" with a PROFINET Controller.

In this context, online means that a connection to a PROFINET IO controller exists, that the controller has downloaded its configuration data to the IE switch 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 on the IE switch.

PNIO Device Name
Here, you enter the PROFINET IO device name (Name of Station) according to the configuration in HW Config.

Clear PNIO Fault State
If the IE switch was integrated in a PROFINET IO environment (with controller) and is then removed from PROFINET IO mode, the fault LED signals that the controller is missing. This fault display can be cleared with this button.

Syntax of the Command Line Interface

Table 4- 31 Agent PROFINET IO Configuration - CLI\AGENT\PNIOCONF>

Command	Description	Comment
info	Shows the current PROFINET IO configuration	-
devname [string]	Sets the PROFINET IO device name.	Administrator only.
clear	Clears a PROFINET IO fault state, if one exists	Administrator only.

4.4.15 Management Access Control List

The Management Access Control List - an overview

On this page, you can increase the security of IE switch. To specify which host can access the management of your IE switch using which IP address, configure the access rules for individual hosts, subnets or all hosts.

You can set the ports via which a host can access the IE switch.

The list of access rules presents this information clearly as shown in the example in the following figure:

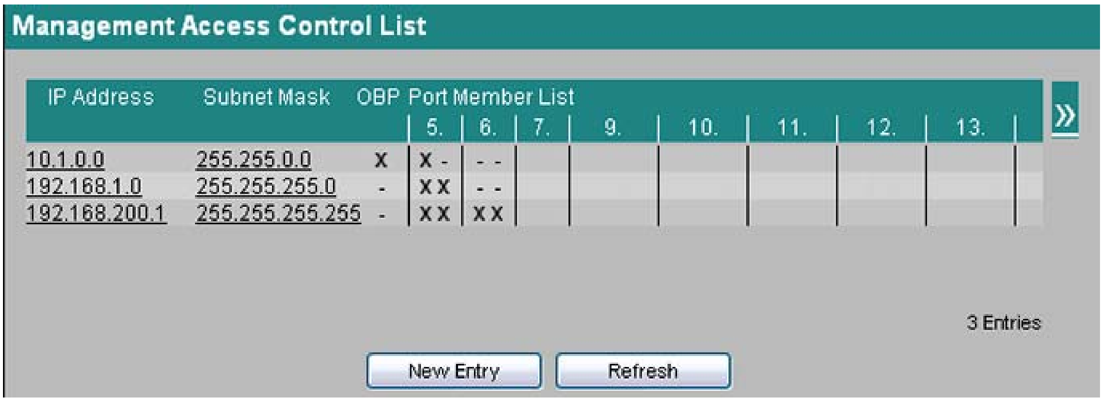


Figure 4-43 Management Access Control List - overview

Note

The option "Out-Band Port Enabled" (OBP) is only available for the SCALANCE X414.

Changing pages

Click on the ">>" and "<<" buttons to page backwards and forwards. On the second page, instead of the ports, you will see any link aggregations that have been set up.

Configuration of the Management Access Control List

NOTICE
Note: A bad configuration may mean that you can no longer access the device. You should therefore configure an access rule allowing you access to the management before you enable the function on the Agent Configuration (Page 77) page.

Access rules

- Access for a host:

  Use a host IP address with the subnet mask 255.255.255.255.
- Access for all hosts of a defined subnet:

  Use a valid combination of IP address and subnet mask.
- Access for all hosts:

  Under IP address and subnet mask, enter 0.0.0.0.

If several rules for access by a host match, the more narrowly defined rule "Best Match" takes effect. If, for example, both the access rule for a single host matches as well as the rule for an entire subnet, the host rule is used.

Creating a new entry

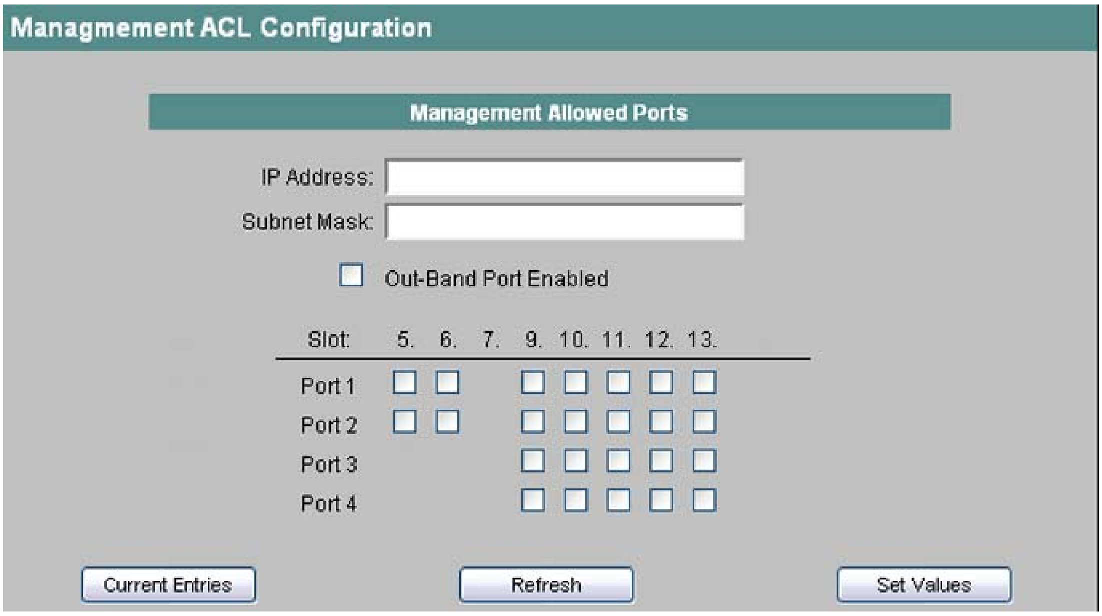


Figure 4-44 Configuration of Management ACL

Follow the steps below to create a new entry:

1. Click the "New Entry" button on the "Management Access Control List" page.
   The page shown above appears.
2. Enter the path cost calculation in the first input box.
3. Enter the subnet mask in the second input box.
4. Only for X414:
   Enable the "Out-Band Port Enabled" option if you want the IP address to access the switch via the out-band port.
5. Enable the ports via which the device may be accessed.
6. Click the "Set Values" button to transfer the information to the device.
7. By clicking the "Current Entries" button, you return to the overview "Management Access Control List".

Editing an existing entry

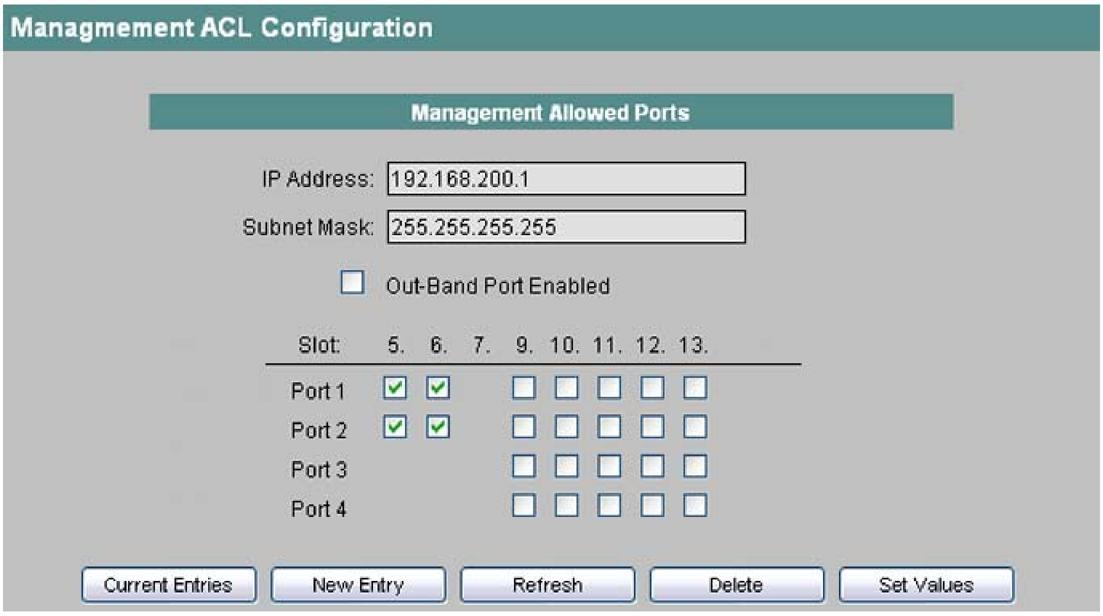


Figure 4-45 Configuration of Management ACL

Follow the steps below to modify an existing entry:

1. Click on the IP address of the entry you want to modify on the "Management Access Control List" page.
   The page shown above appears.
2. Make the changes you require.
3. Click the "Set Values" button to transfer the changed information to the device.
4. By clicking the "Current Entries" button, you return to the overview "Management Access Control List".

Deleting an entry

Follow the steps below to delete an existing entry:

1. Click on the IP address of the entry you want to delete on the "Management Access Control List" page.
   The "Management ACL Configuration" page appears.
2. Click the "Delete" button.
   The entry is deleted and the overview page "Management Access Control List" appears.

Syntax of the Command Line Interface

Table 4- 32 **Management Access Control List - CLI\AGENT\MGMNTACL\>**

Command	Description	Comment
info	Shows the current settings of the Management Access Control List.	
add <IP> <subnet>	Creates a new entry in the Management Access Control List.	Administrator only.
ports <IP> <subnet> <E|D> [ports]	Specifies the ports via which the device may be accessed.	Administrator only.
outband <IP> <subnet> <E|D>	Applies only to the X414: Specifies whether or not the IP address can access the switch via the out-band port.	Administrator only.
delete <IP> <subnet>	Removes an entry from the Management Access Control List.	Administrator only.

4.5 The Switch menu

Introduction

In this menu, you set the parameters for the switch functionality (assign it to layer 2) of the IE switch. This includes the following functions:

- General switch settings such as mirroring, aging, and flow control.
- The filter table for unicast, multicast and broadcast frames.
- The management of multicast groups with IGMP/GMRP.
- The use of the spanning tree protocol.
- Configuration of VLANs and their dynamic configuration with GVRP frames.
- Specifying transfer priorities with CoS to Queue and DSCP to Queue Mapping.
- DCP port filter
- Topology diagnostics with LLDP
- IP address initialization with DHCP relay
- Loop detection
- 1:1 NAT
- Statistics counter for frames per port

4.5.1 Switch Configuration

Protocol settings and switch functionality

The "Switch Configuration" screen appears if you click the "Switch" folder icon. In this screen, you specify which functionality is enabled on the IE switch and which protocols will be used for managing data traffic.

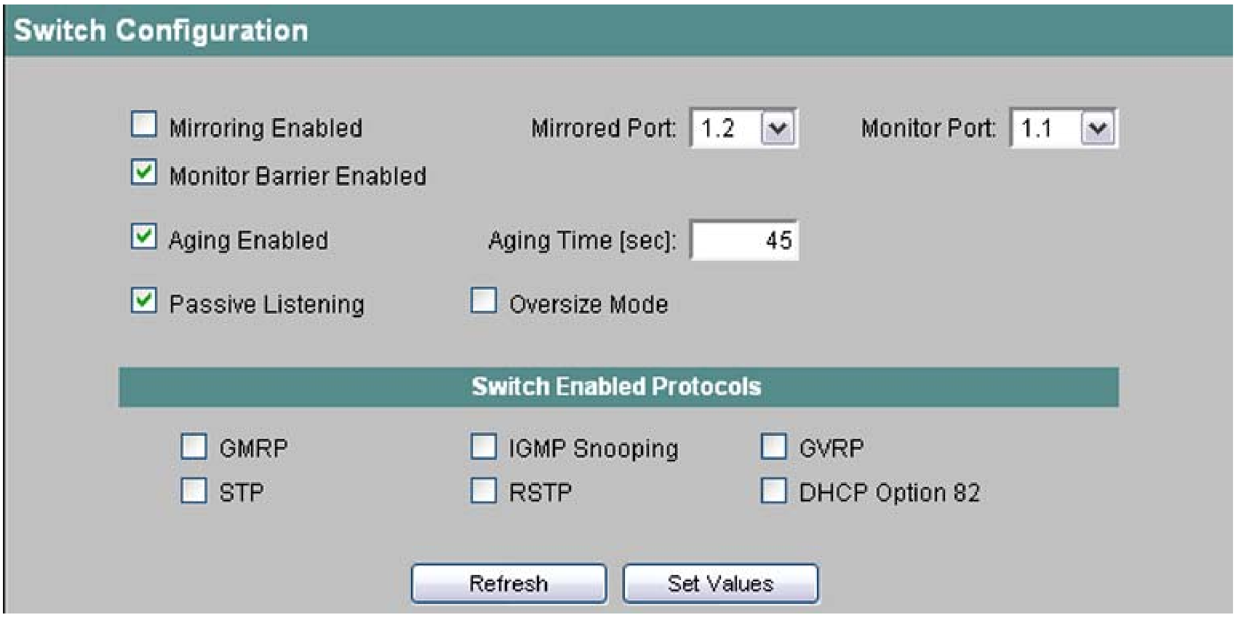


Figure 4-46 Switch Configuration

Mirroring and aging

In the upper part of the page, you can make the following settings:

Mirroring Enabled

Mirroring means that the data traffic of a port (mirrored port) of the IE switch is copied to another port (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 at the mirrored port. This means that the data traffic can be investigated without being affected. This is possible only if a free port is available on the IE switch as the monitor port.

Note

- A ring port cannot be used as a monitor port.
- All ports of an IE switch can be monitored as the mirrored port, however only one port can be selected.
- 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.

Mirrored Port

This is the port whose data traffic is copied to another port.

Select the required port from the drop-down list.

Monitor Port

This is the port to which the data traffic from the mirrored port is copied.

Select the required port from the drop-down list.

Monitor Barrier Enabled

This option is enabled when the module ships.

With this check box, you can restrict communication via the monitor port. If the check box is selected, the monitor port is taken out of normal frame switching. Otherwise communication via the monitor port is unrestricted.

Aging Enabled

An IE switch automatically learns the source addresses of the nodes connected to it. This information is used in the IE switch to forward data frames to the nodes specifically involved. This reduces the network load for the other nodes.

If an IE switch 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, an IE switch does not delete learnt addresses automatically.

Aging Time [sec]

Here, you enter the time after which the IE switch deletes an address if it has not received frames with the corresponding sender address.

On the SCALANCE X408-2, the default for the aging time is 30 s. It can be set between 15 and 3825 seconds in 15 s steps. On the SCALANCE X414-3E, the default is 40 s. Any aging time between 10 and 1000000 seconds can be set here.

Passive Listening

If passive listening is enabled, the IE switch can also react to a reconfiguration without being in (R)STP mode. If an RSTP topology change frame is received, the MAC address table for an X414 is deleted within 1 s and for an X408/X-300 in a maximum of 15 s. Spanning tree BPDUs are also forwarded.

Note

In passive listening mode, the IE switch is not compatible with IEEE 802.1d that forbids forwarding of spanning tree BPDUs when not in (R)STP mode.

Oversize Mode

If you select this check box, frames with a size up to 1,632 bytes instead of 1,522 bytes are permitted.

Protocols for managing data traffic

The lower part of the dialog allows you to enable or disable global functions of the IE switch:

GMRP

GMRP is an acronym for GARP Multicast Registration Protocol. GARP itself stands for Generic Attribute Registration Protocol. This is a mechanism for efficient forwarding of multicast frames.

With a GARP Information Declaration (GID), a node can register with the IE switch as recipient for a multicast address. An IE switch sends this registration to its ports in the form of the GARP Information Propagation (GIP) frame. As a result, this address is also known to other switches and they send multicast frames for this address only to ports that have received a registration for this address. This reduces the load caused by multicast frames in the entire network and for nodes that are not registered for a multicast.

If the check box is selected, GMRP registrations are entered in the multicast filter table for all ports and generated automatically.

If the check box is not selected

- an IE switch does not evaluate received GMRP frames.
- an IE switch does not send its own GMRP frames.

IGMP Configuration

IGMP is an acronym for Internet Group Management Protocol. It is an enhancement of the IP protocol and allows the assignment of IP addresses to multicast groups.

An IE switch evaluates IGMP frames from multicast recipients and stores the information obtained in its multicast filter table. Filter entries resulting from IGMP Configuration are indicated as such in the filter table.

If the check box is selected, IGMP entries are included in the filter table and IGMP frames are forwarded accordingly.

Note

GMRP and IGMP cannot operate at the same time.

GVRP

GVRP is an acronym for GARP VLAN Registration Protocol. If you select the check box, GVRP is permitted. In this case, the VLAN to which a port belongs can be set dynamically with GVRP.

STP (Spanning Tree Protocol)

Spanning tree is a method with which loops are prevented in redundant network structures. You can enable or disable spanning tree functionality with the check box. Typical reconfiguration times with spanning tree are between 20 and 30 seconds.

RSTP (Rapid Spanning Tree Protocol)

The Rapid Spanning Tree Protocol (RSTP) is a further development of the Spanning Tree Protocol. The aim of RSTP is to achieve a faster reconfiguration time in the seconds range.

If you select the check box, RSTP is enabled. If a spanning tree frame is detected at a port, this port reverts from RSTP to spanning tree.

Note

When using RSTP, loops involving duplication of frames or frames being overtaken may occur briefly. If this is not acceptable for your application, use other alternative redundancy methods such as HSR or the slower standard spanning tree.

Note

If passive listening is enabled, the IE switch forwards (R)STP configuration frames transparently even when (R)STP is disabled for it. If it recognizes a topology change frame, it reduces the aging time for a limited period so that the node list is updated more quickly.

Once this period has elapsed, the original aging time applies again.

DHCP Option 82

If option 82 is enabled, the IE Switch adds an "Option 82" field to DHCP queries before the queries are forwarded to the DHCP server (assuming the received query has such a field). The "Option 82" field contains information about the localization of the new client in the network.

As the device identifier of the IE switch, you can set either the IP address or the MAC address. The device identifier and the addresses of one or more DHCP servers can be configured in the DHCP Relay Agent Configuration menu item.

Syntax of the Command Line Interface

Table 4- 33 Switch Configuration - CLI\SWITCH>

<table>
<tr><th>Command</th><th>Description</th><th>Comment</th></tr>
<tr><td>info</td><td>Shows the current settings in the Switch menu.</td><td>-</td></tr>
<tr><td>mirror [E|D]</td><td>Enables/disables mirroring.</td><td>Administrator only</td></tr>
<tr><td>m_ports [<mirrored port> <monitor port>]</td><td>Specifies the ports for mirroring. The first parameter specifies the port whose data traffic will be recorded.
The second parameter specifies the port for the protocol monitor.</td><td>Administrator only</td></tr>
<tr><td>barrier [E|D]</td><td>Enables/disables the monitor barrier function</td><td>Administrator only</td></tr>
<tr><td>aging [E|D]</td><td>Enables/disables aging functionality.</td><td>Administrator only
Default value: Enabled</td></tr>
<tr><td>agetime [seconds]</td><td>Specifies the aging time in seconds.</td><td>Administrator only
The default is 30 seconds (applies to the SCALANCE X408-2)
or 40 seconds (applies to the SCALANCE X414-3E).</td></tr>
<tr><td>gmrp [E|D]</td><td>Enables/disables GMRP functionality for all IE switch ports.</td><td>Administrator only</td></tr>
<tr><td>igmp [E|D]</td><td>Enables/disables IGMP functionality for all IE switch ports.</td><td>Administrator only</td></tr>
<tr><td>gvrp [E|D]</td><td>Enables/disables GVRP functionality for all IE switch ports.</td><td>Administrator only</td></tr>
<tr><td>rstp [D|S|R]</td><td>Enables/disables rapid spanning tree functionality for all IE switch ports.
The meaning of the parameters is as follows:
• D
STP/RSTP is disabled.
• S
Enables spanning tree
• R
Enables rapid spanning tree</td><td>Administrator only</td></tr>
<tr><td>opt82 [E|D]</td><td>Enables/disables the DHCP option 82.</td><td>Administrator only.</td></tr>
<tr><td>plisten [E|D]</td><td>Enables/disables passive listening.</td><td>Administrator only</td></tr>
<tr><td>oversize [E|D]</td><td>Enables/disables the oversize mode function</td><td>Administrator only</td></tr>
<tr><td>macl [E|D]</td><td>Enables/disables the Management ACL function</td><td>Administrator only</td></tr>
<tr><td>blkucast [<E|D> [ports]]</td><td>Display/set Unknown Unicast Blocking Mask.</td><td>Administrator only</td></tr>
</table>

Command	Description	Comment
blkmcast [<E|D> [ports]]	Display/set Unknown Multicast Blocking Mask.	Administrator only
blkbcast [<E|D> [ports]]	Display/set Broadcast Blocking Mask.	Administrator only
fastlrn [<E|D> [ports]]	Display/set Fast Learning Configuration.	Administrator only

4.5.2 Port status

Overview of the configuration of the ports

The "Port Status" screen appears if you click the "Ports" folder icon.

The screen shows the configuration for data transfer for all ports of the IE switch (and, if appropriate, for the ports of the extender).

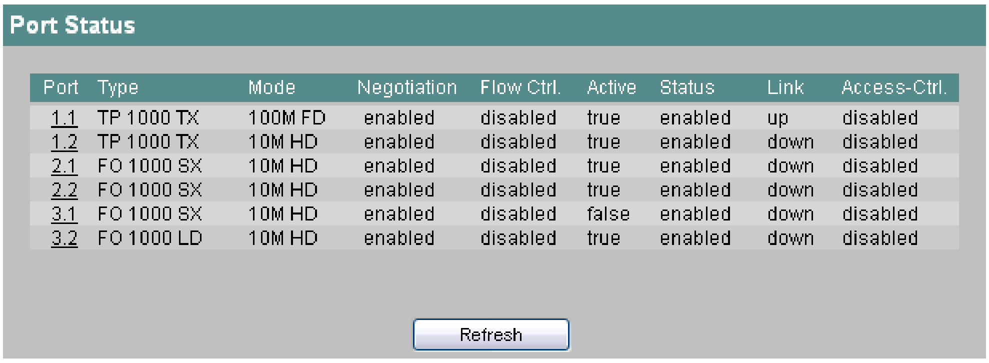


Figure 4-47 Port status

The eight columns of the table display the following information:

Port
This shows the slot and the port to which the following information relates.

Type
Displays the type of port. This information is important because difference modules and therefore different ports can be used in some slots. The following port types are possible:

- TP 100 TX
- FO 100 FX
- FO 100 LD
- FO 100 LH+
- TP 1000 T
- FO 1000 SX
- FO 1000 LD
- FO 1000 LH
- FO 1000 LH+

Mode
The transmission rate (10, 100 or 1000 Mbps) and the transmission mode (full duplex (FD) or half duplex (HD)).

Negotiation
Indicates whether autonegotiation is enabled or disabled.

Flow Ctrl.
Shows whether flow control is enabled or disabled.

Active
Indicates whether or not the port is active (true) or inactive (false). For an inactive port, the communications partner indicates the connection status "Link Down".

Status
Shows whether the port is enabled or disabled. Data traffic is possible only over an enabled port. On the other hand, the communications partner of a port that is turned off indicates the connection status "Link Up".

Note

The "Active" and "Status" states have no influence on the power supply with PoE ports. The configuration of the power supply is separate and is made with the "PoE" menu item.

Link
Status of the link to the network. The following alternatives are possible:

- Up
  The port has a valid link to the network, a link integrity signal is being received.
- down
  The link is down, for example because the connected device is turned off.

Access Control
Shows whether or not the port is locked for unknown MAC addresses. The following statuses are possible:

- enabled:
  A frame with a source address that is not in the address table of the IE switch is discarded. The IE switch switch does not enter the source address of the corresponding node in the address table.
- disabled (default):
  A frame with a source address that is not in the address table of the IE switch is forwarded. The IE switch switch adds the source address of the corresponding node to the address table.

  Note

  "Access Control" is available as of firmware version 2.2 and replaces the former "Lock" function.

Changing the port configuration

Click on the port name in the "Port" column to open the "Port Configuration" page. You can specify how the data transfer is handled over this port.

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:

- Autonegotiation
- Transmission rate
- Transmission mode

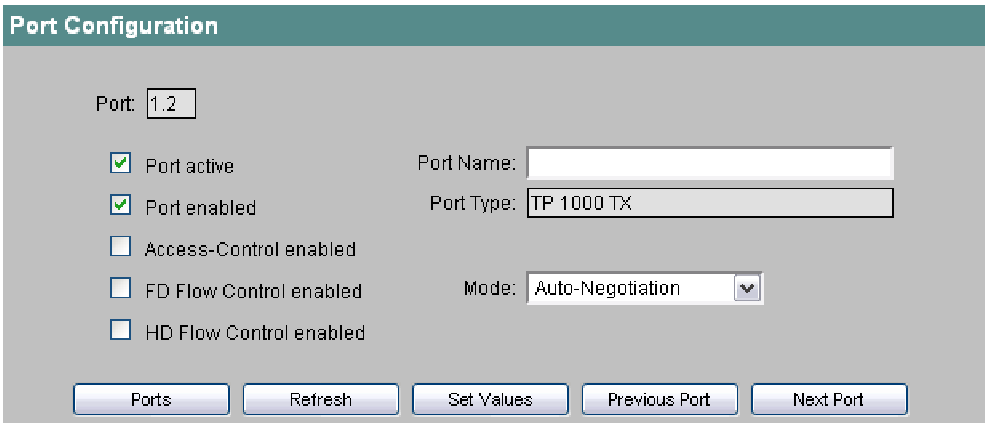


Figure 4-48 Port configuration

Port

Specifies the port and slot whose configuration will be displayed on the page.

Port active

With this check box, you can set the "Link Up" and "Link Down" statuses even for ports that are turned off ("Port enabled" without a check mark). If the check box is selected, the "Link Up" status is indicated to the communication partner even for a port that is turned off.

Port enabled

Select this check box to enable the port for data traffic. If this check box is not selected, the "Link Up" status is indicated to the communications partner of this port anyway. The connection status can be changed with the "Port active" check box.

Access Control enabled

If this check box is selected, the IE switch does not learn unicast addresses at this port.

FD Flow Control enabled

Enables / disables flow control for the full duplex mode. Flow control is, however, only effective if the port operates in full duplex mode. If flow control is enabled but not in effect, the set check mark disappears again after the screen is refreshed; it does not, however, need to be set again if flow control comes into effect.

HD Flow Control enabled
Enables / disables flow control for the half duplex mode. Flow control is, however, only effective if the port operates in half duplex mode.

Note

If the port configuration is set (fixed) to ring ports, correct operation of the redundancy function is no longer possible. For correct operation, the ring ports must be in full duplex mode. It is advisable to set the ring ports to autonegotiation.

Note

With various automatic functions, the IE switch 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 IE switch receives more frames than it can send, for example as the result of different transmission rates.

Mode
In the Mode list box, you can set the transmission speed and duplexity of the port. If you set the mode to autonegotiation, these parameters are automatically negotiated by the IE switch and the connected end device.

Note

Set the mode to autonegotiation if you want to use autocrossover to the partner port.

Port Name
Here, you can enter a name for the port.

Port Type
The type of port is displayed here. You cannot edit this box because the information is hardware-dependent.

Ports
By clicking this button, you return to the table with all ports.

Syntax of the Command Line Interface

Table 4- 34 Port Status - CLI\SWITCH\PORTS>

Command	Description	Comment
info [ports]	Shows the current settings of the ports (actual status) for data traffic.	-
cfg [ports]	Shows the configured settings of the ports (desired status) for data traffic.	-
active [<T|F> [ports]]	Activates (T) or deactivates (F) the specified ports.	Administrator only.
status [<E|D> [ports]	Enables/disables the specified port for data traffic.	Administrator only.
fd_flow [<E|D> [ports]]	Enables/disables flow control in full duplex mode.	Administrator only.
hd_flow [<E|D> [ports]]	Enables/disables flow control in half duplex mode.	Administrator only.
autoneg [<E|D> [ports]]	Enables/disables autonegotiation.	Administrator only.
name <port> [string]	Assigns a name (maximum 64 characters long) for the specified port.	Administrator only.
actrl [<E|D> [ports]]	Enables/disables access control. The "actrl" command replaces the "lock" command as of firmware version 2.2.	Administrator only.
speed [<speed>[ports]]	Specifies the transmission speed and duplicity of the port: • 10H 10 Mbps/half duplex • 10F 10 Mbps/full duplex • 100H 100 Mbps/half duplex • 100F 100 Mbps/full duplex	Administrator only.

4.5.3 Link Aggregation

Bundling network links for redundancy and higher bandwidth

Link aggregation according to IEEE 802.3ad allows several links between neighboring devices to be bundled to achieve higher bandwidths and protection against failure.

Ports on both partner devices are included in link aggregation 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.

Note

The ports bundled into a link aggregation are considered as virtual ports (for example PLC1) and can be used in CLI commands instead of the individual port numbers.

Procedure for configuring link aggregations

1. First, identify the ports you want to put together to form a link aggregation.
2. Configure the link aggregation on both devices.
3. Then run the cabling.

NOTICE
If you cable aggregated links **prior** to configuration, it is possible that you will create loops in the network!

Master Port

The master port of a link aggregation is the port that passes on its settings and even its MAC address to the entire link aggregation.

If you do not configure a master port when you create an aggregation, the port with the lowest port number is used as master.

Displaying the configured link aggregations

The menu displays all the configured link aggregations.

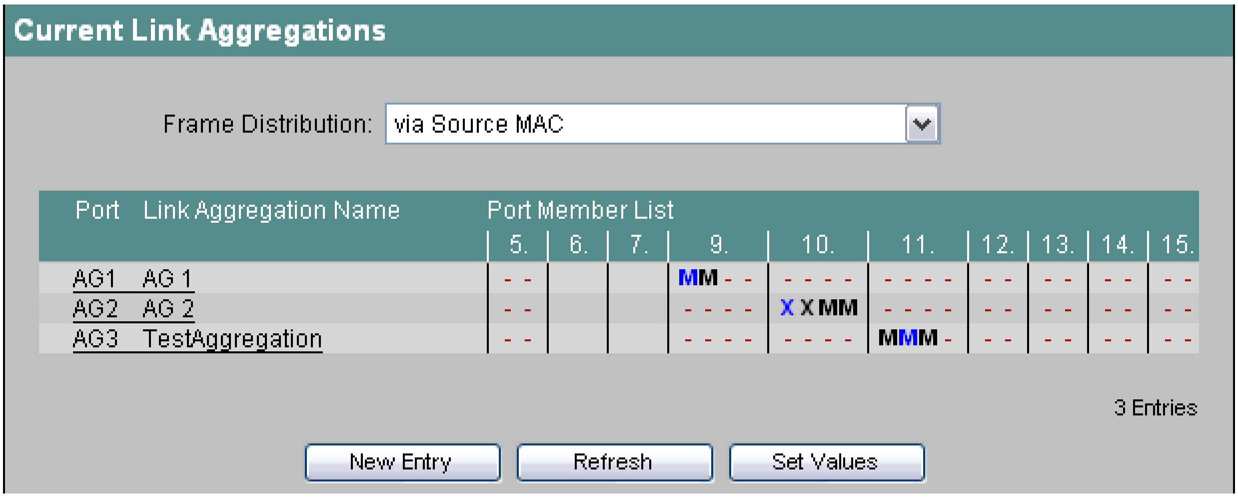


Figure 4-49 Current Link Aggregations

Frame Distribution

Sets the type of distribution of packets on the individual links of an aggregation. Due to hardware restrictions, the possible settings differ on a SCALANCE X-300/408 and a SCALANCE X414.

Port

Shows the virtual port number of this link aggregation. This is assigned internally by the firmware.

Link Aggregation Name

Shows the freely configurable name of the link aggregation. This name can be specified by the user during configuration.

Port Member List

Shows the ports that belong to this aggregation. The meaning is as follows:

- M (black): The port is a member of the aggregation.
- M (blue): The port is a member of the aggregation and is its master port.
- X (black) The port is a member of the aggregation, but is not currently active.
  In this case, port not active means that the port was removed dynamically from the aggregation. The reasons for this may be as follows:
  - Ports of the aggregation have different configurations (for example speed)
  - The port is not connected with the same device
  - The port does not have a link
  - The port was not authenticated according to 802.1x
  - ...
- X (blue) The port is a member of the aggregation and is its master port and is not active.

Note

On a SCALANCE X414-3E, although the gigabit ports 5.1 and 5.2 can be configured with a Fast Ethernet port in an aggregation, they will never be active along with other Fast Ethernet ports, even if they are set to Fast Ethernet.

Creating a new link aggregation

Click the New Entry button to create a new link aggregation. The following screen appears:

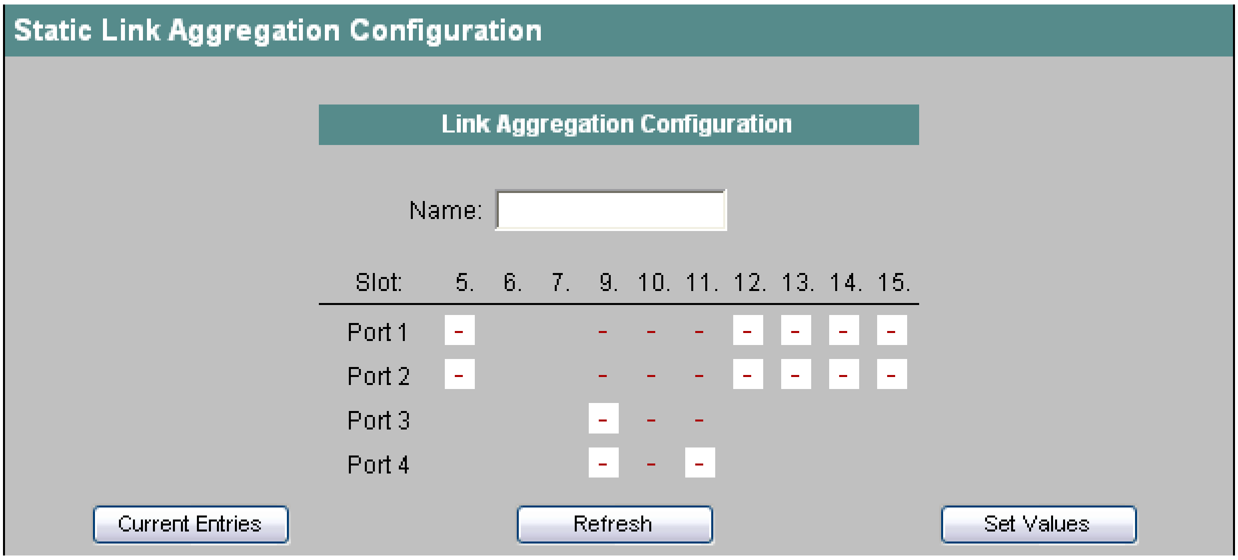


Figure 4-50 Link Aggregation Configuration

Name

Here, you can specify a symbolic name for the new link aggregation. If you do not enter a name here, it is set automatically by the system.

Slot / Port

Here, you can add certain ports to the new aggregation. You can only add ports that are not members of another link aggregation.

The meaning is as follows:

- M (black): The port is a member of the aggregation.
- M (blue): The port is a member of the aggregation and is its master port.

Changing a link aggregation

In the Current Link Aggregation overview screen, click on the Port column or Link Aggregation Name to change the configuration of an existing link aggregation.

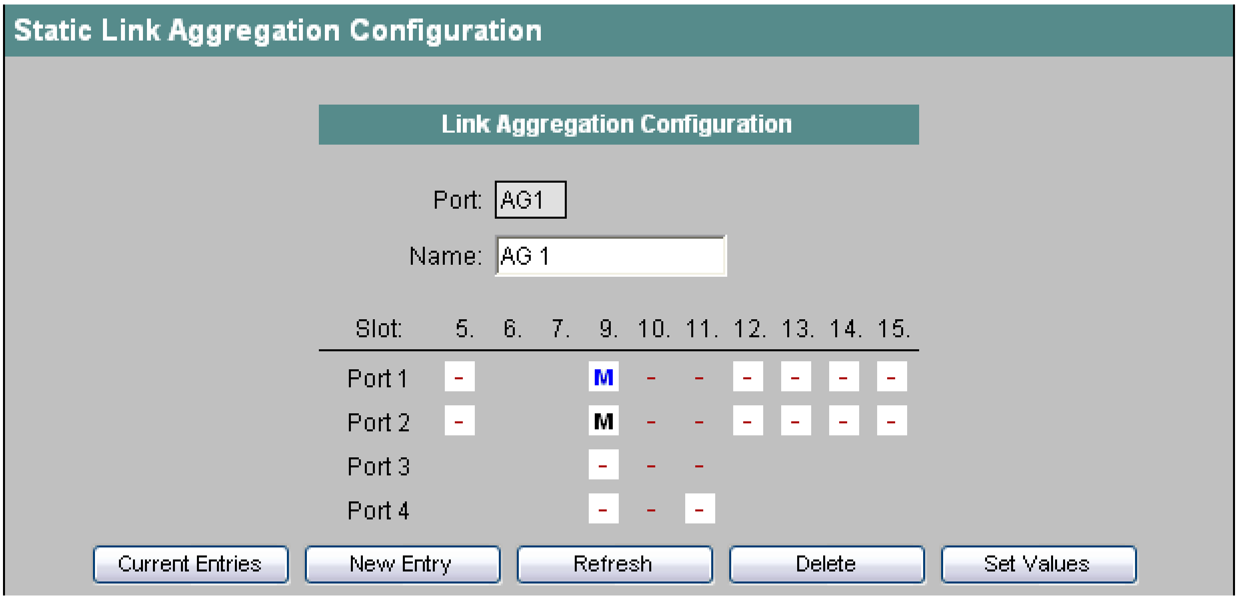


Figure 4-51 Static Link Aggregation Configuration

Port

Displays the virtual port number of the aggregation. This is assigned internally by the system and cannot be modified.

Name

Here, you can change the name of the link aggregation.

Slot / Port

You have the option of adding specific ports to the link aggregation or removing them from it. You can only modify ports that are not members of another link aggregation.

The meaning is as follows:

- M (black): The port is a member of the aggregation.
- M (blue): The port is a member of the aggregation and is its master port.

Changing the master port

To change the master port, follow the steps below:

1. Click on the original master port (blue M) - the marking disappears. If you want to keep the port in the aggregation, click on it a second time (black M)
2. Click on the new master port until a blue M appears.

Syntax of the Command Line Interface

Current Link Aggregation - CLI\SWITCH\LAG>

Command	Description	Comment
info	Shows the current settings of the link aggregation group (actual status).	-
frmdistr [mode]	Sets the type of distribution of packets on the individual links of an aggregation. The following modes exist for X414: • srcmac source MAC address • dstmac destination MAC address • mac source and dest. MAC address • srcip source IP address • dstip destination IP address • ip source and dest. IP address) The following modes exist for X408/X-300: • hash source and dest. MAC address hash • xor source and dest. MAC address Xor	Administrator only.
add <masterport>	Creates a new link aggregation with the specified master port	Administrator only.
master <ID> <masterport>	Changes the master port of a link aggregation.	Administrator only.
name <ID> <string>	Changes the name of a link aggregation.	Administrator only.
ports <ID> <option> [ports]	Changes the members (ports) of a link aggregation - except for the master port. The following options are possible: • - The port is not a member of the link aggregation. • M The port is a member of the link aggregation.	Administrator only.
delete <ID>	Deletes a link aggregation.	Administrator only.

4.5.4 LACP Configuration

Enabling LACP functionality

The LACP (Link Aggregation Control Protocol) handles the selection of the active ports of a link aggregation. You can enable LACP for every link aggregation.

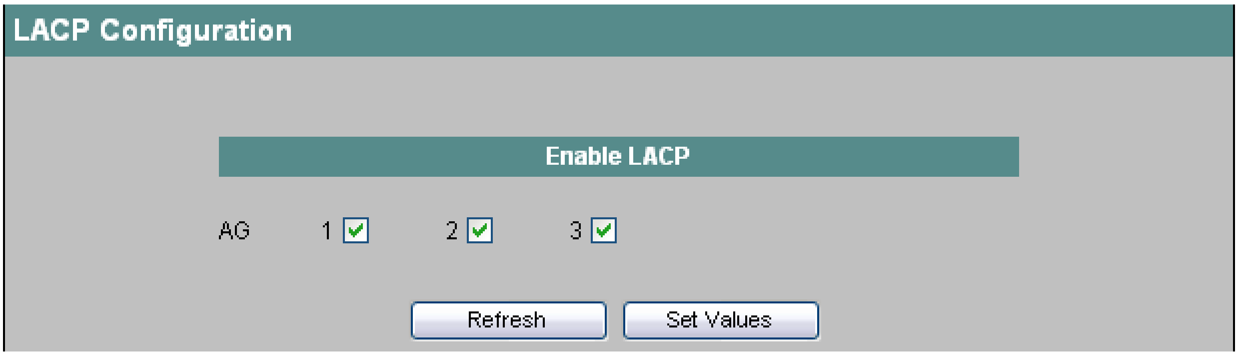


Figure 4-52 LACP Configuration

Enable LACP

Here, you enable LACP.

If LACP is disabled on both systems, all the ports configured in the aggregation become active.

Syntax of the Command Line Interface

Table 4- 35 LACP Configuration - CLI\SWITCH\LAG>

Command	Description	Comment
lacp [<E|D> [IDs]]	Enables/disables LACP for all ports of the specified link aggregation.	Administrator only.

4.5.5 802.1x RADIUS Configuration

Authentication over an external server

The concept of RADIUS is based on an external authentication server. This allows access to the network via the IE switch to be restricted for end devices. First specify the RADIUS server for the authentication procedure on the page "802.1x RADIUS Configuration", see figure below.

Then specify the end devices for which authentication should be performed on the page "802.1x Authenticator Configuration" based on the port number.

Both the end device and the authentication server must support the EAP protocol (Extensive Authentication Protocol).

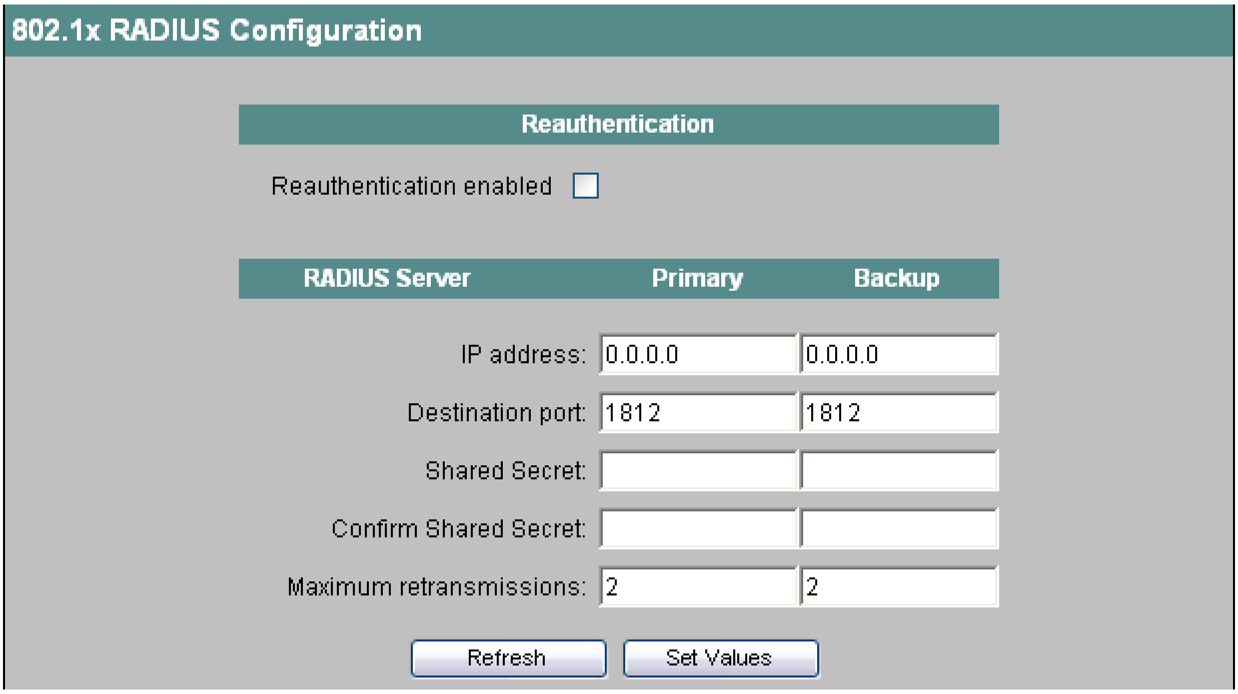


Figure 4-53 802.1x RADIUS Configuration

Reauthentication

The switch can repeat the authentication with the RADIUS server at regular intervals of 1 hour.

Enable or disable the function by clicking the "Reauthentication enabled" check box.

RADIUS Server

You can enter the data for two RADIUS servers; the information in the "Backup" column is used if the server defined in the "Primary" column is not available.

RADIUS server for "Login Mode"

The RADIUS server specified here serves at the same time as the authentication server for the login modes "RADIUS and Local" and "RADIUS", see section System Passwords & Login Mode (Page 47).

Syntax of the Command Line Interface

Table 4- 36 CLI\SWITCH\DOT1X\RADIUS>

Command	Description	Comment
info	Displays the current RADIUS settings.	-
server [<ip>[:port]]	Specifies the IP address and port of the primary RADIUS server.	Administrator only.
serverb [<ip>[:port]]	Specifies the IP address and port of the backup RADIUS server.	Administrator only.
secret <string>	Specifies the password for the primary RADIUS server.	Administrator only.
secretb <string>	Specifies the password for the backup RADIUS server.	Administrator only.
maxreq [number]	Maximum number of requests to the primary RADIUS server.	Administrator only.
maxreqb [number]	Maximum number of requests to the backup RADIUS server.	Administrator only.
reauth [E|D]	Enables / disables reauthentication functionality.	Administrator only.

4.5.6 802.1x Authenticator Configuration

Enabling the authenticator

Based on the port number, specify the end devices for which an authentication procedure should be performed via the RADIUS server.

Click the check box of the relevant port to enable or disable.

As default, the authenticator is not enabled for any port.

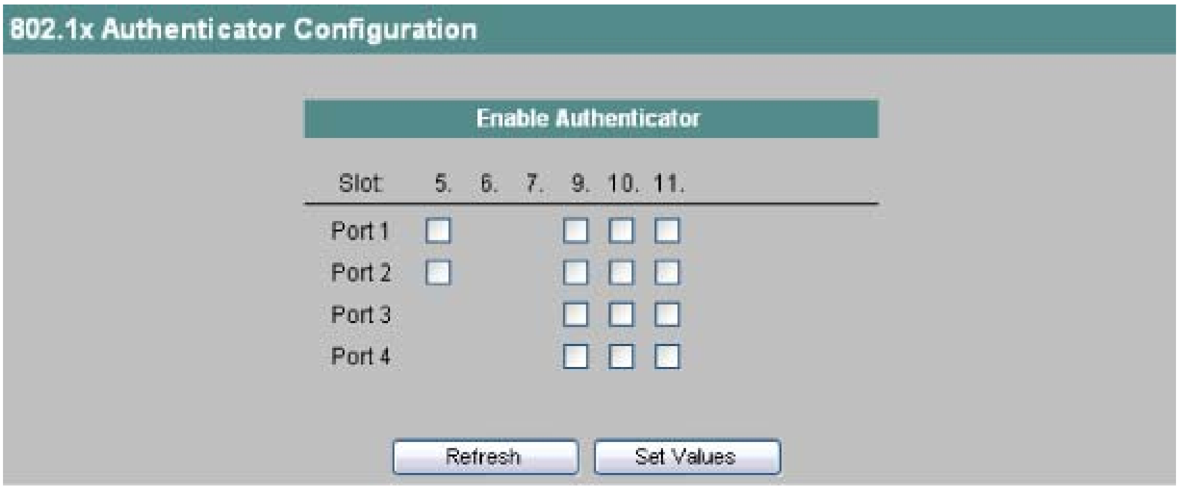


Figure 4-54 802.1x Authenticator Configuration

Syntax of the Command Line Interface

Table 4- 37 802.1x Authenticator Configuration - CLI\SWITCH\DOT1X\AUTH>

Command	Description	Comment
info	Displays the current authenticator settings.	-
ports [<E|D> [ports]]	Enables/Disables the authenticator for the specified ports. If you do not specify any ports, the authenticator is enabled/disabled for all ports.	Administrator only.

4.5.7 Current Unicast Filter (Access Control List)

Address filtering

This menu displays the current content of the 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.

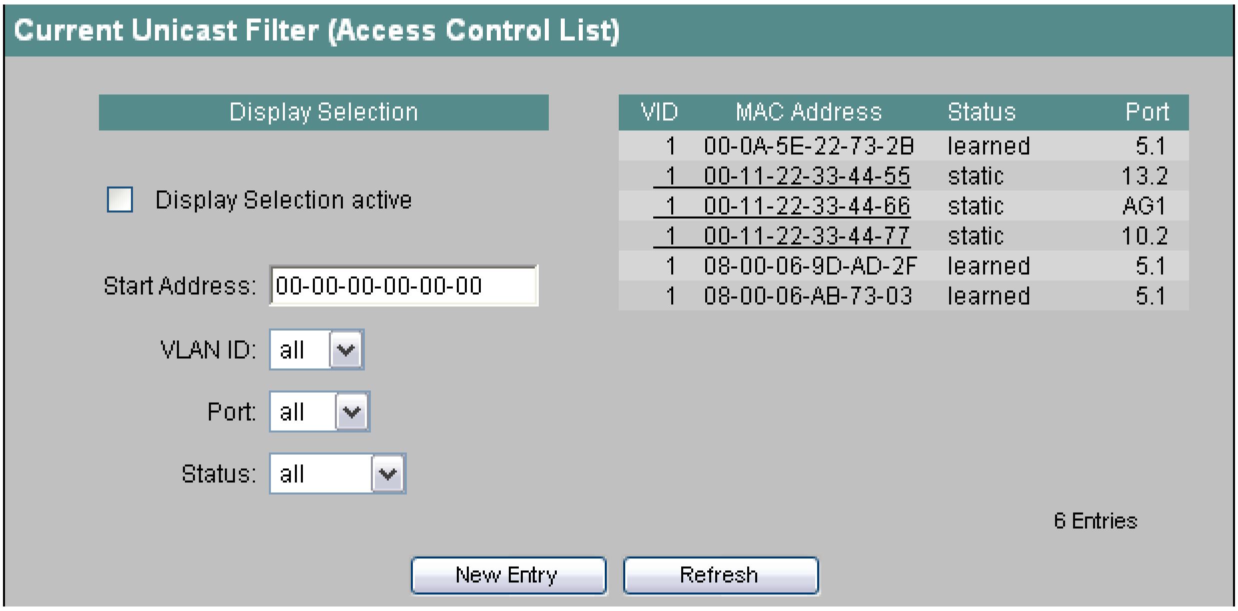


Figure 4-55 Current Unicast Filter

Selecting the displayed addresses

Display Selection active
The display is only restricted to selected elements when this check box is selected, otherwise all addresses are displayed.

Start Address
This parameter specifies the address in the filter table starting at which stored MAC addresses are displayed. If nothing is entered here, the display begins at the VLAN ID. If you enter a specific value here, only addresses with a corresponding VLAN ID are displayed. Valid values for a VLAN ID are between 1 and 4096. If you do not want to make a selection for the VLAN ID, select the "all" entry.

Port
Here, you can restrict the display to addresses of nodes at particular ports. If you select the "all" entry, addresses at all ports are displayed.

Status
With this list box, you can restrict the display to addresses that have a particular status. Possible values for the status are as follows:

- learned (learned addresses)
- static (configured by the user)
- all (learned addresses and configured addresses)

Access Control List

Unicast filters can be used for access control. With the aid of the Access Control function (as of firmware version 2.2 - the function was previously called Lock!) for individual ports (see "Access Control Port Configuration menu item" or "the Port Status menu"), individual ports can be locked for unknown nodes. If the Access Control function is enabled on a port, packets arriving from unknown MAC addresses are discarded immediately.

Since ports with Access Control enabled cannot learn any MAC addresses, learned addresses on these ports are automatically deleted after Access Control is enabled. To include a device in the list of known nodes, a unicast entry must be created (on the relevant port) for its MAC address.

To enter all connected nodes automatically, there is a function for automatic learning (see section ACL Learning menu item).

Information in the filter table

The four columns of the filter table show the following information:

- **VID**
  The VLAN-ID assigned to this MAC address. If no VLAN-ID is assigned to a MAC address, 1 is displayed here
- **MAC Address**
  The MAC address of the node that an IE switch has learned or the user has configured.
- **Status**
  Shows the status of each address entry. Here, learned means that the specified address was learned as a result of receiving a frame from this node. The static entry means that 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 switch is restarted. Invalid means that these value are not evaluated by the SCALANCE X408. These values were entered via Web Based Management without a port number.
- **Port**
  Specifies the slot and port over which the node with the specified address can be reached. Frames received by the IE switch whose destination address matches this address will be forwarded to this port.

Configuring a filter

Clicking on a MAC address with the *static* status opens the page for configuring the filters:

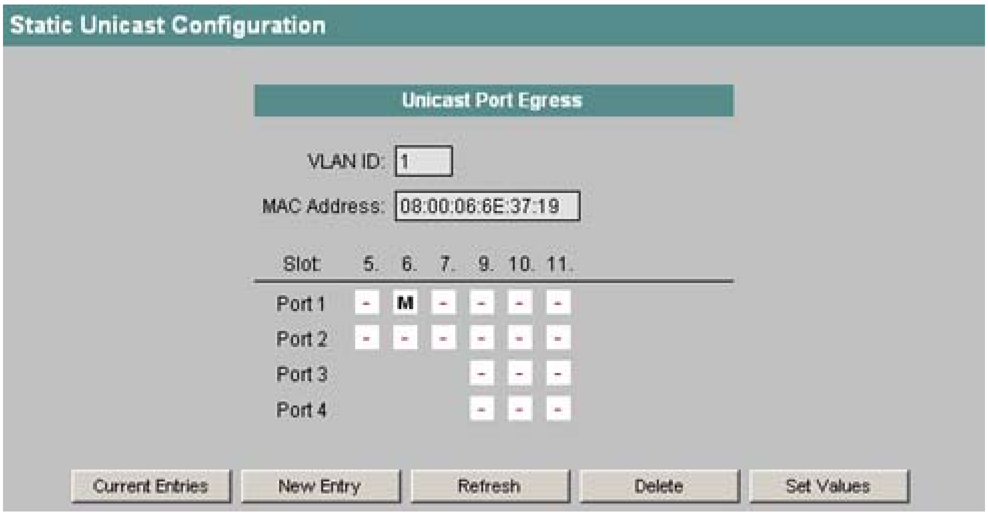


Figure 4-56 Static Unicast Configuration

Slot / Port

Select the slot and the port to which the frames with the entered destination address will be forwarded. After clicking on the appropriate box, status information is displayed and has the following meaning:

- M
  (Member) Unicast frames are sent over this port.
- –
  Unicast frames are not forwarded via this port.
- #
  The port is invalid.
- ?
  The VLAN configuration contradicts the unicast configuration. This can occur when a destination port was selected in the unicast configuration that does not belong to the VLAN.

Creating a new entry

Click on the "New Entry" button to add an entry to the address table. The "Static Unicast Configuration" page opens in which you can make the necessary entries:

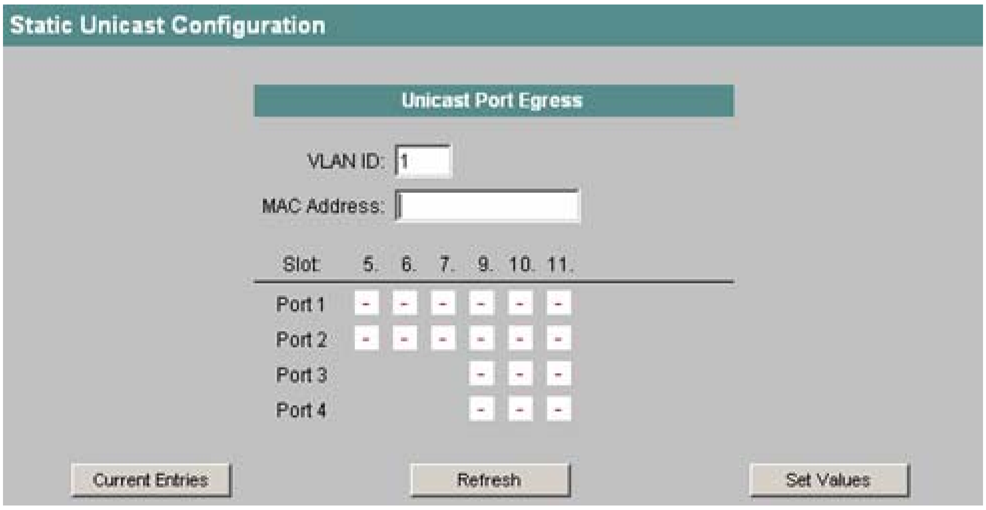


Figure 4-57 Static Unicast Configuration II

VLAN ID
Enter the ID of the VLAN to which the MAC address belongs. If nothing is set, the VLAN ID 1 (default VLAN) is set as the basic setting.

MAC Address
Enter the MAC address you want to add to the address table. This address matches the target address of a received frame.

Slot / Port
Select the slot and the port to which the frames with the entered destination address will be forwarded. After clicking on the appropriate box, "M" appears.

Invalid ports are marked with "#". If a port is marked with "?", the VLAN configuration contradicts the unicast configuration.

Note

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

Current Entries
By clicking this button, you return to the list of MAC addresses.

New entry
Click this button to create a new entry in the filter table.

Delete
Click this button to delete the displayed entry from the filter table.

Syntax of the Command Line Interface

Table 4- 38 Current Unicast Filter - CLI\SWITCH\UCAST>

Command	Description	Comment
info	Shows the content of the address table of an IE switch.	-
find [VLAN-ID]<MAC address> [S|L] [port]	Searches for a MAC address in the address table of an IE switch. You can also see the ports to which a received frame with this (destination) address is sent. If you do not specify a VLAN-ID, all VLANs are browsed for the specified MAC address. As an option, you can also specify a port. Browsing is then restricted to the specified port. As a further option, you can also restrict browsing to static and learned entries: • S Static entries • L Learned entries	-
add [VLAN-ID]<MAC address> <port>	Inserts a static entry for a unicast address in the address table.	Administrator only.
edit [VLAN-ID] <MAC address> <port>	Changes an entry in the address table.	Administrator only.
delete [VLAN-ID] <MAC address>	Deletes a static entry from the address table.	Administrator only.

4.5.8 Access Control List Learning

Start Learning / Stop Learning

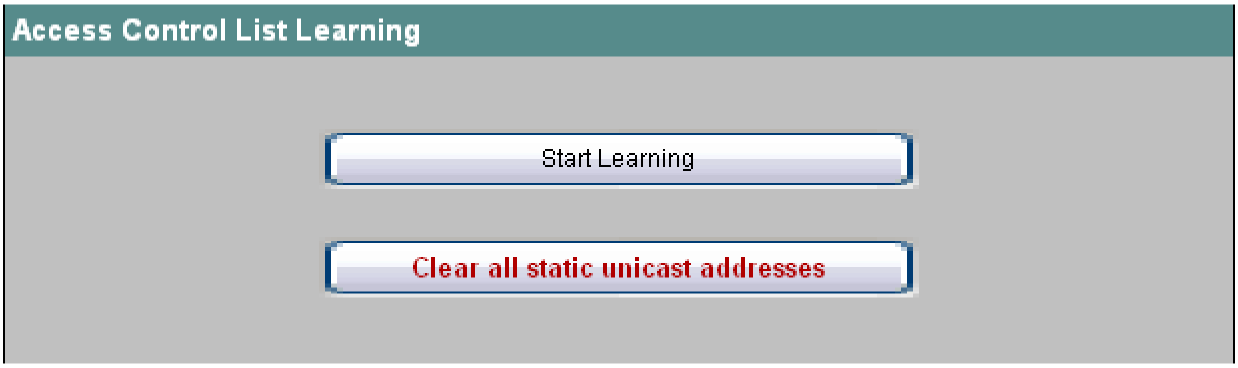


Figure 4-58 Access Control List Learning

With the aid of the automatic learning function, all devices connected to the IE switch can be entered automatically in the Access Control List (see section "Current Unicast-Filter (Access Control List) menu item)". As long as this function is enabled, all learned unicast addresses are created immediately as static unicast entries. Learning stops only after selecting on Stop Learning. 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 can be found.

By enabling the Access Control function, the only packets accepted on the relevant ports are those from nodes known on completion of the learning phase (static unicast entries).

Note

If the Access Control 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. If you do not want a port to learn addresses, simply enable access control on it before enabling learning.

Clear all static unicast addresses

In large networks with lots of nodes, automatic learning may lead to a large number of unwanted 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.

Syntax of the Command Line Interface

Table 4- 39 Access Control List Learning - CLI\SWITCH\UCAST>

Command	Description	Comment
learning [start|stop]	No parameter Displays the current status of the automatic learning. • start Starts automatic learning. • stop Stops automatic learning.	Administrator only.
clear	Deletes all static unicast entries.	Administrator only.

4.5.9 Access Control Port Configuration

Enabling the Access Control function

By selecting the relevant options, you specify whether or not Access Control is enabled for each individual port. If the function is enabled for a port, packets from unknown MAC addresses are discarded immediately. Only packets from known nodes (see Current Unicast Filter (Access Control List) menu item) are accepted.

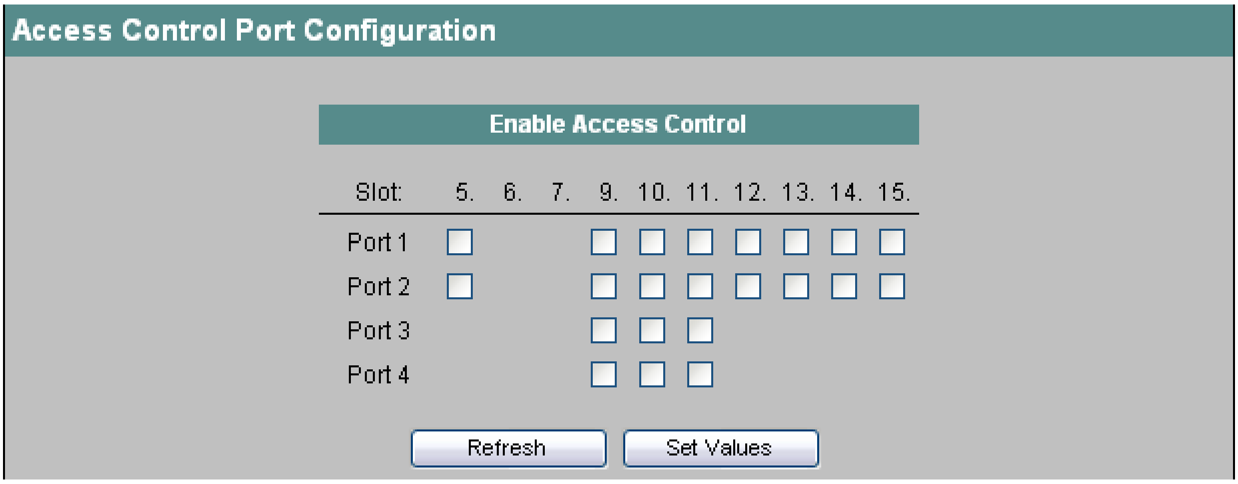


Figure 4-59 Access Control Port Configuration

Syntax of the Command Line Interface

Table 4- 40 Access Control Port Configuration - CLI\SWITCH\UCAST>

Command	Description	Comment
actrl [<E|D> [ports]]	Enables/Disables the Access Control function for the specified ports. If you do not specify any ports, Access Control is enabled/disabled for all ports.	Administrator only.

4.5.10 Unknown Unicast Blocking Mask

Disabling the forwarding of unknown unicast frames

In this menu, you can disable the forwarding of unknown unicast frames for individual ports.

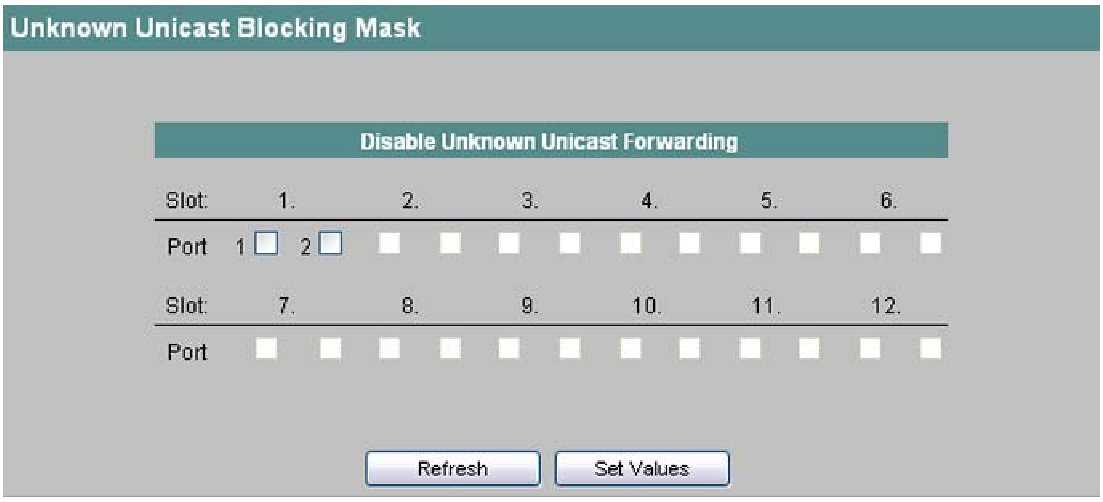


Figure 4-60 Unknown Unicast Blocking Mask

Disable Unknown Unicast Forwarding

Here, you specify the ports for which the forwarding of unknown unicast frames will be disabled.

Syntax of the Command Line Interface

Table 4- 41 Unknown Unicast Blocking Mask - CLI\SWITCH\>

Command	Description	Comment
blkucast [<E|D> [ports]]	Enables/disables the blocking of unicasts on the specified ports.	Administrator only.

4.5.11 Current Multicast 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 the senders of unicast frames, multicast frames produce a higher load for a switch. Generally, multicast frames are sent to all ports of a switch. 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 Groups" menu item, shows the multicast frames currently entered in the filter table and their destination ports. The entries can be dynamic (an IE switch has learned them) or static (the user has set them).

Note

If the filter table for a SCALANCE X414-3E contains more than 500 learned entries, the reconfiguration time in redundant networks can be longer than 300 milliseconds with HSR or 200 milliseconds with MRP.

Changing pages

Click on the ">>" or "<<" buttons to page backwards and forwards.

On the second page, instead of the ports, you will see any link aggregations that have been set up.

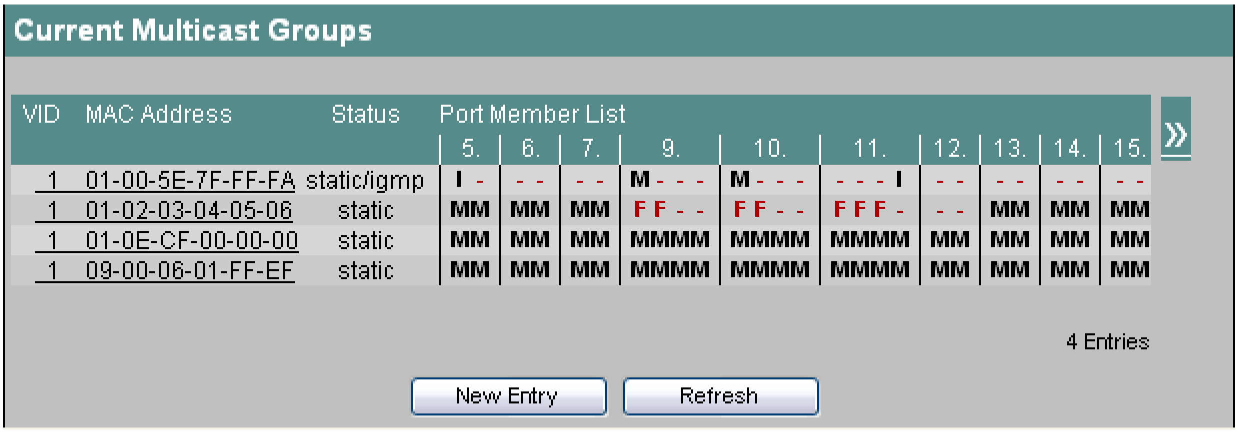


Figure 4-61 Current Multicast Groups

Information in the filter table

The four areas of the filter table show the following information:

VID
The VLAN-ID assigned to this MAC address.

MAC Address
The MAC address of the node that the IE switch 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 switch is restarted.
- 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:

- M
  (Member) Multicast frames are sent via this port.
  M (in red)
  Multicast is configured in a VLAN that is, however, not configured on the relevant port. Due to the different VLAN-ID, the multicast cannot be forwarded 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 will be sent over this port.
- F
  (Forbidden) Not a member of the multicast group. Moreover, this address must not be an address learned dynamically with GMRP or IGMP.

Creating a new entry

Click on the "New Entry" button to add an entry to the address table. The Static Multicast Configuration page opens in which you can make the necessary entries:

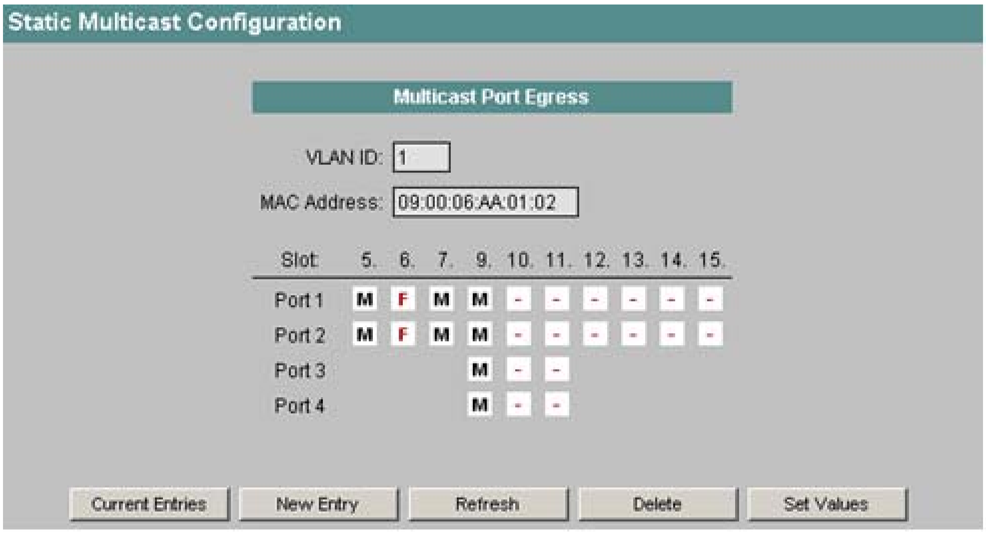


Figure 4-62 Static Multicast Configuration

VLAN ID
Enter the ID of the VLAN to which the MAC address belongs. If nothing is set, the VLAN ID 1 is set as the basic setting.

MAC Address
Enter the MAC address you want to add to the address table.

Slot / Port
Here, select how a port should respond to multicast frames:

- M
  Member, multicast frames are sent over this port.
- –
  Not a member of the multicast group. No multicast frames are sent via this port.
- F
  Forbidden, not a member of the multicast group. Moreover, this address may not be an address learned dynamically with GMRP.

- #
  The port is invalid.
- ?
  The port is not a member in the specified VLAN.

Note

For multicast addresses, you can specify more than one port (destination node).

Current Entries
By clicking this button, you return to the list of MAC addresses.

New entry
Click this button to create a new entry in the filter table.

Delete
Click this button to delete the displayed entry from the filter table.

Changing an address entry

Click on a MAC address with the "static" status (underscored in the address list) to open the "Static Multicast Configuration" page for this address. Make the settings you require and confirm your entries by clicking the "Set Values" button.

Syntax of the Command Line Interface

Table 4- 42 Current Multicast Groups - CLI\SWITCH\MCAST>

Command	Description	Comment
info	Shows the content of the address table of an IE switch.	-
add <VLAN-ID> <MAC address> [<option> [ports]]	Inserts a static entry for a multicast address in the address table. The following abbreviations are available for the <option> parameter: • – Not a member of the multicast group. No multicast frames are sent via this port. • m Multicast frames are sent via this port. • f Not a member of the multicast group. Moreover, this address may not be an address learned dynamically with GMRP. Examples: • add 2 01:02:03:04:05:06 m 5.1-5.2 Assigns the MAC address of the VLAN-ID 2 and ports 5.1 and 5.2 are members. • add 3 01:02:03:04:05:06 m Creates an entry for VLAN-ID 3, all existing ports are members.	Administrator only.
find [VLAN-ID] <MAC address>	Searches for a MAC address in the address table of an IE switch. You can also see the ports to which a received frame with this (destination) address is sent. If you do not specify a VLAN-ID, all VLANs are browsed for the specified MAC address.	-
edit <VLAN-ID> <MAC address> <option> [ports]	Changes an entry in the address table. For the <option> parameter, the same abbreviations area available as for the add command.	Administrator only.
delete <VLAN-ID> <MAC address>	Deletes a static entry from the address table.	Administrator only.

4.5.12 GMRP Configuration

Enabling 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.

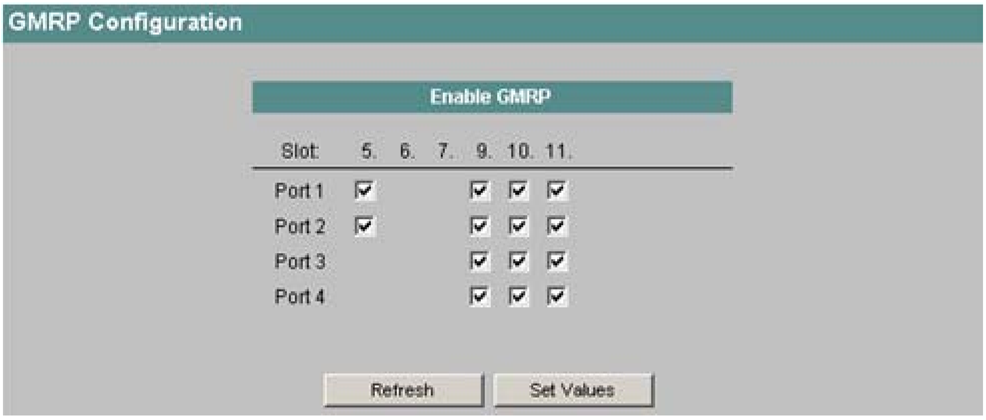


Figure 4-63 GMRP Configuration

Syntax of the Command Line Interface

Table 4- 43 GMRP Configuration - CLI\SWITCH\MCAST>

Command	Description	Comment
gmrpport [<E|D> [ports]]	Enables/Disables GMRP functionality for the specified ports. If you do not specify any ports, GMRP is enabled/disabled for all ports.	Administrator only.

4.5.13 IGMP Configuration

Specifying the 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; port-specific configuration is not possible in this case.

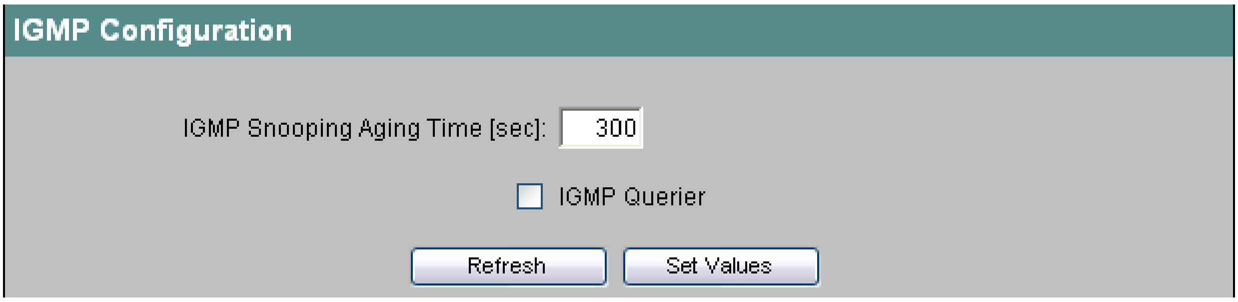


Figure 4-64 IGMP Configuration

IGMP Snooping Aging Time [sec]
Here, you enter a time in seconds for the aging time.

IGMP Querier
Enable this option if you want the IE switch to send IGMP queries as well.

Syntax of the Command Line Interface

Table 4- 44 IGMP Configuration - CLI\SWITCH\MCAST\IGMP>

Command	Description	Comment
igmptime [number]	Specifies the IGMP aging time in seconds. Without parameters, this command displays the IGMP aging time.	Administrator only.
igmpqry [E|D]	Displays/sets IGMP Query Enable	Administrator only.

4.5.14 Broadcast Blocking Mask

Blocking the forwarding of broadcast frames

In this menu, you can block the forwarding of broadcast frames for individual ports.

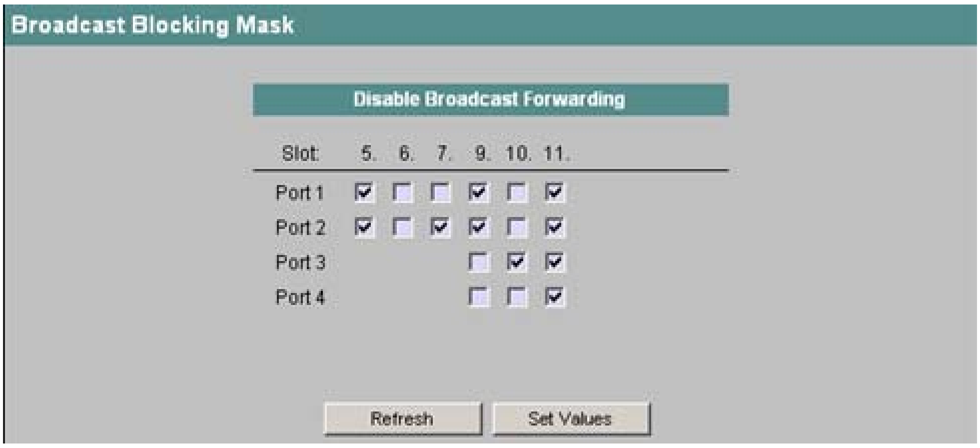


Figure 4-65 Broadcast Blocking Mask

Disable Broadcast Forwarding
Here, you specify the ports for which the forwarding of broadcast frames will be blocked.

Note

Some communication protocols work only with the support of broadcast. In these cases, blocking can lead to loss of data communication. Only make entries here when you are sure that you do not need broadcast and explicitly want to avoid it.

Syntax of the Command Line Interface

Table 4- 45 Broadcast Blocking Mask - CLI\SWITCH\>

Command	Description	Comment
blkbcast [<E|D> [ports]]	Enables/Disables the blocking of broadcasts on the specified ports.	Administrator only.

4.5.15 Unknown Unicast Blocking Mask

Disabling the forwarding of unknown multicast frames

In this menu, you can disable the forwarding of unknown multicast frames for individual ports.

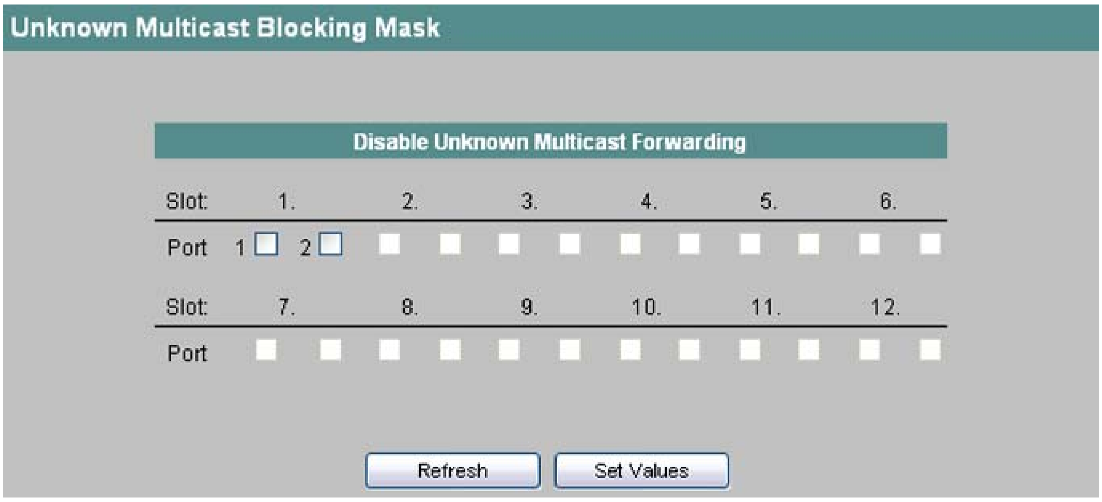


Figure 4-66 Unknown Unicast Blocking Mask

Disable Unknown Multicast Forwarding

Here, you specify the ports for which the forwarding of unknown multicast frames will be disabled.

Syntax of the Command Line Interface

Table 4- 46 Unknown Multicast Blocking Mask - CLI\SWITCH\>

Command	Description	Comment
blkbmcast [<E|D> [ports]]	Enables/Disables the blocking of multicasts on the specified ports.	Administrator only.

4.5.16 Fast learning

With Fast Learning, the MAC addresses learned dynamically at a port are deleted from the address table immediately as soon as there is a link down at the relevant port, for example by replugging an end device. This means that the switch recognizes whether or not a port assignment is valid more quickly than normally.

Fast Learning is specified for each port individually.

Configuration of the ports

In the dialog shown below, click the relevant check boxes of the ports at which Fast Learning will be enabled.

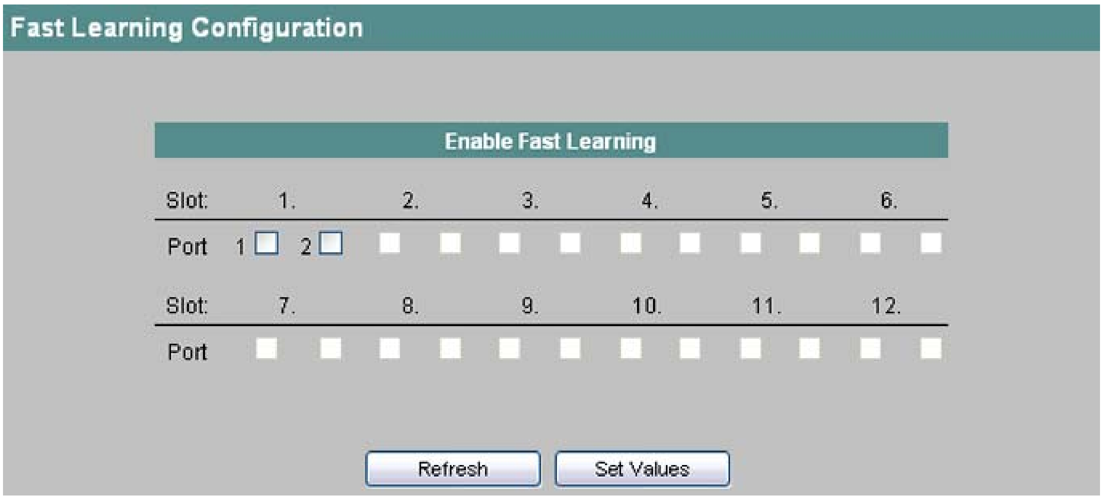


Figure 4-67 Configuration for "Fast Learning"

Syntax of the Command Line Interface

Table 4- 47 Fast Learning Configuration - CLI\SWITCH\>

Command	Description	Comment
fastlrn [<E|D> [ports]]	Enables/disables Fast Learning at the relevant port.	Administrator only.

4.5.17 Load Limits Configuration (SCALANCE X414-3E)

Limiting the number of incoming frames

In this dialog, you can specify the maximum number of packets received from one port per second. Due to hardware considerations, several ports are grouped together in a port block. The set values (packets [s]) are, however, valid per port. You can specify the category of frame for which the entered limit values will apply:

- Unicast (destination lookup failure)
- Multicast
- Broadcast

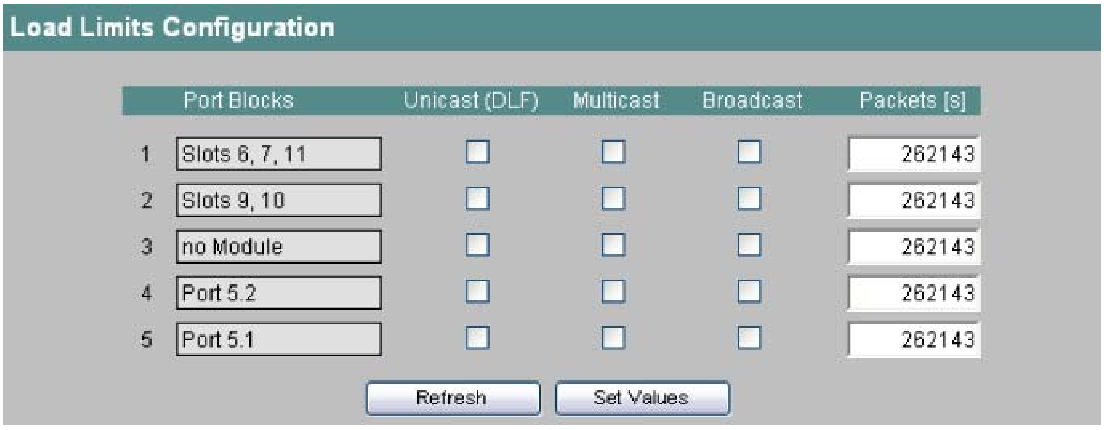


Figure 4-68 Load Limits Configuration

Port Blocks
The ports are assigned to the following port blocks; the settings apply to all ports of a port block:

- Portblock 1
  The ports on slots 6, 7, and 11.
- Portblock 2
  The ports on slots 9 and 10.
- Portblock 3
  No module.
- Portblock 4
  Port 2 on slot 5.
- Portblock 5
  Port 1 on slot 5.

This column only lists the slots actually being used. The text boxes are read-only.

Unicast (DLF), Multicast, Broadcast
The maximum number of packets per second applies to the packet categories whose check box is selected.

Packets [s]
The maximum number of packets that a port block receives per second. Packets that exceed this limit value are discarded.

Note

The ring ports send multicast frames at cyclic intervals to detect line breaks. For port blocks that contain ring ports, you should therefore not limit the receipt of multicast frames to ensure that the redundancy manager functions correctly.

Syntax of the Command Line Interface

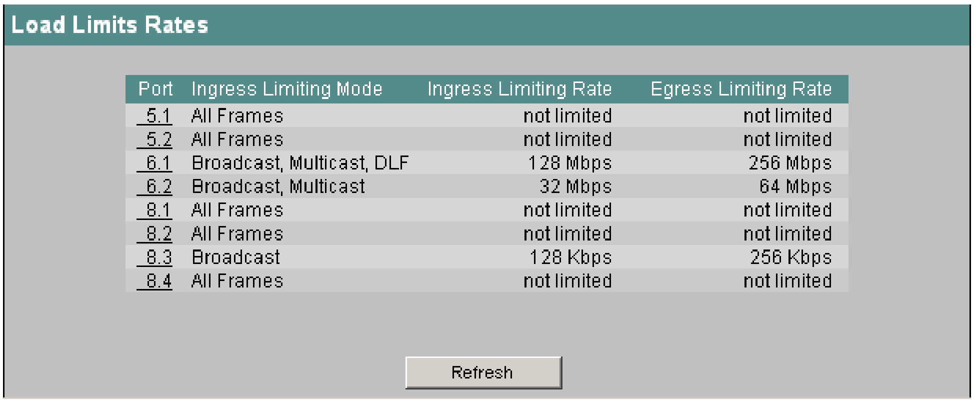
Table 4- 48 Load Limits Configuration - CLI\SWITCH\LIMITS>

Command	Description	Comment
info <Blocks>	Shows the current settings for limiting packets. The settings are displayed according to port blocks. The port blocks are defined as follows: • Port 1 on slot 5 • Port 2 on slot 5 • The ports on slots 6, 7 and 11. • The ports on slots 9 and 10. • The ports of an installed extender, in other words, the ports of slots 12 and 13 of a twisted pair extender and the ports 12 through 15 of a media module extender.	If a parameter (blocks) is specified, the CLI only displays the selected values.
inmode <E|D> <E|D> <E|D> [blocks]	Specifies the ingress limiting mode for ports. The three entries for E or D are (in this order) for • Unicast (DLF) • Multicast • Broadcast The port blocks are defined as for the info command. Examples: • inmode E D E 1 Enables unicast and broadcast, disables multicast for port block 1. • Inmode D E D Disables unicast and broadcast, enables multicast for all port blocks.	Administrator only. If the parameter (blocks) is not specified, all blocks are changed.
ingress <packets> [blocks]	Specifies the maximum number of incoming packets processed by the IE switch for each port block. The port blocks are defined as for the info command.	Administrator only. If the parameter (blocks) is not specified, all blocks are changed.

4.5.18 Load Limits Rates (SCALANCE X-300/X408-2)

Limiting the transfer rate of incoming and outgoing data

The configured load limitation is displayed in this menu (maximum number of frames per second). The set values are valid per port. You can specify the category of frame for which the entered limit values will apply. You can configure by clicking on the relevant entry.



Port	Ingress Limiting Mode	Ingress Limiting Rate	Egress Limiting Rate
5.1	All Frames	not limited	not limited
5.2	All Frames	not limited	not limited
6.1	Broadcast, Multicast, DLF	128 Mbps	256 Mbps
6.2	Broadcast, Multicast	32 Mbps	64 Mbps
8.1	All Frames	not limited	not limited
8.2	All Frames	not limited	not limited
8.3	Broadcast	128 Kbps	256 Kbps
8.4	All Frames	not limited	not limited

Figure 4-69 Load Limits Rates

Port
Displays the slot and the port to which the information relates. You can change the configuration by clicking on the relevant entry in the "Port" column.

Ingress Limiting Mode
Displays the configured frame types to which the limit values for incoming data relate.

Ingress Limiting Rate
Displays the configured limit values for the transfer rates of the incoming data.

Egress Limiting Rate
Displays the configured limit values for the transfer rates of the outgoing data.

Note

The limits for the outgoing data always relate to all packets.

Configuring limits

If you click on an entry in the "Port" column, the "Load Limits Rates Configuration" screen opens.

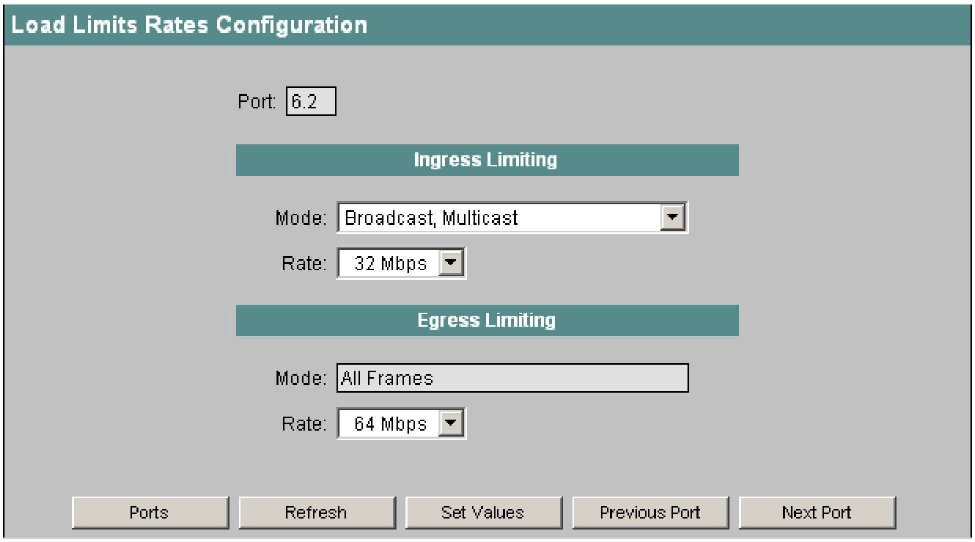


Figure 4-70 Load Limits Rates Configuration

Port
Displays the slot and the port to which the information relates. This field cannot be edited.

Modefor ingress limiting
Here, you can specify the categories of frames for which the selected transfer rate for incoming data relates:

- Unicast (destination lookup failure)
- Multicast
- Broadcast

Rate for ingress limiting
Here, you can select the maximum transfer rate for incoming data from the available values. If you select "not limited", the "Ingress Limiting Mode" has no effect.

Mode for the egress limiting
Indicates that the transfer rate for outgoing data applies to all frames. This field cannot be edited.

Rate for egress limiting
Here, you can select the maximum transfer rate for outgoing data from the available values.

Note

The ring ports send multicast frames at cyclic intervals to detect line breaks. For ring ports, you should therefore not limit the receipt of multicast frames to ensure that the redundancy manager functions correctly.

Syntax of the Command Line Interface

Table 4- 49 Load Limits Configuration - CLI\SWITCH\LIMITS>

Command	Description	Comment
info [ports]	Shows the current settings for limiting packets. The settings are displayed according to ports.	If a parameter (ports) is specified, the CLI only displays the selected values.
inmode <mode> [ports]	Specifies the ingress limiting mode for ports. The <mode> parameter can have the following values: • B Broadcast • BM Broadcast, Multicast • BMU Broadcast, Multicast, Unicast (DLF) • ALL All frames Example: • inmode B 5.1 Sets the limiting mode for port 5.1 to broadcast.	If only the <mode> parameter is specified, the settings are changed for all ports.
ingress <rate> [ports]	Specifies the ingress limiting rate for ports. The <rate> parameter can have the following values: • 128k, 256k, 512k • 1m, 2m, 4m, 8m, 16m, 32m, 64m, 128m, 256m • k stands for kilobits per second and m for megabits per second. Example: • ingress 256K 5.1, 6.2 Sets the ingress limiting rate for ports 5.1 and 6.2 to 256 Kbps.	If only the <rate> parameter is specified, the settings are changed for all ports.
egress <rate> [ports]	Specifies the egress limiting rate for ports. The abbreviations for the <rate> parameter are the same as those of the ingress command. Example: • egress 2M 5.2, 8.1-8.4 Sets the egress limiting rate for ports 5.2 and 8.1 through 8.4 to 2 Mbps.	If only the <rate> parameter is specified, the settings are changed for all ports.

4.5.19 Current VLAN Configuration

Network definition regardless of the spatial location of the nodes

A VLAN (virtual LAN) is a network to which nodes can be assigned regardless of their physical location. Multicast and broadcast frames are possible only within the limits set by the logical network structure, such frames cannot be sent into the virtual network. For this reason VLANs 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.

Versions of VLANs

There are various types of VLAN:

- Port-based VLAN (level 2)
- MAC address-based VLAN (level 2)
- IP address–based VLAN (level 3)

An IE switch supports port-based VLAN. This makes it possible to set parameters for the IE switch or to configure it using GVRP frames.

How to configure port-based VLANs

Follow the steps below to configure your VLANs:

1. Specify the nodes for the individual VLANs.
2. Assign the VLAN-ID for each node and each IE switch and specify the device to which there is a connection and over which port the connection is established.
3. Set the following configuration on the IE switch:
   – Definition of all VLANs used on this device.
   – Specify which VLAN will be supported on which port.
   – Specify how the frames will be processed entering and leaving the ports (ingress / egress filter).
   – Specify whether frames are sent over the port with or without tagging.
   – Decide whether the IE switch will be configured statically or whether it can be configured dynamically with GVRP.

Important rules for VLANs

Make sure you keep to the following rules when configuring and operating your VLANs:

- To achieve switchover times in the ring of 300 ms when using VLANs or multicast groups, all ring ports must be created statically as members in all VLANs and all multicast groups.
- Frames with VLAN-ID "0" (for example only priority-tagged frames) are treated like untagged frames.

- As default, all ports on the IE switch send frames without a VLAN tag to ensure that the end node can receive these frames. This basic setting is necessary since it is not always certain whether a node can interpret tagged frames.
- As default, an IE switch that supports VLANs has the parameter assignment VLAN identifier 1 (default VLAN) at all ports.

Note

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

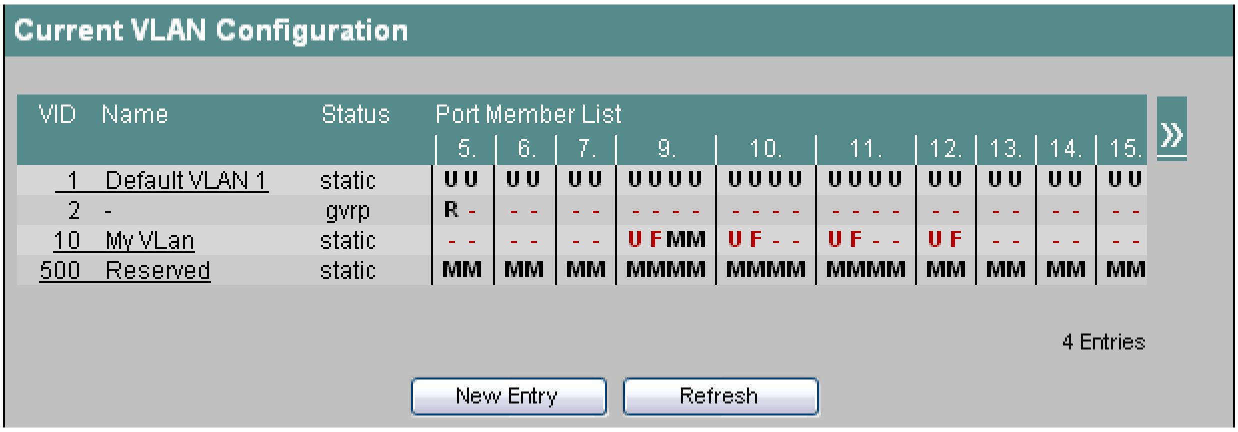
If an end node is connected to a port, outgoing frames should be sent without a tag (static access port). If, however, there is a further switch at this port, the frame should have a tag added (trunk port).

VLANs with the IE switch

The Current VLAN Configuration page shows the current assignment of the ports in terms of VLAN configuration.

Changing pages
Click on the ">>" or "<<" buttons to page backwards and forwards.

On the second page, instead of the ports, you will see any link aggregations that have been set up.



Current VLAN Configuration

VID	Name	Status	Port Member List 5.	6.	7.	9.	10.	11.	12.	13.	14.	15.
1	Default VLAN 1	static	U U	U U	U U	U U U U	U U U U	U U U U	U U	U U	U U	U U
2	-	gvrp	R -	- -	- -	- - - -	- - - -	- - - -	- -	- -	- -	- -
10	My VLan	static	- -	- -	- -	U F M M	U F - -	U F - -	U F	- -	- -	- -
500	Reserved	static	M M	M M	M M	M M M M	M M M M	M M M M	M M	M M	M M	M M

4 Entries

New Entry Refresh

Figure 4-71 Current VLAN Configuration

The four areas of the table show the following information:

VID
The VLAN identifier (VID), a number between 1 and 4094.

Name
This name is assigned when a VLAN is defined. It only provides information and has no effect on the configuration.

If the static status is shown for an entry, you can click on the VID or name to open the Static VLAN Configuration page. Here, you can configure the individual ports to specify the VLAN to which they belong. The VLAN ID and name can, however, only be specified when you create a new entry and they cannot be modified again afterwards. If you want to change an entry, you must first delete the entry and then create it again with the required change included.

Status
Shows the type of 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 IE switch.

Port Member List
Shows the VIDs set for the slots or ports. The meaning of the entries is as follows:

- "-"
  The port is not a member of the specified VLAN.
- M
  (Member) The port is a member of the VLAN, sent frames include a VLAN tag with the VID specified in the first column.
- R
  (Registered) The port is a member of the VLAN, registration was by a GVRP frame.
- U
  (Untagged) The port is a member of the VLAN, sent frames do not include a VLAN tag.
  U (in red)
  This VLAN is not configured as port VLAN. Sent frames do not contain a VLAN tag.
- F
  (Forbidden) The port is not a member of the VLAN and it is not possible for the VLAN to be registered dynamically at this port over GVRP.

With a new definition, all ports have the identifier "-".

VLAN configuration

Click the New Entry button to specify how frames are sent via ports when working with a VLAN. The Static VLAN Configuration page opens in which you can make the necessary entries:

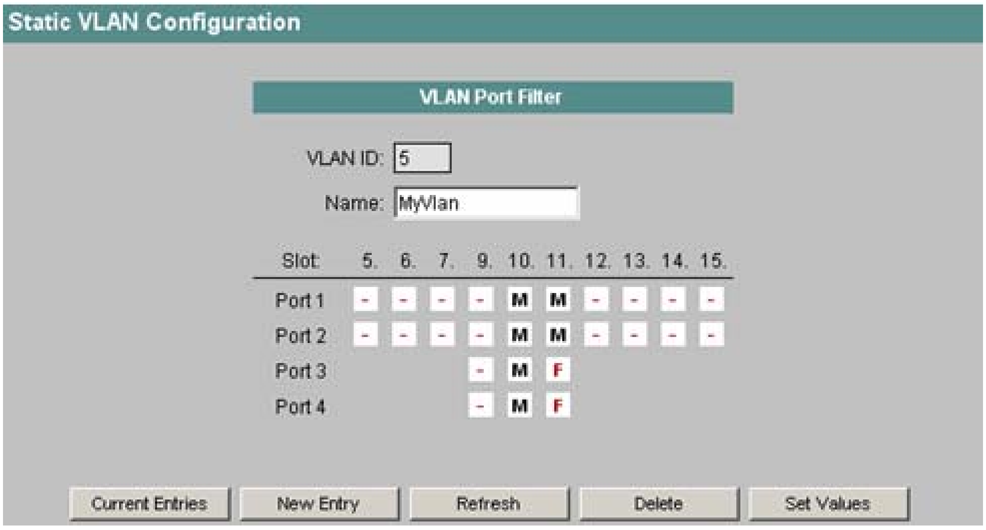


Figure 4-72 Static VLAN Configuration

VLAN ID
Enter the ID of the VLAN here. The VLAN-ID is a number between 1 and 4094.

Name
Here, enter a name for the VLAN. The name has no effect on the configuration.

Slot/Port
Here, you can specify how the port responds in relation to the specified VLAN when sending frames. As default, the boxes have "-" entered. By clicking repeatedly, you move from one entry to the next. The meaning of the entries is as follows:

- "-"
  The port is not a member of the specified VLAN.
- M
  (Member) The port is a member of the VLAN, sent frames include a VLAN tag with the VID specified in the first row.
- R
  (Registered) The port is a member of the VLAN, registration was by a GVRP frame.
- U
  (Untagged) The port is a member of the VLAN, sent frames do not include a VLAN tag. Use U if end devices that do not support VLAN tags are addressed via this port.
- F
  (Forbidden) The port is not a member of the VLAN and it is not possible for the VLAN to be registered dynamically at this port over GVRP.

Current Entries
By clicking this button, you return to the list of VLANs.

New Entry
Click on this button to make the settings for a new VLAN.

Set Values
Click this button to store the values you have entered in the configuration of the IE switch.

Delete
Click this button to delete the displayed configuration.

Syntax of the Command Line Interface

Table 4- 50 Current VLAN Configuration - CLI\SWITCH\VLAN>

Command	Description	Comment
info	Shows the currently configured VLANs and their relationship to the ports.	
add <VLAN-ID> [<option> [ports]]	Inserts a new VLAN. The following abbreviations are available for the <option> parameter. • - The port is not a member of the VLAN. • m The port is a member of the VLAN, frames are sent with a VLAN tag. • u The port is a member of the VLAN, frames are sent without a VLAN tag. • f The port is not a member of the VLAN and it cannot be configured as belonging to the VLAN dynamically by GVRP. Examples: • add 2 Creates an entry with the VLAN-ID 2 and the default name "Vlan 2". • add 4 m Creates an entry with the VLAN-ID 4 and the default name "Vlan4". All existing ports are members.	Administrator only.
edit <VLAN-ID> [<option> [ports]]	Changes the membership of ports in a VLAN. The abbreviations for the <option> parameter are the same as those of the add command. Examples: • edit 3 - 10.1 Removes port 10.1 from the VLAN with ID 3.	Administrator only.
name <VLAN-ID> <name>	Changes the name of a VLAN.	Administrator only.
delete <VLAN-ID>	Deletes the VLAN with the specified ID from the configuration of the IE switch.	Administrator only.

4.5.20 VLAN Port Parameters

Processing received frames

This page shows the rules according to which an IE switch handles received frames:


VLAN Port Parameters

Port	Priority	Port VID	Acceptable Frames	Ingress Filtering
5.1	0	1	all	enabled
5.2	0	1	all	enabled
9.1	0	1	all	enabled
9.2	0	1	all	enabled
9.3	0	1	all	enabled
9.4	0	1	all	enabled
10.1	0	1	all	enabled
10.2	0	1	all	enabled
10.3	0	1	all	enabled
10.4	0	1	all	enabled
11.1	0	1	all	enabled
11.2	0	1	all	enabled
11.3	0	1	all	enabled
11.4	0	1	all	enabled

Refresh

Figure 4-73 VLAN Port Parameters

The five columns of the table show the following information:

Port
This shows the slot and the port to which the following information relates.

Priority
The CoS priority (Class of Service) used in the VLAN tag. If a frame without tag is received, a priority can be assigned to it per port. This priority specifies how the frame is further processed compared with other frames.
There are a total of eight priorities with values 0 through 7, where 7 represents the highest priority (IEEE 802.1p Port Priority). For more detailed information on frame tagging, refer to Appendix C.

Port VID
If a received frame has no VLAN tag, it has a tag added with the VLAN-ID specified here and is sent out according to the switch rules for the port.

Acceptable Frames
This specifies how untagged frames are handled. The following alternatives are possible:

- tagged only
  The IE switch discards all untagged frames.
- all
  The IE switch forwards all frames.

Ingress Filtering
Here, you can see whether the VID of received frames is evaluated (enabled) or not (disabled).

Configuration of a port for VLAN

After clicking on one of the entries in the Ports column, you change to the page for configuring the port properties for receipt of frames:

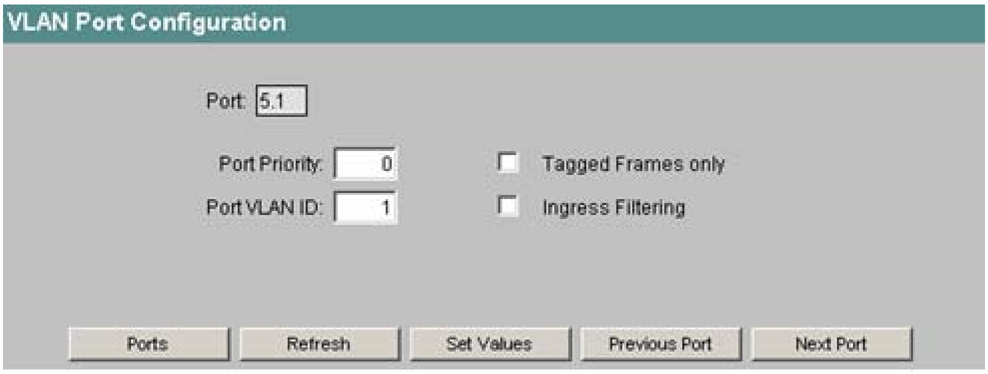


Figure 4-74 VLAN Port Configuration

Port
This read-only box displays the slot and port number to which the information on this page relates.

Port Priority
The priority assigned to untagged frames.

Port VLAN ID
The VLAN-ID assigned to untagged frames.

Tagged Frames only
If you activate this check box, untagged frames are discarded. Otherwise, the forwarding rules apply according to the configuration.

Ingress Filtering
If you enable this check box, the VLAN-ID of received frames decides how they are forwarded: To use the VLAN-ID of the received frame, the VLAN must have been created on the IE switch and the port must be a member of the VLAN.
Frames with the configured port VLAN-ID are forwarded, frames with a different VLAN-ID are discarded when they are received. Frames without a VLAN-ID are received and forwarded to the port VLAN-ID.

Syntax of the Command Line Interface

Table 4- 51 VLAN Port Parameters - CLI\SWITCH\VLAN\PORTS>

Command	Description	Comment
info	Displays an overview of the ports and corresponding VLAN settings.	-
vid [<VLAN-ID> [ports]]	Received frames without a VLAN tag at the specified ports are given a VLAN tag with the <VLAN-ID>.	Administrator only.
prio [<0...7> [ports]]	Specifies the priority of ports.	Administrator only.
ingress [<E|D> [ports]]	Enables/disables the evaluation of the VID of received frames.	Administrator only.
untagged [<E|D> [ports]]	Specifies the processing of frames without a VLAN tag. When this is enabled, frames are also accepted without a VLAN tag, otherwise not.	Administrator only.

4.5.21 GVRP Configuration

Enabling GVRP functionality

With a GVRP frame, an end node or switch can register for a specific VID at a port of the IE switch. You can enable each port for GVRP functionality on the GVRP Configuration page.

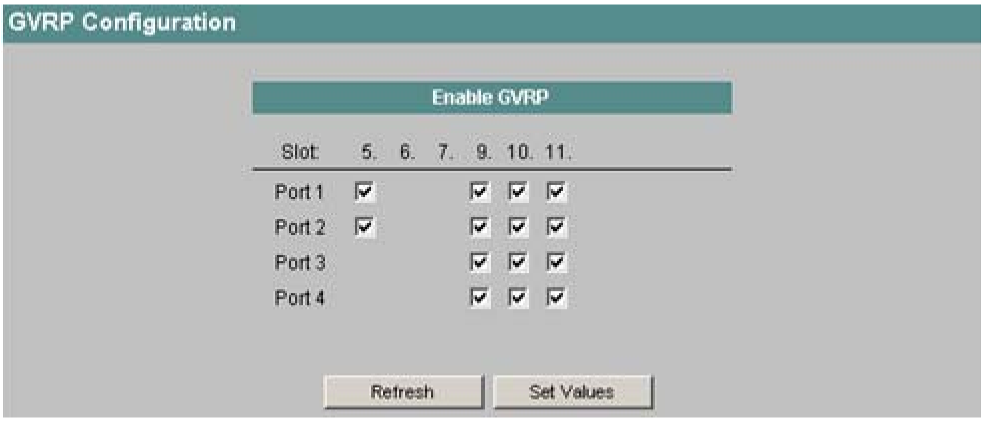


Figure 4-75 GVRP Configuration

Enable GVRP

If you select an option, the IE switch allows the registration of a VLAN by GVRP frames at the relevant port. The IE switch can also send GVRP frames over this port.

Syntax of the Command Line Interface

Table 4- 52 GVRP Configuration - CLI\SWITCH\VLAN>

Command	Description	Comment
gvrpport [<E|D> [ports]]	Enables/disables dynamic registration of VLANs with GVRP for the specified ports.	Administrator only.

4.5.22 Spanning Tree Configuration

Avoiding loops on redundant connections

The spanning tree algorithm (R/STP) 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 deactivating 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 switches 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. The root bridge is the bridge that controls the spanning tree algorithm for all involved components. BPDUs also bring about the status change of the bridge ports.

Rapid Spanning Tree

The rapid spanning tree algorithm is based on the spanning tree algorithm. This was optimized in terms of the reconfiguration time. Typical reconfiguration times for Spanning Tree are between 20 and 30 seconds. With rapid spanning tree, the reconfiguration times are around 1 second. This was achieved by the following measures:

- Edge Ports
  A port defined as an edge port is switched active directly following a link up. 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.
- Point-to-point (direct communication between two neighboring switches)
  By directly linking the switches, 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 IE switch can establish a connection over the alternate port without any delay by reconfiguring.
- Filter table
  In rapid spanning tree, ports affected by a reconfiguration are immediately deleted from the filter table. With spanning tree, on the other hand, the point at which a port is deleted is decided by the time when the port was entered in the filter table.
- 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.

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.

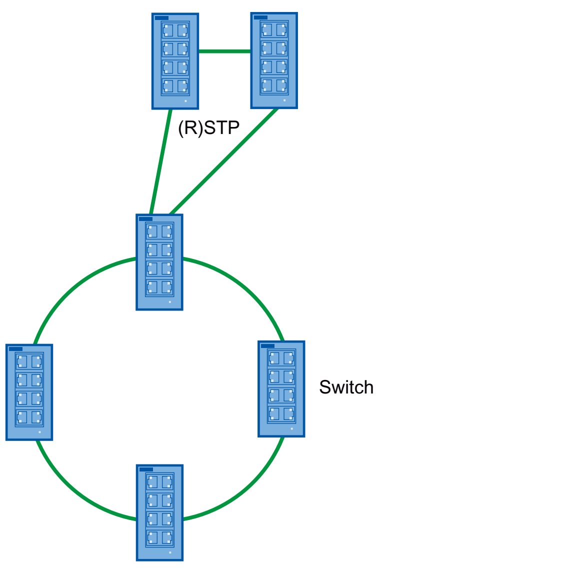
(Rapid) Spanning Tree and media redundancy

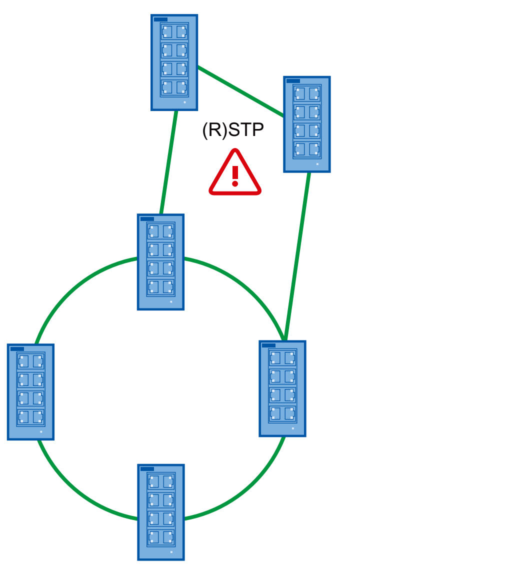
NOTICE
A redundant (R)STP connection is only possible on one single device in the ring. Otherwise circulating frames will result and lead to a loss of data traffic.

It is possible to enable (Rapid) Spanning Tree at the same time as the media redundancy methods MRP (Media Redundancy Protocol) and HSR (High Speed Redundancy). During configuration, make sure that the redundant (R)STP connection is only on one device in the ring. If (R)STP is connected as a ring via the redundancy ring, this will lead to circulating frames and to failure of the data traffic.

The following figures illustrate the permitted (R)STP connection and an impermissible connection.

Permitted (R)STP connection to ring redundancy	Impermissible (R)STP connection to ring redundancy





Spanning tree configuration with an IE switch

The parameters for the spanning tree protocol are displayed and set in the "Spanning Tree Configuration" dialog:

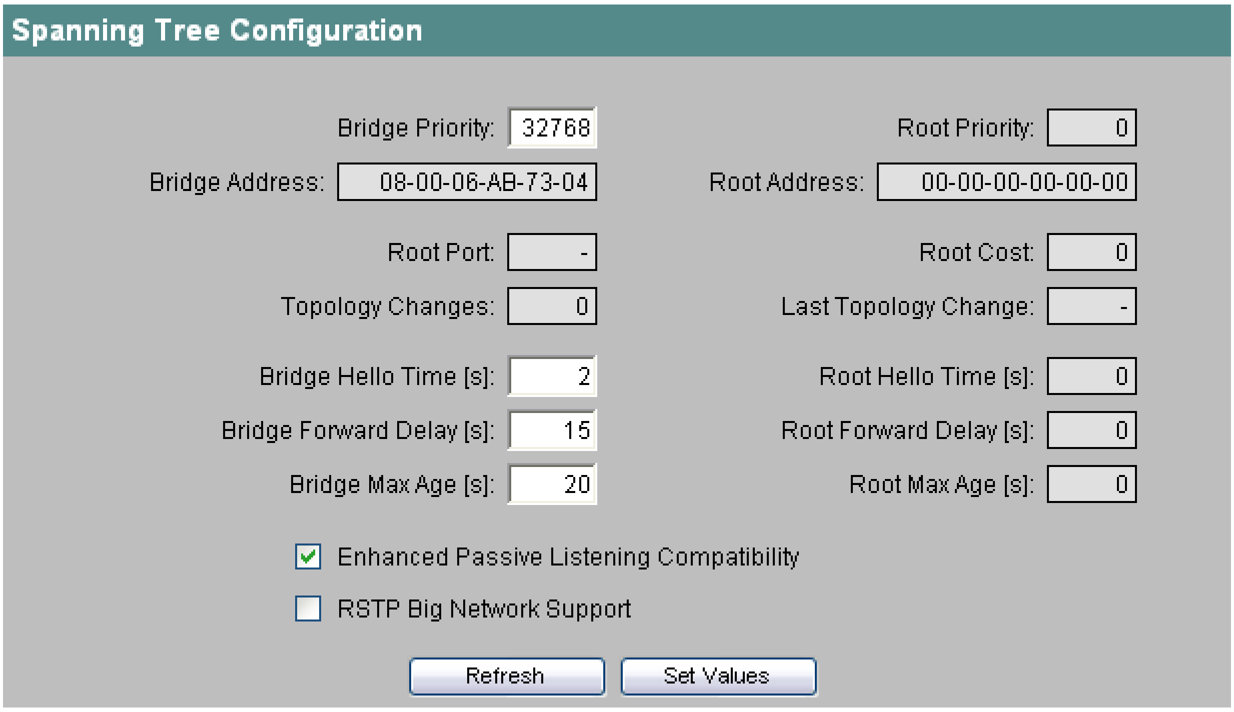


Figure 4-76 Spanning Tree Configuration

The left-hand side of the page shows the configuration of the IE switch. The right-hand side shows the configuration of the root bridge that can be derived from the spanning tree frames received by an IE switch. For this reason, the data shown here is read-only. If an IE switch is the root bridge, the information on the left and right matches. The meaning of the parameters is as follows:

Bridge Priority / Root Priority
Which switch 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 switches in a network have the same priority, the switch 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 65,535.

Bridge Address / Root Address
The MAC address of the IE switch or root bridge.

Root Port
The port over which the device communicates with the root bridge.

Topology Changes / Last Topology Change
The entry for the IE switch shows the number of reconfiguration actions due to the spanning tree mechanism since the last startup. For the root bridge, the duration is displayed in minutes (m appended after the number) since the last reconfiguration.

Bridge Hello Time / Root Hello Time
Each bridge sends configuration frames (BPDUs) regularly. The interval between two such frames is the Hello time.

Bridge Forward Delay / Root Forward Delay
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 value for this parameter is 20.

Enhanced Passive Listening Compatibility
Here, you enable/disable the sending of TCN (Topology Change Notification) frames via RSTP edge ports. In conjunction with the "Auto Edge Port" function (see Spanning Tree Port Parameters menu item), this parameter is necessary to link (R)STP networks with HSR rings. Otherwise no TCN frames will be sent via edge ports; this is, however, necessary for the passive listening function on ring nodes (refer to the operating instructions of the relevant switch).

RSTP Big Network Support
Here, you enable/disable support of big RSTP rings with up to 80 bridges.

Syntax of the Command Line Interface

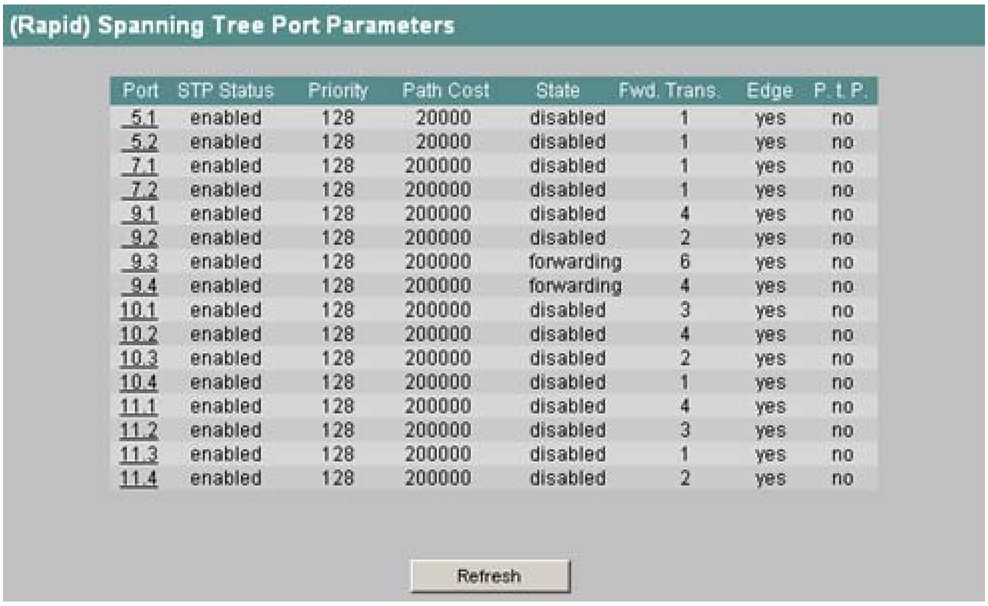
Table 4- 53 Spanning Tree Configuration - CLI\SWITCH\STP>

Command	Description	Comment
info	Shows the current spanning tree configuration.	-
bprio [0...61440]	Specifies the bridge priority for the IE switch.	Administrator only.
hellotm [1 ... 10]	Specifies the interval between two BPDUs in seconds.	Administrator only.
fwddelay [4 ... 30]	Specifies the delay time for the effectiveness of configuration information (specified in seconds).	Administrator only. Default value: 15 s
maxage [6 ... 40]	Maximum age for configuration information.	Administrator only. Default value: 20 s
eplc [E|D]	Enables/disables enhanced passive listening compatibility	Administrator only.
bnsupp[E|D]	Enables big network support	Administrator only.

4.5.23 Spanning Tree Port Parameters

Port-specific parameters

This page displays the current port parameters that were either set by the user or set as a result of the automatic functions of the IE switch.



(Rapid) Spanning Tree Port Parameters

Port	STP Status	Priority	Path Cost	State	Fwd. Trans.	Edge	P. t. P.
5.1	enabled	128	20000	disabled	1	yes	no
5.2	enabled	128	20000	disabled	1	yes	no
7.1	enabled	128	200000	disabled	1	yes	no
7.2	enabled	128	200000	disabled	1	yes	no
9.1	enabled	128	200000	disabled	4	yes	no
9.2	enabled	128	200000	disabled	2	yes	no
9.3	enabled	128	200000	forwarding	6	yes	no
9.4	enabled	128	200000	forwarding	4	yes	no
10.1	enabled	128	200000	disabled	3	yes	no
10.2	enabled	128	200000	disabled	4	yes	no
10.3	enabled	128	200000	disabled	2	yes	no
10.4	enabled	128	200000	disabled	1	yes	no
11.1	enabled	128	200000	disabled	4	yes	no
11.2	enabled	128	200000	disabled	3	yes	no
11.3	enabled	128	200000	disabled	1	yes	no
11.4	enabled	128	200000	disabled	2	yes	no

Refresh

Figure 4-77 (Rapid) Spanning Tree Port Parameters

The eight columns of the port table show the following information:

Port
Specifies the slot and port to which the information relates.

STP Status
Shows whether spanning tree is enabled or disabled for the port.

Priority
If the path calculated by spanning tree is possible over several ports of a switch, the port with the highest priority (in other words the lowest value for this parameter) is selected. A value from 0 through 255 can be specified for the priority; the default is 128.

Path Cost
This parameter is used to calculate the path that will be selected. The lower the value, the greater the probability that the corresponding path will be used. If several ports of a switch have the same value, the port with the lowest port number is selected.
The calculation of the path cost is based largely on the transmission rate. The higher the achievable transmission rate, the lower the value for Path Cost should be.
Typical values for spanning tree are as follows:

- 1000 Mbps = 4
- 100 Mbps = 19
- 10 Mbps = 100

Typical values for rapid spanning tree:

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

The values can, however, also be set individually.

State
Displays the current status of the port. The following statuses are possible:

- disabled
  The port only receives and is not involved in the STP configuration.
- blocking
  In the blocking mode, BPDUs are received.
- 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 again (in other words, the node addresses).
- forwarding
  Following the reconfiguration time, the port is once again active in the network; it receives and forwards data frames.

FWD Transitions
Specifies the number of transitions from the listening to forwarding status.

Edge

The following entries are possible in this column:

- yes
  An edge port is connected to this port.
- no
  There is a spanning tree or rapid spanning tree device on this port.

  If an edge port is connected, an IE switch can switch over the port more quickly without taking into account spanning tree frames. If a spanning tree frame is received despite this setting, the port automatically changes to the no setting for switches.

P.t.P.

There is a point-to-point link when two RSTP-compliant network components are connected together over this port. There are 2 possible statuses :

- Yes
  There is a point-to-point link.
- No
  There is not a point-to-point link.

Configuration of a port for (Rapid) Spanning Tree

Note

(R)STP cannot be enabled on the ring ports and the standby ports.

If you click on a port name in the first column of "(Rapid) Spanning Tree Port Parameters", you go to the "Spanning Tree Port Configuration" page:

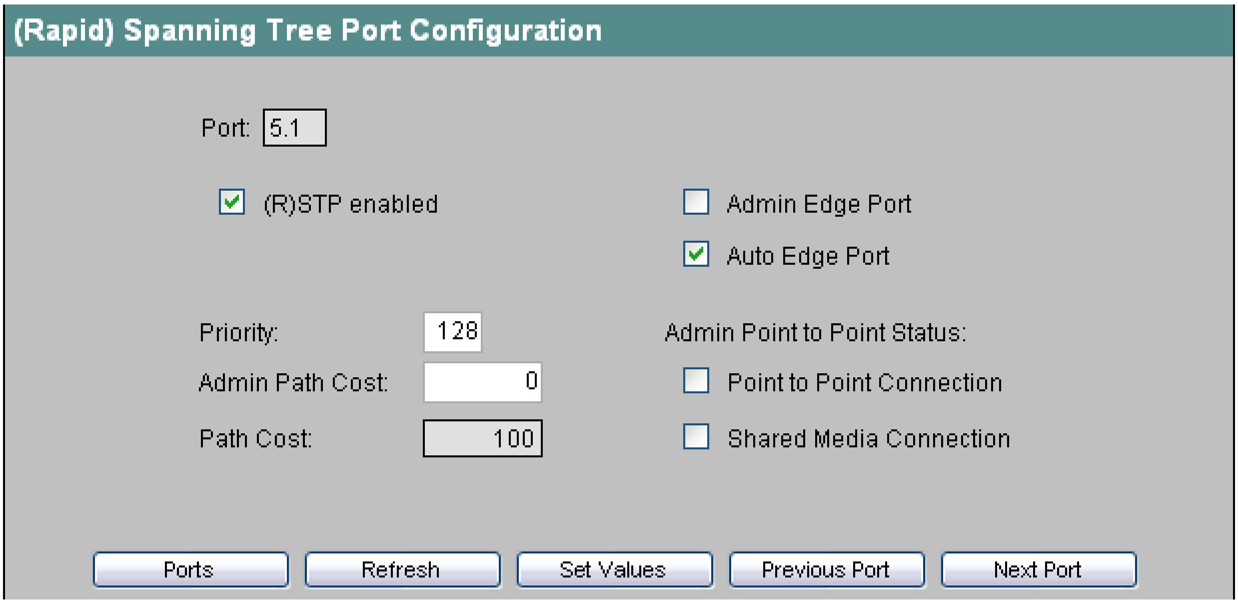


Figure 4-78 (Rapid) Spanning Tree Port Configuration

(R)STP enabled
Enable this check box, if you want the port to use the (rapid) spanning tree protocol.

Admin Edge Port
Enable this check box if an end device is connected to this port, otherwise a reconfiguration of the network will be triggered by every link change.

Auto Edge Port
Enable this option if you want a connected end device to be detected automatically on this port. This option is useful in conjunction with passive listening (refer to the operating instructions of the relevant IE switch) because reconfiguration is faster if the main link fails.

Priority
Enter a value here for the port priority between 0 and 255.

Admin Path Cost
Here, you can enter a value for the Path Cost parameter. If you enter a zero, the value for the path costs will be calculated.

Path Cost
This box displays the calculated value for the path costs if a zero is entered in the Admin Path Cost box. If you enter a value other than zero in Admin Path Cost, the Path Cost text box shows this value.

Admin Point to Point Status
There are three possible settings:

- Point to Point Connection and Shared Media Connection are not selected:
  Point-to-point is detected automatically. If the port is set to half duplex, a point-to-point link is not assumed.
- Shared Media Connection is selected:
  Despite a full duplex connection, a point-to-point link is not assumed.
- Point-to-Point Connection is selected:
  Despite a half duplex connection, a point-to-point link is assumed.

Note

Point-to-point means a direct connection between two switches. Shared Media Connection could, for example, be a connection to a hub.

Syntax of the Command Line Interface

Table 4- 54 Spanning Tree Ports Parameters - SWITCH\STP\PORTS>

Command	Description	Comment
info	Shows an overview of the ports and the corresponding rapid spanning tree settings.	-
stpport [<E|D> [ports]]	Enables/disables the spanning tree algorithm for the specified ports.	Administrator only. If you want to specify several ports as parameters, you can separate the port numbers with blanks or hyphens.
prio [<0...255> [ports]]	Specifies the priority of the port.	Administrator only.
pathcost [<0...65535> [ports]]	Specifies the path costs for the port.	Administrator only.
admedge [<T|F> [ports]]	Specifies whether a • T end device or a • F switch is connected to this port that supports Spanning Tree or Rapid Spanning Tree. If a (rapid) spanning tree protocol is received, the value F is displayed.	

Command	Description	Comment
autoedge [<T|F> [ports]]	Specifies whether at this port it should be automatically detected whether a • T end device or a • F switch is connected.	Administrator only.
ptp [<A|T|F> [ports]]	The point-to-point link establishes a direct link between two switches. In this case, you have the following options: • A The port recognizes a PtP port based on the duplexity. If the connection is full duplex, it is assumed to be PtP, if it is half duplex, no PtP connection is assumed (shared medium). • T Specifies a PtP link, even though half duplex is being used. • F Specifies that there is no PtP link over the relevant port even with full duplex.	-

4.5.24 QoS Configuration

QoS

Different applications make different demands on networks. For pure file transfer, the overall throughput is decisive, while the individual latency and loss rate is less significant. For real-time communication, for example Voice over IP, on the other hand, latency, jitter and the loss rate are much more important because they directly affect understandability.

Transmission priorities

The X-300/400 IE switches support CoS to Queue and DSCP to Queue Mapping, with which packets from different sources with different priority can be forwarded. To allow downward compatibility with earlier firmware versions, DSCP Mapping is disabled in the default setting.

Overview

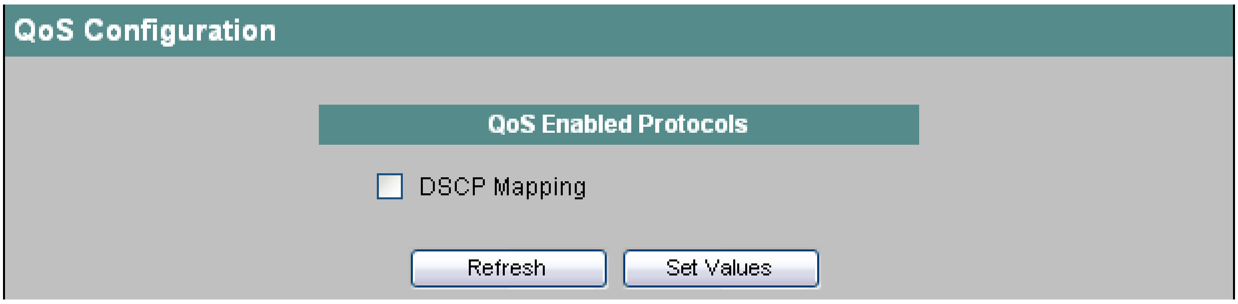


Figure 4-79 QoS Configuration

DSCP Mapping
Enables/disables DSCP to Queue Mapping

Syntax of the Command Line Interface

Table 4- 55 QoS Configuration - CLI\SWITCH\QOS>

Command	Description	Comment
dscpmap [E|D]	Enables/disables DSCP to Queue Mapping.	Administrator only.

4.5.25 CoS to Queue Mapping

CoS Queue

Here, CoS priorities are assigned to certain traffic queues.

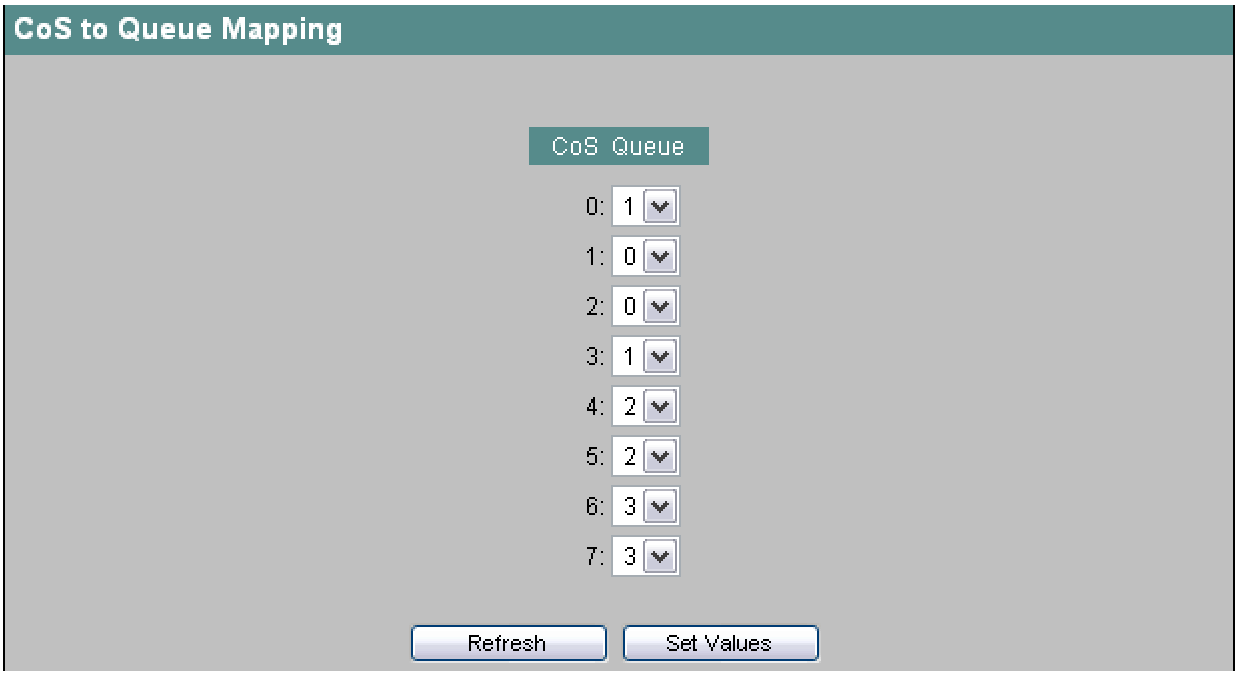


Figure 4-80 CoS to Queue Mapping

CoS
The order of CoS priorities of the incoming packets.

Queue
The traffic-forwarding queue (send priority) that is assigned the CoS priority.

Syntax of the Command Line Interface

Table 4- 56 QOS Configuration - CLI\SWITCH\QOS>

Command	Description	Comment
cos [<0..3> <0..7>]	Assigns CoS priorities to certain traffic queues: • Parameter 1 Queue • Parameter 2 CoS priority	Administrator only.

4.5.26 DSCP to Queue Mapping

DSCP Queue

Here, DSCP settings are assigned to various traffic queues.

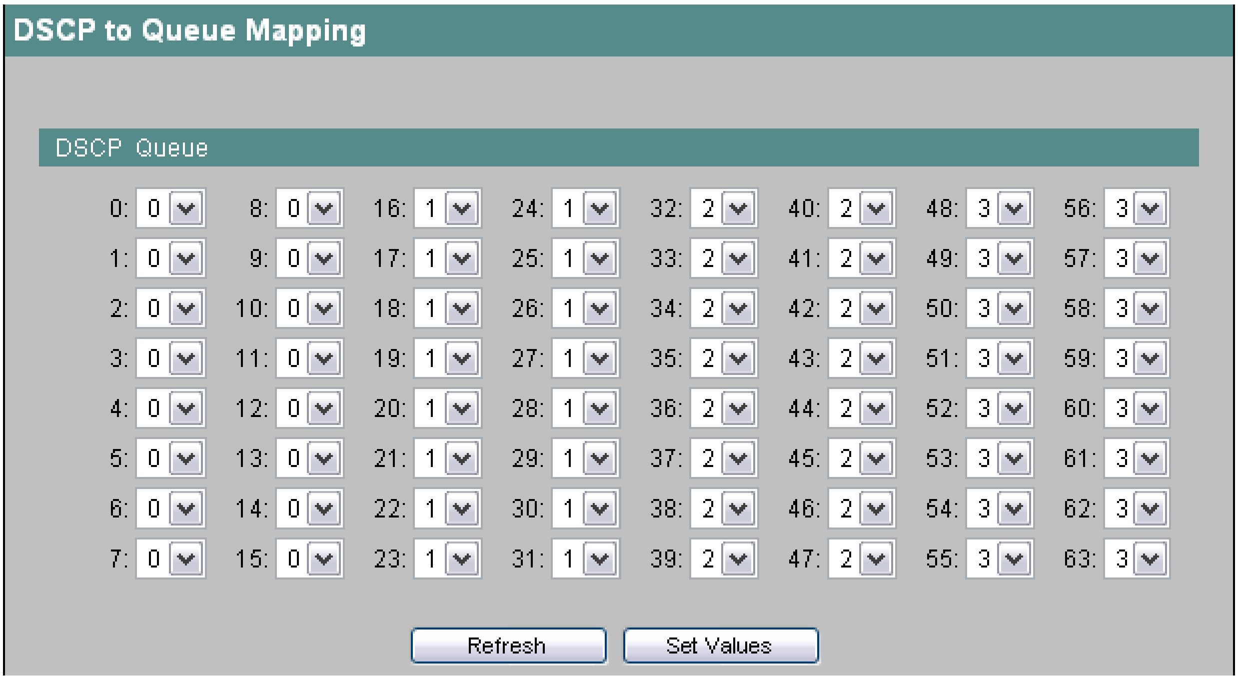


Figure 4-81 DSCP to Queue Mapping

DSCP
The order of DSCP priorities of the incoming packets.

Queue
The traffic-forwarding queue (send priority) that is assigned the DSCP value.

Syntax of the Command Line Interface

Table 4- 57 QoS Configuration - CLI\SWITCH\QOS>

Command	Description	Comment
dscp [<0..3> <0..63>]	Assigns DSCP settings to certain traffic queues: • Parameter 1 Queue • Parameter 2 DSCP value	Administrator only.

4.5.27 DCP Configuration

Applications

The DCP protocol is used by STEP 7 and the PST Tool for configuration and diagnostics of IE switches. 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 per port, 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.

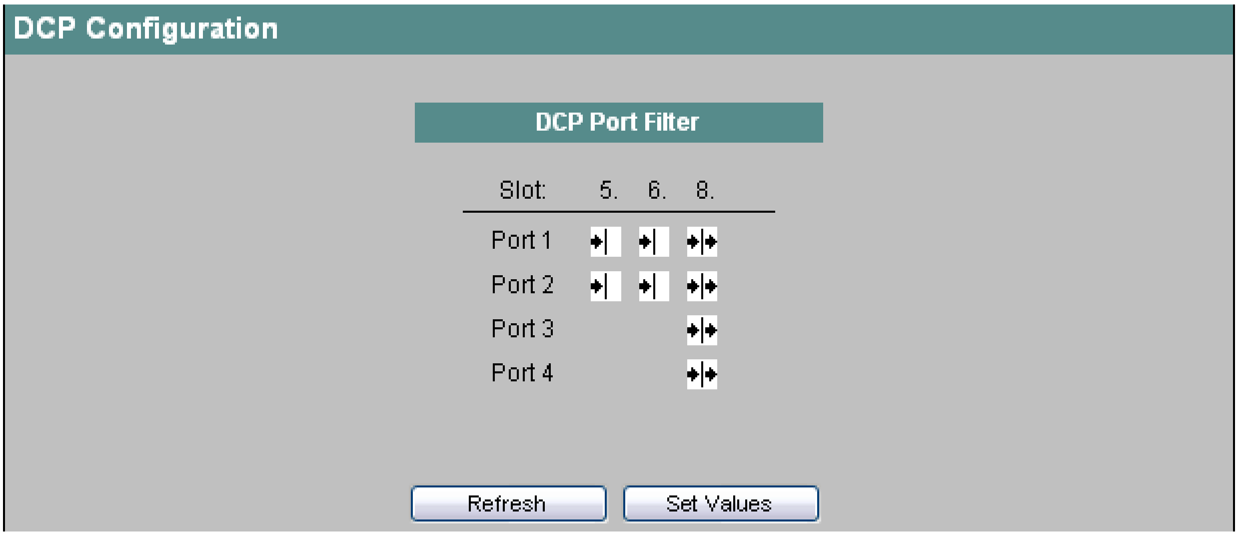
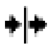


Figure 4-82 DCP Configuration

Here, you select the ports that will support sending of DCP frames:

Rx-only: This port can only receive DCP frames.



Tx and Rx: This port can receive and send DCP frames.

Syntax of the Command Line Interface

Table 4- 58 Current Multicast Groups - CLI\SWITCH\DCP>

Command	Description	Comment
info	Displays the current DCP settings.	-
dcpport <mode> [ports]	Changes the LLDP settings for a port. If no port is specified, all ports are changed. The <mode> parameter can have the following values: • rx receive only • e receive and send	Administrator only.

4.5.28 LLDP Configuration

Applications

PROFINET uses the LLDP protocol for topology diagnostics. In the default setting, LLDP is enabled for all ports; in other words, LLDP packets are sent and received on all ports. With this function, you have the option of enabling or disabling sending and/or receiving per port.

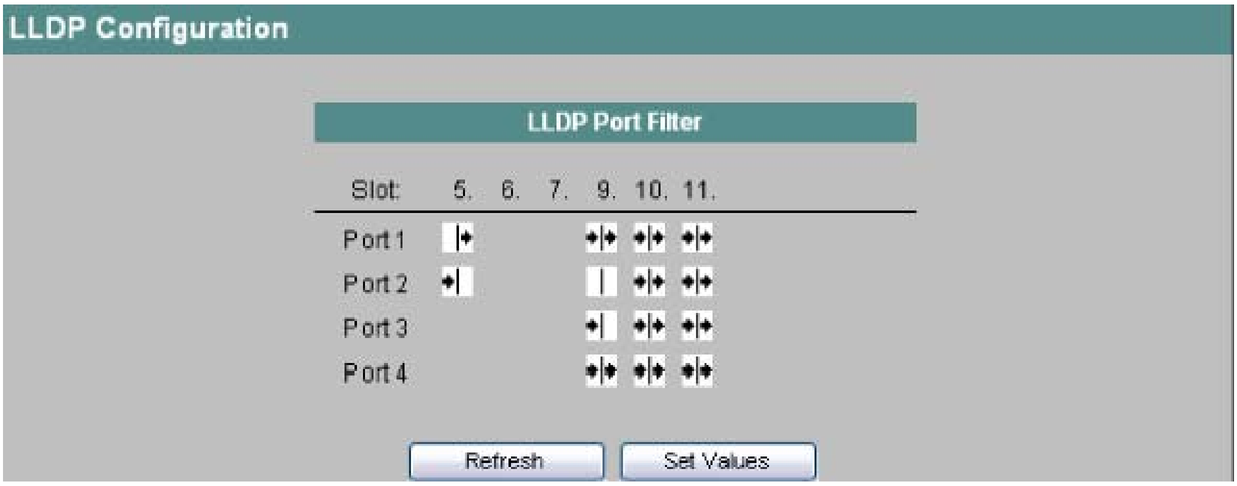


Figure 4-83 LLDP Configuration

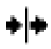
Slot / Port

Here, you select the ports that support reception and/or sending of LLDP frames

:

Rx-only: This port can only receive LLDP frames.

Tx-only: This port can only send LLDP frames.



Tx and Rx: This port can receive and send LLDP frames.

Disabled: This port can neither receive nor send LLDP frames.

Syntax of the Command Line Interface

Table 4- 59 Current Multicast Groups - CLI\SWITCH\LLDP>

Command	Description	Comment
info	Displays the current LLDP settings.	-
lldpport <mode> [ports]	Changes the LLDP settings for a port. If no port is specified, all ports are changed. The <mode> parameter can have the following values: • rx receive only • tx send only • e receive and send • d neither receive nor send	Administrator only.

4.5.29 DHCP Relay Agent Configuration

Applications

The DHCP Relay function intercedes between a DHCP server and an end device connected to a specific port to assign an IP address to this end device. To achieve this the switch forwards the port number of the end device along with the DHCP query to the DHCP server.

Specifying the DHCP server IP addresses

You can specify up to 4 DHCP server IP addresses for the DHCP relay agent (see also Switch Configuration menu item). If a DHCP server cannot be reached, the IE switch then has the option of using a different DHCP server.

Note

The DHCP relay agent is only enabled if the "DHCP Option 82" option is enabled in the Switch Configuration menu.

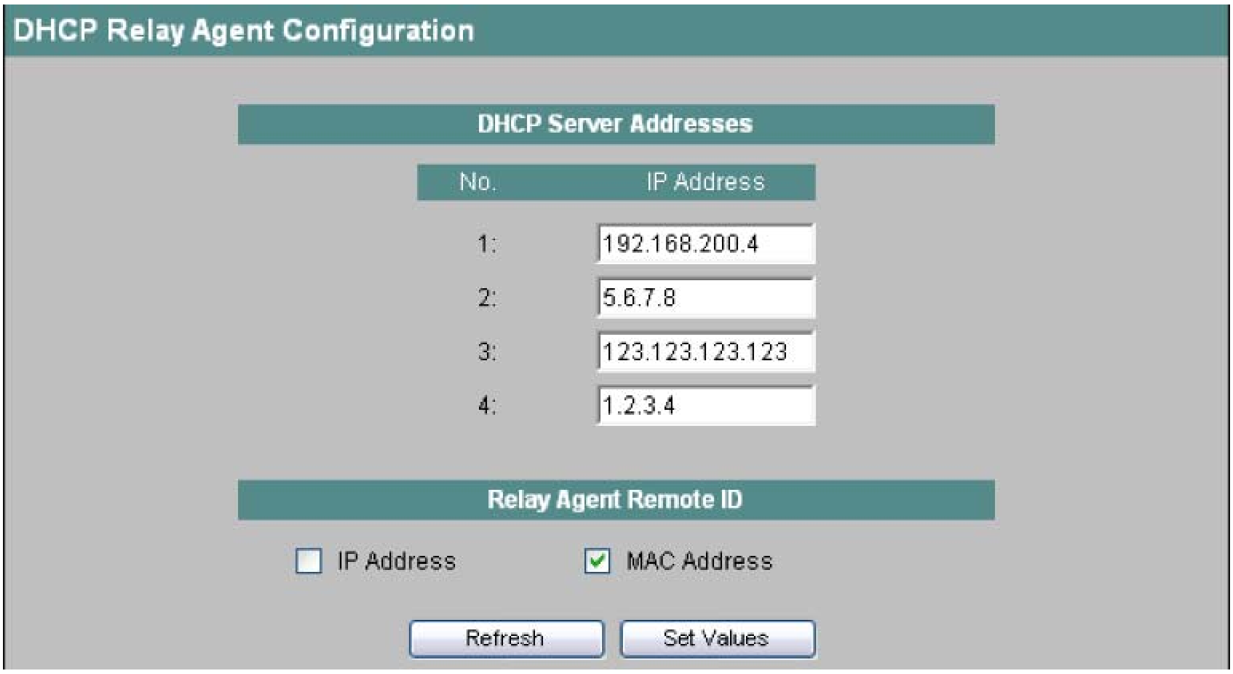


Figure 4-84 DHCP Relay Agent Configuration

"IP-Address" input box
Here, you enter the addresses of the DHCP servers to which the IE Switch will forward DHCP requests.

Relay Agent Remote ID
Here, you can select whether or not the relay agent uses its IP address from the agent configuration or its MAC address as the remote ID.

Syntax of the Command Line Interface

Table 4- 60 DHCP Relay Agent Configuration - CLI\SWITCH\RELAGENT>

Command	Description	Comment
info	Shows the current settings of the DHCP relay agent.	-
server <number> <IP address>	Specifies the IP address of the DHCP server <number>.	Administrator only. Default value: 0.0.0.0
remoteid [IP|MAC]	Specifies the relay agent remote ID	Administrator only.

4.5.30 DHCP Relay Agent Port Configuration

DHCP Relay Agent Port Parameters

This page displays the currently configured port-specific parameters of the DHCP relay agent.

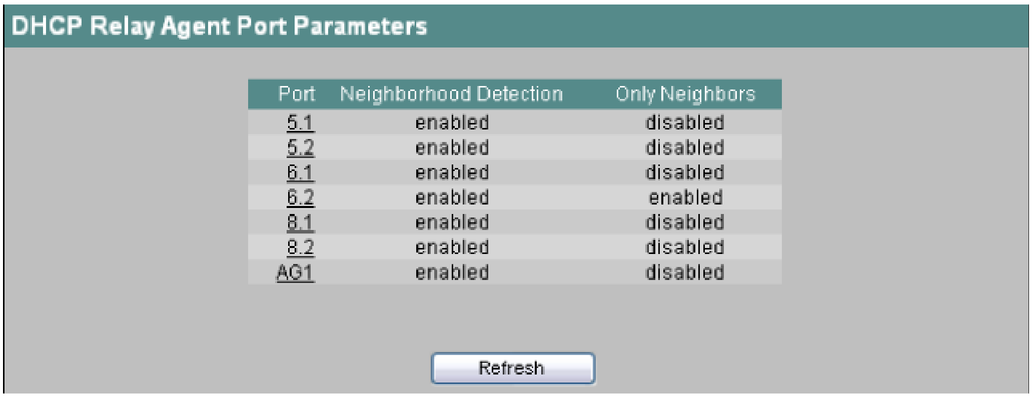


Figure 4-85 DHCP Relay Agent Port Parameters

The three columns of the port table show the following information:

Port
Specifies the slot and port to which the information relates. The name of the aggregation is shown here if link aggregations are configured.

Neighborhood Detection
Shows whether or not detection of neighbors is enabled for this port.

Only Neighbors
Shows whether the DHCP relay agent functions only for direct neighbors on this port.

Configuration of a port for the DHCP relay agent

If you now click on a port name in the first column of the port table, you open the "DHCP Relay Agent Port Configuration" page.

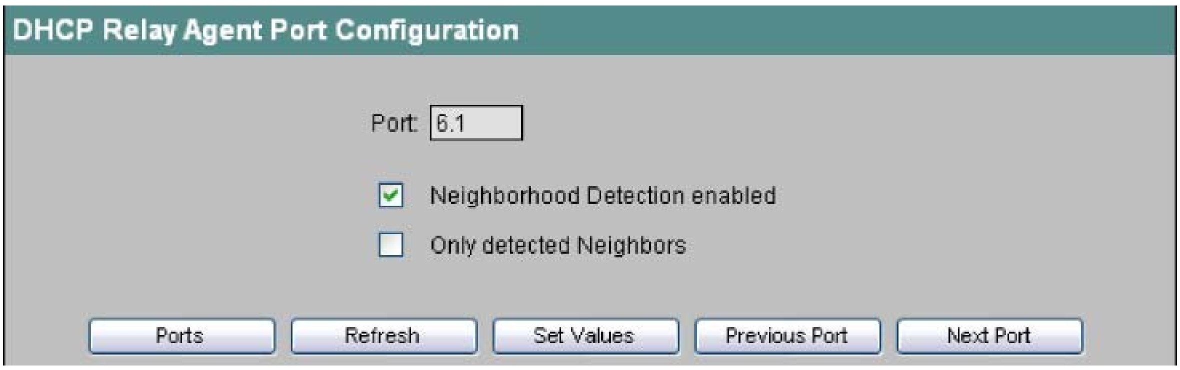


Figure 4-86 DHCP Relay Agent Configuration

Neighborhood Detection enabled
Enable this option if you want to attempt to assign DHCP requests to a neighbor before forwarding.

Only detected Neighbors
Enable this option if you only want DHCP requests to be forwarded if they originate from detected neighbors.

Syntax of the Command Line Interface

Table 4- 61 DHCP Relay Agent Port Parameters - CLI\SWITCH\RELAGENT\PORTS>

Command	Description	Comment
info	Show all the port parameters of the DHCP relay agent	-

4.5.31 Precision Time Protocol (PTP) complying with IEEE 1588

Introduction

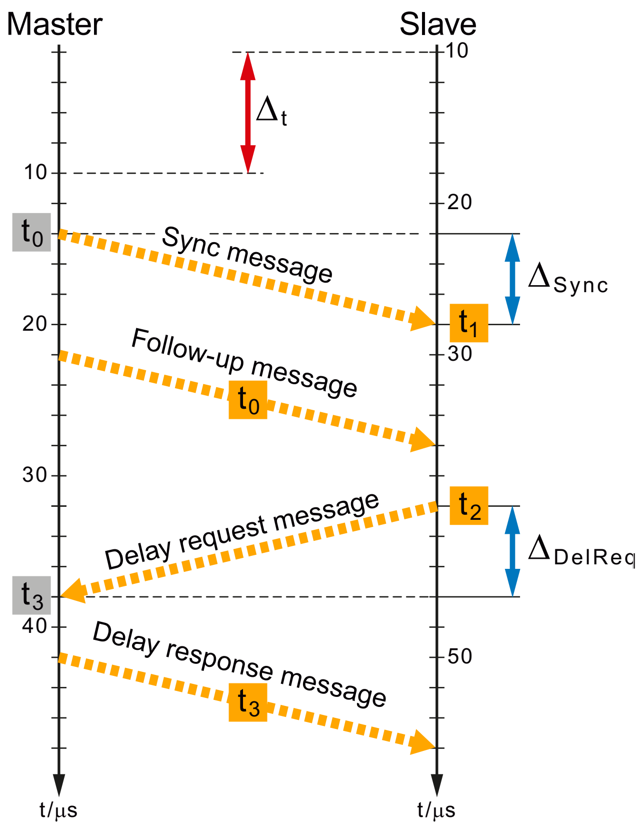
The Precision Time Protocol (PTP) complying with IEEE 1588v2 allows the time-of-day synchronization of devices (time slaves) connected to the ports of a SCALANCE X300. These devices forward the synchronization frames through the network using the "Transparent Clock" (TC) mechanism. The connection mechanisms "end-to-end" and "peer-to-peer" are supported.

Note

PTP is supported only by the following devices of the SCALANCE X300 product line:

- The device X308-2M.
- All devices of the X300 EEC product group.
- All devices of the XR300 product group.
- All devices of the XR300 EEC product group.

Delay request response mechanism



A device in the network takes over the function of the time master (Best Master Clock, BMC) that sets the reference time for all other devices. The master sends synchronization messages cyclically, in the example shown at time t_0. The time t_1 when this message arrived is stored by the slave. In a second message (follow-up message), the master informs the slave of the exact time t_0 when the synchronization message was sent.

However, with only these two values, neither the deviation of the slave clock nor the message delay time can be calculated. For this reason, the slave then sends a delay request message to the master and stores the time t_2 at which this message was sent. Using a delay response message, the master informs the slave of the time t_3 at which it received this message.

In the following calculations, it is assumed that the transfer of a message from the master to the slave takes exactly the same amount of time as the transfer of a message in the opposite direction. This is the situation on a direct cable connection.

From the calculated values for Δ_{Sync} and Δ_{DelReq} the difference between the time of receipt and time of sending is obtained:

$\Delta_{Sync} = t_1 - t_0$

$\Delta_{DelReq} = t_3 - t_2$

If the time of the slave time deviates from the time of the master by the amount Δ_t, these two calculations still do not provide the actual value for the message delay time Δ_D because the send and receive times are based on different reference systems. The simplest way to calculate the actual message delay time Δ_D is to take the average value:

$\Delta_D = (\Delta_{Sync} + \Delta_{DelReq}) / 2$

The deviation of the slave clock Δ_t results when Δ_{Sync} is reduced by the actual message delay time Δ_D:

$\Delta_t = \Delta_{Sync} - \Delta_D$

If Δ_t is positive, the clock of the slave is "fast". If Δ_t has a negative value, the clock of slave is "slow".

Example

At time t_0 = 14 µs, the master sends a sync message that arrives at the slave at time t_1 = 28 µs. The value for Δ_{Sync} is calculated from this:

$\Delta_{Sync} = t_1 - t_0 = 28\ \mu s - 14\ \mu s = 14\ \mu s$

If the clocks of the master and slave were exactly synchronized, the message delay time would be 14 µs which cannot however be concluded based on this single measurement.

For this reason, the slave sends a delay request message at time t_2 = 40 µs that arrives at the master at time t_3 = 38 µs. The value for Δ_{DelReq} is the difference between the time of receipt and time of sending this message:

$\Delta_{DelReq} = t_3 - t_2 = 38\ \mu s - 40\ \mu s = -2\ \mu s$

The actual message delay time Δ_D is the average value of Δ_{Sync} and Δ_{DelReq} because this eliminates the time deviation of the two device clocks:

$\Delta_D = (\Delta_{Sync} + \Delta_{DelReq}) / 2$

$\Delta_D = (14\ \mu s - 2\ \mu s) / 2 = 6\ \mu s$

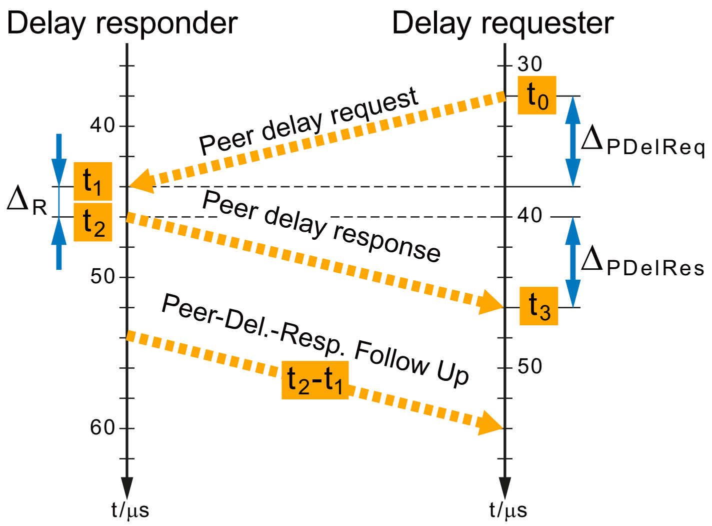
The deviation of the slave clock is

$\Delta_t = \Delta_{Sync} - \Delta_D = 14\ \mu s - 6\ \mu s = 8\ \mu s$

The slave clock is therefore "fast" and needs to be corrected by 8 µs.

Peer delay mechanism

The aim of the peer delay mechanism is to calculate the delay time of a message between two ports of PTP-compliant devices. In contrast to a delay request response message that is transported between the slave and master also over several network nodes, peer delay messages are only exchanged with the relevant neighbor node, hence the name "peer delay".



The delay requester sends a peer delay request message to a neighboring node, the delay responder, and stores the time t_0 at which this message was sent. The delay responder then immediately sends back a peer delay response message. In the correction field of the peer delay response follow-up message, it enters the time difference between the send time t_2 of the peer delay response message and the time t_1 when the peer delay request message was received:

$\Delta_R = t_2 - t_1$

At the time of receipt t_3 of the peer delay response message, the delay requester then has all the data required to calculate the message delay time to the neighboring node:

$\Delta_{PDelReq} = \Delta_{PDelRes} = (t_3 - t_0 - \Delta_R) / 2$

To calculate the deviation of a slave clock, sync messages and follow-up messages must be evaluated with the peer delay mechanism as well. The section "Peer-to-peer transparent clock" contains a description of the complete synchronization cycle.

Synchronization regardless of the topology of the network

The calculations shown in the sections above apply only on condition that the message exchange is via a direct connecting cable between the two communications partners. Normally, however, networks consist of several switches that have to transport the time of day messages between the time master and slave. How the synchronization is acheived via several switches depends on the device category to which a switches are assigned (boundary clock or transparent clock) and which method is used to calculate the message delay time (delay request response mechanism or peer delay mechanism).

The mechanism used to handle PTP messages must be configured for each device. Both delay mechanisms cannot be used at the same time in one network section. All the devices within a section must be configured for either the delay request response mechanism or the peer delay mechanism. All the switches involved should support PTP to achieve precise time-of-day synchronization. A switch that does not support PTP cannot guarantee constant message delay times between the master and slave due to queuing.

Boundary clock

This switch adopts the role of slave at one port and synchronizes itself with the time master. For the other connected devices, it adopts the function of master and sends synchronization frames cyclically to these nodes. In a network with several switches and end devices, the BMC algorithm handles the task of selecting the most precise clock in the network automatically. A master-slave hierarchy results in which each switch synchronizes itself with the neighboring switch in the direction of the BMC.

Synchronization mechanisms with boundary clocks

If a boundary clock is configured for the delay request response mechanism, it sends delay request messages to the time master and sync and follow-up messages to the slaves.

With the peer delay mechanism, the boundary clock calculates the message delay time to the neighboring device for each port. It synchronizes itself by evaluating the sync and follow-up messages of the master. The boundary clock allows the synchronization of the slaves by sending sync and follow-up messages.

Transparent clock

A transparent clock does not synchronize itself with a time master but forwards PTP messages between the time master and the slaves to be synchronized. Compared with the boundary clock, the transplant clock allows more precise synchronization because the error in the synchronization of the boundary clock is omitted. With several switches in a row in a linear bus or ring topology, it is therefore preferable to configure these as transparent clocks.

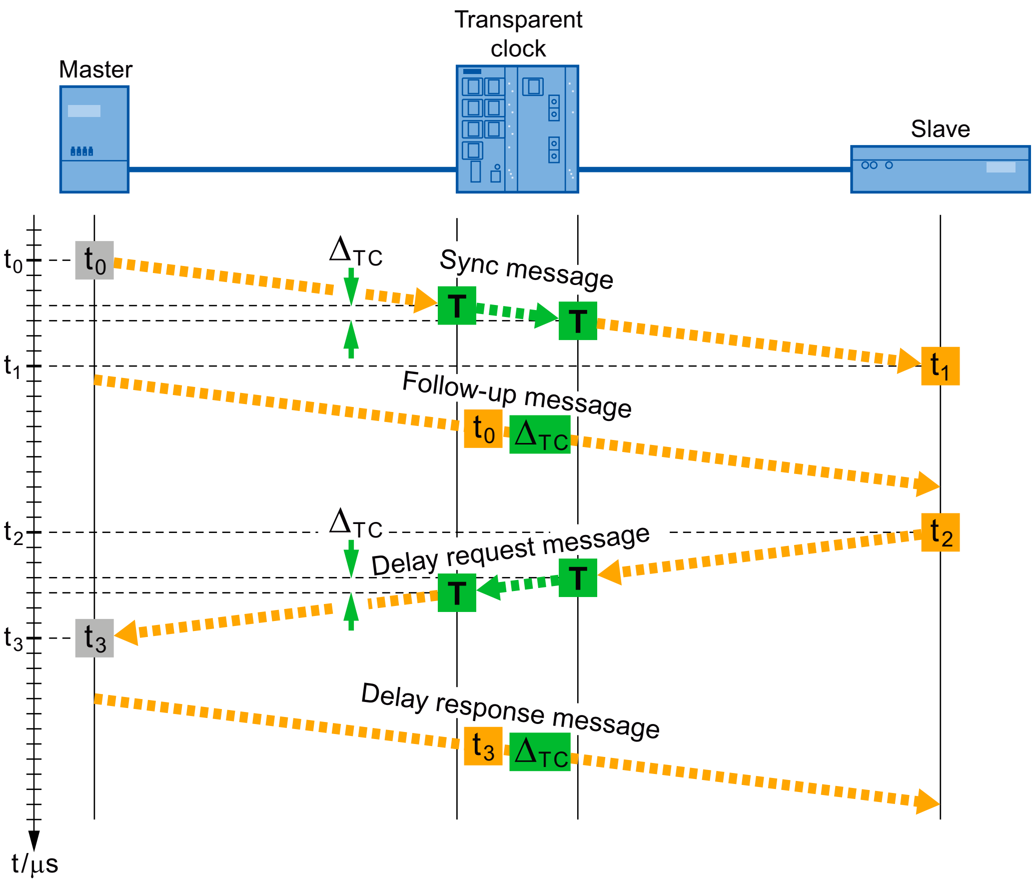
Even when there are topology changes in the network, the transparent clock still provides a more precise synchronization than the boundary clock. Regardless of its position in the topology, the function of the transparent clock is to forward synchronization frames. With a boundary clock, the assignments of master and slave to the individual ports and therefore to the entire synchronization hierarchy change. It can take several seconds before all the devices have resynchronized with the time master.

Synchronization mechanisms with transparent clocks

When calculating the actual message delay times over several network nodes, the time required for processing a message in a transparent clock must also be taken into account. This means that the transparent clock must calculate the time between receiving a message at the input port and forwarding it at the output port and send this value to the slave. To this end, there is a correction field in the PTP message in which the switches can make appropriate entries. The slave takes this information into account in the calculation of the message delay time.

The way that a transparent clock handles this correction information depends on the delay mechanism that was configured. With the delay request response mechanism, this is known as an end-to-end transparent clock and with the peer delay mechanism a peer-to-peer transparent clock.

End-to-end transparent clock

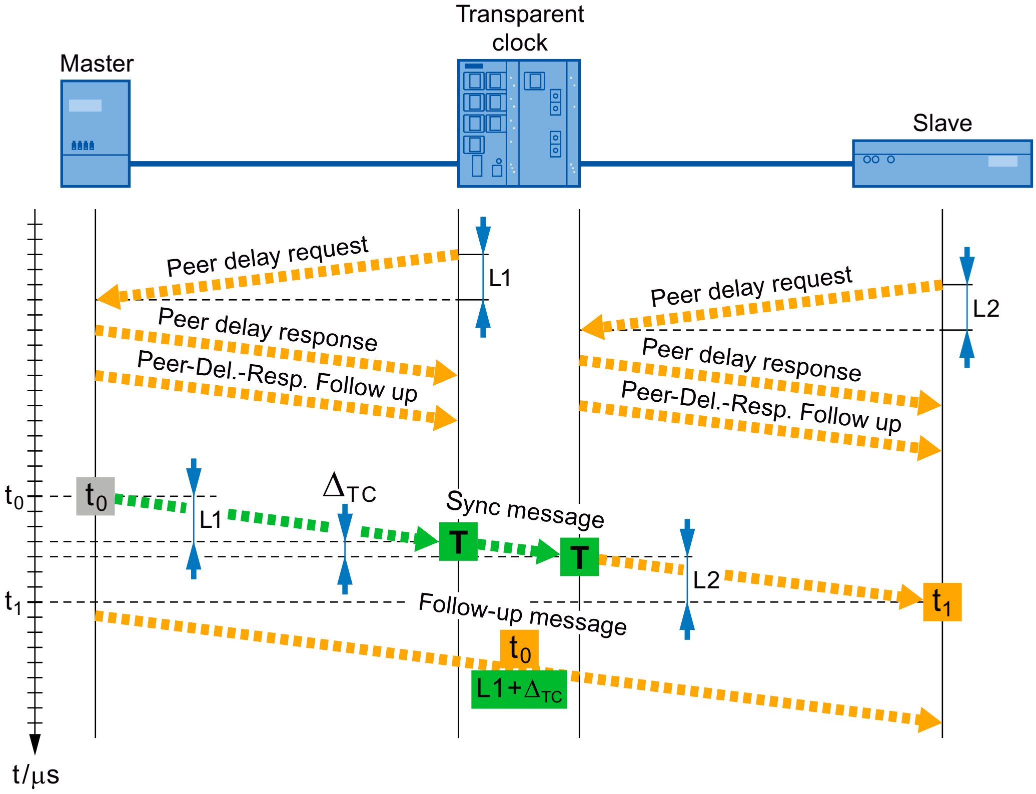


In the example shown, the time master sends a synchronization message. The time Δ_{TC} between receiving this message at the input port and forwarding it at the output port is entered in the correction field of the follow-up message by the transparent clock. The time at which this is sent t_0 is also received by the slave with the follow-up message and it can use this as described above to make the necessary calculations.

If a message on the way to a slave is forwarded by other transparent clocks, each device adds its time Δ_{TC} to the content of the correction field of the follow-up message. When the synchronization message arrives at the slave, the correction field contains the sum of all the times required to process the messages in the transparent clocks. The device also handles the delay request messages in the same way.

The slave corrects the message delay time by the value Δ_{TC} or, with several transparent clocks, by the sum of all the Δ_{TC} values and can synchronize its time of day as described in the section "Delay request response mechanism".

Peer-to-peer transparent clock



With the peer delay mechanism, each device calculates the delay time of a message to the neighboring device for its ports. The transparent clock obtains the message delay time L1 to the master, the slave obtains the value L2 for the message delay time to the transparent clock.

The processing of the synchronization message by the transparent clock takes a time of Δ_{TC}. The transparent clock enters the sum of L1 and Δ_{TC} in the correction field of the follow-up message. The slave then adds the content of the correction field to the message delay time L2 for the input port via which the synchronization message was received. In this way it obtains the delay time of a message between master and slave.

If a message on the way to the slave is forwarded by several transparent clocks, each transparent clock changes the content of the correction field of the follow-up message: The message delay time to the neighbor via which the synchronization message was received, and the time Δ_{TC} for processing the message are added to the content of the correction field.

One particular advantage of the peer-to-peer transparent clock is that the message delay times to the neighboring device are also calculated for blocked ports. When the network is reconfigured, this means that the slave has correct message delay times available very quickly.

4.5.32 Configuration of the Precision Time Protocol with the WBM

IEEE 1588 with SCALANCE devices

Note

The IEEE 1588 menu item is available with the following devices as of firmware version 3.5.0:

- SCALANCE X308-2M
- SCALANCE X308-2M PoE
- SCALANCE X302-7EEC
- SCALANCE X307-2EEC
- SCALANCE XR324-12M
- SCALANCE XR324-4M PoE
- SCALANCE XR324-4M EEC

The synchronization frames are forwarded through the network using to the "transparent clock" mechanism and the correction mechanisms "end to end" and "peer-to-peer" are supported.

The SCALANCE devices operate as a "two-step clock". They support the use both of one-step clocks as well as two-step clocks in the network.

The IEEE 1588v2 standard defines mechanisms with which highly precise time of day synchronization of devices in a network can be achieved. The listed SCALANCE devices also support time-of-day synchronization according to IEEE 1588v2 with appropriate hardware. The IEEE 1588v2 functionality is disabled on these devices when they are supplied and following a "Reset to factory default". To be able to use IEEE 1588v2, enable this function and configure every port that is on the synchronization path as well as ports that are blocked due to redundancy mechanisms. IEEE 1588v2 can also be used with redundancy mechanisms in the ring such as HSR, standby linking of rings, MRP and RSTP. The following sections describe the configuration options of Web Based Management.

1588 Configuration

On this page, you specify how the device will process PTP messages.

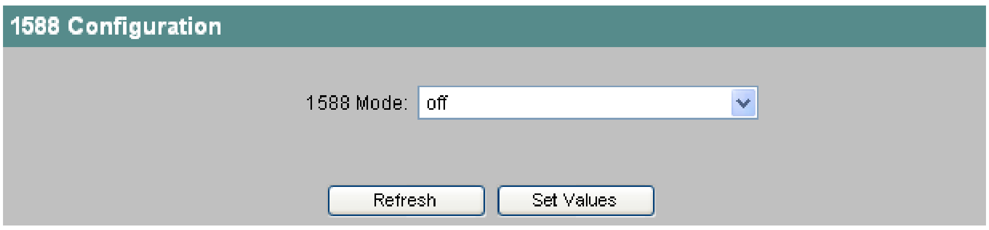


Figure 4-87 1588 Configuration

1588 Mode
You can make the following settings:

- off
  The device does not process any PTP messages. PTP messages are, however, forwarded according to the rules of the switch.
- Transparent Clock
  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.

1588 Transparent Clock Configuration

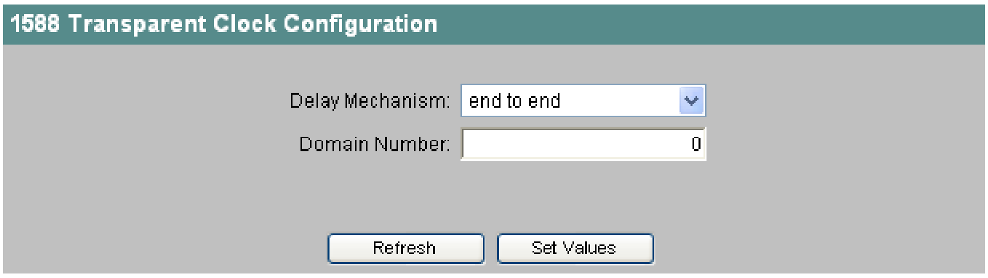


Figure 4-88 1588 transparent clock

Delay Mechanism
Specify the delay mechanism the device will work with:

- End to End (delay request response mechanism will be used)
- Peer to Peer (peer delay mechanism will be used)

Domain Number
Enter the domain number for the device here. The device ignores PTP messages with a different domain number. A SCALANCE device can only be assigned to one synchronization domain.

1588 Transparent Clock Port Parameters

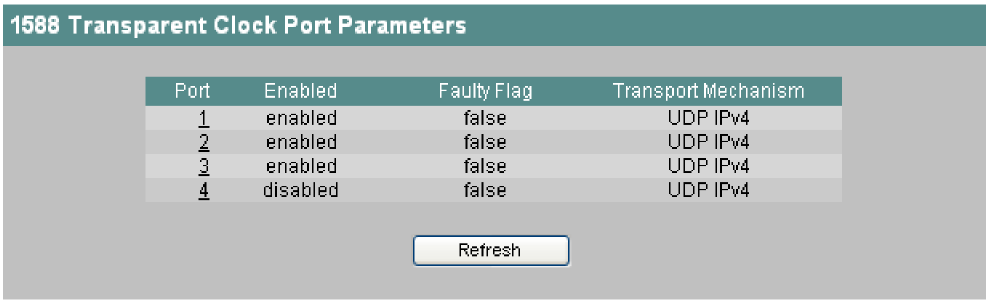


Figure 4-89 1588 Transparent Clock Port Parameters

The table shows detailed information about the individual ports:

Port
The port number. With modular devices, the slot number and port number are displayed separated by a dot. If you click on a port number, the corresponding page "1588 Transparent Clock Port Configuration" is displayed.

Enabled
The port status. The following entries are possible:

- disabled
  The port is not involved in PTP.
- enabled
  The port processes PTP messages.

Faulty Flag
The error status relating to PTP.

- true
  An error occurred.
- false
  No error has occurred on this port.

Transport Mechanism
Either "Ethernet" or "UDP IPv4".

1588 Transparent Clock Port Configuration

You open this page if you click on a port number in the table on the "Transparent Clock Port Parameters" page.

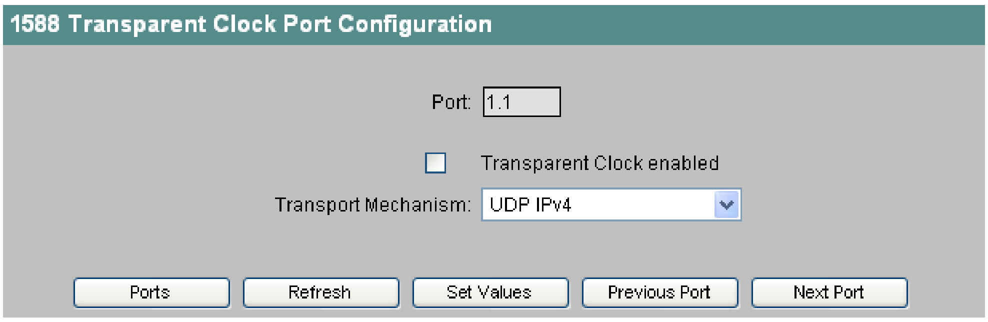


Figure 4-90 1588 Transparent Clock Port Configuration

Port
The port number. With modular devices, the slot number and port number are displayed separated by a dot.

Transparent Clock enabled
Select this check box one if you want the device to process PTP messages via this port.

Transport Mechanism
Choose how this port will handle PTP message data traffic. You can make different settings for the ports of a device, however, the relevant communications partner must support the selected transport mechanism. The following settings are possible:

- Ethernet
- UDP IPv4

Ports
If you click this button, you change to the "Transport Clock Port Parameters" page.

Previous Port und Next Port
If you click this button, you change directly to the configuration page of the previous or next port without needing to call the "Transparent Clock Port Parameters" page.

4.5.33 Configuration of the Precision Time Protocol with the CLI

CLI\SWITCH\1588>

<table>
<tr><th>Command</th><th colspan="2">Description</th><th>Comment</th></tr>
<tr><td rowspan="3">mode [off|TC]</td><td colspan="2">Enables/disables the Precision Time Protocol for the device and specifies how the device will react in terms of PTP:</td><td rowspan="3">Administrator only.</td></tr>
<tr><td>off</td><td>The device does not process any PTP messages.</td></tr>
<tr><td>TC</td><td>Transparent clock</td></tr>
<tr><td>TC</td><td colspan="2">Opens the menu for configuring a device as a transparent clock.</td><td>Administrator only.</td></tr>
</table>

CLI\SWITCH\1588\TC>

<table>
<tr><th>Command</th><th colspan="2">Description</th><th>Comment</th></tr>
<tr><td rowspan="3">delaymec [E2E|P2P]</td><td colspan="2">Specifies the delay mechanism for the device:</td><td rowspan="3">Administrator only.</td></tr>
<tr><td>E2E</td><td>End-to-end
(delay request response mechanism will be used).</td></tr>
<tr><td>P2P</td><td>Peer-to-peer
(peer delay mechanism will be used).</td></tr>
<tr><td>domainnb [number]</td><td colspan="2">Specifies the identification number for the time domain. Only devices within the domain are synchronized, PTP messages with a different domain number are discarded.</td><td>Administrator only.</td></tr>
<tr><td>PORTS</td><td colspan="2">Opens the PORTS menu.</td><td>Administrator only.</td></tr>
</table>

CLI\SWITCH\1588\TC\PORTS>

<table>
<tr><th>Command</th><th colspan="2">Description</th><th>Comment</th></tr>
<tr><td>tcstate <E|D> [ports]</td><td colspan="2">Enables/disables the specified ports.
A range of ports is specified with a hyphen. Several ports are separated by blanks or commas.</td><td>Administrator only.</td></tr>
<tr><td rowspan="3">transmec <IPv4|ETH> [ports]</td><td colspan="2">Specifies the protocol for transferring the PTP messages. This protocol must also be supported by the communications partner of the port.</td><td rowspan="3">Administrator only.</td></tr>
<tr><td>IPv4</td><td>Internet Protocol (Layer 3)</td></tr>
<tr><td>ETH</td><td>Ethernet (Layer 2)</td></tr>
</table>

4.5.34 Port Diagnostics (SCALANCE X-300/X408-2)

Switch Port Diagnostics

With this dialog, each individual Ethernet port can run independent fault diagnostics on the cable. This allows short-circuits and cable breaks to be localized.

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

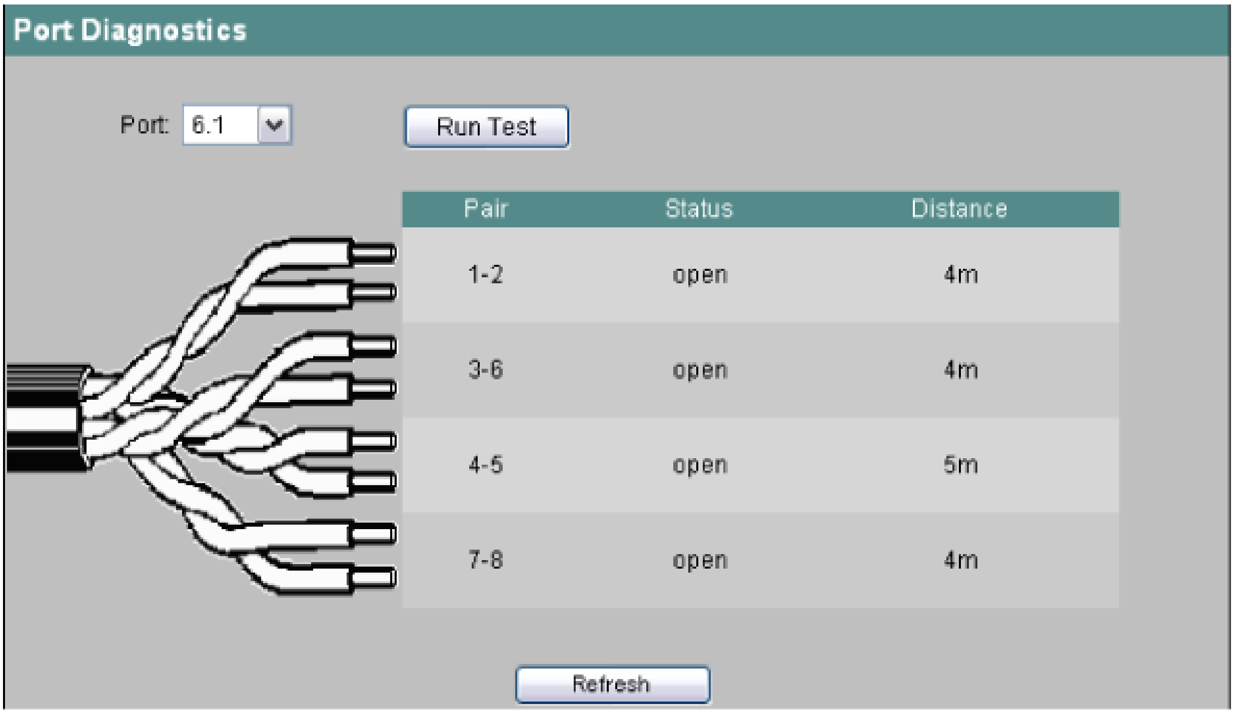


Figure 4-91 Port Diagnostics

Port
The port to be tested is specified here.

Run Test
This button activates the test.

Pair
Displays the pair of wires in the cable.
Pairs 4-5 and 7-8 are not used with Fast Ethernet.

Status
Displays the status of the cable.

Distance
Displays the distance to the cable end, cable break, or short-circuit.

Syntax of the Command Line Interface

Table 4- 62 Port-Diagnostics - CLI\SWITCH\PORTDIAG>

Command	Description	Comment
runtest [Ports]	Tests the specified ports. If no port is specified, all are tested.	Administrator only.

4.5.35 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.

NOTICE
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.

Application example

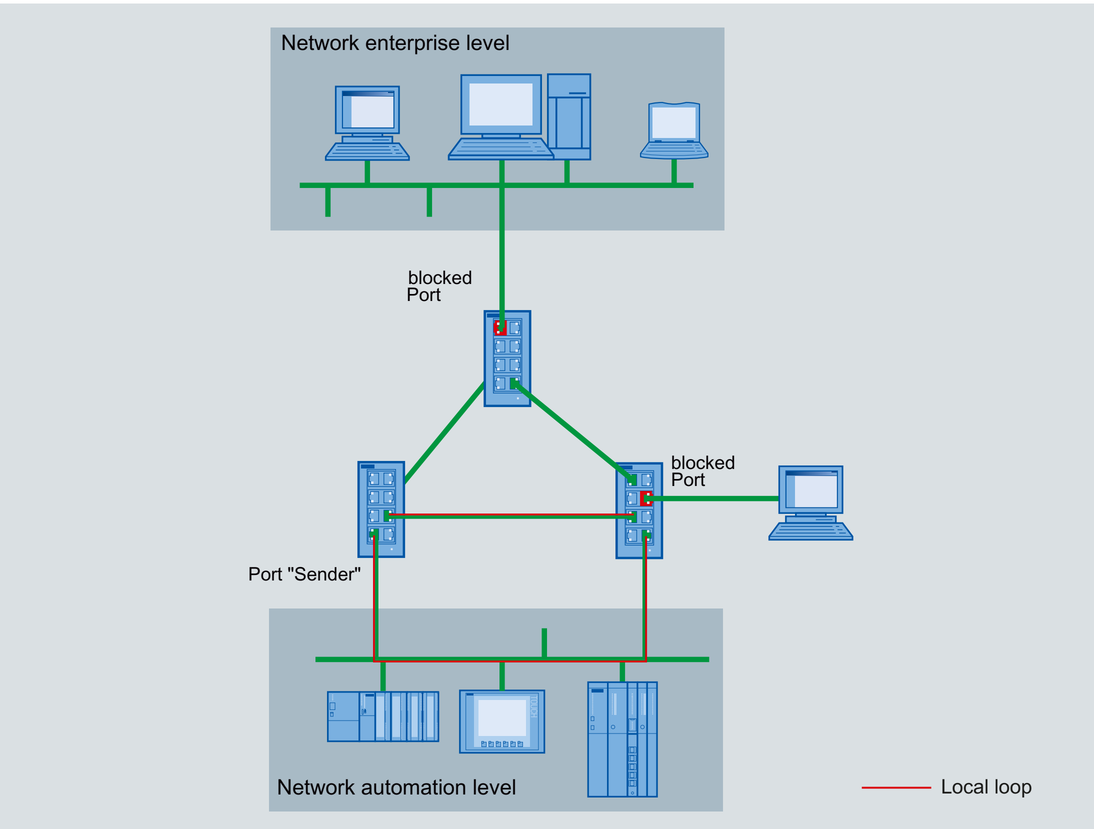


Figure 4-92 Loop detection with a configured sender

The figure above shows the networking of the enterprise level and automation level via an MRP/HSR ring. The blocked ports marked red were set to "Disable port".

If a loop occurs in the network at the automation level, this is detected as a Remote Loop. No loop detection frames can be forwarded to the network at the enterprise level or to the end device due to the blocked ports.

If a "Local Loop" occurs, the port can be blocked automatically following a specified number of loop detection frames.

How to make the settings for loop detection is shown in the following sections based on the WBM pages.

Loop Detection Configuration

On this page, make the settings for loop detection that apply to all ports.

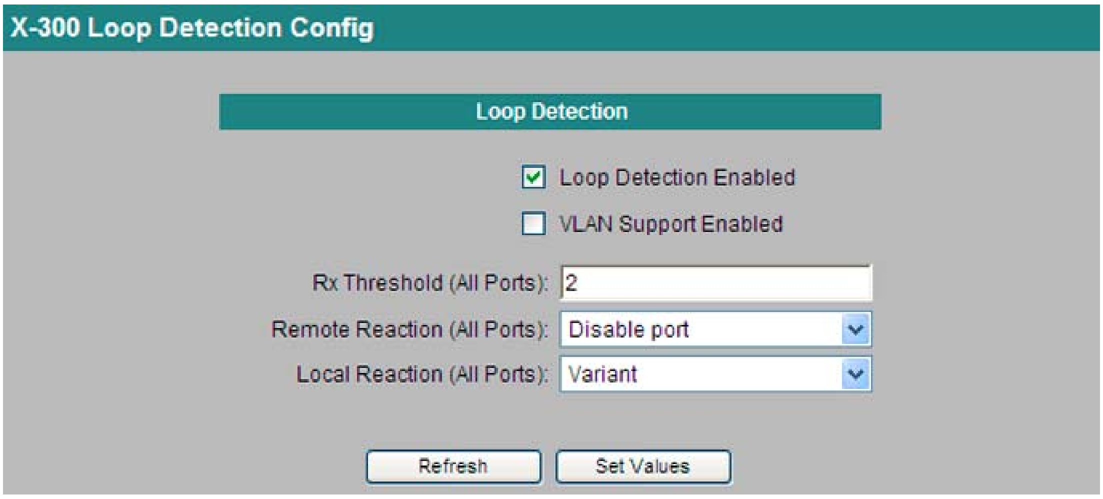


Figure 4-93 Configuration for loop detection

NOTICE
Loops can only be detected between devices that forward loop detection frames. Loops via network components whose ports were blocked are not detected.

Loop Detection Enabled

Enable or disable loop detection by clicking the check box.
If loop detection is disabled, the loop detection frames of other devices are forwarded.

VLAN Support Enabled

By clicking the check box, specify for all ports whether or not loop detection frames are sent out for all configured VLANs configured at the relevant ports.
If VLAN support is disabled, only loop detection frames without a VLAN tag are sent.

Rx Threshold (All Ports):

By entering a number, specify the number of received loop detection frames as of which a loop is assumed.
If a port-specific setting was made, see below, "Variant" is displayed.

Remote Reaction (All Ports):

Specify how the device will react if a remote loop occurs. Select one of the two options from the drop-down list:

No reaction:	A loop has no effect on the port at which the loop occurs.
Disable port:	The port at which the loop occurs is blocked.

If a port-specific setting was made, see below, no selection can be made here. "Variant" is displayed.

Local Reaction (All Ports):

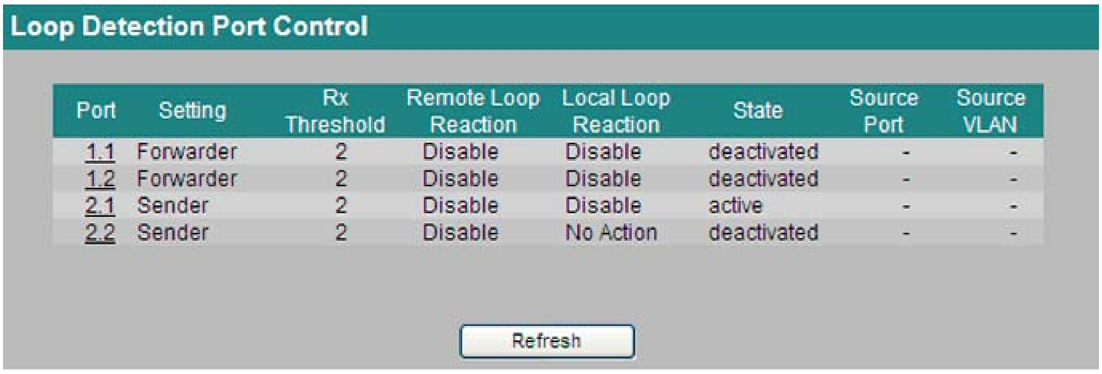
Specify how the device will react if a local loop occurs. Select one of the two options from the drop-down list:

No reaction:	A loop has no effect on the port at which the loop occurs.
Disable port:	The port is blocked.

If a port-specific setting was made, see below, no selection can be made here. "Variant" is displayed.

Loop Detection Port Control

Make these specific settings from individual ports on this page.


Loop Detection Port Control

Port	Setting	Rx Threshold	Remote Loop Reaction	Local Loop Reaction	State	Source Port	Source VLAN
1.1	Forwarder	2	Disable	Disable	deactivated	-	-
1.2	Forwarder	2	Disable	Disable	deactivated	-	-
2.1	Sender	2	Disable	Disable	active	-	-
2.2	Sender	2	Disable	No Action	deactivated	-	-

Refresh

Figure 4-94 Loop Detection Port Control

Click on a port number in the "Port" column to configure this port. The page shown below appears:

Loop Detection Port Configuration

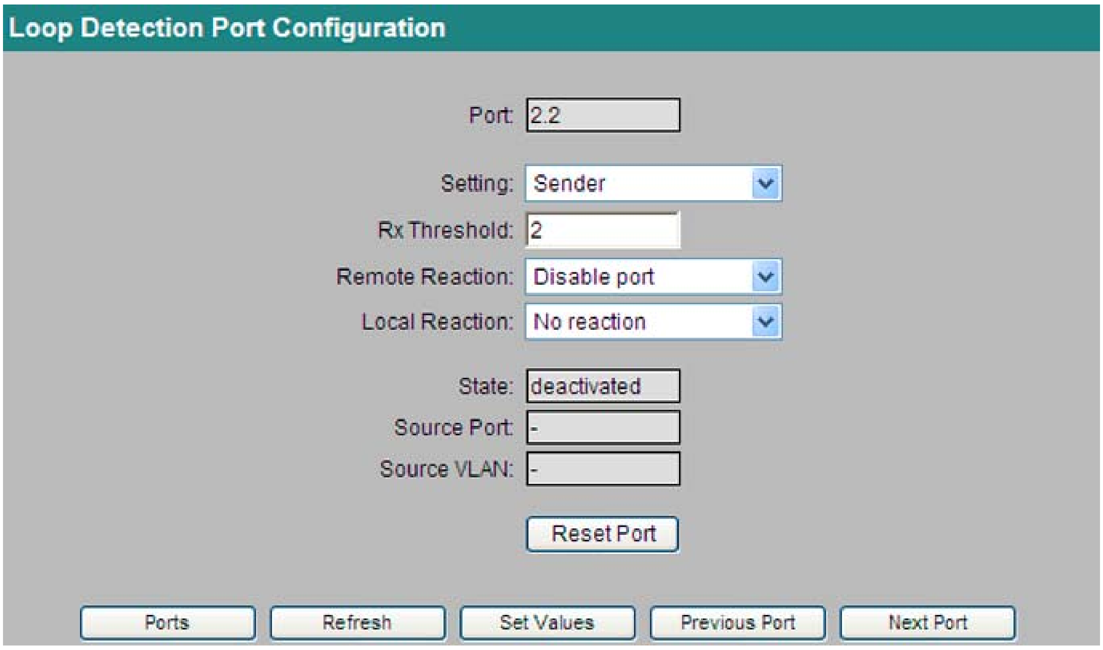


Figure 4-95 Loop Detection Port Configuration

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".

Port:

This box shows the number of the selected port.

Setting:

Specify how the port handles loop detection frames. Select one of the following options from the drop-down list:

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.

Rx Threshold:

By entering a number, specify the number of received loop detection frames as of which a loop is assumed.

If more loop detection frames than specified are received, the forwarding of the loop detection frames is blocked.

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 reaction:	A loop has has no effect on the port.
Disable port:	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 reaction:	A loop has has no effect on the port.
Disable port:	The port is blocked.

State:

This box shows whether loop detection is enabled or disabled for this port.

Source Port:

This box shows the receiver 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 Port" button

After a loop in the network has been eliminated, click this button to reset the port again.

Syntax of the Command Line Interface

Table 4- 63 Loop Detection Configuration - CLI\SWITCH\LOOPD >

Command	Description	Comment
info	Displays information about the "Loop Detection Configuration".	
loopd [E | D]	Enables / disables loop detection.	Administrator only.
loopdp <port> [B | F | S]	Defines the behavior of a port for loop detection: • "Blocked" • "Forwarder" • "Sender"	Administrator only.
rxthres <port> <count>	Specifies the Rx.Threshold.	Administrator only.
local <port> [N | D]	Specifies the reaction to a local loop.	Administrator only.
remote <port> [N | D]	Specifies the reaction to a remote loop.	Administrator only.
reset <port>	Reactivates the port if it was deactivated due to a detected loop.	Administrator only.

4.5.36 NAT - Network Address Translation

Network Address Translation (NAT) means the translation of a network address in a router related to a data stream. This does not necessarily only mean the IP address. If nodes with local addresses take over server functions for the outside, not only the IP addresses but also the port numbers will be replaced in the router.

The most common reason for the use of NAT is that the IP addresses of the devices in the local network should not be visible to the outside.

Traditional NAT

With Traditional NAT, connections are only permitted in one direction, originating from the local network. Traditional NAT distinguishes between the methods Basic NAT and NAPT (Network Address Port Translation).

In Basic NAT, a pool of global/external addresses is kept available for the translation and each internal address is converted to an external address.

With NAPT, the transport identifiers, for example port numbers, are included in the translation. For this reason, this method only requires a single external address for translation.

1:1 NAT with SCALANCE X300/X400

A special variant of NAT that is used with SCALANCE X300/X400 is 1:1 NAT, also known as bidirectional NAT. This variant allows connection establishment in both directions; in other words, also originating from the external network into the local network. The translation of the network addresses is performed using a static table. In this table, you specify 1:1 the global IP address into which a local IP address will be translated and vice versa.

NAT configuration

Note

The NAT function uses a lot of computing capacity. If you want to use the switch as a NAT device, you should therefore disable as many of the other functions and protocols (RSTP, HSR/MRP, PTP, etc.) as possible. This results in a higher data throughput for the NAT frames.

Click on the "NAT" folder in the menu tree to go to the "Network Address Translation" window. This window shows the current NAT settings.

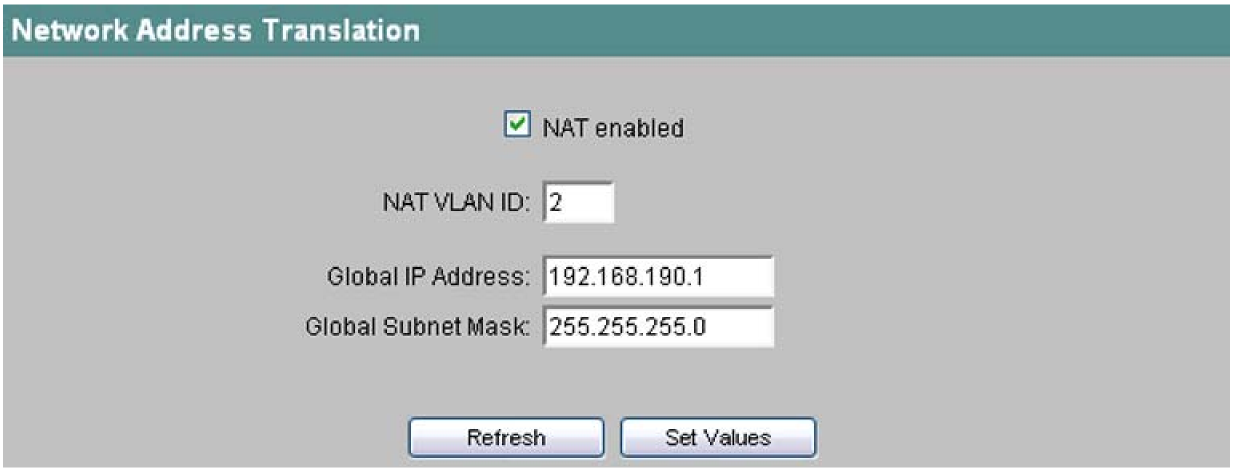


Figure 4-96 Network Address Translation

NAT enabled

Enable or disable the NAT function by clicking the check box.

NAT VLAN ID:

In the input box, enter the ID of a configured virtual LAN for the global network attachment.

Global IP Address:

In the input box, enter the global IP address for the dynamic address translation.

Global Subnet Mask:

Enter the global subnet mask in the input box.

Static NAT table

In the menu tree, the "NAT" folder contains the subsection "Basic NAT". Click this item to go to the static address table.

Figure 4-97 Static NAT table

Creating a new entry

1. Click the "New Entry" button.
   The "Basic Network Address Translation Entry" window appears.
2. In the "Local IP" box, enter the local IP address to be translated.
3. In the "Global IP" box, enter the corresponding global IP address.
4. Click the "Set Values" button to save the settings.

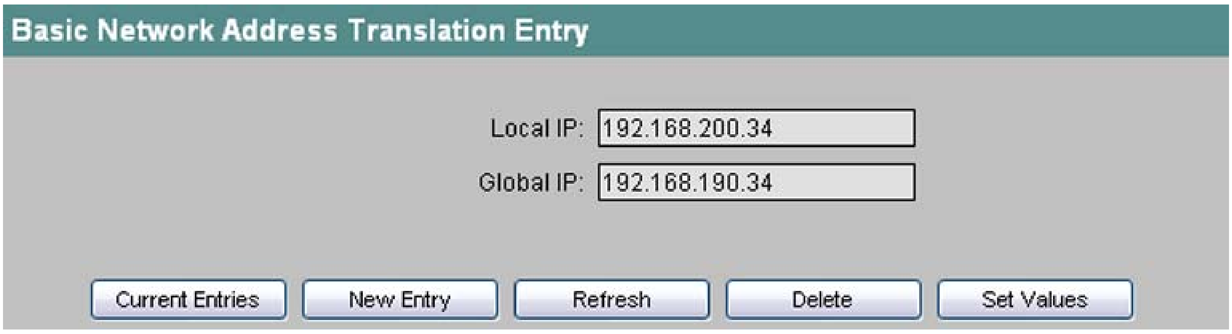


Figure 4-98 Creating a NAT entry

Deleting an existing entry

1. Click on an existing IP address in the "Basic Network Address Translation" window.
   The "Basic Network Address Translation Entry" window appears.
2. Click the "Delete" button to delete this entry.

Syntax of the Command Line Interface

NAT - Network Address Translation

Table 4- 64 CLI\SWITCH\NAT>

Command	Description	Comment
info	Displays the current NAT settings.	
nat [<E|D>]	Enables/disables the NAT function.	Administrator only.
config <VID> <IP> <subnet>	Specifies the NAT settings VLAN ID, IP address and subnet mask.	Administrator only.
BASIC	Opens the "Basic NAT" menu item.	Administrator only.

Table 4- 65 CLI\SWITCH\NAT\BASIC>

Command	Description	Comment
info	Displays the current NAT entries.	
add <local IP> <global IP>	Creates a new NAT entry.	Administrator only.
delete <local IP> <global IP>	Deletes an existing NAT entry.	Administrator only.

4.6 The Statistics menu

Counting and evaluation of received frames

An IE switch has internal statistics counters with which it counts the number of received frames for each port according to the following criteria:

- Frame length
- Message frame type
- Bad frames

This information provides you with an overview of the data traffic and any problems on the network.

Syntax of the Command Line Interface

Table 4- 66 Statistics - CLI\SWITCH\STATS>

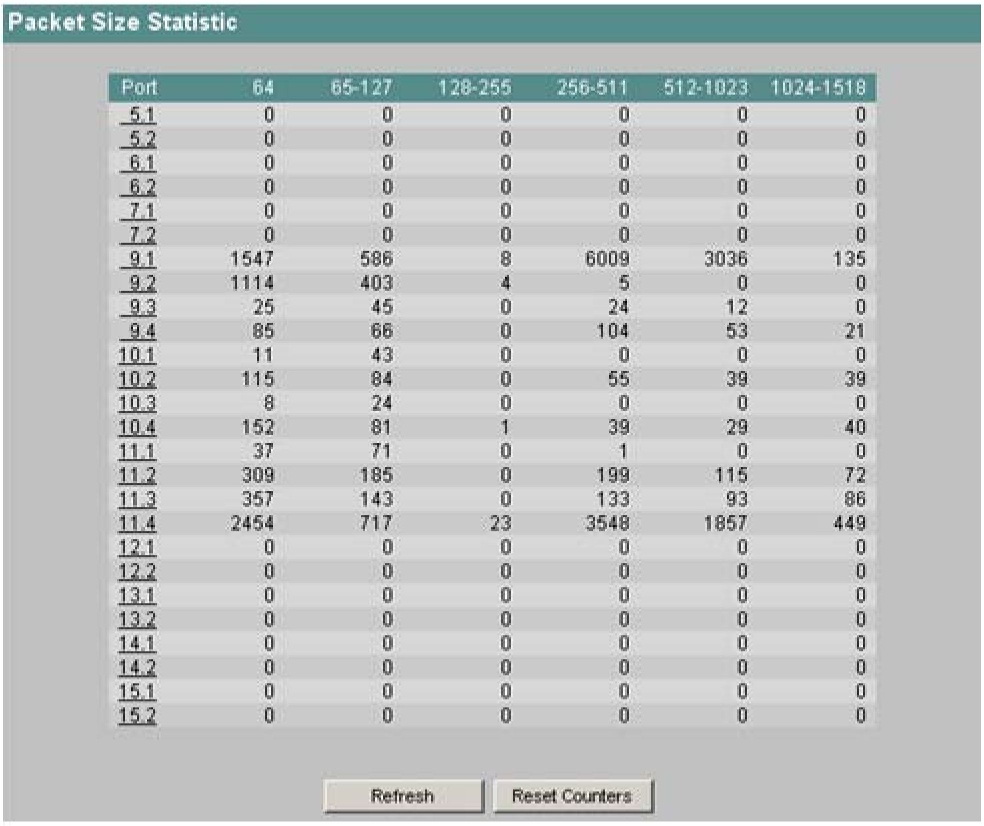
Command	Description	Comment
clear	The clear command resets the counters.	Administrator only.

4.6.1 Packet Size Statistic

Received frames sorted by length

The "Packet Size Statistics" page displays how many packets of which size were received at each port.

If you click the "Reset Counters" button, you reset the counters for all ports.


Packet Size Statistic

Port	64	65-127	128-255	256-511	512-1023	1024-1518
5.1	0	0	0	0	0	0
5.2	0	0	0	0	0	0
6.1	0	0	0	0	0	0
6.2	0	0	0	0	0	0
7.1	0	0	0	0	0	0
7.2	0	0	0	0	0	0
9.1	1547	586	8	6009	3036	135
9.2	1114	403	4	5	0	0
9.3	25	45	0	24	12	0
9.4	85	66	0	104	53	21
10.1	11	43	0	0	0	0
10.2	115	84	0	55	39	39
10.3	8	24	0	0	0	0
10.4	152	81	1	39	29	40
11.1	37	71	0	1	0	0
11.2	309	185	0	199	115	72
11.3	357	143	0	133	93	86
11.4	2454	717	23	3548	1857	449
12.1	0	0	0	0	0	0
12.2	0	0	0	0	0	0
13.1	0	0	0	0	0	0
13.2	0	0	0	0	0	0
14.1	0	0	0	0	0	0
14.2	0	0	0	0	0	0
15.1	0	0	0	0	0	0
15.2	0	0	0	0	0	0

Refresh | Reset Counters

Figure 4-99 Packet Size Statistic

If you click on an entry in the Port column, the "Packet Size Statistics graphic" is displayed for the selected port. You then see a configurable graphical representation of the counter value.

Graphic representation of the statistics

This page displays the number of frames received at each port graphically. The display is dependent on the frame length. There is a separate element in the graphic for each of the following ranges:

- 64 bytes
- 65 - 127 bytes
- 128 -255 bytes

- 256 -511 bytes
- 512 -1023 bytes
- 1024 -1518 bytes

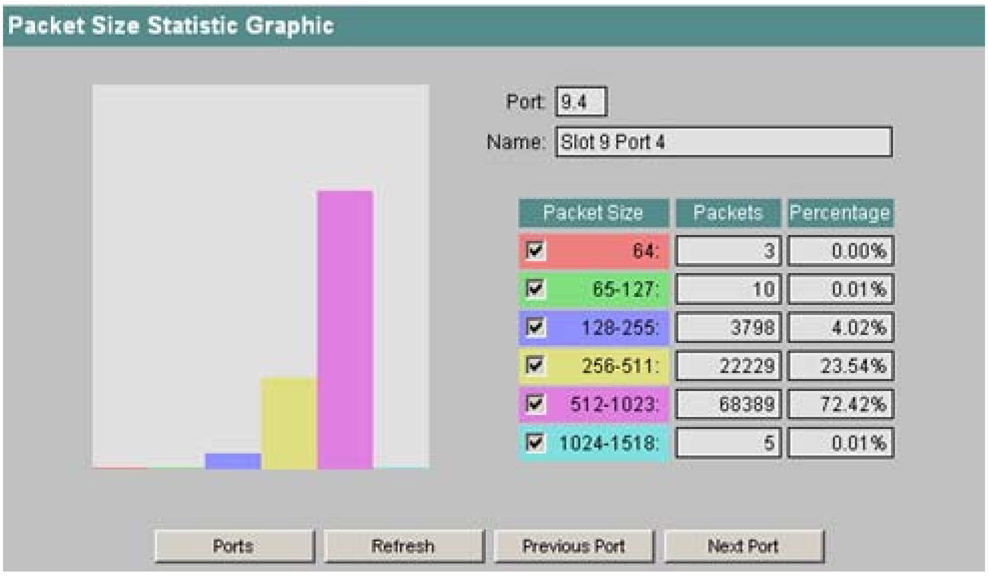


Figure 4-100 Packet Size Statistic Graphics

With the check box in the "Packet Size" column, you decide the content of the graphic. The value in the "Packets" column in the graphic is only displayed for a certain range if the appropriate check box is selected. The "Percentage" column shows the packets in a certain length range as a percentage of the total packets for this port. When the percentage is calculated, ranges are included only if their check boxes are selected.

With the "Previous Port" and "Next Port" buttons, you can change to the display of the previous or next port.

Syntax of the Command Line Interface

Table 4- 67 Statistics - CLI\ SWITCH\STATS>

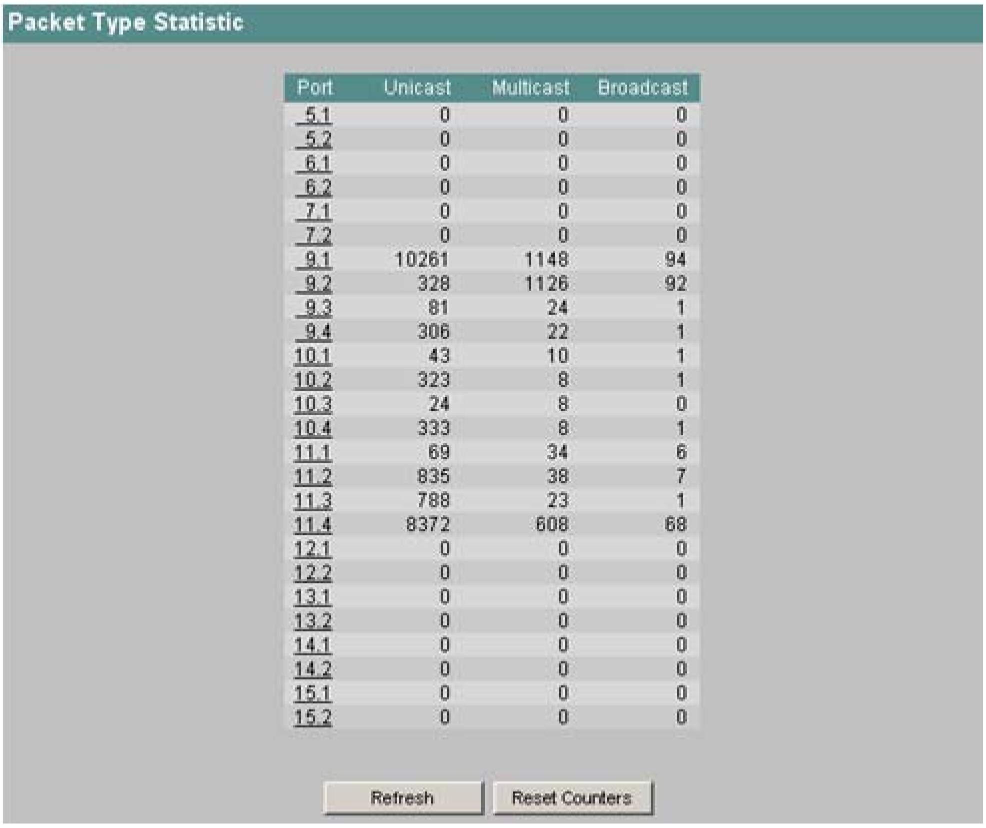
Command	Description	Comment
size [ports]	Shows the number of received frames sorted according to frame length. Several ports can be specified. Example: • size 5.1, 6.1-7.2 Shows the lengths of the frames received at ports 5.1 and 6.1 through 7.2.	-

4.6.2 Packet Type Statistic

Received frames sorted by type

The "Packet Type Statistics" page displays how many frames of the type "unicast", "multicast", and "broadcast" were received at each port.

If you click the "Reset Counters" button, you reset the counters for all ports.



Packet Type Statistic

Port	Unicast	Multicast	Broadcast
5.1	0	0	0
5.2	0	0	0
6.1	0	0	0
6.2	0	0	0
7.1	0	0	0
7.2	0	0	0
9.1	10261	1148	94
9.2	328	1126	92
9.3	81	24	1
9.4	306	22	1
10.1	43	10	1
10.2	323	8	1
10.3	24	8	0
10.4	333	8	1
11.1	69	34	6
11.2	835	38	7
11.3	788	23	1
11.4	8372	608	68
12.1	0	0	0
12.2	0	0	0
13.1	0	0	0
13.2	0	0	0
14.1	0	0	0
14.2	0	0	0
15.1	0	0	0
15.2	0	0	0

Refresh
Reset Counters

Figure 4-101 Packet Type Statistic

If you click on an entry in the Port column, the "Packet Type Statistics graphic" is displayed for the selected port. You then see a configurable graphical representation of the counter value.

Graphic representation of the statistics

This page displays the number of frames received at each port graphically. The display depends on the packet type. There is a separate element in the graphic for each of the following ranges:

- Unicast
- Multicast
- Broadcast

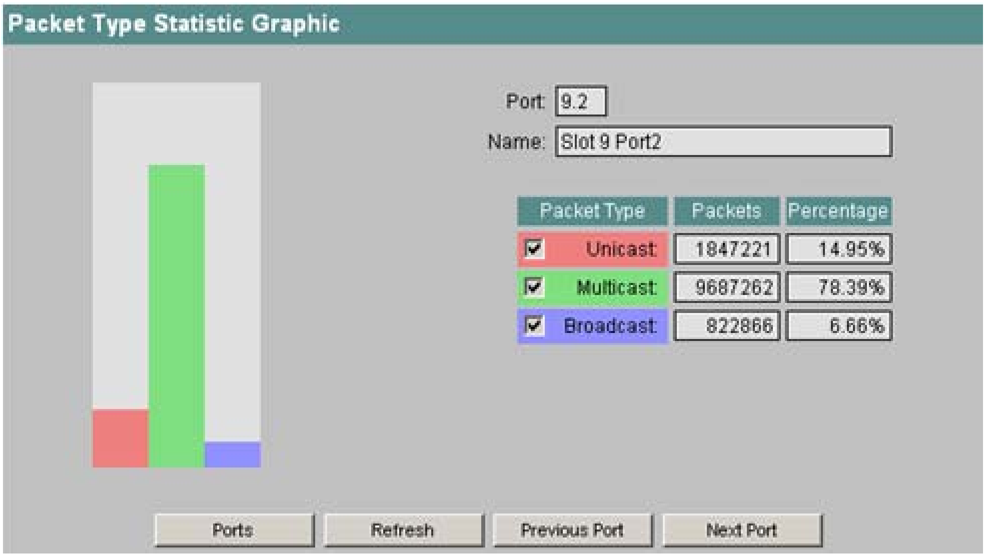


Figure 4-102 Packet Type Statistic Graphic

With the check box in the "Packet Type" column, you decide the content of the graphic. The value in the "Packets" column in the graphic is only displayed for a certain packet type if the appropriate check box is selected. The "Percentage" column shows the packets of a certain type as a percentage of the total packets for this port. When the percentage is calculated, packet types are included only if their check boxes are selected.

With the "Previous Port" and "Next Port" buttons, you can change to the display of the previous or next port.

Syntax of the Command Line Interface

Table 4- 68 Statistics - CLI\SWITCH\STATS>

Command	Description	Comment
type [ports]	Shows the number of received frames sorted according to frame type. Several ports can be specified. Example: • type 5.1, 6.1-7.2 Shows the types of the frames received at ports 5.1 and 6.1 through 7.2.	-

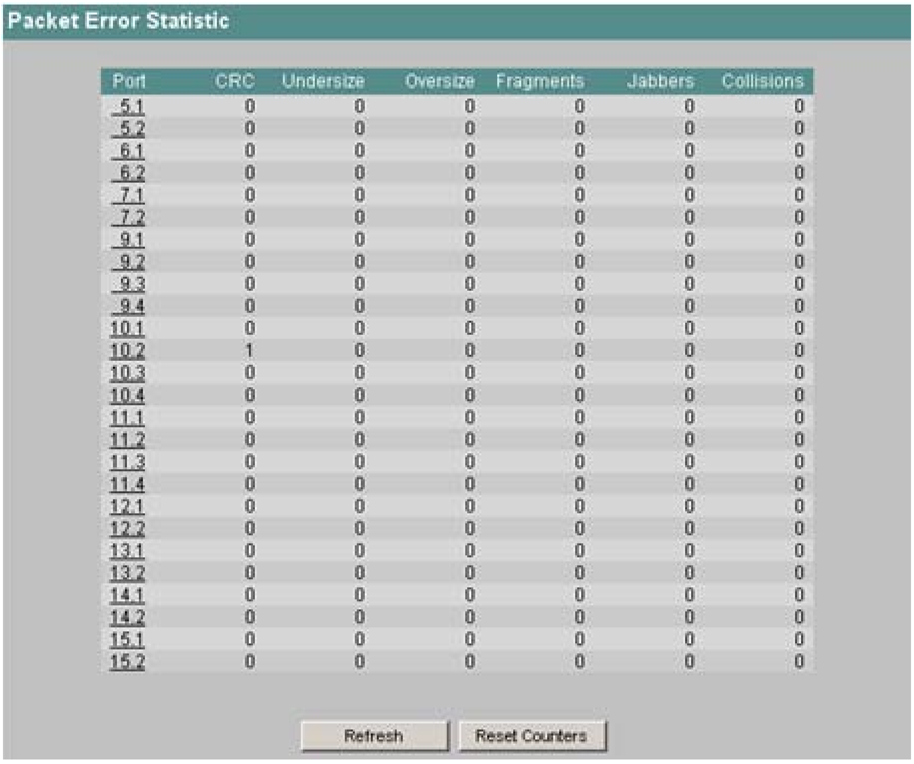
4.6.3 Error Statistic

Errors in received packets

The "Packet Error Statistics" page shows how many bad frames were received per port. The following error types are distinguished:

- CRC
  Packets whose content did not match the CRC checksum.
- Undersize
  Packets with a length less than 64 bytes.
- Oversize
  Packets with a length greater than 1518 or 1522 bytes for frames with a VLAN tag.
- Fragments
  Packets with a length less than 64 bytes and a bad CRC checksum.
- Jabbers
  Packets with a length greater than 1518 or 1522 bytes for frames with a VLAN tag and a bad CRC checksum.
- Collisions
  Detected collisions.

If you click the "Reset Counters" button, you reset the counters for all ports.


Packet Error Statistic

Port	CRC	Undersize	Oversize	Fragments	Jabbers	Collisions
5.1	0	0	0	0	0	0
5.2	0	0	0	0	0	0
6.1	0	0	0	0	0	0
6.2	0	0	0	0	0	0
7.1	0	0	0	0	0	0
7.2	0	0	0	0	0	0
9.1	0	0	0	0	0	0
9.2	0	0	0	0	0	0
9.3	0	0	0	0	0	0
9.4	0	0	0	0	0	0
10.1	0	0	0	0	0	0
10.2	1	0	0	0	0	0
10.3	0	0	0	0	0	0
10.4	0	0	0	0	0	0
11.1	0	0	0	0	0	0
11.2	0	0	0	0	0	0
11.3	0	0	0	0	0	0
11.4	0	0	0	0	0	0
12.1	0	0	0	0	0	0
12.2	0	0	0	0	0	0
13.1	0	0	0	0	0	0
13.2	0	0	0	0	0	0
14.1	0	0	0	0	0	0
14.2	0	0	0	0	0	0
15.1	0	0	0	0	0	0
15.2	0	0	0	0	0	0

Figure 4-103 Packet Error Statistic

If you click on an entry in the "Port" column, the "Packet Error Statistics graphic" is displayed for the selected port. You then see a configurable graphical representation of the counter value.

Graphic representation of the statistics

This page displays the number of bad frames graphically. The display is dependent on the cause of the error. There is a separate element in the graphic for each of the following causes of error:

- CRC
- Undersize
- Oversize
- Jabbers
- Collisions

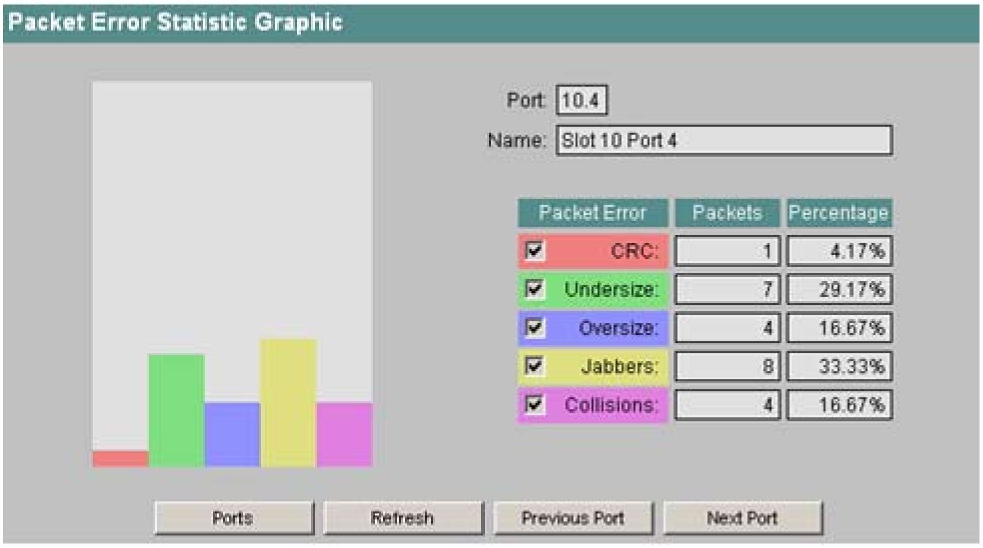


Figure 4-104 Packet Error Statistic Graphic

With the check box in the "Packet Error" column, you decide the content of the graphic. The value in the "Packets" column in the graphic is only displayed for a certain packet type if the appropriate check box is selected. The "Percentage" column shows the errors of a certain type as a percentage of the total errors for this port. When the percentage is calculated, error types are included only if their check boxes are selected.

With the "Previous Port" and "Next Port" buttons, you can change to the display of the previous or next port.

Syntax of the Command Line Interface

Table 4- 69 Statistics - CLI\SWITCH\STATS>

Command	Description	Comment
error [ports]	Shows the number of received frames sorted according to frame errors. Several ports can be specified. Example: • error 5.1, 6.1-7.2 Shows the bad frames received at ports 5.1 and 6.1 through 7.2.	-

4.7 The PoE menu item

Settings for Power over Ethernet

SCALANCE devices of the "PoE" version, can supply other PoE-compliant devices with power via an Ethernet cable. 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.

The overview page shows information on the power supplied by the SCALANCE device with PoE and detailed information on each individual PoE port.

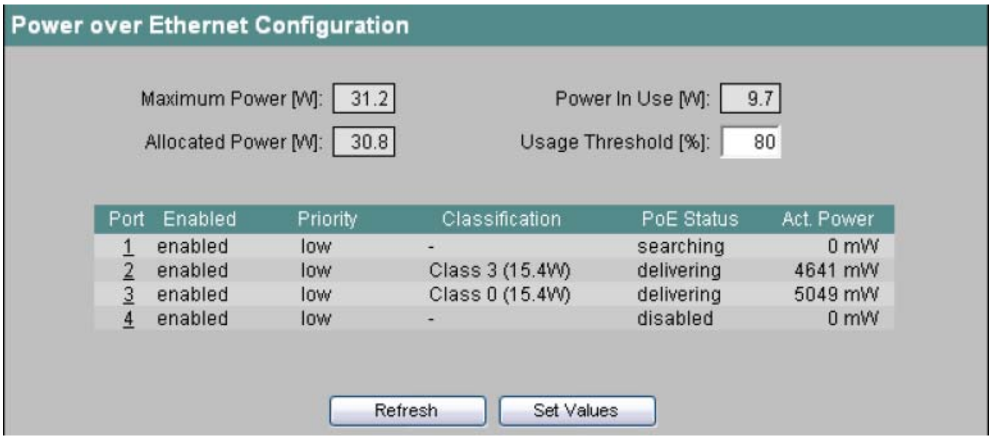


Figure 4-105 Information on the SCALANCE PoE configuration

Maximum Power [W] (read-only)
Maximum power that the SCALANCE provides to supply PoE devices.

Allocated Power [W] (read-only)

Sum of the power reserved by the PoE devices.

Power in Use [W] (read-only)
Sum of the power being used by the end devices.

Usage Threshold [%]

As soon as the power being used by the connected devices exceeds this percentage of the maximum power, an event is triggered.

Making settings for a port

Click on a number in the "Port" column to open the "PoE Port Configuration" page.

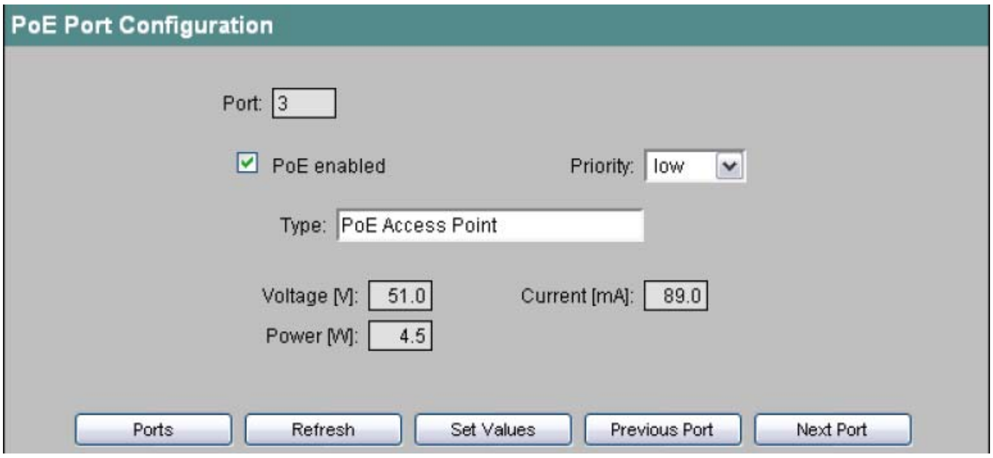


Figure 4-106 Detailed information on the power supply of a port

PoE enabled
If the check box is selected, the PoE power supply for this port is enabled.

Priority
Specifies the priority of this port for the power supply. The following settings are possible:
- low
- high
- critical

If two ports have the same priority setting, the port with lower number has preference.

Type
Here, you can enter a string to describe the connected device in greater detail. The maximum length is 64 characters.

Voltage [V] (read-only)
The voltage being applied to this port.

Current [mA] (read-only)
The current with which a device is supplied from this port.

Power [W] (read-only)
This is the power the SCALANCE output at this port.

Syntax of the Command Line Interface

Table 4- 70 CLI\POE>

Command	Description	Comment
info [ports]	Displays information about PoE for the relevant port.	-
pseusage [percent]	Sets a value (percentage) for the Usage Threshold parameter. As soon as the power being used by the connected devices exceeds this percentage of the maximum power, an event is triggered. If you call this command without parameters, the current value is displayed.	Administrator only.
status [<E|D> [ports]]	Enables/disables PoE power supply for the specified port.	Administrator only.
prio [<LOW|HIGH|CRITICAL> [ports]]	Sets the priority for the power supply for the specified port. If no port is specified, the value applies to all ports.	Administrator only.
type <port> [string]	Specifies a string describing the connected device in greater detail. The maximum length is 64 characters.	Administrator only.

4.8 The Router menu (SCALANCE X414-3E)

Note

The routing function is available only with the SCALANCE X414-3E.

Introduction to the procedure

To set up a SCALANCE X414-3E as a router, first create at least two subnets and assign each subnet to a previously defined VLAN. You can then enter the static routes and/or enable the router protocols RIP or OSPF.

For information on configuring VLANs, refer to the section "Current VLAN Configuration menu item".

4.8.1 Router Configuration

Introduction

The "Router Configuration" screen appears if you click the *Router* folder icon. In this screen, you can set up the SCALANCE X414-3E as an IPv4 router.

To distribute the routing information in the network, you can use the RIPv2 and OSPFv2 protocols that you can select here. You can see the detailed settings for the protocols in the relevant sub-dialogs.

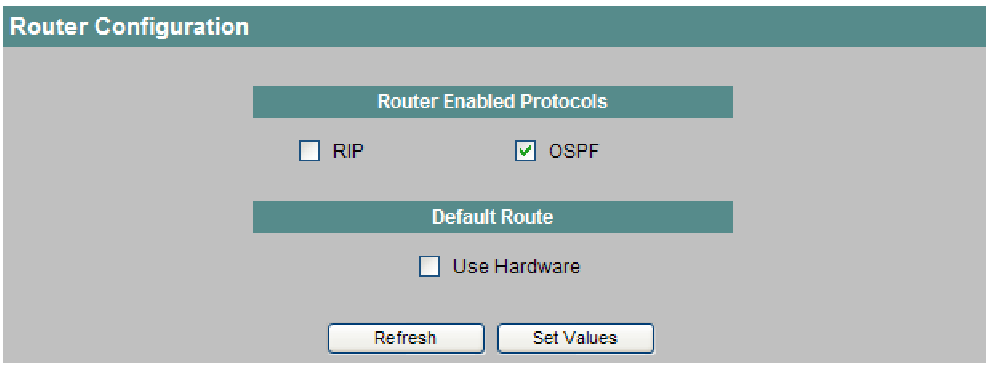


Figure 4-107 Router Configuration

Settings for the SCALANCE X-400

RIP
Enables the "Routing Information Protocol version 2" option (RIP).

Note

The router uses the RIP protocol as soon as at least one interface was configured for RIP.

OSPF
Enables the "Open Shortest Path First protocol version 2" option (OSPF).

Note

The router uses the OSPF protocol as soon as at least one interface for OSPF is configured and a router ID has been specified.

Use Hardware
The SCALANCE X-414 provides the option of high-speed hardware routing. Select this check box if you want to enable hardware routing for the default addresses.

Note

If the default route is entered in the hardware, this reduces the number of subnets that can be reached using routing to 14.

With dynamically learned routes (RIP or OSPF), the routing mechanism automatically removes the default routes from the hardware when necessary.

Syntax of the Command Line Interface

Table 4- 71 Router Configuration - CLI\ROUTER>

Command	Description	Comment
setrip <E|D>	Enables/Disables RIP	Administrator only.
setospf <E|D>	Enables/Disables OSPF	Administrator only.
defrthw <E|D>	Enables/disables hardware routing for default addresses.	Administrator only.

4.8.2 Router Subnets

Creating subnets

To operate the SCALANCE X414-3E as an IPv4 router, you need to create several (at least two) subnets.

The agent configuration corresponds to the first subnet (see section "Agent menu"). The data can only be modified there.

All other subnets can be created here ("New Entry" button). A subnet always relates to a VLAN ID that was created previously in the VLAN dialog.

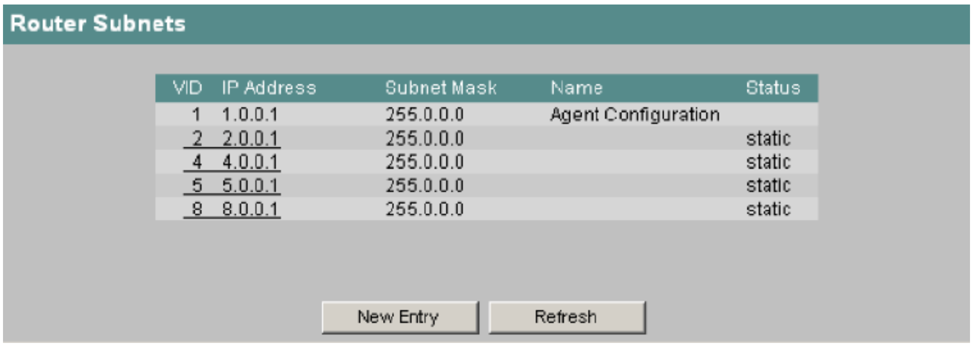


Figure 4-108 Router Subnets

VID
VLAN ID of the IP subnet.

IP Address
IP address of the subnet (must be unique).

Subnet Mask
Subnet mask of the IP subnet. The "ones" entered left justified in the bit representation of the subnet mask specify the network ID of the IP address.

Name
Freely selectable name for the subnet. The predefined name of the first subnet that must match the agent configuration is called "Agent Configuration".

Status
Status of the subnet. The following two statuses are possible:

- Static
- invalid:
  A subnet with the "invalid" status indicates a configuration error that must be eliminated.
- BOOTP:
  Bootstrap protocol (protocol for automatic assignment of IP addresses)
- DHCP:
  Dynamic Host Configuration Protocol (expansion of BOOTP)

Creating a new IP subnet

You can create a new subnet by clicking the "New Entry" button in the "Router Subnets" dialog. You make the settings for the subnet in the "Router Subnet Configuration" menu.

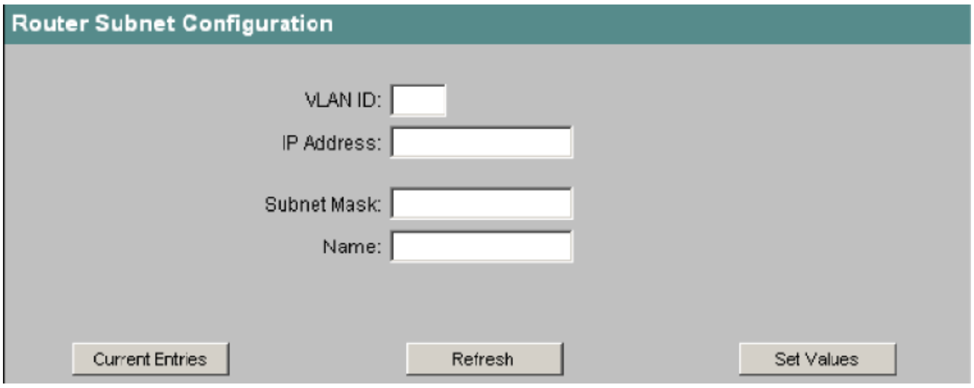


Figure 4-109 Router Subnets Configuration

VLAN ID

Here, enter the ID of the VLAN (VID see the section "Current VLAN Configuration menu item") via which packets of this IP subnet will be transmitted (range of values of the ID: 1 through 4094).

Note

The agent VLAN ID must not be used again. All other IDs can be used more than once.

IP Address

Enter the IP address of the IP subnet. IP addresses must not be used more than once.

Note

By appending the "/" character and a number between 1 and 30, the subnet can also be defined at the same time.

Subnet Mask

Here, you enter the subnet mask of the IP subnet you are creating. The subnet mask must be made up of a left-justified bit field of ones.

Name

Here, you enter the name of the subnet (this is no effect on the functionality).

Syntax of the Command Line Interface

Table 4- 72 Subnets - CLI\ROUTER\SUBNETS>

Command	Description	Comment
info	Displays the current subnets.	Administrator only.
add <VID> <IP> <subnet> [name]	Adds a news subnet. The subnet parameter identifies the subnet mask.	Administrator only.
edit <VID> <IP> [subnet] [name]	Modifies a subnet. The subnet parameter identifies the subnet mask.	Administrator only.
delete <VID> <IP>	Deletes a subnet.	Administrator only.

The "info" CLI command displays a table (analogous to the table in the Web Interface). The "Status" column is, however, restricted to two characters here (St).

The following statuses are possible (see also Web Interface):

- BP (BOOTP)
- DP (DHCP)
- st (static)
- ?? (invalid)

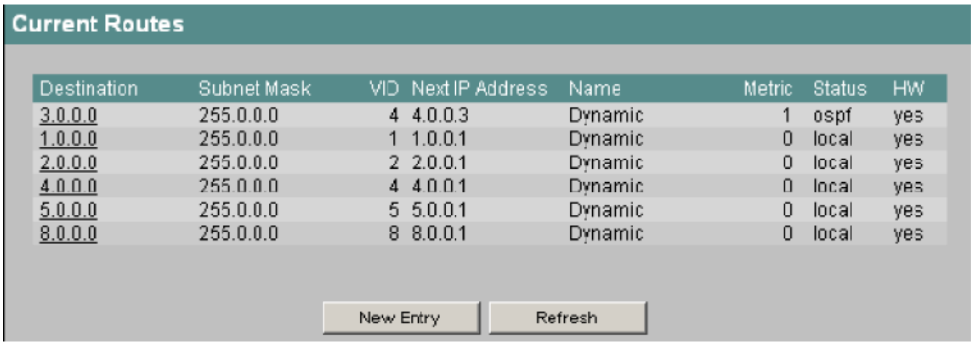
4.8.3 Current Routes

Routing table

The routing table is displayed in this dialog. Static routing table entries can also be created here.

A routing table is generally a list of rules according to which received packets will be forwarded. If a packet is waiting for routing, its destination address is compared with the addresses in the routing table. The entry whose address along with the subnet mask matches best (using the longest prefix match method) then describes how the packet will be forwarded.

Entries in the routing table with the "local" status, indicate the configured subnets.



Destination	Subnet Mask	VID	Next IP Address	Name	Metric	Status	HW
3.0.0.0	255.0.0.0	4	4.0.0.3	Dynamic	1	ospf	yes
1.0.0.0	255.0.0.0	1	1.0.0.1	Dynamic	0	local	yes
2.0.0.0	255.0.0.0	2	2.0.0.1	Dynamic	0	local	yes
4.0.0.0	255.0.0.0	4	4.0.0.1	Dynamic	0	local	yes
5.0.0.0	255.0.0.0	5	5.0.0.1	Dynamic	0	local	yes
8.0.0.0	255.0.0.0	8	8.0.0.1	Dynamic	0	local	yes

Figure 4-110 Current Routes

Destination
Destination address of this route.

Subnet Mask
Identifies the valid bits of the Destination column. It must consist of left-justified ones.

VID
The VID identifies the VLAN ID via whose IP subnet a packet will be forwarded when the rule is used.

Next IP Address
The next IP address identifies the IP address of the device to be accessed next.

Name
The name does not influence the routing process.
A name can be entered for static routes.
If the route is dynamic, the name is also set to "Dynamic".

Metric
The Metric column displays the distance between router and destination.

Status
The status of a route indicates whether this was generated by the OSPF or RIP protocol as a static route or local.
Static routes are created manually with the "New Entry" button.
Local routes are created automatically when a subnet is created.

HW
The HW (hardware) column identifies the assignment of the route to the hardware. The available options are as follows:

- Yes:
  Can be stored in the hardware
- In use:
  Is already stored in the hardware
- No:
  Must not be stored in the hardware
  With static routes, "Yes" or "No" can be set. The routes are stored in the hardware and displayed as "In use" only when they are actually being used.

Creating a new static route

With the "New Entry" button in the "Current Routes" dialog, you can create a new route. Routes created in this way are always static.

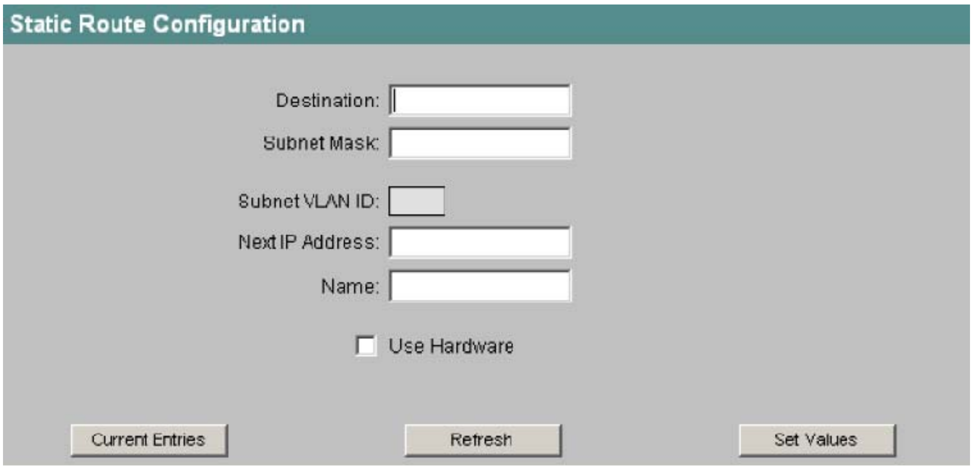


Figure 4-111 Static Route Configuration

Destination
Here, you enter an IP address to which the routing table entry relates.

Subnet Mask
Enter the subnet mask of the routing entry here. This shows which bits of the address are valid for the routing comparison.

Subnet VLAN ID
The subnet VLAN ID is calculated automatically from the next IP address and is empty in new systems.

Next IP Address
Here, enter the address of the next router to which the packets of this route will be sent. The router must be located in a connected subnet.

Name
Here, you enter the name of the route (this is no effect on the functionality).

Use Hardware
Enable this check box, if you want the route to be written to the hardware. If the option is enabled, the route is written to the hardware the first time a packet is successfully forwarded and can then be used more quickly.

Note

The route can only be written to the hardware when there is still adequate storage space available.

Syntax of the Command Line Interface

Table 4- 73 Current Routes - CLI\ROUTER\ROUTES>

Command	Description	Comment
info	Displays the current routes.	Administrator only.
add <IP> <subnet> <nextIP> [E|D] [name]	Adds a new route. E|D parameter for enabling/disabling "Use Hardware".	Administrator only.
edit <IP> [nextIP] [E|D] [name]	Modifies a route. E|D parameter for enabling/disabling "Use Hardware".	Administrator only.
delete <IP>	Deletes a route.	Administrator only.

The "info" CLI command displays a table (analogous to the table in the Web Interface). The "Metric" and "Status" columns are, however, restricted to two characters here (Me; St).
The following statuses are possible:

- OS (OSPF)
- RI (RIP)
- st (static)
- lo (local)
- ot (other)
- ?? (invalid)

The following are possible in the "Hardware" column (HW) (see also Web Interface):

- Yes: X (upper case X)
- In use: * (asterisk)
- No: - (minus sign)

4.8.4 RIPv2 Configuration

Introduction

In the "RIPv2 Configuration" dialog, you can set the general parameters of the RIP protocol as well as view certain basic statistics counters.

Note

The settings made here take effect only if RIP is enabled in the "Router Configuration" dialog.

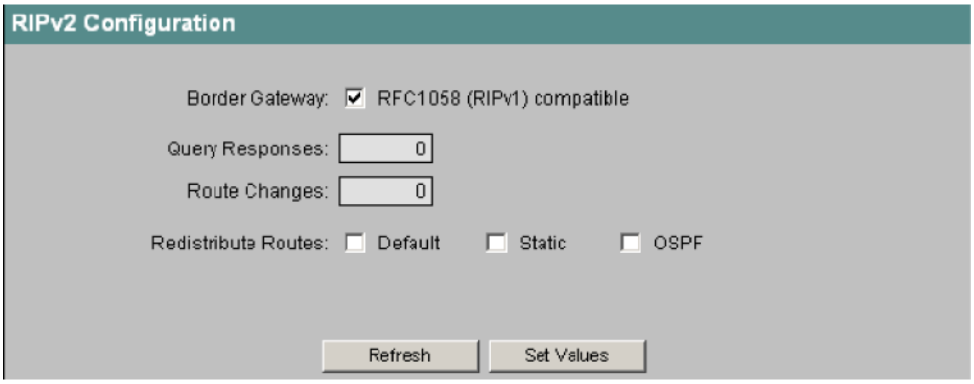


Figure 4-112 RIPv2 Configuration

Border Gateway
Enable this check box only if you operate the router along with original RIPv1 routers. In this case, subnet routes are grouped together in specific classes and so-called supernets are not propagated. This provides you with the greatest possible compatibility with RIPv1 routers.

Query Responses
Number of a special routing queries responded to.

Route Changes
Number of modifications made in the routing table.

Redistribute Routes (Default/Static/OSPF)
Here, you can specify which known routes are forwarded over RIP. You can make different decisions for the route types Default, Static and OSPF.

Note

Please enable this check box only for gateways between different networks (border gateways). Enabling the Default and Static options, in particular, can cause problems (for example, increased load caused by traffic in forwarding loops) if they are enabled at too many points in the network.

Syntax of the Command Line Interface

Table 4- 74 RIPv2 Configuration - CLI\ROUTER\RIP>

Command	Description	Comment
info	Shows the current RIP configuration.	-
rfc1058 <E|D>	Sets RFC1058 (RIPv1) compatibility.	Administrator only.
redistr <E|D> <E|D> <E|D>	Enables/disables “redistribute routes”. • Parameter 1 default routes • Parameter 2 static routes • Parameter 3 OSPF routes	Administrator only.

4.8.5 RIPv2 Interfaces

Introduction

The "RIPv2 Interfaces" dialog displays an overview of all IP subnets in which the RIP protocol is used.

With the "New Entry" button, you can register new subnets for RIP.

Note

Before a subnet can be registered for RIP, it must first be created in the "Router Subnets" menu.

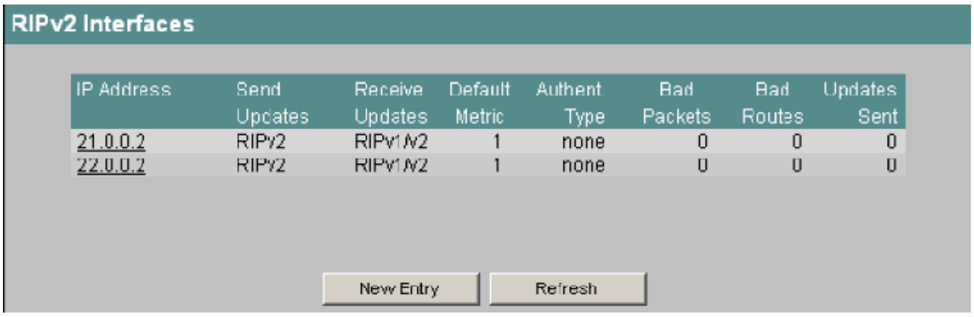


Figure 4-113 RIPv2 Interfaces

IP Address
IP address of the RIP-compliant subnet (only identifier for this table). All other subnet parameters such as the subnet mask can be found in the "Router Subnets" dialog.

Send Updates
This column displays how updates will be sent. The following are available:

- no send:
  No updates are sent
- RIPv1:
  Send RIPv1 updates according to RFC 1058
- RIPv1-compat:
  Send RIPv2 updates according to the rules of RFC 1058 as broadcasts
- RIPv2:
  Send RIPv2 updates as multicast
- RIPv1 demand and RIPv2 demand:
  RIP the packets are sent only as responses to explicit queries.
  Use this option only if your router needs to communicate with another router over the WAN interface.

Receive Updates
This column displays the form in which received RIP packets will be accepted. The following are available:

- no receive:
  No packets are accepted.
- RIPv1:
  Only packets from RIPv1 routers are accepted.
- RIPv2:
  Only packets from RIPv2 routers are received and processed.
- RIPv1/v2:
  All variants of the RIP protocol are accepted on this interface.

Default Metric
This column displays the metric assigned to the default route on this interface.
The value 0 indicates that no default route is propagated.
Otherwise the values 1..15 are valid.

Authent. Type
The authentication type is displayed in this column. This can be:

- no authentication
- simple password
- MD5 authentication.

Bad Packets
Counter for received RIP packets that were deleted and therefore ignored.

Bad Routes
Number of routes of valid RIP packets that could not be taken into consideration.

Updates Sent
Number of "Triggered Updates" for this interface

Creating a new RIPv2 interface

You can create a new interface by clicking the "New Entry" button in the "RIP Interfaces" dialog. This opens the following dialog.

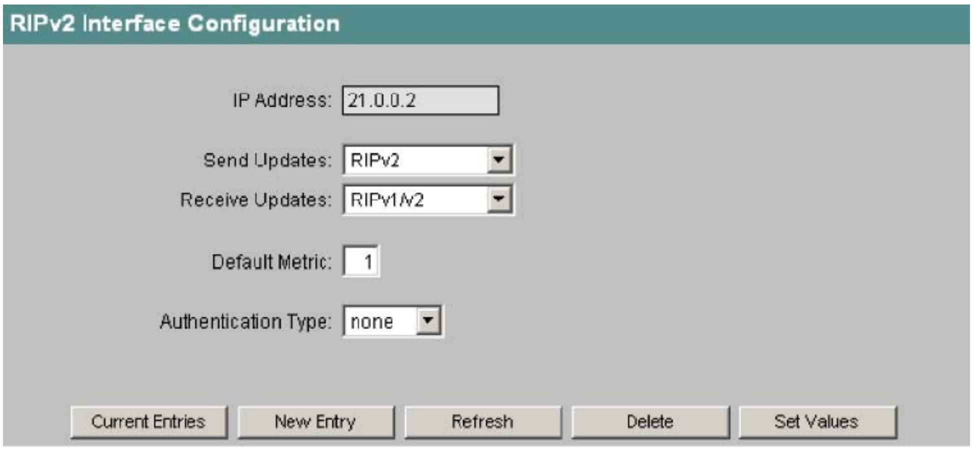


Figure 4-114 RIPv2 Interface Configuration

IP Address

Here, you enter the IP address of the interface on which RIP will be configured. This IP address must already be configured as an IP subnet.

Send-Updates

Here, you select how the RIP updates will be sent. The update packets contain the routing table of the local system. The following are available:

- no send:
  Do not send updates
- RIPv1:
  Send RIPv1 updates according to the rules of RFC 1058
- RIPv1-compat:
  Send RIPv2 updates according to the rules of RFC 1058 as broadcasts
- RIPv2:
  Send RIPv2 updates as multicast
- The values "RIPv1 demand" and "RIPv2 demand" are required only for WAN interfaces. In this case, RIP the packets are sent only as a response to an explicit query.

Note

If there are no RIPv1 devices whatsoever in your network, you should set "RIPv2".

Receive-Updates

Here, select the rules according to which received packets will be accepted. The following are available:

- no receive:
  Do not receive updates
- RIPv1:
  Receive RIPv1 updates
- RIPv2:
  Receive RIPv2 updates
- RIPv1/v2:
  Receive RIPv1 and RIPv2 updates

Default Metric

Here, you specify the metric with which the default route will be propagated on this interface. RIP uses the hop metric in which distances are specified as the "number of routers used" (range of values: 1-15 (0 disables the default route)).
The following applies: The higher value, the longer packets require to their destination.

Authentication Type

Here, select the authentication method of the RIP packets. The following options are available:

- none: no authentication (default)
- simple: authentication with password and confirmation
- MD5: authentication using the Keyed MD5 method (password, confirmation and key ID)
- These methods are simply used to determine the authenticity of a packet; they do not encrypt data.

Key ID

Note

The "Key ID" text box is displayed only if the authentication method was set to MD5.

Enter the key ID here with which the password will be used as the key. Since the key ID is transferred with the protocol, the same key must be stored under the same key ID on all neighboring routers.

Password/Confirmation

Note

The "Password/Confirmation" text box is displayed only if the authentication method was set to MD5 or simple.

If authentication uses a password, a key is required via MD5 that can be entered here.

Syntax of the Command Line Interface

Table 4- 75 RIPv2 Interfaces - CLI\ROUTER\RIP\RIP\IFACE>

Command	Description	Comment
info	Displays the current interfaces.	-
add <IP> [SendUpd] [RecvUpd] [Metric]	Adds a new interface. Possible parameters for SendUpd: • SV1 RIPv1 • SV1C RIPv1 Comp. • SV1D RIPv1 Dem. • SV2 RIPv2 • SV2D RIPv2 Dem. • SNO No Send Possible parameters for RecvUpd: • RV1 RIPv1 • RV2 RIPv2 • RV1V2 RIPv1/v2 • RNO No Receive	Administrator only.
edit <IP> [SendUpd] [RecvUpd] [Metric]	Modifies an interface. Possible parameters for SendUpd and RecvUpd as for the add command.	Administrator only.
auth <IP> <authtype> [password] [key-id]	Modifies the authentication of an interface. Possible types: • None • Simple • MD5 (the "Key-Id" is only required here)	Administrator only.
delete <IP>	Deletes an interface.	Administrator only.

4.8.6 OSPFv2 Configuration

Introduction

In the "OSPFv2 Configuration" dialog and its sub-dialogs, you can set the OSPF parameters.

OSPFv2 divides the administrated IPv4 network (autonomous system) into various areas. Within these areas, the link statuses of all routers are exchanged so that each router has a complete view of the network. This view is maintained in the link state database (LSDB). As a result, each router can determine all routes within the area itself according to the Dijkstra algorithm.

There is no uniform view between the areas. For this reason, exchange of routes is restricted to collective routes that can be determined according to the distant vector algorithm.

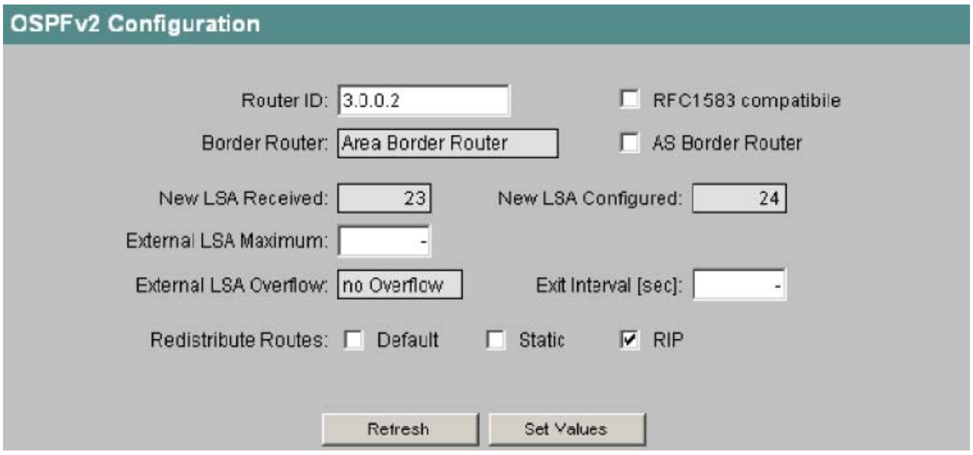


Figure 4-115 OSPFv2 Configuration

Router ID
Here, you set the address of an OSPF interface. The IP address must be unique.

RFC 1583 compatible
You only require this setting if you are still using old OSPFv2 routers that are not compatible with RFC 2328.

Border Router
Displays the border router status. If the local system is an active member in at least two areas, this is an area border router.

AS Border Router
Enable this option if this router operates as an AS border router; in other words, delivers to several protocol worlds (for example, if you operate an additional RIP network).

New LSA received
Number of link state advertisements that were received. Updates and its own LSAs are not counted.

New LSA configured
Number of different LSAs sent by this local system.

External LSA Maximum
Here, enter the maximum number of external LSAs if you want to limit the external LSDB.

External LSA Overflow
Indicates whether the maximum number of external LSAs was exceeded.

Exit Interval (sec)
Here, you enter the time in seconds after which the OSPF router will reattempt to come out of the overflow status. 0 means that the OSPF router only attempts to leave the overflow status after restarting (triggered by disable and enable in the main menu of the router).

Redistribute Routes (Default/Static/RIP)
Here, you can specify which known routes are forwarded over OSPF. You make different decisions for the route types Default, Static and RIP.

Note

Please enable this check box only for gateways between different networks (border gateways). Enabling the Default and Static options, in particular, can cause problems (for example, forwarding loops) if they are enabled at too many points in the network.

Syntax of the Command Line Interface

Table 4- 76 OSPFv2 Configuration - CLI\ROUTER\OSPF>

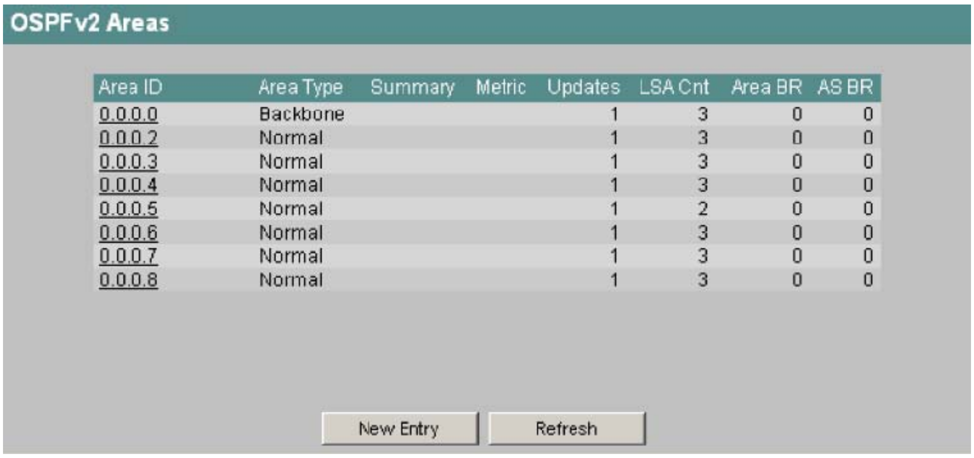
Command	Description	Comment
info	Displays the current OSPF configuration.	-
id <IP>	Sets the router ID (IP address).	Administrator only.
rfc1583 <E|D>	Sets the RFC1583 compatibility.	Administrator only.
asbr <E|D>	Enables/disables AS border router.	Administrator only.
lsamax <number>	Sets the external LSA maximum.	Administrator only.
exitint <sec>	Sets the external exit interval.	Administrator only.
redistr <E|D> <E|D> <E|D>	Enables/disables “Redistribute routes”. • Parameter 1 default routes • Parameter 2 static routes • Parameter 3 RIP routes	Administrator only.
ospfdbg [E|D] [debugtype]	Enables/disables OSPF debug functions. Enter "ospfdbg ?" for help.	Administrator only.

4.8.7 OSPFv2 Areas

Overview

An autonomous system can be divided into smaller areas (see the section OSPFv2 Configuration menu item).

In this dialog, you can monitor the OSPF areas of the router. Apart from configuration parameters, you can also see statistical values.



Area ID	Area Type	Summary	Metric	Updates	LSA Cnt	Area BR	AS BR
0.0.0.0	Backbone			1	3	0	0
0.0.0.2	Normal			1	3	0	0
0.0.0.3	Normal			1	3	0	0
0.0.0.4	Normal			1	3	0	0
0.0.0.5	Normal			1	2	0	0
0.0.0.6	Normal			1	3	0	0
0.0.0.7	Normal			1	3	0	0
0.0.0.8	Normal			1	3	0	0

Figure 4-116 OSPFv2 Areas

Area ID
Shows the ID of this area. An area ID consists of 4 numbers each between 0 and 255 and it must be unique.
The area 0.0.0.0 is known as the backbone area.
The LSDB of this area is synchronized for all routers in an area.

Area Type
Shows the type of the area. The following area types are possible:

- Standard
- Stub
- NSSA
- Backbone: The backbone area is highlighted here.

Summary
Indicates whether summary LSAs can be generated for this area. This column is significant only for stub areas. The following entries are possible:

- import: Summary LSAs are sent to this area
- disregard: Summary LSAs are not sent to this area

Metric
Shows the metric of the propagated default route of the stub areas. Nothing is displayed for any other areas.

Updates
Number of routing table calculations

LSA Cnt
Number of LSAs in the LSDB of this area

Area BR
Number of reachable area border routers (ABR) within this area

ASBR
Number of reachable autonomous system border routers (ASBR) in this area.

Creating a new OSPFv2 area

With the "New Entry" button in the "OSPFv2 Areas" dialog, you can create a new area.

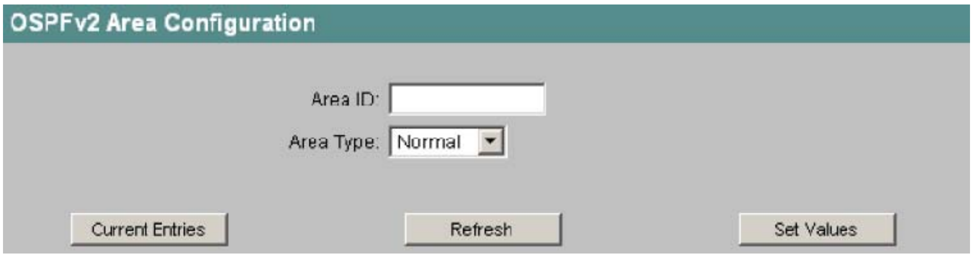


Figure 4-117 OSPFv2 Area Configuration

Area ID
Enter the ID of the area here.

Area Type
The following area types exist:

- Standard
- Stub
- NSSA

Note

For the backbone area, the selected area type must be "Normal" and the area ID 0.0.0.0.

Import Summary

Note

The "Import Summary" check box is displayed only when the "Stub" area type was set.

Enable this option to generate and propagate the summary LSAs in this area. In this case, no default route is necessary for communication within the entire network.

Note

If there is only one border router in this stub area, you do not need to activate this option.

Default Metric

Note

The "Default Metric" text box is displayed only when the "Stub" area type was set.

Here, enter the metric of your default route that will be propagated in the area.

Syntax of the Command Line Interface

Table 4- 77 OSPFv2 Areas - CLI\ROUTER\OSPF\AREAS>

Command	Description	Comment
info	Displays the current areas.	-
add <areaID> <type> [E|D] [metric]	Adds a new area. Possible types: • Standard • Stub • NSSA The [E|D] and metric parameters are possible only for a stub area. • E Enable importing summary • D Disable importing summary	Administrator only.
edit <areaID> [type] [E|D] [metric]	Modifies an area. Possible types: • Standard • Stub • NSSA The [E|D] and metric parameters are possible only for a stub area. • E Enable importing summary • D Disable importing summary	Administrator only.
delete <areaID>	Deletes an area	Administrator only.

Example

The command

```
add 0.0.0.3 Stub d 2
```

generates a stub area "0.0.0.3" for which no summary LSAs are generated. The default route is assigned metric "2".

4.8.8 OSPFv2 Area Ranges

Overview

You can create address ranges in the "Area Ranges" dialog that allow various address ranges to be grouped when propagating. This allows the number of summary LSAs in the areas to be reduced.

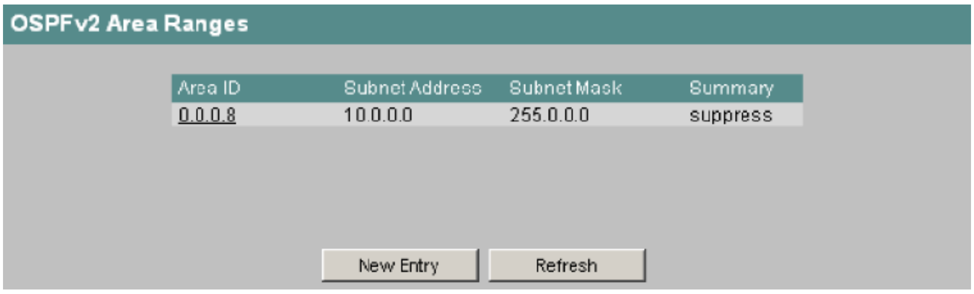


Figure 4-118 OSPFv2 Area Ranges

Area ID
Area ID to which the address range relates.

Subnet Address
Address of the network area to be grouped.

Subnet Mask
Subnet mask of the grouped network area.

Summary
Indicates whether the group address range will be advertised or suppressed.

Creating a new OSPFv2 area range

With the "New Entry" button in the "OSPFv2 Area Ranges" dialog, you can create up to four area ranges for an area.

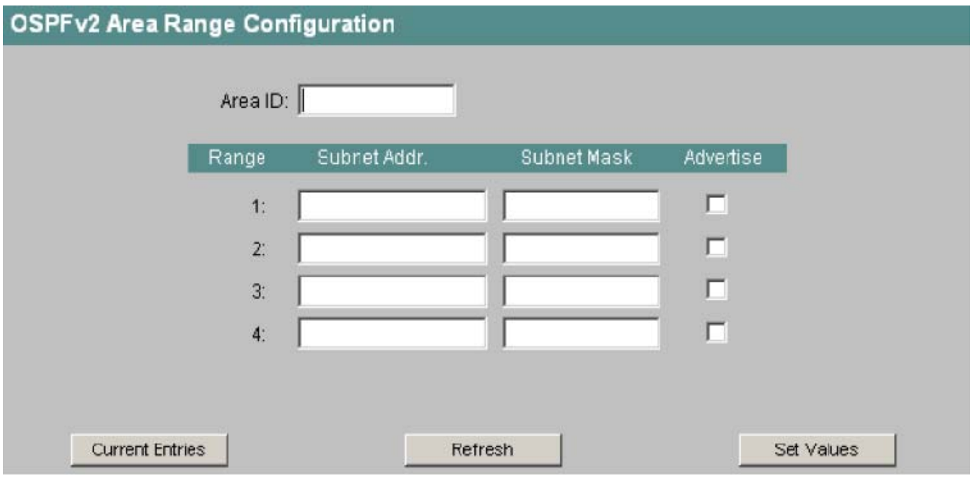


Figure 4-119 OSPFv2 Area Range Configuration

Area ID
Here, enter the ID of the area for which you want to create an address range.

Subnet Addr.
Here, you enter the address of the network to be grouped.

Subnet Mask
Here, you enter the subnet mask of the network to be grouped.

Advertise
Enable this option to propagate the grouped network.

Syntax of the Command Line Interface

Table 4- 78 OSPFv2 Area Ranges - CLI\ROUTER\OSPF\AREAS\RANGES>

Command	Description	Comment
info	Displays the current area ranges.	-
add <AreaID> <SNAddr> <SNMask> [E|D]	Adds a new area range. • E Enables advertising summary • D Disables advertising summary	Administrator only.
edit <AreaID> <SNAddr> <SNMask> <E|D>	Modifies an area range.	Administrator only.
delete <AreaID> <SNAddr> <SNMask>	Deletes an area range.	Administrator only.

4.8.9 OSPFv2 Interfaces

Overview

In this dialog, you can monitor all the IP interfaces configured for OSPF. Apart from the configuration parameters, some statistical values can also be monitored in the double-page display.

Click on the ">>" or "<<" buttons to page backwards and forwards.

OSPFv2 Interfaces: 1st Page

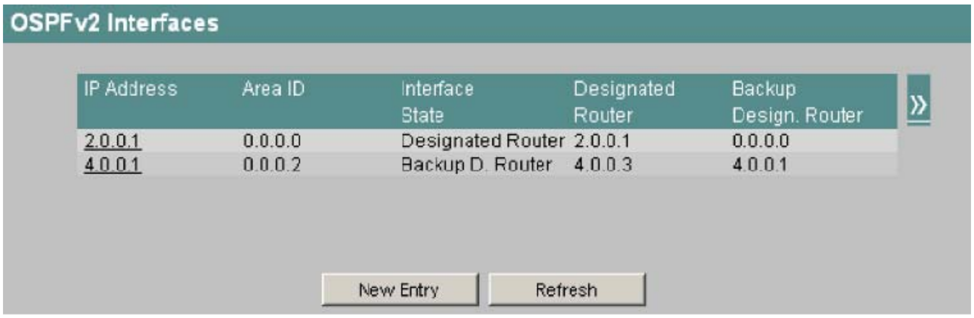


Figure 4-120 OSPFv2 Interfaces page 1

IP Address
IP address of the configured OSPF interface.

Area ID
Specifies the area that belongs to this interface.

Interface State
Indicates the state of the interface. This can be:

- Down: Nothing is connected to the interface
- Waiting: Starting up and negotiating the interface
- Designated Router: The router has the main responsibility for this network and the network LSA will be created
- Backup D. Router: The router is backup for the designated router
- Other: The interface has started up and the router is neither designated nor backup designated router.

Designated Router
IP address of the designated router for this interface.

Backup Designated Router
IP address of the backup designated router for this interface.

OSPFv2 Interfaces: 2nd Page

OSPFv2 Interfaces

IP Address	OSPF Status	Metric	Priority	Trans Delay	Retrans Interval	Hello Interval	Dead Interval	Authent. Type	Events
2.0.0.1	enabled	10	1	1	5	10	40	none	0
4.0.0.1	enabled	1	1	1	5	10	40	none	0

2 Entries

New Entry | Refresh

Figure 4-121 OSPFv2 Interfaces page 2

IP Address:
IP address of the interface.

OSPF Status
OSPF status of this interface. The following statuses are possible:

- Enabled: The interface is available for OSPF.
- Disabled: The interface is not available for OSPF.

Metric
Path costs of the router on this interface.

Priority
Priority of the router on this interface. The priority plays a part in the selection of the designated router on the network. The higher the number, the higher the priority.

Trans Delay
Estimated time (in seconds) that a link state update packet requires for transmission. On LANs, this parameter is normally 1.

Retrans Interval
Specifies the interval after which packets whose receipt was not confirmed in the database synchronization are transferred again.

Hello Interval
Specifies the interval at which Hello packets are sent.

Dead Interval
Specifies the interval after which a router is classified as "no longer existing" if no further Hello packets are received from it.

Authent. Type
Authentication method selected on this interface. The following are available:

- none: no authentication
- simple: authentication using a password
- MD5: authentication with keyed MD5 method

Events
Number of changes to the interface status.

Creating a new OSPFv2 interface

With the "New Entry" button in the "OSPFv2 Interfaces" dialog, you can configure a new IP interface for OSPF.

Note

Before an interface can be created as an OSPF interface, it must first be created as an IP subnet.

NOTICE
Take particular care when selecting the parameters. A correct neighbor-neighbor relationship is possible only when identical parameters are configured on all routers of an IP subnet. Otherwise, the impression is that the routers cannot see each other.

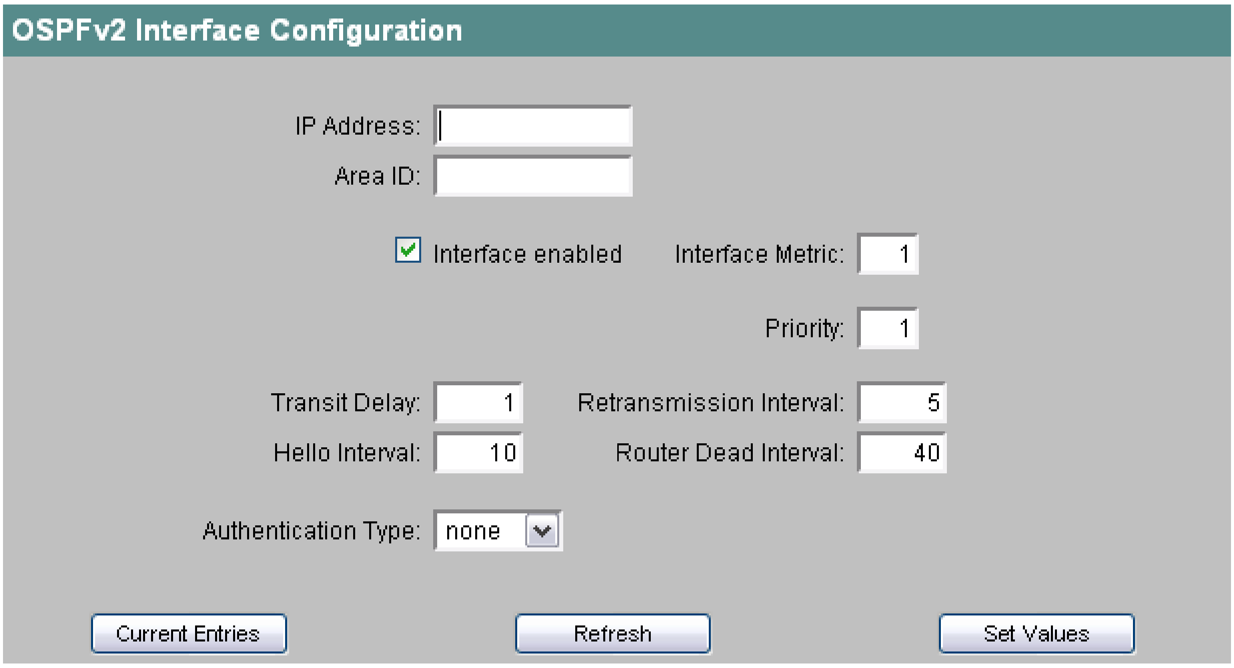


Figure 4-122 OSPFv2 Interface Configuration

IP Address
Enter the IP address of the interface you want to configure.

Area ID
Here, you enter the area ID to which this interface will belong.

Interface enabled
Select this option if you want this interface to be involved in OSPF traffic.

Metric
Path costs of the router on this interface. Default is 1. Enter higher values here for slower networks.

Priority
Enter the router priority here. This only plays a part in the selection of designated router. This parameter can be selected differently on routers within the same IP subnet.

Transit Delay
Here, you enter the expected delay (in seconds) when sending a link update packet. In local area networks, the value 1 is normally selected (range of values: 1 through 3600).

Retransmission Interval
Here, you enter the time (in seconds) after which a packet will be transmitted again if no confirmation was received. In a LAN, the value 5 is normally selected.

Hello Interval
Here, you enter the interval (in seconds) between two Hello packets (range of values: 1 through 65,535).

Router Dead Interval
Here, enter an interval (in seconds) after which a router is shown as "failed" if no further Hello packets are received from it during this time.

Authentication Type
Select the authentication method of this interface here. You can choose between:

- none: no authentication
- simple: authentication using a password
- MD5: authentication with keyed MD5 method

Key ID

Note

The "Key ID" text box is displayed only if the authentication method was set to MD5. Only then is it possible to use several keys.

Enter the key ID here with which the password will be used as the key. Since the key ID is transferred with the protocol, the same key must be stored under the same key ID on all neighboring routers.

Password/Confirmation
If authentication uses a password, a key is required via MD5 that can be entered here.

Syntax of the Command Line Interface

Table 4- 79 OSPFv2 Interfaces - CLI\ROUTER\OSPF\AREAS\IFACE>

Command	Description	Comment
info	Displays the current interfaces.	-
add <IP> <AreaID> [E|D] [priority]	Adds a new interface. • E Enable interface • D Disable interface	Administrator only.
edit <IP> [AreaID] [E|D] [priority]	Modifies an interface. • E Enable interface • D Disable interface	Administrator only.
timing <IP> [<setting=value>]	Changes the timing settings of an interface. Possible settings: • TD Trans. Delay • RI Retrans Interval • HI Hello Interval • DI Dead Interval	Administrator only.
auth <IP> <authtype> [password]	Modifies the authentication of an interface Possible types: • None • Simple • MD5	Administrator only.
metric <IP> <metric>	Changes the path costs of an interface	Administrator only.
delete <IP>	Deletes an interface.	Administrator only.

4.8.10 OSPFv2 Virtual Links

Overview

Each area border router (each router connected to two or more areas) must have access to the backbone area for reasons associated with the protocol. If such a router is not connected directly to the backbone area, a virtual link to the backbone area is created.

In this menu, you can monitor this virtual link.

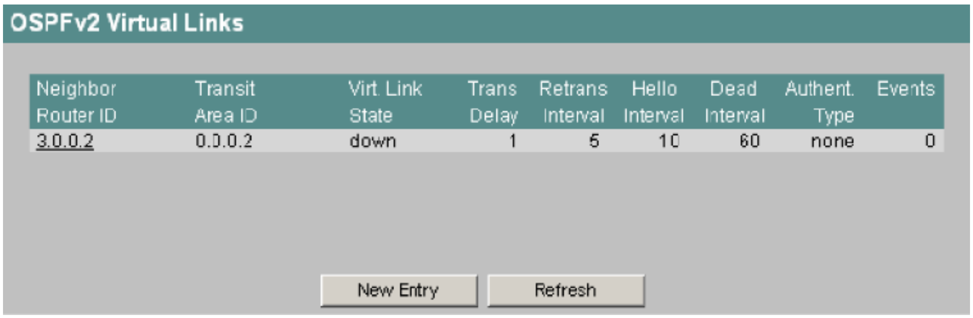


Figure 4-123 OSPFv2 Virtual Links

Neighbor Router ID
Router ID of the configured neighbor.

Transit Area ID
Area ID of the area via which the router will have a virtual connection to the neighbor.

Virt. Link State
State of the virtual link. The following states are possible:

- down: The virtual link cannot be used
- point-to-point: The virtual link can be used

Trans Delay
Estimated time (in seconds) that a link state update packet requires for transmission over the virtual link.

Retrans Interval
Interval (in seconds) after which packets whose receipt was not confirmed are transferred again.

Hello Interval
Interval (in seconds) at which Hello packets are sent over the virtual link.

Dead Interval
Interval (in seconds) after which the neighbor router is classified as "failed" if no further Hello packets are received from it.

Authent. Type
Authentication method of the virtual link. The following are available:

- none: no authentication
- simple: authentication using a password
- MD5: authentication with keyed MD5 method

Events
Number of changes to the interface status.

Creating a new virtual link

With the "New Entry" button in the " OSPFv2 Virtual Links " dialog, you can create a new virtual link.

Note

Remember that when you create 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.

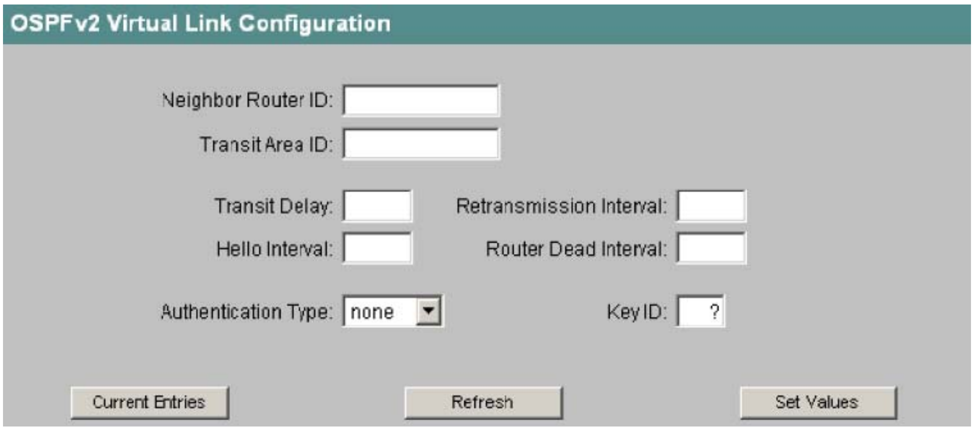


Figure 4-124 OSPFv2 Virtual Link Configuration

Neighbor Router ID
Here, you enter the router ID of the partner device at the other end of the virtual link.

Transit Area ID
Here, you enter the area ID via which the two partners are connected.

Transit Delay
Here, you enter the expected delay (in seconds) when sending a link update packet (range of values: 1 through 3600).

Retransmission Interval
Here, you enter the time (in seconds) after which a packet will be transmitted again if no confirmation was received (range of values: 1 through 3600).

Hello Interval
Here, you enter the interval (in seconds) between two Hello packets (range of values: 1 through 65,535).

Router Dead Interval
Here, enter an interval (in seconds) after which a neighboring router is shown as "failed" if no further Hello packets are received from it during this time.

Authentication Type
Select the authentication method of the virtual link here. You can choose between

- none: no authentication
- simple: authentication using a password
- MD5: authentication with keyed MD5 method

Key ID

Note

The "Key ID" text box is displayed only if the authentication method was set to MD5. Only then is it possible to use several keys.

Enter the key ID here with which the password will be used as the key. Since the key ID is transferred with the protocol, the same key must be stored under the same key ID on all neighboring routers.

Password/Confirmation
If authentication uses a password, a key is required via MD5 that can be entered here.

Syntax of the Command Line Interface

Table 4- 80 OSPFv2 Virtual Links - CLI\ROUTER\OSPF\AREAS\VLINKS>

Command	Description	Comment
info	Displays the current virtual links.	-
add<RtrID> <AreaID> [<setting=value>]	Adds a new virtual link. Possible settings: • TD Trans. Delay • RI Retrans Interval • HI Hello Interval • DI Dead Interval	-
edit <RtrID> <AreaID> [<setting=value>]	Modifies a virtual link. Possible settings: • TD Trans. Delay • RI Retrans Interval • HI Hello Interval • DI Dead Interval	-
auth <RtrID> <AreaID> <authtype> [password]	Changes the authentication of a virtual link. Possible types: • None • Simple • MD5	-
Delete <RtrID> <AreaID>	Deletes a virtual link.	-

Example

The command

```
add 1.1.1.51 0.0.0.2
```

creates a virtual link to the router with ID "1.1.1.51" via the transit area "0.0.0.2". The remaining parameters are set to the default values.

4.8.11 OSPFv2 Neighbors

Overview

In this dialog, you can monitor the OSPF neighbors. These include the dynamically detected neighbors in the relevant networks and the configured virtual neighbors.

Figure 4-125 Current OSPFv2 Neighbors

Neighbor IP Address
IP address of the neighbor in this network.

Neighbor Router ID
Router ID of the neighbor. The two addresses can match.

Neighbor State
Status of the neighbor. The status can adopt the following values:

- down: The neighbor is not reachable
- attempt and init: Short-lived statuses during initialization
- two-way: Two-way receipt of Hello packets
- exchange start, exchange and loading: Statuses during the exchange of the link state database
- full: Status when the databases are synchronized.

Note

The "full" status is the normal status with a stable neighbor if one of the partners is a designated router or a backup designated router. Otherwise the "two-way" status is the normal stable status.

Transit Area ID
Transit area ID of the neighbor if the neighbor is virtual.

Assoc. Area Type
Status of the area over which the neighbor-neighbor relation is maintained. The following area types are possible:

- Standard
- Stub
- NSSA

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

Hello Suppr.
Displays suppressed Hello packets to the neighbor. This field normally displays "no".

Retrans Queue
Length of the queue with packets still to be transmitted.

Events
Number of status changes.

Note

The "full" status is the normal status with a stable neighbor if one of the partners is a designated router or a backup designated router. Otherwise the "two-way" status is the normal stable status.

Syntax of the Command Line Interface

Table 4- 81 OSPFv2 Neighbors - CLI\ROUTER\OSPF>

Command	Description	Comment
neighbrs	Displays the current neighbors.	-

4.8.12 OSPFv2 State Database

Overview

The link state database is the central database for managing all links with in an area. It consists of the link state advertisements (LSAs). The most important data of these LSAs is displayed in this dialog.

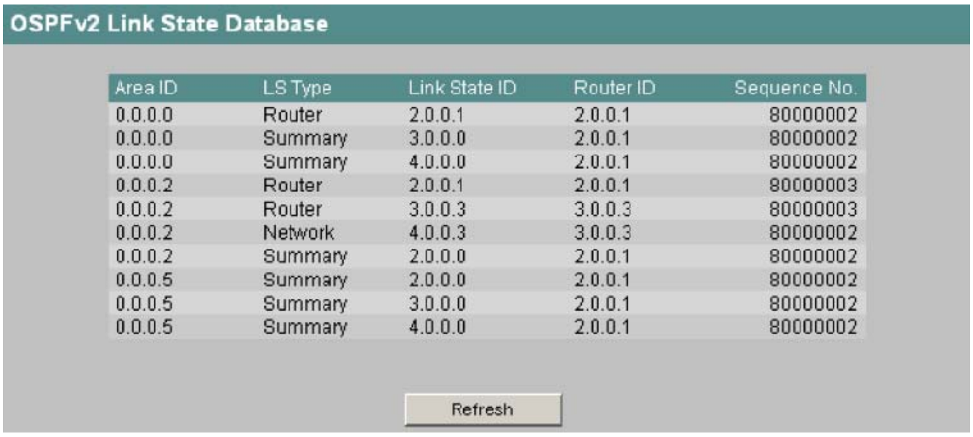


Figure 4-126 OSPFv2 Link State Database

Area ID
Area ID to which this link state advertisement (LSA) belongs.

LS Type
Type of LSA. This can be:

- Router
- Network
- Summary
- ASBR (Autonomous System Border Router).

Link State ID
Unique ID of the LSA.

Router ID
Router that generated this LSA.

Sequence No.
Sequence number of the LSA. Each time an LSA is renewed, this sequential number is incremented by one.

Syntax of the Command Line Interface

Table 4- 82 OSPFv2 State Database - CLI\ROUTER\OSPF>

Command	Description	Comment
lnkstate	Displays the current links state table.	-

Note

For more detailed information on LSAs, refer to the section on configuration and diagnostics over SNMP.

4.8.13 VRRP

Introduction

In the submenus of the "VRRP" menu, you can set the VRRP parameters.

The VRRP introduces redundancy to the IPv4 network. Various IP routers can take over the routing functionality of another router if the actual router fails. To allow this, several routers in an IP subnet are grouped together to form one virtual router This virtual router is assigned a list of IPv4 addresses for which the relevant master takes on the routing functionality.

4.8.14 VRRP Virtual Routers

Introduction

In this dialog, you can monitor the virtual routers of this system.

With the "New Entry" button, you can create new virtual routers.
A maximum of 32 virtual routers can be configured.

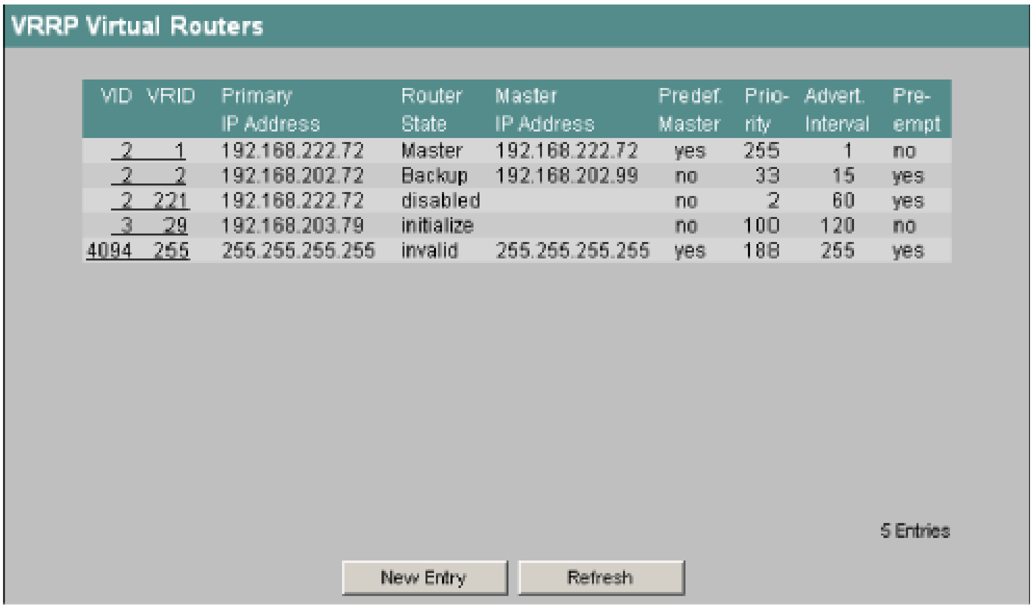


Figure 4-127 VRRP Virtual Routers

VID
VLAN ID of the subnet. The IP addresses set up for this and all subnet parameters can be found in the "Router Subnets" menu.

VRID
The ID of the virtual router is displayed in this column. This assigned ID must be unique for this VLAN. Valid values are 1 through 255.

Primary IP Address
The primary IP address on this VLAN is displayed in this column. The entry 0.0.0.0 means that the smallest address on this VLAN is used. Otherwise all IP addresses configured on this VLAN in the "Router Subnets" menu are valid addresses.

Router State
The current state of the virtual router is displayed in this column. Possible values are:

- Master: This router handles the routing functionality for all assigned IP addresses.
- Backup: Currently, a different router handles the routing functionality is in the "Master" state. The displayed router takes over the redundancy function and is ready to take over if the master fails.
- Disabled: This router was disabled by the administrator. It no longer handles router redundancy.

- Initialize: The virtual router has just been turned on. It will soon change to the "Master" or "Backup" state.
- Invalid: The configuration of this virtual router is invalid. Please check the configuration.

Master IP Address
The IP address of the router currently handling routing functionality is displayed in this column.

Predef. Master
This column indicates whether at least one redundant router address belongs to this IE Switch X-400. In this case, the priority is predefined at 255 and the IE Switch X-400 immediately changes to the "Master" status when it is turned on.

Priority
The priority of the virtual router is set in this column. Valid values are 1 through 255. 255 is intended for the owner of the redundant router addresses. All other priorities can be distributed freely among the redundant routers. The higher the priority, the earlier the router becomes "Master".

Advert. Interval
This column shows the interval at which the master router sends its advertisement packets.

Preempt
This column indicates whether a router with higher priority will interrupt a different router with lower priority.

Creating or changing a virtual router

With the "New Entry" button in the "VRRP Virtual Routers" dialog, you can create a new virtual router.

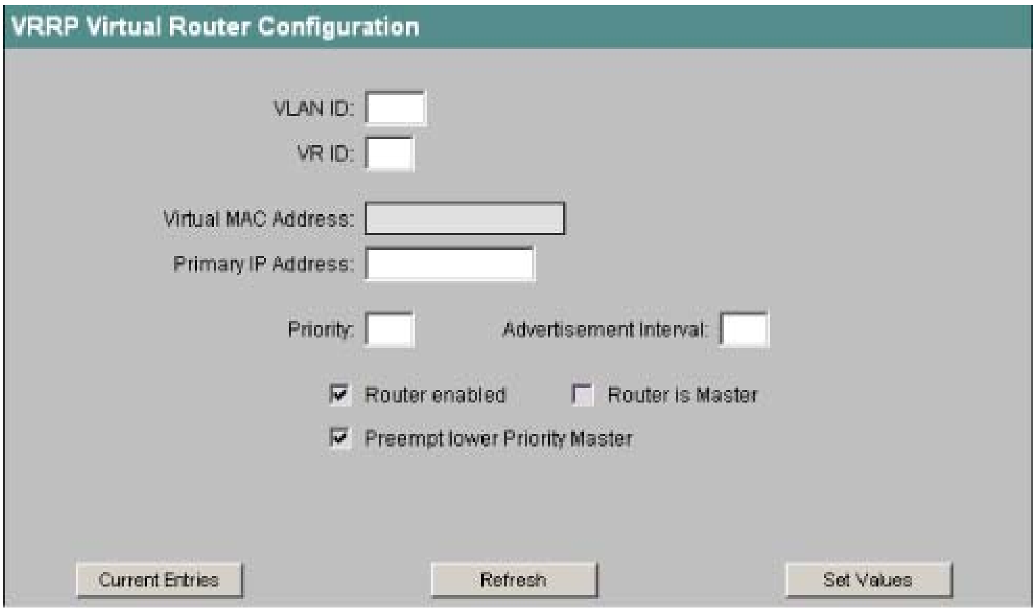


Figure 4-128 VRRP Virtual Router Configuration

VLAN ID
Here, you enter the VLAN on which the virtual router will be active. Valid values are all IDs of VLANs that have at least one configured IP subnet.

VR ID
Enter the ID of the virtual router here. This must be unique on the connected LAN.

Virtual MAC Address
The virtual MAC address is derived automatically from the IP of the virtual router and a fixed prefix.

Primary IP Address
Here, you enter the address that will be used as the IP source address as soon as this virtual router changes to the "Master" state.

Note

If you have only configured one IP subnet on this VLAN, no entry is necessary (0.0.0.0). If, on the other hand, you have configured several IP subnets on this VLAN and you want a particular address to be used as the source address for VRRP packets, you should enter this address here. Otherwise, the numerically smallest IP address will be used.

Priority
Enter the priority of this virtual router here. Valid values are 1 through 255. Priority 255 is intended for the owner of the router addresses. All other priorities can be distributed freely among the redundant routers. The higher the priority, the earlier the router becomes "Master".

Advertisement Interval
Here, you enter the interval in seconds after which a router in the "Master" state repeats the sending of an advertisement packet.

Router enabled
Here, you decide whether the router takes part in the VRRP protocol.

Router is Master
Here, you decide whether the router should be in the "Master" status from the start. In this case, the primary IP address is added immediately to the router addresses.

Preempt lower Priority Master
Here, you decide whether this router can interrupt a different router with lower priority.

Syntax of the Command Line Interface

VRRP - CLI\VRRP\ROUTERS>

Command	Description	Comment
info	Displays the current virtual routers.	-
add <VID> <VRID>	Adds a new virtual router.	Administrator only.
status <VID> <VRID> <E|D>	Enables/disables a virtual router	Administrator only.
master <VID> <VRID> <E|D>	Specifies whether or not the virtual router is master.	Administrator only.
preempt <VID> <VRID> <E|D>	Specifies whether higher priority routers can interrupt.	Administrator only.
primip <VID> <VRID> <IP>	Changes the primary IP address of a virtual router.	Administrator only.
priority <VID> <VRID> <0..255>	Changes the priority of a virtual router.	Administrator only.
advint <VID> <VRID> <0..255>	Changes the interval at which a virtual router sends advertisement packets.	Administrator only.
delete <VID> <VRID>	Deletes a virtual router.	Administrator only.

4.8.15 VRRP Associated IP Addresses

Introduction

In this menu item, you can view the redundant IP addresses of the virtual routers.

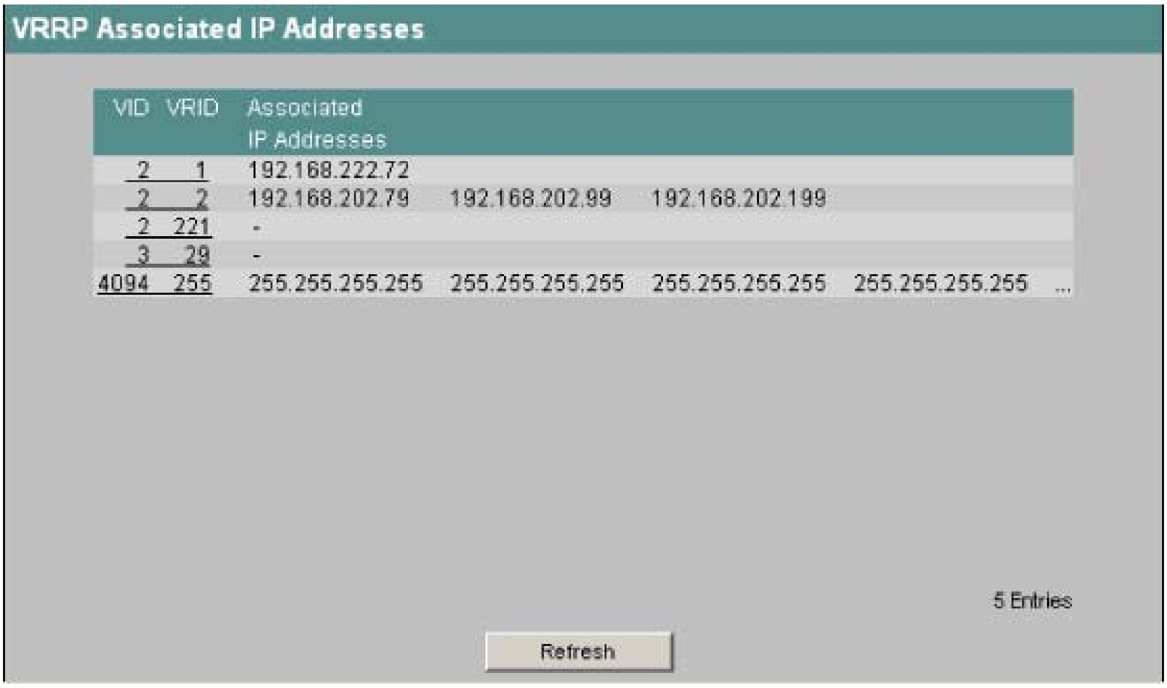


Figure 4-129 VRRP Associated IP Addresses

VID
VLAN ID of the subnet. The IP addresses set up for this and all subnet parameters can be found in the "Router Subnets" menu.

VRID
The ID of the virtual router is displayed in this column. This assigned ID must be unique for this VLAN. Valid values are 1 through 255.

Associated IP Addresses
This column displays 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.

Creating or changing the monitored IP addresses

With the link in the first two columns, you can add, change or delete IP addresses to be monitored.

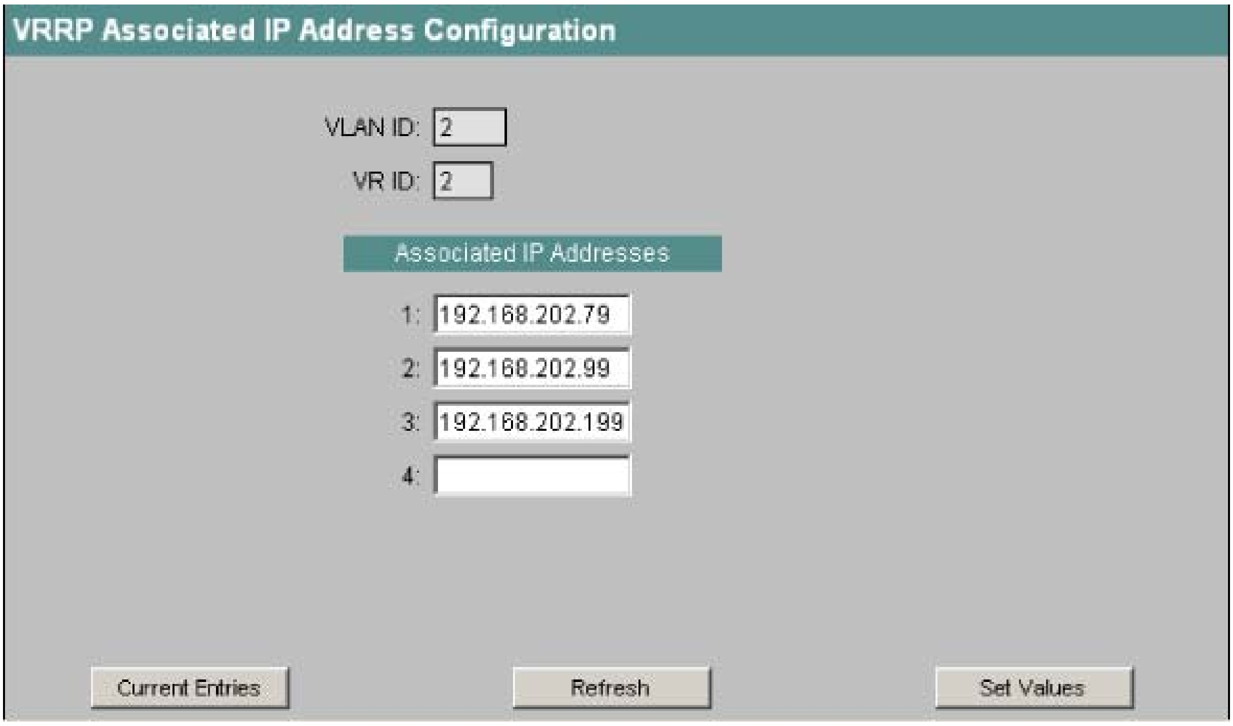


Figure 4-130 VRRP Associated IP Address Configuration

VLAN ID
Shows the VLAN on which the configured virtual router is located.

VR ID
Shows the ID of this virtual router.

Text box 1:, Text box 2:, Text box 3: Text box 4:
Here, you enter the redundant IP addresses to be monitored in this virtual router.

Syntax of the Command Line Interface

VRRP - CLI\ROUTER\VRRP\ADDR>

Command	Description	Comment
info	Shows the currently monitored IP addresses.	-
add <VID> <VRID> <IP>	Adds a new IP address to be monitored.	Administrator only.
delete <VID> <VRID> <IP>	Deletes a monitored IP address.	Administrator only.

4.8.16 VRRP Statistics

Introduction

In this menu, you can view the statistics of the VRRP protocol and all configured virtual routers.

You can reset these statistics to 0 with the "Reset Counters" button.

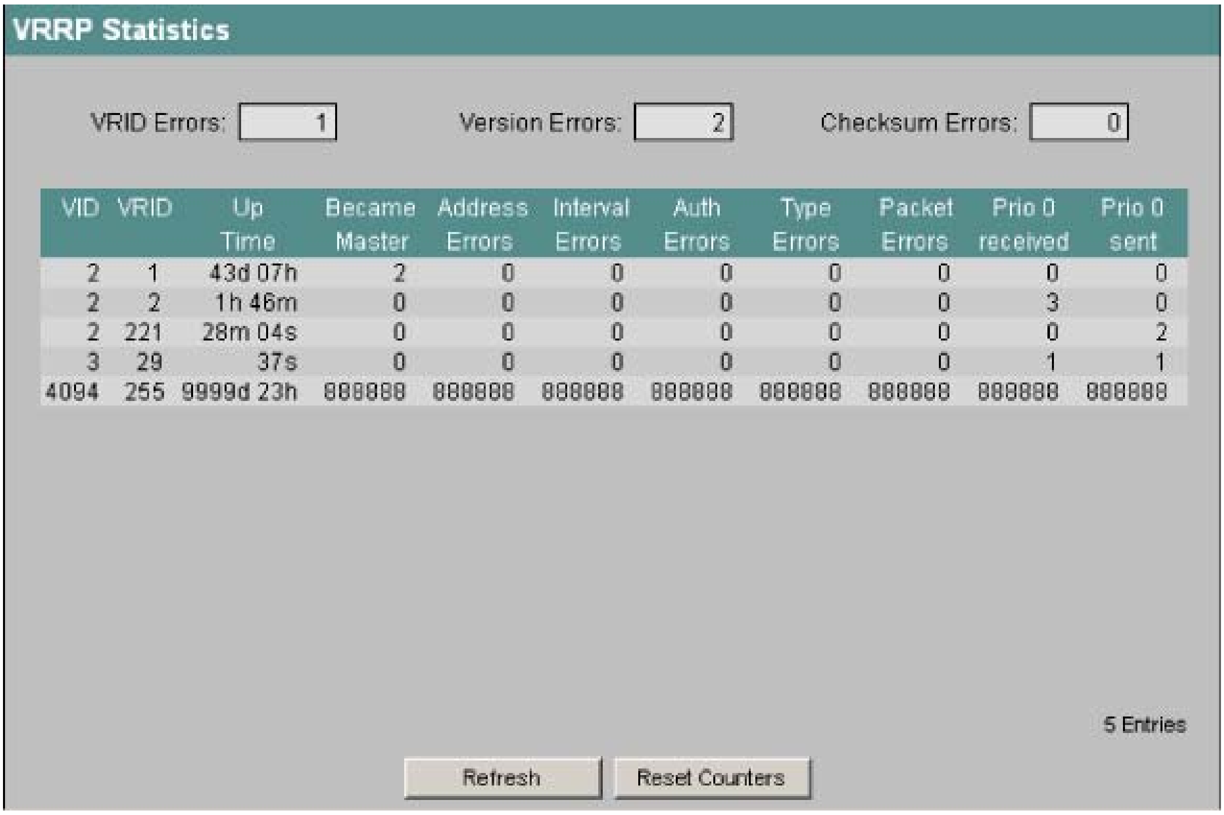


Figure 4-131 VRRP Statistics

VRID Errors
Shows the number of received VRRP packets containing an unsupported VRID.

Version Errors
Shows the number of received VRRP packets containing an invalid version number.

Checksum Errors
Shows the number of received VRRP packets containing an invalid checksum.

VID
VLAN ID of the subnet. The IP addresses set up for this and all subnet parameters can be found in the "Router Subnets" menu.

VRID
The ID of the virtual router is displayed in this column. This assigned ID must be unique for this VLAN. Valid values are 1 through 255.

Up Time
This column shows the time at which the virtual router went into operation.

Note

The MIB object "vrrpOperVirtualRouterUpTime" represents the time at which the virtual router was turned on. To make the information clearer, the "Up Time" column shows how long the virtual router has been turned on.
More precisely, the "Up Time" column shows the difference between the current sysUpTime and the MIB object.

Became Master
Shows how often this virtual router changed to the "Master" state.

Address Errors
Shows how often a packet was received that contained a bad address list.

Interval Errors
This column shows the number of bad received packets whose advertisement interval no longer matches the locally set value.

Auth Errors
This column shows the number of bad received packets whose authentication type was not type 0. Type 0 is the only acceptable type and means "no authentication".

Note

The "Auth Errors" column is the sum of the MIB objects "vrrpStatsInvalidAthType" and "vrrpStatsAuthTypeMismatch".

Type Errors
This column shows the number of bad received packets whose VRRP was not set correctly.

Packet Errors
This column shows the number of bad received packets. This includes both packets with an incorrect length as well as packets whose TTL value was incorrect in the IP header.

Note

The "Packet Errors" column is the sum of the MIB objects "vrrpStatsPacketLengthErrors" and "vrrpStatsIpTtlErrors".

Prio 0 received
Displays how many packets with priority 0 were received. 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
Displays how many 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.

Syntax of the Command Line Interface

VRRP - CLI\ROUTER\VRRP\STAT

Command	Description	Comment
About	Displays the VRRP statistics.	-
resetc	Resets the statistics to 0.	Administrator only.

5 Configuration and diagnostics over SNMP

Configuration of an IE switch over SNMP

Using SNMP (**S**imple **N**etwork **M**anagement **P**rotocol), a network management station can configure and monitor SNMP-compliant nodes such as an IE switch. To allow this, a management agent is installed on the node with which the management station exchanges data using Get and Set requests. The IE switch supports SNMPvV1, SNMPv2, and SNMPv3.

The configurable data is stored on the IE switch in a database known as the MIB (**M**anagement **I**nformation **B**ase) that is accessed by the management station or Web Based Management.

SIMATIC NET SNMP OPC Server

The SNMP OPC server makes available the SNMP information from TCP/IP networks on the IOPC interface with SNMP (Simple Network Management Protocol). With the aid of the SNMP OPC server, any OPC client systems (such as WinCC) can now access diagnostic and parameter data of SNMP-compliant components.

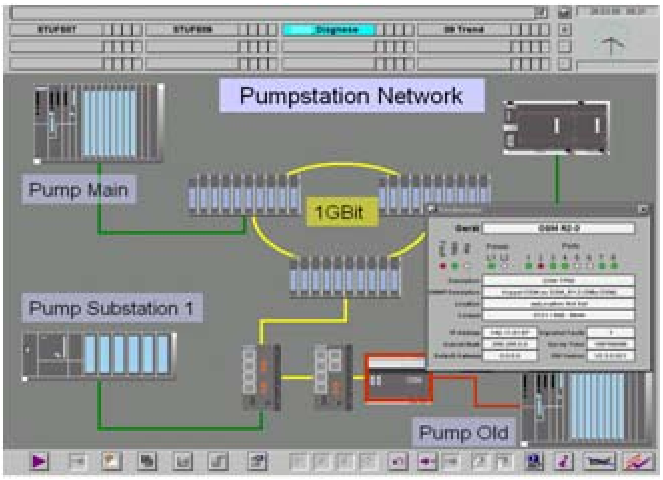


Figure 5-1 WinCC example of network diagnostics with the SIMATIC NET SNMP OPC server

Non SNMP-compliant components can also be included in the plant visualization using their IP addresses. This allows, for example not only simple device diagnostics but also detailed information such as redundant network structures or network load distributions of entire TCP/IP networks to be displayed. With the additional monitoring of this data, device failures can be detected and localized quickly. This increases operational safety and improves plant availability. You configure the devices to be monitored by the SNMP OPC server using STEP 7 (as an alternative you can use NCM PC).

You will find further information on the SNMP OPC server from SIMATIC NET at the following address

http://www.automation.siemens.com/mcms/industrial-communication/en/ie/software/network-management/snmp-opc-server/Pages/snmp-opc-server.aspx

SNMP OPC MIB compiler and profile files

The range of information that can be monitored by the devices with the SNMP OPC server depends on the particular device profile. With the integrated MIB compiler, existing profiles can be modified and new device profiles created for any SNMP-compliant device.

The MIB compiler of the SNMP OPC server requires MIB files according to the SMIv1 standard. This means that you require a modified version of the private SMIv2 MIB file of the IE switch. The SMIv1 MIB of the IE switch and a complete device profile can be downloaded from the following URL:

http://support.automation.siemens.com/WW/view/en/22015045

Standard MIBs

A distinction is made between standardized MIBs defined in RFCs and private MIBs. Private MIBs contain product-specific expansions that are not included in standard MIBs.

An IE switch supports the following MIBs:

- RFC 1213: MIB II (all groups except egp and transmission)
- RFC 2233: Interface MIB (conformance group 4, 5, 6, 7, 10, 11, 13)
- RFC 1286, RFC 1493: Bridge MIB (dot1dBase and dot1dStp)
- RFC 1724: RIP Version 2 MIB Extension (SCALANCE X414-3E)
- RFC 1757: RMON MIB (statistics, history, alarm, event)
- RFC 1850: OSPF Version 2 Management Information Base (SCALANCE X414-3E)
- RFC 2665: EtherLike MIB (dot3StatsTable for SMIv2)
- RFC 2674p: P BRIDGE MIB (conformance group 1, 2, 3, 4, 6, 8, 9)
- RFC 2674q: Q BRIDGE MIB (conformance group 1, 3, 4, 6, 7, 8, 5 to some extent)
- RFC 1907: SNMPv2 MIB (conformance group 5, 6, 7, 8, 9)
- RFC 2571: SNMP FRAMEWORK MIB (SNMPv3 MIB: Conformance group 1)
- RFC 2572: SNMP MPD MIB (SNMPv3 MIB: Conformance group 1)
- RFC 2573: SNMP NOTIFICATION MIB
  (SNMPv3 MIB: Conformance group 1, 2)
- RFC 2573: SNMP PROXY MIB
- RFC 2573: SNMP TARGET MIB (SNMPv3 MIB: Conformance group 1, 2, 3)
- RFC 2574: SNMP-USER-BASED-SM-MIB
  (SNMPv3 MIB: Conformance group 1)

- RFC 2575: SNMP VIEW-BASED ACM MIB
  (SNMPv3 MIB: Conformance group 1)
- RFC 2787: VRRP-MIB (Virtual Router Redundancy Protocol, SCALANCE X414-3E only)

Private MIB

For information on the private MIB of the IE switch, refer to Appendix B of this manual.

Access to the private MIB file of an IE switch

Follow the steps below to access the private MIB file of an IE switch:

1. Open Web Based Management.
2. Select the "System -> Save & Load HTTP" menu item
3. Click on the "Save Private MIB" button.
4. You will be prompted to select a storage location and a name for the file or to accept the proposed file name.

6 PROFINET IO functionality

6.1 Configuring with PROFINET IO

Using PROFINET IO

One option for diagnostics, parameter assignment, and generation of alarm messages of the connected IE switch is to use PROFINET IO.

Here, you can see how you can use the options of PROFINET IO for a connected IE switch.

In the example, it is assumed that a PROFINET IO Controller V2 is already configured with a PROFINET IO chain (see also PROFINET IO System Manual).

Note

STEP 7 V5.4 SP5 or a higher version is required.

Based on the example of a SCALANCE X-400, the following section shows a hardware configuration with a PROFINET IO line.

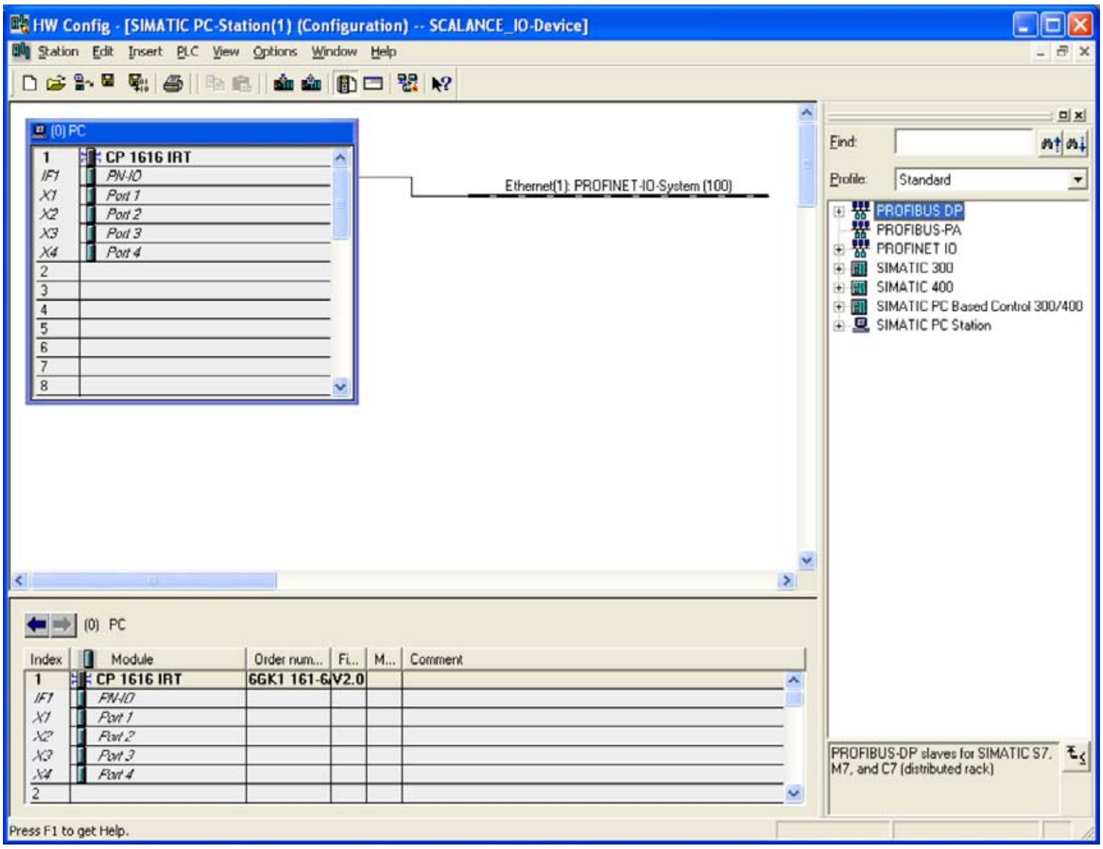


Figure 6-1 HW Config PROFINET IO station setup

Linking IE switches

To include the individual IE switches as PN IO devices, the IE switch must exist in the module catalog under PROFINET IO.

Procedure

If the devices are not yet included in STEP 7, follow the steps below:

1. In the dialog, select HW Config -> Options "Install GSD files".
   The following screen appears:

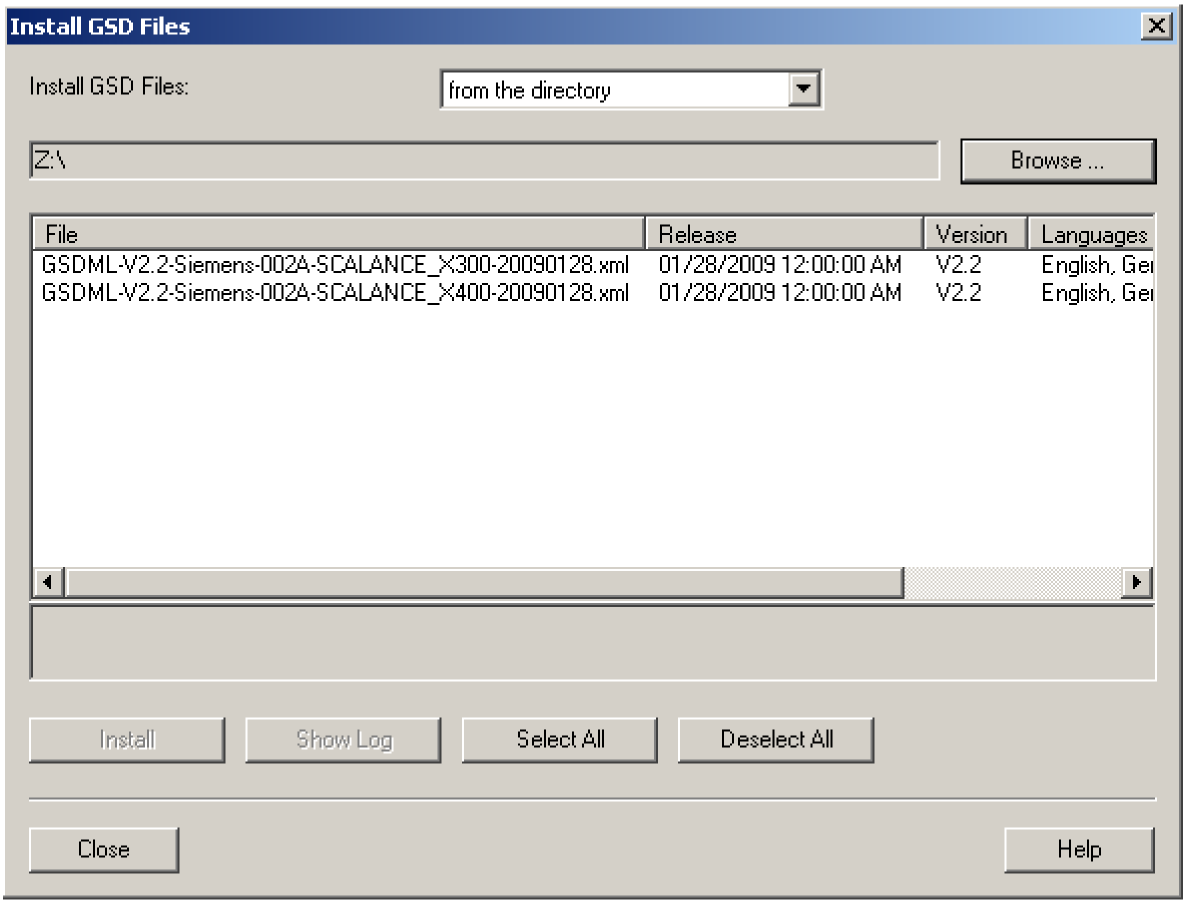


Figure 6-2 Install GSD files

2. Using the "Browse" function go to the supplied xml file (for example GSDML-V2.2-Siemens-002A-SCALANCE_X400-YYYYMMDD.xml - Y, M and D stand for the issue date of the file).

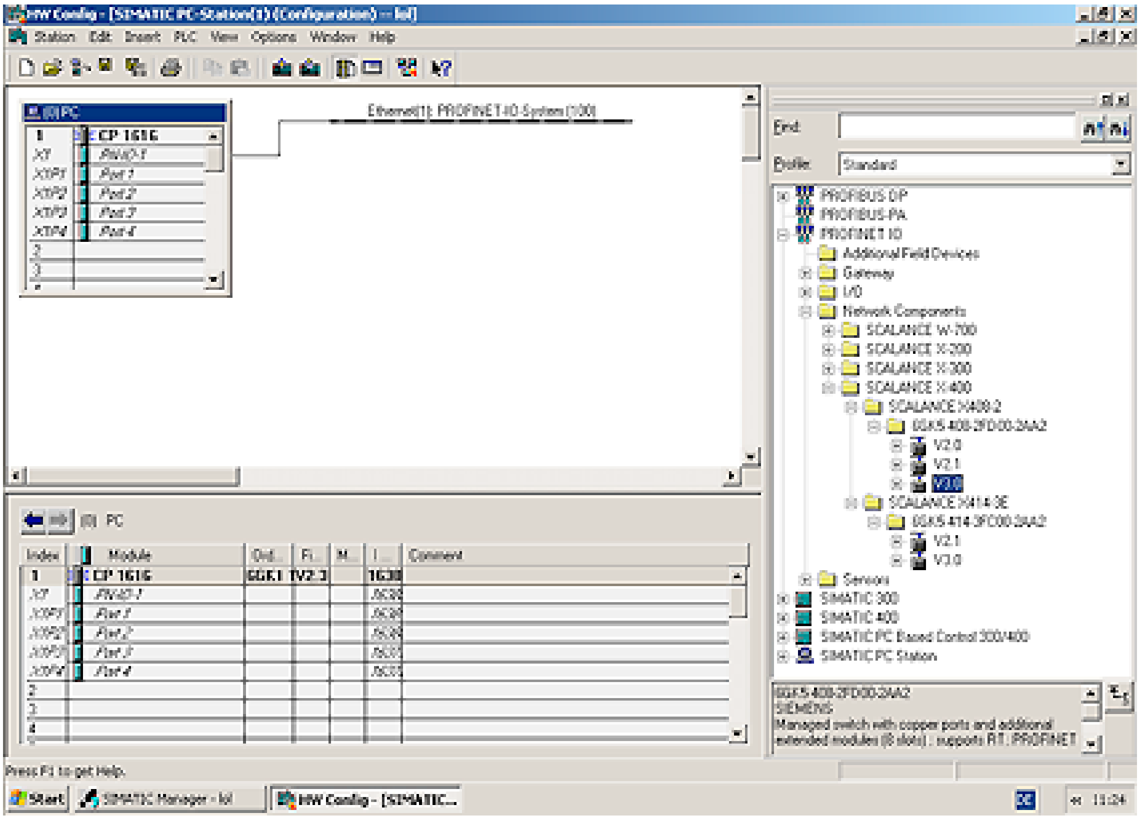


Figure 6-3 HW Config PROFINET IO - inserting a SCALANCE switch

3. Then adopt the file using the "Install" function.
   The IE switches are now included in the module catalog (refer to the module catalog in the following figure).

4. Take the IE switch you require from the hardware catalog (here, for example, SCALANCE X408-2 (PROFINET IO > Network Components > SCALANCE X-400 Switches > SCALANCE X408-2)). Drag the selected SCALANCE to the PROFINET IO system.

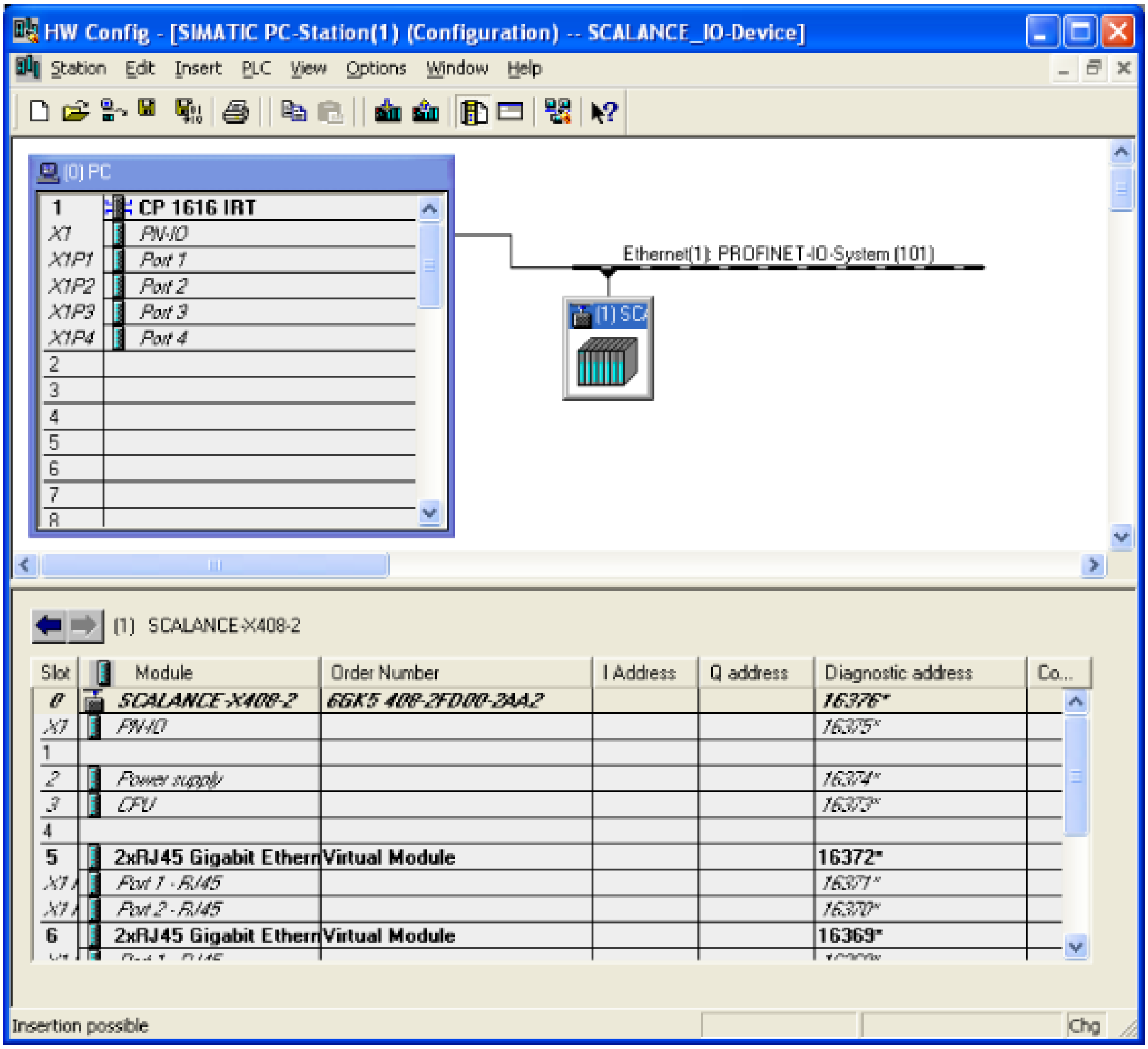


Figure 6-4 HW Config PROFINET IO setting global parameters

5. Click on the "(1)SCALANCE" icon so that the slots of the IE switch are displayed in the lower part of the screen. By double-clicking on slot=0, you can set the global parameters of the IE switch (substitute module) as shown in the figure.
6. You can set the parameters assigned to the relevant module on slots 2 and 3.

7. Click on the slots of the ports to set the port-specific parameters.

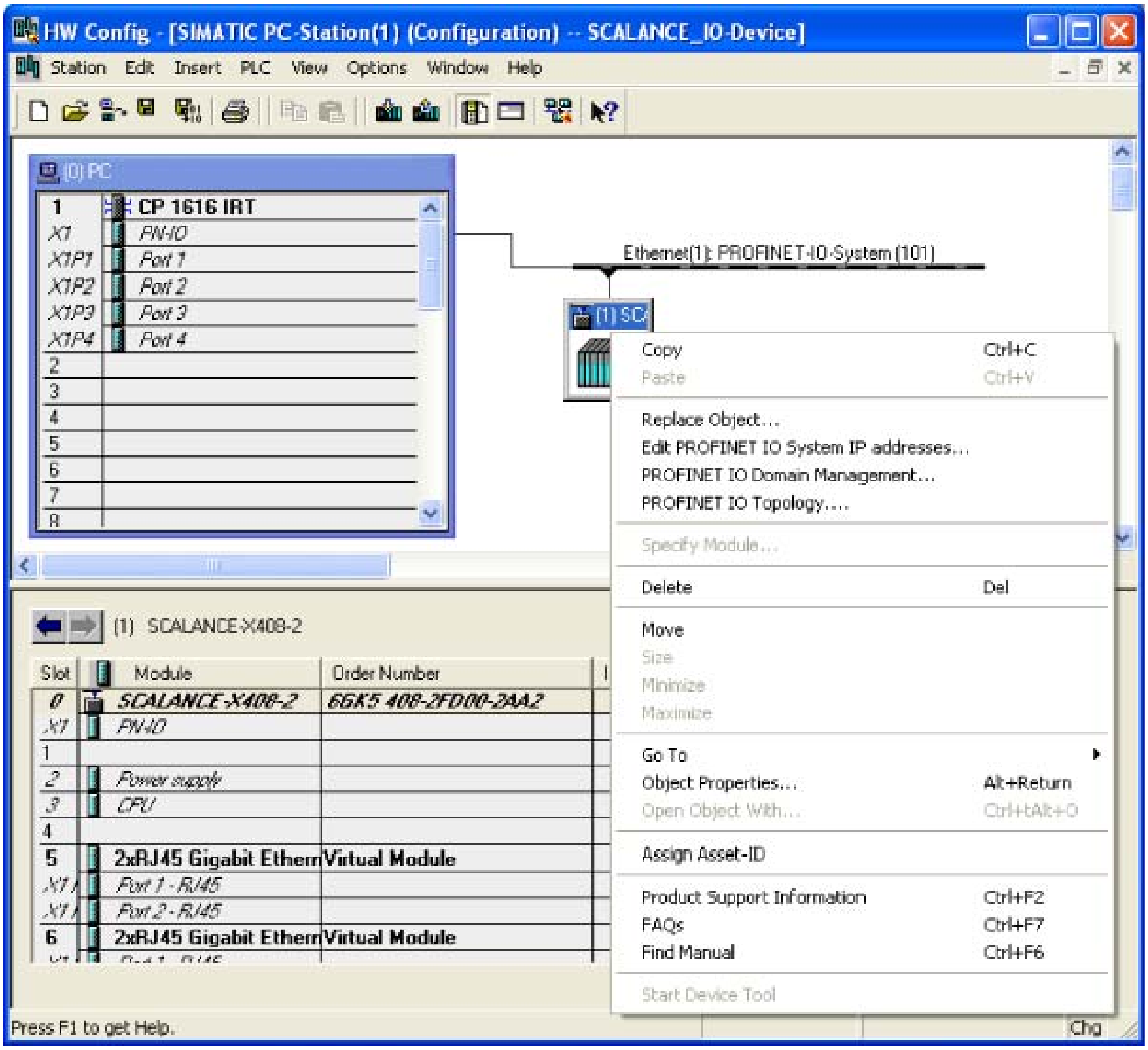


Figure 6-5 HW-Config

8. Open the "Object Properties of the SCALANCE X408-2" dialog in HW Config (right-click on the Icon -> Object Properties) and enter the name of the PROFINET IO device. Click OK to exit the dialog.

9. Select the Station > Save and Compile menu command.
10. Interconnect the devices over the network and turn on the power supplies of the networked devices.

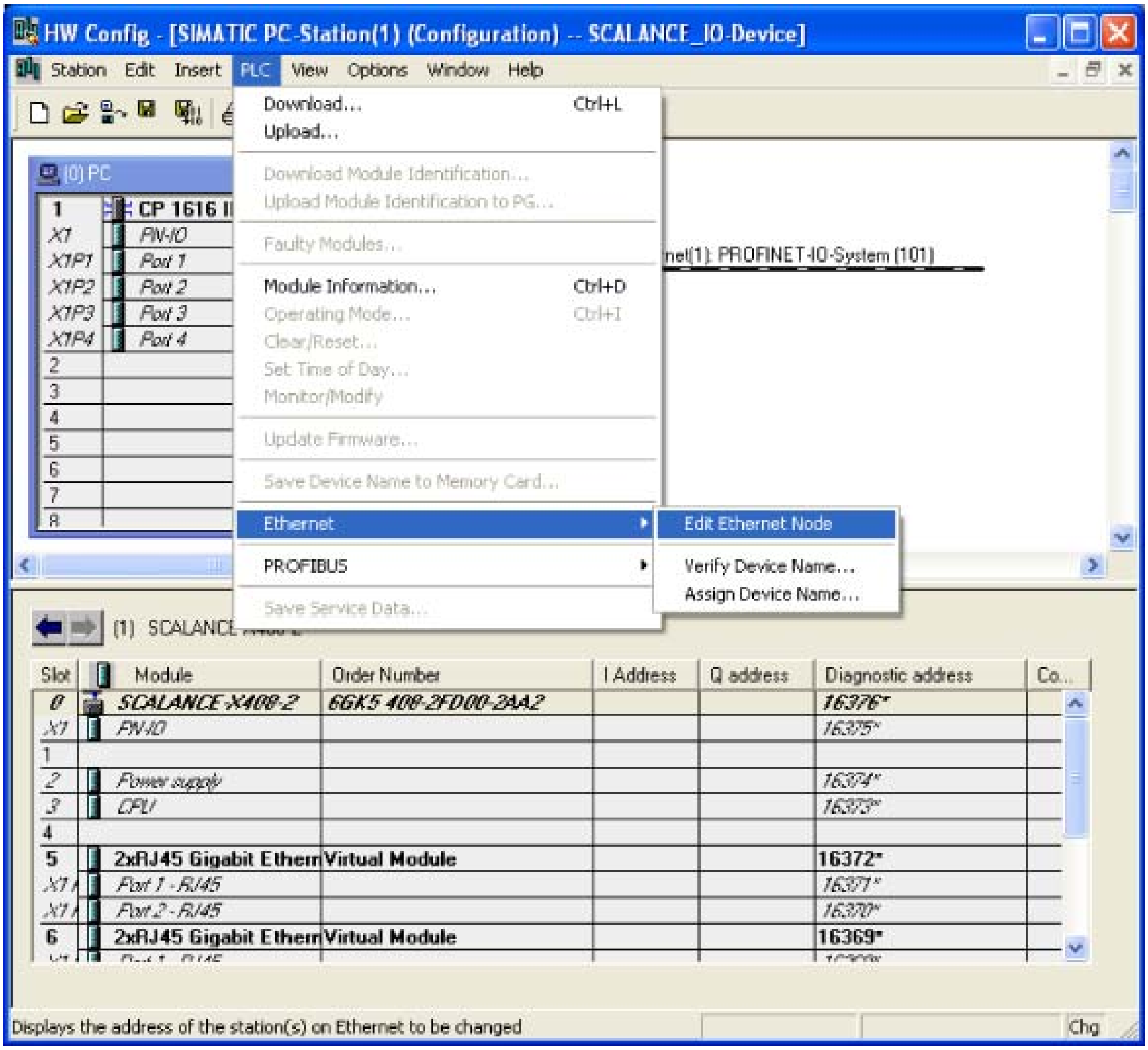


Figure 6-6 HW Config assigning PROFINET IO device names

To transfer the name to the SCALANCE X408-2, you require an online connection from the PG to the PROFINET IO device.

1. You transfer the device name to the SCALANCE X408-2 with PLC > Ethernet > Assign Device Name.

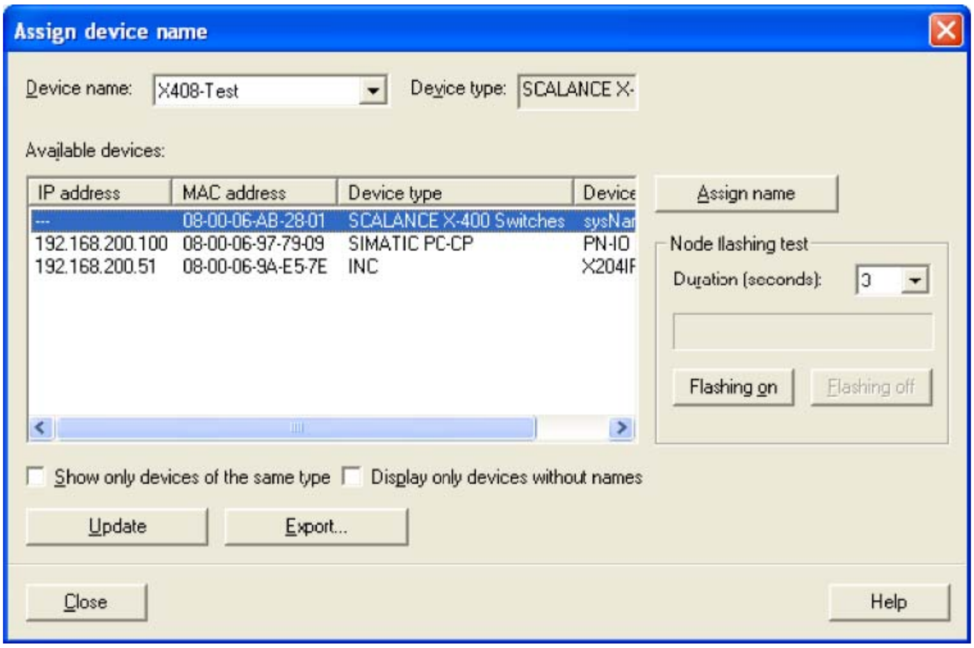


Figure 6-7 Assigning a device name

If you are using multiple PROFINET IO devices, multiple PROFINET IO devices are also indicated in the "Assign device name" dialog. In this case, you should compare the MAC address of the device with the indicated MAC address and select the correct IO device. You can also check the assignment visually with the "Flashing On/Off" button (all the LEDs of the selected IE switch flash).

1. Click on the "Assign Name" button in the "Assign Device Names" dialog box. The device name is stored permanently on the IE switch. After assigning the name, the device name you assigned appears in the dialog box.
2. Download the hardware configuration to the controller (in this example, the CP 1616). Select PLC > Download to Module

6.2 Settings in HW Config

Note

For the IE Switch X-400, the power supply and the C-PLUG interrupt settings are spread over two screens "Power Supply" and "CPU". For the IE Switch X-300, these settings are made in one screen.

Power supply monitoring

Here, you set the parameters of the IE switch relevant to the power supply.

Redundant power supply

- Not monitored
  The failure of one of the two power supplies does not cause an alarm.
- Monitored
  The failure of one of the two power supplies causes an alarm.

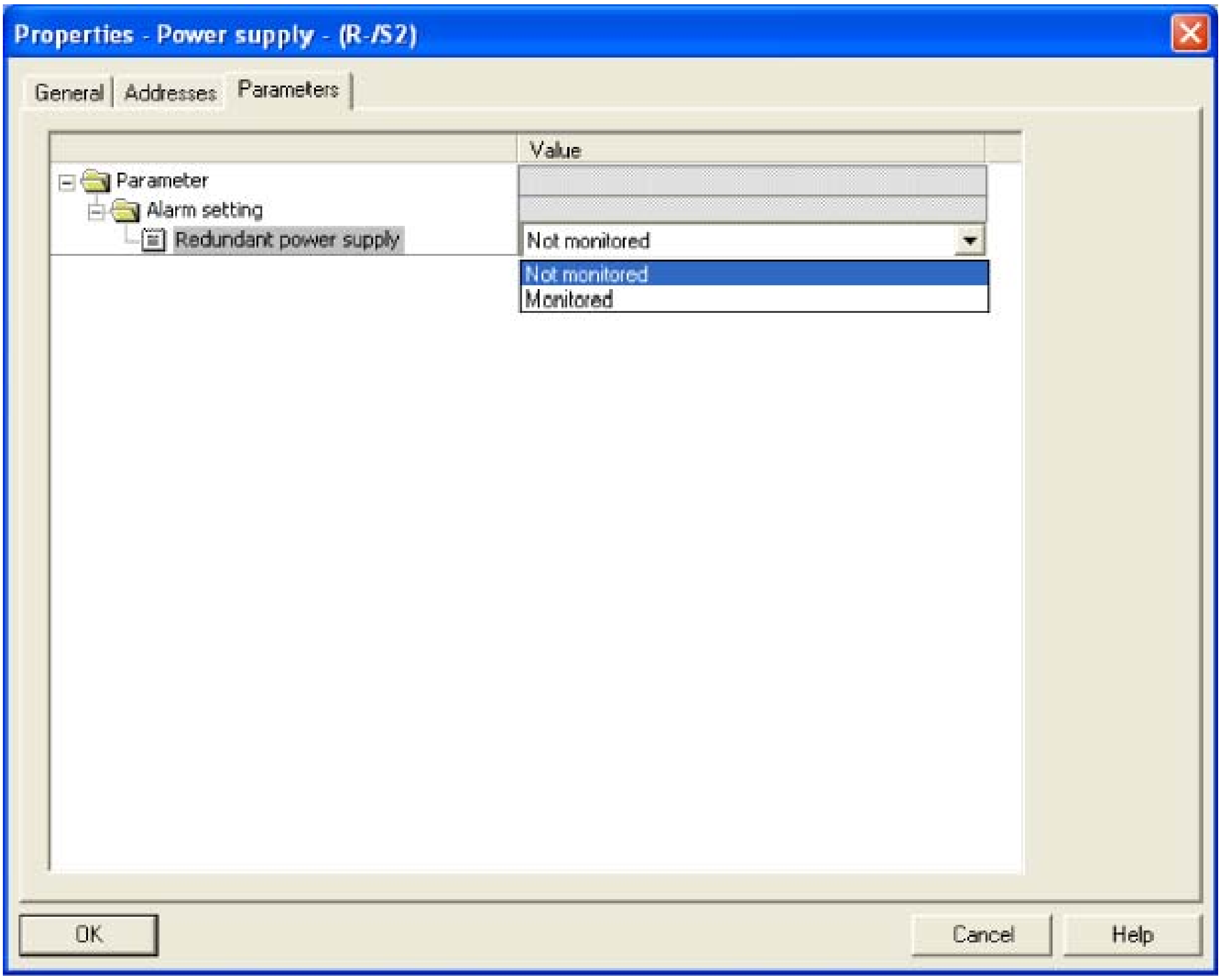


Figure 6-8 Properties - Power supply for an IE Switch X-400

CPU monitoring

Here, you set the parameters of the IE switch relevant to the CPU module.

C-PLUG

- Not monitored
  The C-PLUG is not monitored.
- Monitored
  A C-PLUG fault causes an alarm.

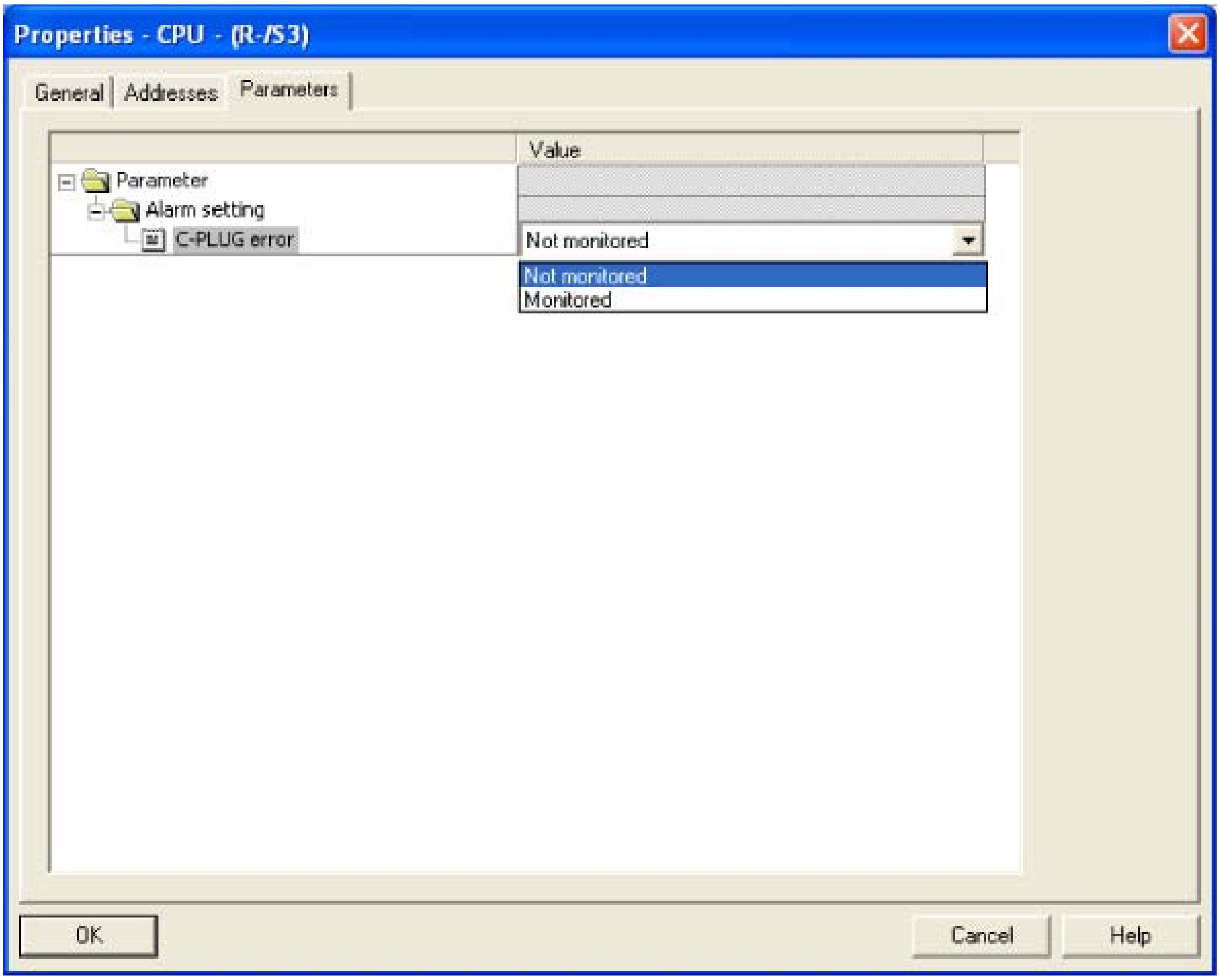


Figure 6-9 Properties - CPU with an IE Switch X-400

Power supply monitoring and CPU monitoring for an IE Switch X-300

The same options are available here as described in the earlier part the chapter.

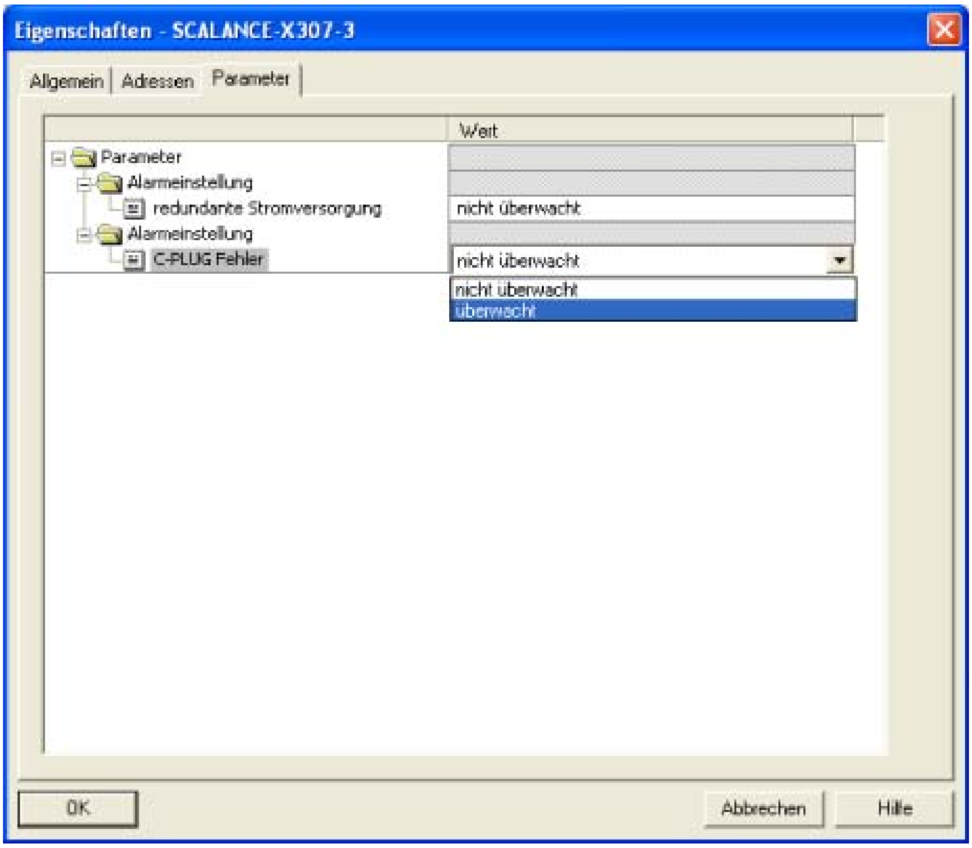


Figure 6-10 Properties - power supply and CPU for an IE Switch X-300

Port-specific settings

Here, you can make the settings for the individual ports of the IE switches.
The following screen shows these settings based on the example of a SCALANCE X408-2.

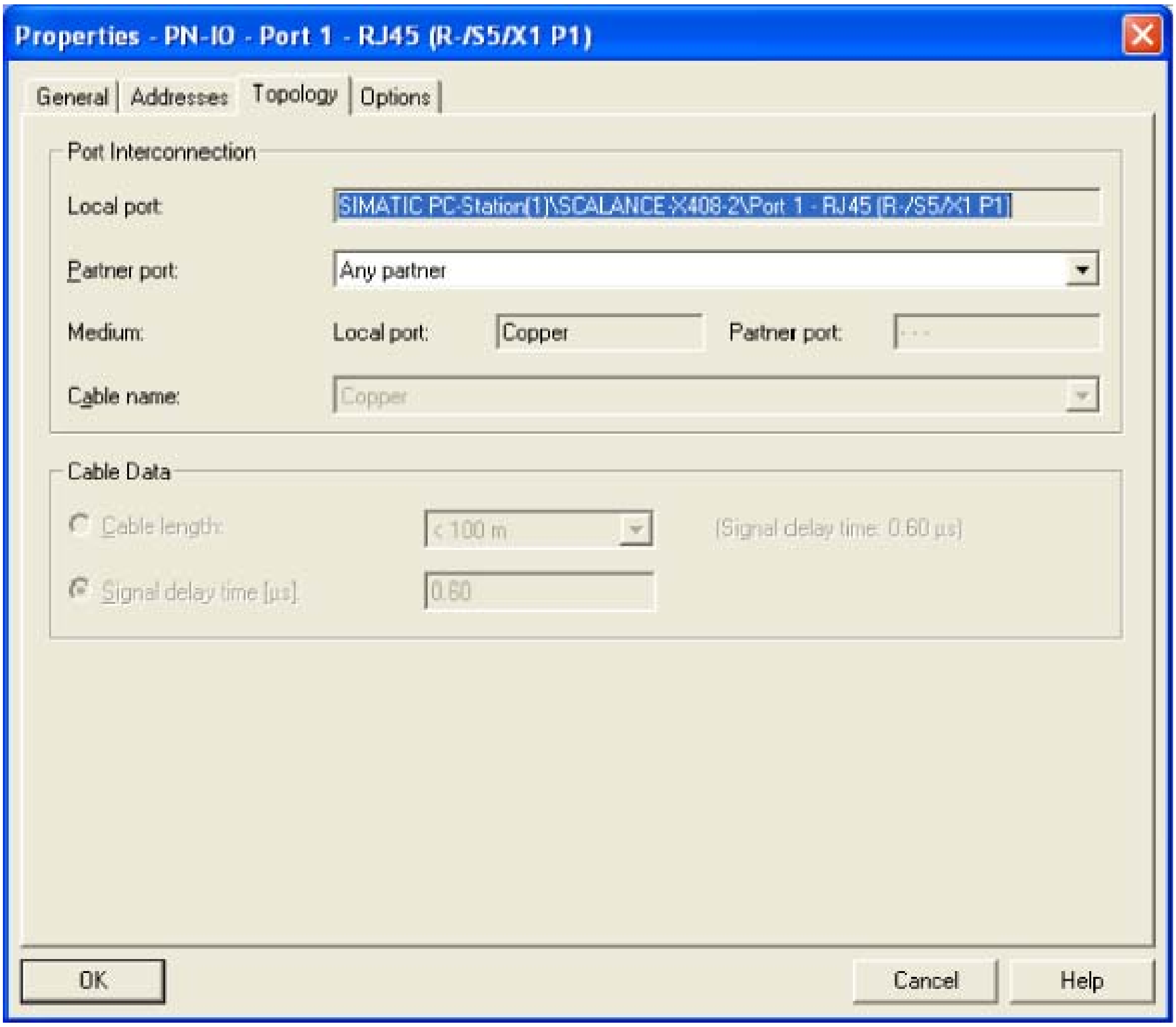


Figure 6-11 Properties - RJ-45 Gigabit Ethernet

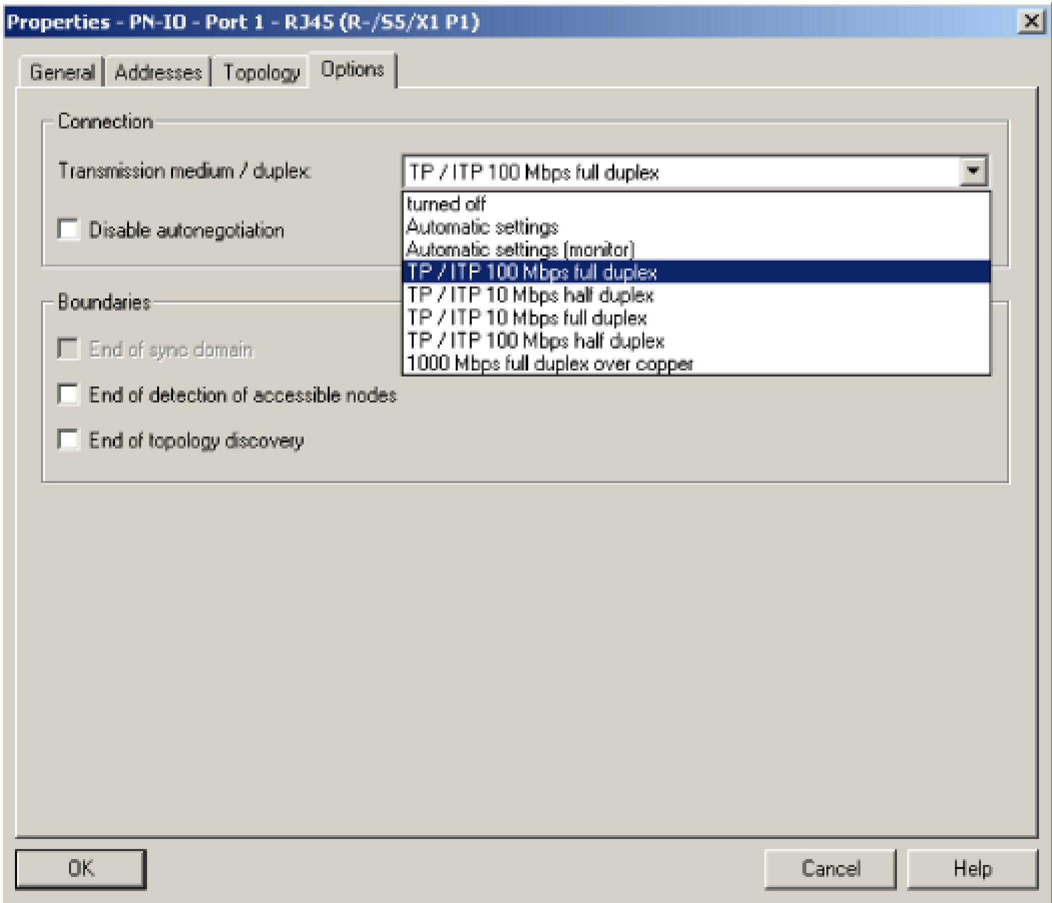


Figure 6-12 Properties - RJ-45 Gigabit Ethernet port options

Settings made during configuration

The transmission rate of the port can be set to Autonegotiation or fixed, for example, at 100 Mbps full duplex.

6.3 Access options over PROFINET IO

Note

The slot functions X-300 table applies to all IE switches X-300 with the exception of the following devices that have their own tables:

- X308-2M slot functions
- Slot functions of the XR-324-12M
- Slot functions of the X302-7EEC and X307-2EEC
- Slot functions of the XR324-4M EEC

Slot functions X-300

The IE Switches X-300 have a subslot per switch port in slot 0.
Functions that cannot be assigned uniquely to one port are assigned to the device access point (slot 0).

Slot 0	Subslot 1	• Alarms • Data records (4.5)	Device Access Point (DAP) • Interface connection • C-PLUG • Redundant power supply
	Subslot 8001 - 8010 SCALANCE X304-2FE: Subslot 8001 - 8006 SCALANCE X306-1LD FE: Subslot 8001 - 8007 SCALANCE X320-1FE: Subslot 8001 - 8021 SCALANCE X320-3LD: Subslot 8001 - 8023	• Alarms (IEC) • Data records (IEC)	Switch port 1 - 10 (or 1 - 6, 1 - 7, 1 - 21, 1 - 23) • Alarm response • Port state

X308-2M slot functions

the IE switch X308-2M has 3 slots. The fixed slots are assigned to slot 0. The other slots, each with 2 ports, are assigned to slot 1 and slot 2.
Functions that cannot be assigned uniquely to a port are assigned to the Device Access Point (slot 0).

Slot 0	Subslot 1	• Alarms • Data records (4.5)	Device Access Point (DAP) • Interface connection • C-PLUG • Redundant power supply
	Subslot 8001 - 8004	• Alarms (IEC) • Data records (IEC)	Switch port 1 - 4 • Alarm response • Port state
Slot 1; slot 2	Subslot 8001 - 8002	• Alarms (IEC) • Data records (IEC)	Switch port 5 - 6; Switch port 7 - 8 • Alarm response • Port state

Slot functions of the XR324-12M

The IE Switch XR324-12M has several slots (slot 1 - slot 12) each with 2 ports.
Functions that cannot be specifically assigned to a port are assigned to the device access point (slot 0).

Slot 0	Subslot 1	• Alarms • Data records (4.5)	Device Access Point (DAP) • Interface connection • C-PLUG • Redundant power supply
Slot 1 to slot 12	Subslot 8001 - 8002	• Alarms (IEC) • Data records (IEC)	Switch port 1 - 24 • Alarm response • Port state

Slot functions of the X302-7EEC and X307-2EEC

The IE Switch X302-7EEC and X307-2EEC has a subslot per switch in slot 0. Functions that cannot be assigned uniquely to one port are assigned to the device access point (slot 0).

Slot 0	Subslot 1	• Alarms • Data records (4.5)	Device Access Point (DAP) • Interface connection • C-PLUG • Redundant power supply
	Subslot 8001 - 8009	• Alarms (IEC) • Data records (IEC)	Switch port 1 - 9 • Alarm response • Port state

Slot functions of the XR324-4M EEC

The IE Switch XR324-4M EEC has several slots. The fixed slots are assigned to slot 0. The other slots each with 2 ports are assigned to slot 1 and slot 4.
Functions that cannot be assigned specifically to one port are assigned to the device access point (slot 0).

Slot 0	Subslot 1	• Alarms • Data records (4.5)	Device Access Point (DAP) • Interface connection • C-PLUG • Redundant power supply
	Subslot 8001-8016	• Alarms (IEC) • Data records (IEC)	Switch port 1-16 • Alarm response • Port state
Slot 1 to slot 4	Subslot 8001 - 8002	• Alarms (IEC) • Data records (IEC)	Switch port 1.1 - 4.2 • Alarm response • Port state

Slot functions X-400

The IE Switch X-400 has several slots each with up to four ports. Functions that cannot be assigned uniquely to a port are assigned to the Device Access Point (slot 0) or to the other higher-level modules (CPU and power module).

Slot 0	Subslot 1	• Alarms (IEC) • Data records (IEC)	Device Access Point (DAP) • Interface connection
Slot 2	Subslot 1	• Alarms 0x200 • Data records 10,12	Power module • Redundant power supply
Slot 3 (X408) Slot 4 (X414)	Subslot 1	• Alarms 0x201, 0x202, 0x203, 0x204 • Data records 11,13	CPU module • C-PLUG
Slots 5, 6 and 8 (X408) Slots 5-7, 9-15 (X414)	Subslot 8001-800n	• Alarms (IEC) • Data records (IEC)	Switch port 5.1-8.4 (X408) Switch port 5.1-15.2 (X414) • Alarm response • Port state

Generating alarms

The user configures exactly the assignment and required properties of the ports. This makes it necessary to match the configuration and installation. If the setting in STEP 7 requires that port 3 is not linked, this must be taken into account during installation. The power fault mask set by STEP 7 is stored retentively and the port fault mask is reset. If you exit DataEX, the settings in the fault mask made by STEP 7 are retained and continue to apply even without PROFINET operation.

- Influence of the SELECT/SET button during DataEX.
  Pressing the button, to set the fault mask has no effect. The port LEDs flashing indicates to the user that there has been no change in the fault mask.
- Effect of other signaling mechanisms during DataEX
  The fault mask is displayed as set by STEP 7 both in the Web interface and in CLI. Changes are not possible. The message "Setting not possible because of PROFINET IO" is displayed.

Structure of the data records

Note

Data records 4 and 5 relate to the IE Switch X-300, data records 10 to 13 to the IE Switch X-400.

Data record 4:

Access: Read-write,

Structure:

typedef struct {

Word BlockType;

Word BlockLength;

Byte BlockVersionHigh:

Byte BlockVersionLow:

DWord Alarm_enable; };

BlockType:

1: Constant

BlockLength:

6: Constant in device data, designates the length without Type+ Length

BlockVersionHigh:

1: Constant in device data, designates the major version

BlockVersionLow:

1: Constant in device data, designates the minor version

Enable_alarms:

This bit list specifies what is to be monitored. If a bit is set, this alarm source is enabled.

Reserved Bit 2 - 31	C-PLUG Bit 1	Red_power Bit 0
0	0: No C-PLUG monitoring	0: No monitoring of the redundant power supply
	1: Missing or incorrect C-PLUG generates alarm	1: Monitoring of the redundant power supply

Data record 5:

Supplies the current alarm setting for this port

Access: Read-only

typedef struct {

Word BlockType;

Word BlockLength;

Byte BlockVersionHigh;

Byte BlockVersionLow;

DWord status; };

BlockType:

1: Constant

BlockLength:

6: Constant in device data, designates the length without Type+ Length

BlockVersionHigh:

1: Constant in device data, designates the major version

BlockVersionLow:

1: Constant in device data, designates the minor version

Status:

Reserved Bits 8-31	C-PLUG_status Bits 4-7	Reserved Bits 2-3	Fault_line_status Bit 1	Power line redundancy Bit 0
0	Information regarding the configuration plug of the network component 0: C-PLUG inserted and ok 1:C-PLUG not inserted 2: C-PLUG inserted but not ok (incorrect type) 3: C-PLUG inserted but not ok (checksum error)		Information regarding the current state of the signaling contact 0: Fault line passive 1: Fault line active	This bit provides information about the redundant power supply 0: not redundant 1: redundant

Data record 10 (power supply, parameter assignment)

Access: Read Write,

Structure:

typedef struct {

Word BlockType;

Word BlockLength;

Byte BlockVersionHigh:

Byte BlockVersionLow:

DWord Alarm_enable; };

BlockType

1: Constant

BlockLength

6: Constant in device data, designates the length without Type+ Length

BlockVersionHigh

1: Constant in device data, designates the major version

BlockVersionLow

1: Constant in device data, designates the minor version

Enable_alarms

Reserved Bits 1-31	Red_power Bit 0
0	0: No monitoring of the redundant power supply
	1: Monitoring of the redundant power supply

Data record 11 (CPU, parameter assignment)

Structure

typedef struct {

Word BlockType;

Word BlockLength;

Byte BlockVersionHigh:

Byte BlockVersionLow:

Word Alarm_Mode;

DWord Alarm_Parameter; };

BlockType

1: Constant

BlockLength

6: Constant in device data, designates the length without Type+ Length

BlockVersionHigh

1: Constant in device data, designates the major version

BlockVersionLow

1: Constant in device data, designates the minor version

Alarm_Mode

Reserved Bits 2-31	Enhanced_Alarm_Mode Bit 1	Show_C-PLUG_Error Bit 0
0	No function	0: No monitoring of the C-PLUG
		1: Missing or incorrect C-PLUG generates an alarm.

Data record 12 (power supply, module status)

Supplies the current alarm setting for this port

Access: Read-only

typedef struct {

Word BlockType;

Word BlockLength;

Byte BlockVersionHigh;

Byte BlockVersionLow;

DWord status; };

BlockType

1: Constant

BlockLength

6: Constant in device data, designates the length without Type+ Length

BlockVersionHigh

1: Constant in device data, designates the major version

BlockVersionLow

1: Constant in device data, designates the minor version

Status

Reserved Bits 2-31	Fault_line_status Bit 1	Power line redundancy Bit 0
0	Information regarding the current state of the signaling contact 0: Fault line passive 1: Fault line active	This bit provides information about the redundant power supply 0: not redundant 1: redundant

Data record 13 (CPU, module status)

Structure

```
typedef struct {
Word BlockType;
Word BlockLength;
Byte BlockVersionHigh;
Byte BlockVersionLow;
DWord PortState;
byte PortType;
byte reserved; };
```

BlockType

1: Constant

BlockLength

6: Constant in device data, designates the length without Type+ Length

BlockVersionHigh

1: Constant in device data, designates the major version

BlockVersionLow

1: Constant in device data, designates the minor version

Status

Reserved Bits 2-31	C-PLUG_status Bits 0-1
0	Information regarding the C-PLUG of the network component 0: C-PLUG inserted and OK 1: C-PLUG not inserted 2: C-PLUG inserted but not OK (incorrect type) 3: C-PLUG inserted but not OK (checksum error)

6.4 Data record 0x802A (PDPortDataReal)

Structure

```
typdef struct{
Word BlockType;
Word BlockLength;
Byte BlockVersionHigh;
Byte BlockVersionLow;
Word Padding;
Word SlotNumber;
Word SubslotNumber;
Byte LengthOwnPortID;
8 Byte OwnPortID;
Byte NumberOfPeers;
Word Padding;
Byte LengthPeerPortID;
8 Byte PeerPortID;
Byte LengthPeerChassisID;
8 Byte PeerChassisID;
Word Padding;
DWord LineDelay;
6 Byte PeerMACAddress;
Word Padding;
Word MAUType;
Word Padding;
DWord DomainBoundary;
DWord MulticastBoundary;
Word LinkState;
Word Padding;
DWord MediaType;};
```

BlockType

Constant = 0x020F

BlockLength

Constant, describes the length of the data record without the BlockType and BlockLength fields.

BlockVersionHigh

Constant = 1, designates the major version.

BlockVersionLow

Constant = 0, designates the minor version.

SlotNumber

Slot number, refer to the section "Access options via PROFINET IO"

SubslotNumber

Subslot number, refer to the section "Access options via PROFINET IO"

LengthOwnPortID

Length of the OwnPortID field in bytes.

OwnPortID

ID of the port used.

NumberOfPeers

Number of neighboring ports.

LengthPeerPortID

Length of the PeerPortID field in bytes.

PeerPortID

ID of the neighboring port.

LengthPeerChassisID

Length of the PeerChassisID field in bytes.

PeerChassisID

ID of the neighboring device.

LineDelay

LineDelay.FormatIndicator = 0

Value (hexadecimal)	Meaning
0x00000000	Line delay and cable delay unknown.
0x00000001 – 0x7FFFFFFF	Line delay in nanoseconds.

LineDelay.FormatIndicator = 1

Value (hexadecimal)	Meaning
0x00000000	Reserved
0x00000001 – 0x7FFFFFFF	Cable delay in nanoseconds.

PeerMACAddress

MAC address of the neighboring device.

MAUType

Value (hexadecimal)	Meaning
0x0000 – 0x0004	Reserved
0x0005	10BASET
0x0006-0x0009	Reserved
0x000A	10BASETXHD
0x000B	10BASETXFD
0x000C	10BASEFLHD
0x000D	10BASEFLFD
0x000F	100BASETXHD
0x0010	100BASETXFD (default)
0x0011	100BASEFXHD
0x0012	100BASEFXFD
0x0013 – 0x0014	Reserved
0x0015	1000BASEXHD
0x0016	1000BASEXFD
0x0017	1000BASELXHD
0x0018	1000BASELXFD
0x0019	1000BASESXHD
0x001A	1000BASESXFD
0x001B – 0x001C	Reserved
0x001D	1000BASETHD
0x001E	1000BASETFD
0x001F	10GigBASEFX
0x0020 – 0x002D	Reserved
0x002E	100BASELX10
0x002F – 0x0035	Reserved
0x0036	100BASEPXFD
0x0037 – 0xFFFF	Reserved

DomainBoundary

Specifies which multicast addresses are blocked.

MulticastBoundary

The individual bits of the DWord variables specify which of the 32 first RT_CLASS_2 multicast addresses (from 01-0E-CF-00-02-00 bis 01-0E-CF-00-02-1F) is blocked.

Bit	Value	Meaning
0	1	The multicast MAC address 01-0E-CF-00-02-00 will be blocked.
	0	The multicast MAC address 01-0E-CF-00-02-00 will not be blocked.
...	1	The multicast MAC address 01-0E-CF-00-02-xx will be blocked.
	0	The multicast MAC address 01-0E-CF-00-02-xx will not be blocked.
31	1	The multicast MAC address 01-0E-CF-00-02-1F will be blocked.
	0	The multicast MAC address 01-0E-CF-00-02-1F will not be blocked.

LinkState

Value (hexadecimal)	Meaning
0x00	Unknown
0x01	Disabled / discard
0x02	Blocked
0x03	Port listening enabled
0x04	Learn
0x05	Forward
0x06	Interrupted
0x07 – 0xFF	Reserved

MediaType

Value (hexadecimal)	Meaning
0x00	Unknown
0x01	Copper cable
0x02	Fiber-optic cable
0x00	Wireless communication
0x04 – 0xFFFFFFFF	Reserved

Note

You will find further information on the IEC data record in IEC 61158.

6.5 MRP configuration in PROFINET IO

To configure in STEP 7, open the "Media redundancy" tab in the properties dialog of the PROFINET interface of the relevant device.

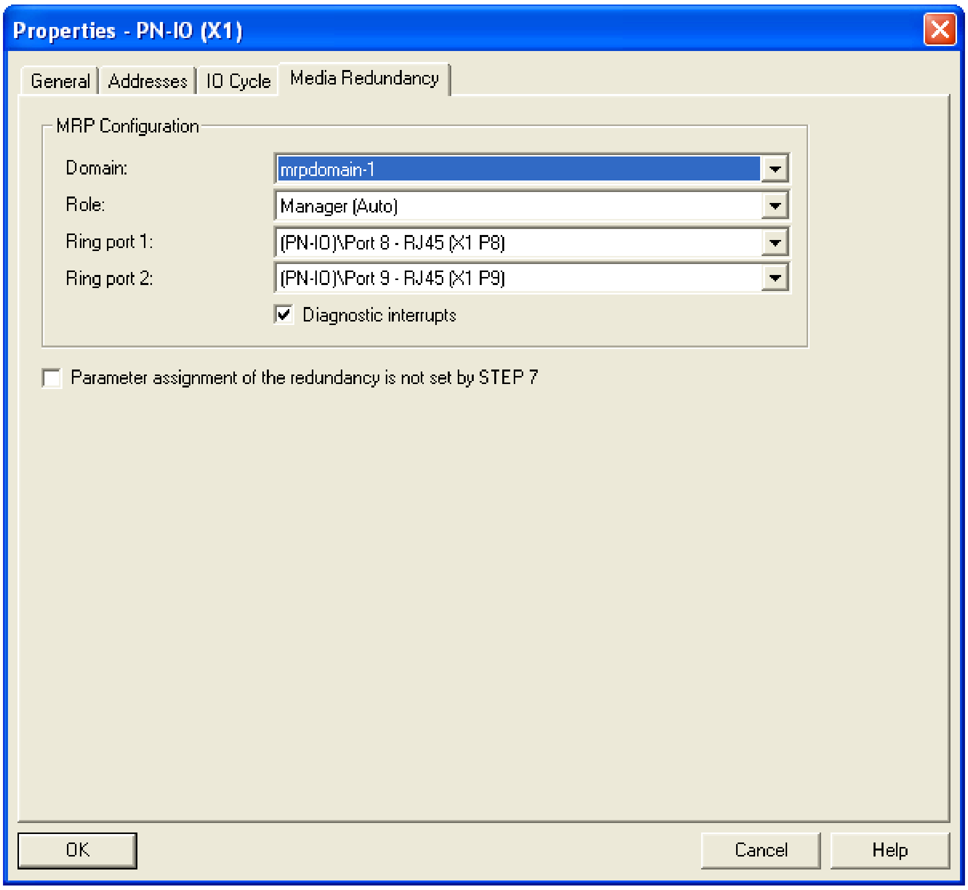


Figure 6-13 Properties dialog of the PROFINET interface of a CP, "Media redundancy" tab

You can set the following parameters in the "MRP configuration" box to configure MRP for the device:

- Domain
- Role
- Ring port
- Diagnostic interrupts

These settings are described below.

Domain

Select the name "mrpdomain-1" from the 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 "default-mrpdomain", the factory settings for "Role" and "Ring ports" also remain active.

NOTICE

PN IO operation of the SCALANCE XR-324-12M only with a module in slot 1

PROFINET IO operation of the SCALANCE XR-324-12M is only possible if there is a module inserted in slot 1 of this device.

The factory settings for "default-mrpdomain" are ports 1 and 2 for MRP, which means that these two ports must exist on the device.

CAUTION

Default ring port definition XR-324-12M (fully modular device) in an offline project

On the SCALANCE XR-324-12M, the ring ports are automatically assigned to the first ports configured offline during the configuration of MRP with STEP 7 when "default-mrpdomain" is selected.

You should therefore check whether the configured ring ports match the connected ring ports.

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 "default-mrpdomain".

  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"):

  – Select the "Manager" role for one device (and one only) that will be redundancy manager in the ring.

  – For all other devices in the ring topology, select the role of "Client".

  > **NOTICE**
  >
  > 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.

  > **NOTICE**
  >
  > If you reset to the factory settings, the MRP role of the device is also reset. 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

> **NOTICE**
>
> If you reset to the factory settings, the ring port settings are also reset. With the appropriate attachment, a previously correctly configured ring node can cause circulating frames and therefore the failure of the data traffic.

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

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.

Diagnostics interrupts

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

The following diagnostic interrupts can be generated:

- Wiring or port error

  Diagnostic interrupts are generated if the following errors occur at the ring ports:

  – 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

Select this check box if you want to configure media redundancy with WBM, CLI or SNMP. The parameter boxes in the MRP configuration group box are then reset and grayed out. The remaining entries have no significance.

C-PLUG

7

Application

The C-PLUG is an exchangeable medium for storage of the configuration data of the modular switch and ships with the product. This means that the configuration data remains available if the basic device is replaced.

NOTICE
The C-PLUG must only be removed or inserted when the power supply to the device is turned off.

How it works

Power is supplied by the end device. The C-PLUG retains all data permanently when the power is turned off.

If an empty C-PLUG (factory settings or deleted with the Clean function) is inserted, all the configuration data of an IE switch is saved to it automatically when the device starts up. Changes to the configuration during operation are saved on the C-PLUG without operator intervention if this is in the *ACCEPTED* status.

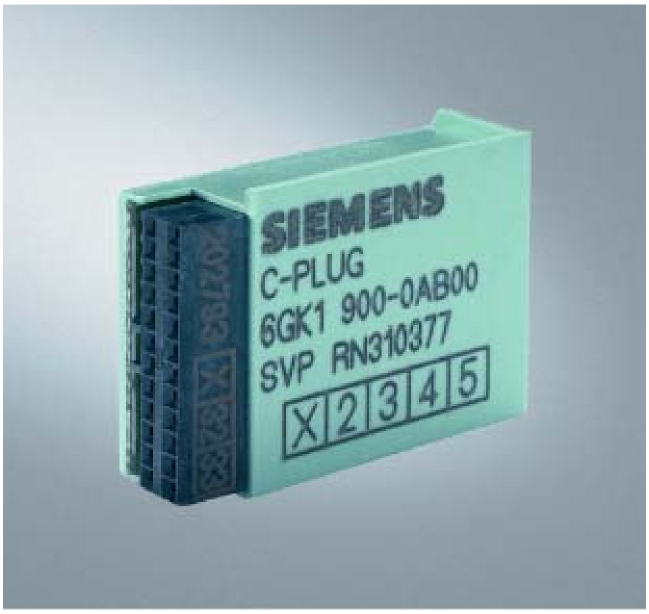


Figure 7-1 C-PLUG

An IE switch with an "ACCEPTED" C-PLUG inserted uses the configuration data of the C-PLUG automatically when it starts up. Acceptance is possible only when the data was written by a compatible device type.

This allows a basic device to be replaced quickly and simply. The C-PLUG is taken from the failed component and inserted in the replacement. The first time it is started up, the replacement device has the same configuration as the failed device except for the MAC address set by the vendor.

NOTICE
If an IE switch is replaced, the configuration with media modules and when using a SCALANCE X414-3E also the settings of the DIL switches and the optional configuration of extender modules must be adopted.

Diagnostics

Inserting a C-PLUG that does not contain the configuration of a compatible device type, accidentally removing the C-PLUG or general malfunctions of the C-PLUG are signaled by the diagnostics mechanisms of the device (LEDs, WEB-based management, SNMP, and CLI).

Startup behavior

	C-PLUG	IE switch startup
1	not found	with internal configuration (if it exists) or with factory defaults.
2	empty	with internal configuration, immediately copies this automatically to the C-PLUG
3	written with own configuration data	with C-PLUG configuration
4	written with other configuration data	with third-party C-PLUG configuration
5	written with configuration data of a different device type	with internal configuration, red LED on power module and log entry
6	defective	with internal configuration, red LED on power module and log entry

In cases 2 and 3, the configuration data on the switch CPU and the C-PLUG is identical. In cases 4 and 5, the configuration data is different and can be synchronized manually. In case 6, you can attempt to reformat the C-PLUG with the clean function. If problems persist, replace the C-PLUG.

NOTICE
In case 4 (replacement) of a SCALANCE X414-3E, the DIL switch settings of the C-PLUG and not the physical switch settings are adopted. A deviation is signaled by the diagnostic options.

8 Firmware update

8.1 Firmware update with functional firmware

8.1.1 Firmware update over HTTP/HTTPS

Web Based Management or Command Line Interface

For information on a firmware updates using HTTP/HTTPS, refer to the section "System Save & Load menu item".

8.1.2 Firmware update over TFTP

Web Based Management or Command Line Interface

For information on a firmware updates using TFTP, refer to the section "System Save & Load menu item".

8.1.3 Firmware updates over FTP

Access over the console

If an IE switch has an IP address and there is an Ethernet connection to a PC or PG, follow the steps below to update the firmware:

1. Open a console window and type in the command ftp followed by the IP address of the IE switch.
   Example:
   ftp 192.168.20.54
2. For the login and password enter the same values as you use for WBM and CLI.
3. Enter the "put" command followed by the name of the firmware file.
   Example:
   put v100031.lad
4. Once the file has been loaded, the IE switch closes the FTP connection and restarts.

8.2 Firmware update using the boot software with an IE Switch X-400/XR-300

Necessity of an update using the boot software

A firmware update using the boot software is necessary when the update cannot be performed using the firmware. Possible reasons for this are bad firmware or a loss of power during the flash operation.

How to start the bootloader mode

A PC or PG must be connected to the serial interface of the IE Switch X-400/XR-300. Follow the steps below to change to the bootloader mode:

1. Switch the IE Switch X-400/XR-300 to display mode A or D. The device automatically switches to display mode A if the SET/SEL button is not pressed for longer than one minute.
2. Press the SET/SEL button for longer than 12 seconds. The device is restarted.
3. While it is restarting, press any key on the PC or PG keyboard.

If there is no functional firmware on the IE Switch X-400/XR-300, the IE Switch X-400/XR-300 automatically starts in a mode in which it can communicate with the integrated FTP server. This is only possible if the IE Switch X-400/XR-300 has an IP address.

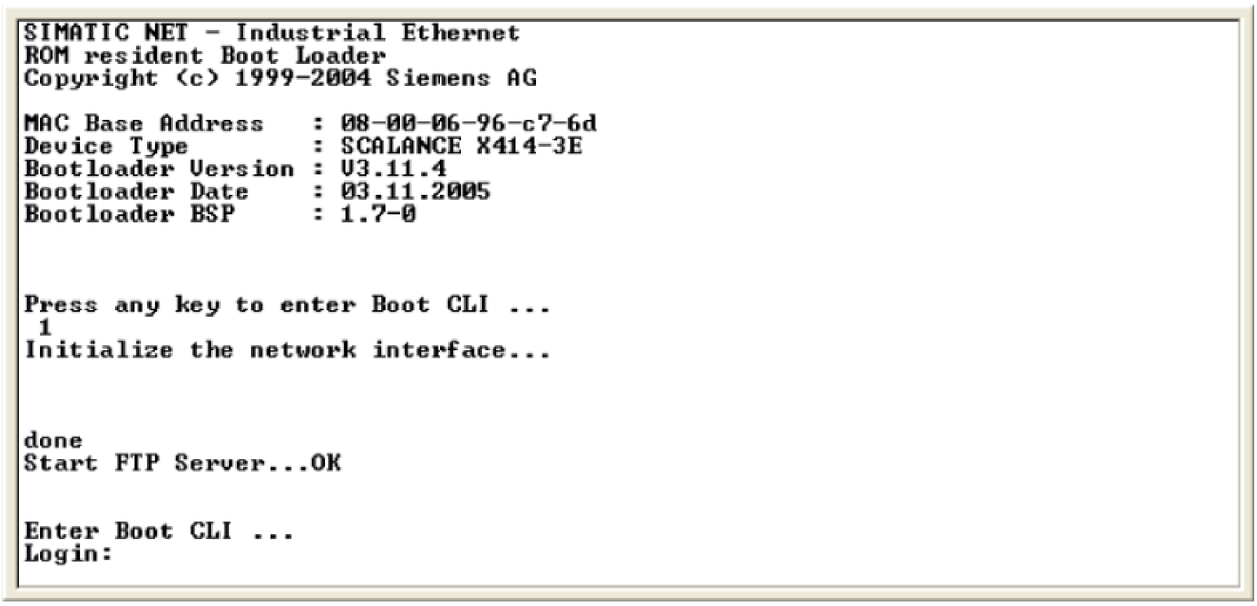
8.2.1 Firmware update over the serial port

Procedure

Follow the steps outlined below to download the firmware over the serial interface of an IE Switch X-400/XR-300:

1. Connect a PC with a terminal program (for example HyperTerminal) to the serial interface of the IE Switch X-400/XR-300 and start the terminal program. You will find additional information on this topic in Appendix A.

2. Reset the IE Switch X-400/XR-300. Switch to display mode A or display mode D (the device automatically switches to display mode A if the SET/SEL button is not pressed for longer than one minute). Press the SET/SEL button for longer than 12 seconds. Press any key to stop the bootloader during startup. HyperTerminal displays the following message:



```
SIMATIC NET - Industrial Ethernet
ROM resident Boot Loader
Copyright (c) 1999-2004 Siemens AG

MAC Base Address    : 08-00-06-96-c7-6d
Device Type         : SCALANCE X414-3E
Bootloader Version  : V3.11.4
Bootloader Date     : 03.11.2005
Bootloader BSP      : 1.7-0


Press any key to enter Boot CLI ...
 1
Initialize the network interface...


done
Start FTP Server...OK


Enter Boot CLI ...
Login:
```

Figure 8-1 HyperTerminal

3. Log in to the command line interface of the bootloader with the following information:
   Login: siemens
   Password: siemens
4. Enter the ldimage command. Hyperterminal then displays the following message:
   XMODEM .... waiting for file
   ATTENTION: do not switch off till the COMPLETED or FAILED message appears
   ... CCCCCCC

5. Select the Transfer > Send File menu command. HyperTerminal opens the following dialog:

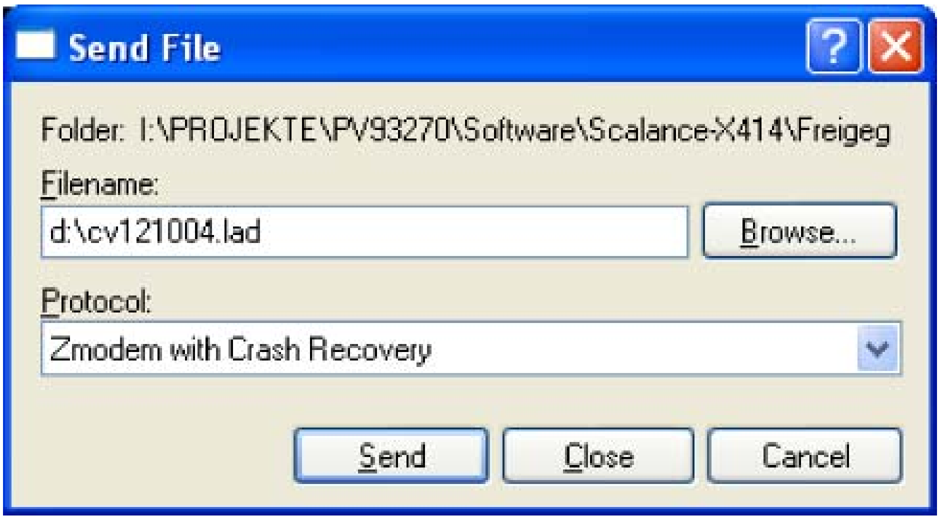


Figure 8-2 Send File dialog

6. Enter the name of the file to be loaded and select Xmodem as the protocol. Click on the Send button to start the upload. A dialog then opens that displays the progress of the upload:

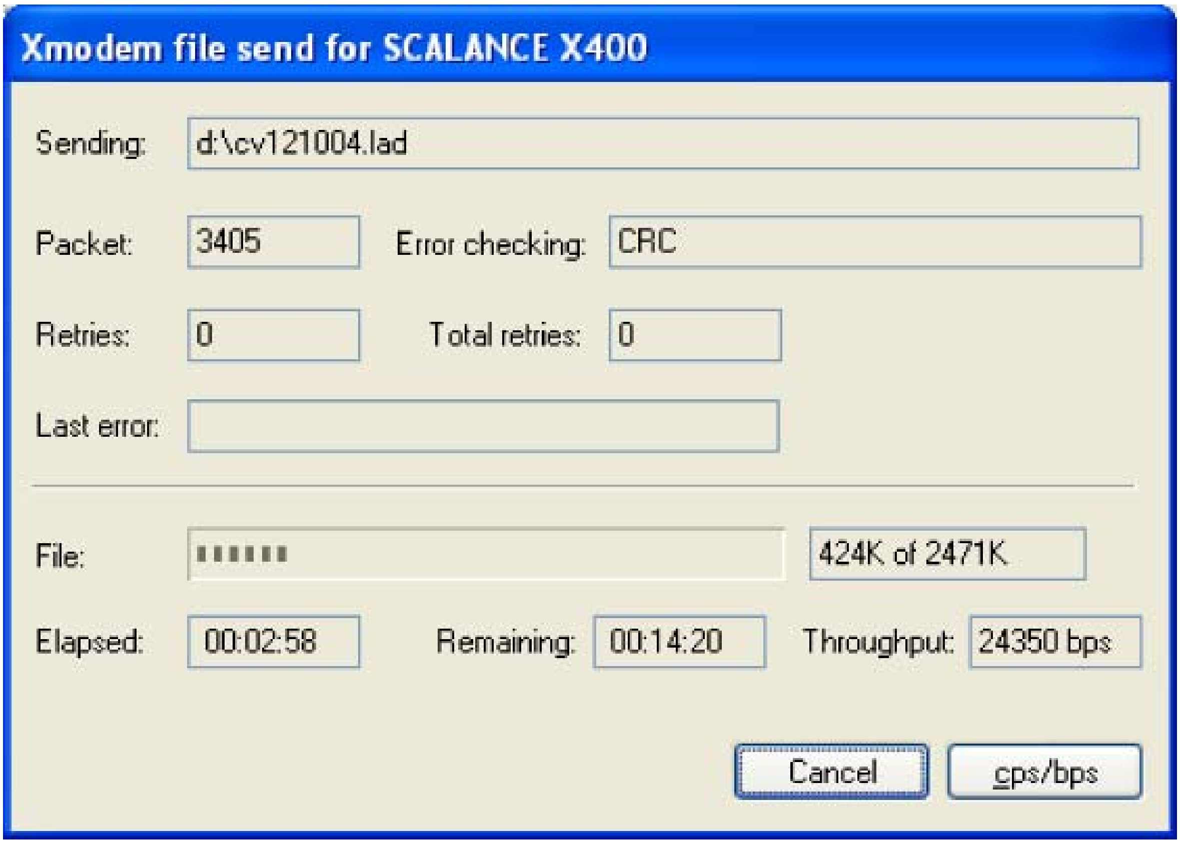


Figure 8-3 Sending a file with Xmodem

7. On completion of the upload, Hyperterminal displays the following message:

   FlashWrite .....COMPLETED

   Restart the device.

Note

During the upload, do not interrupt the connection between the PC and IE Switch X-400/XR-300 or turn off the power supply to the IE Switch X-400/XR-300.

If the upload is interrupted by a problem on the signal line, the device will boot with the old firmware the next time it is started up. You will then need to upload the firmware again.

If the firmware is not stored completely on the IE Switch X-400/XR-300 due to a loss of power, the message "Can't load image from flash -> wrong crc" appears after booting. Once again, you must then upload the firmware again.

8.2.2 Firmware update over an Ethernet port and FTP

Procedure

If the boot function of the IE switch has an IP address and there is an Ethernet connection to a PC or PG, follow the steps below to update the firmware:

1. Open a console window and type in the command ftp followed by the IP address of the IE switch. Example:
   ftp 192.168.20.54
2. For both the login and password, enter *siemens*.
3. Enter the command put followed by the name of the firmware file. Example:
   put V211005.lad
4. Once the file has been loaded, the IE switch closes the FTP connection and restarts. Make sure that you wait until the automatic restart is completed.

Appendix A

A

A.1 PC attachment at the serial interface of a SCALANCE X400

HyperTerminal

The HyperTerminal program is available in the Windows 95 / 98 / NT / 2000 / XP operating systems in the "Start > Programs > Accessories" menu. You can use this program for the following tasks:

- Downloading firmware via the serial interface of the IE Switch X-400.
- Entering commands over the Command Line Interface

Procedure

Follow the steps below to connect a PC to the IE Switch X-400:

1. Connect the serial interface of the PC with the serial interface of the IE Switch X-400 with a commercially available null modem cable.
2. Select the File > New Connection menu command in the HyperTerminal program. The Properties window for a new connection opens.
3. Set the following parameters for the connection:
   Bits per second: 115200
   Data bits 8
   Parity: None
   Stop bits: 1
   Protocol: None

X-400 pinout (null modem cable)

For connection to the PC, a null modem cable has either a 9-pin or a 24-pin D-sub female connector and a 9-pin D-sub female connector at the other end. The following table shows the pin assignment for both cable variants:

	PC connector			SCALANCE X-400 Connector
Signal name	25-pin jack Pin	9-pin jack Pin	Connected With	9-pin jack Pin
TD (Transmit Data)	2	3		3
RD (Receive Data)	3	2		2
RTS (Request to Send)	4	7		7
CTS (Clear to Send)	5	8		8
SG (Signal Ground)	7	5		5
DTR (Data Set Ready)	6	6		6
DTR (Data Terminal Ready)	20	4		4

Figure A-1 Pin assignment table

Note

With SIMATIC programming devices, the serial interface may be a 25-pin female connector. In this case, use a commercially available gender changer (25-pin male to 25-pin male).

A.2 PC attachment at the serial interface of a SCALANCE X300

HyperTerminal

The HyperTerminal program is available in the Windows 95 / 98 / NT / 2000 / XP operating systems in the "Start > Programs > Accessories" menu. You can use this program for the following tasks:

- Downloading firmware via the serial interface of the IE Switch XR-300.
- Entering commands over the Command Line Interface

Procedure

Follow the steps below to connect a PC to the IE Switch XR-300:

1. Connect the serial interface of the PC with the serial interface of the IE Switch XR-300 with the supplied connecting cable for the diagnostics port.
2. Select the File > New Connection menu command in the HyperTerminal program. The Properties window for a new connection opens.
3. Set the following parameters for the connection:
   Bits per second: 115200
   Data bits 8
   Parity: None
   Stop bits: 1
   Protocol: None

Pinout of the XR-300 (connecting cable for the diagnostics port)

Note

With rack devices (R), the connecting cable for the diagnostic port ships with the product.

A connecting cable for the diagnostics port has a 9-pin D-sub female connector for the PC and an RJ-11 plug at the other end. The following table shows the pinout.

RJ-11 plug		D-sub (9-pin, female)	
Pin number	**Assignment**	**Pin number**	**Assignment**
1	n.c.	1	n.c.
2	n.c.	2	RD (Receive Data)
3	TD (Transmit Data)	3	TD (Transmit Data)
4	SG (Signal Ground)	4	n.c.
5	RD (Receive Data)	5	SG (Signal Ground)
6	n.c.	6	n.c.
		7	n.c.
		8	n.c.
		9	n.c.

Appendix B

B

B.1 MIB variables of a SCALANCE X300/X400

Important variables in the MIB II standard

Below, you will find a list with some of the SNMP variables from the MIB II set for monitoring device status. MIB II describes all the SNMP variables that are usually supported by all SNMP-compliant devices.

Variables in the System directory

Table B- 1 Variables in the System directory

Variables	Access rights	Description
sysDescr	Read only	A string with up to 256 characters is used. This value contains a vendor-specific identification of the device.
sysObjectID	Read only	The address (object identifier) used to access device-specific SNMP variables is output here: 1.3.6.1.4.1.4196.1.1.5.4 If no private OIDs have been declared, the object identifier is [0,0]. Here, the value 0 is set as default.
sysUpTime	Read only	Time since the last reset (for example, after power up). The value is shown in hundredths of a second.
sysContact	Read and write	A contact person can be entered here. (Default: empty string). Possible value: string with a maximum of 255 characters.
sysName	Read and write	A name for the device can be entered here. (Default: empty string) Possible value: string with a maximum of 255 characters.

Variables	Access rights	Description
sysLocation	Read and write	Here, the location of the device can be entered (default: empty string). Possible value: string with a maximum of 255 characters.
sysService	Read only	Shows the functions (services) provided by the component according to the ISO/OSI model. Level functionality: • Physical (for example repeater) • Datalink/subnet (for example bridges, switches) • Internet (for example IP gateways, routers) • End to end (for example IP hosts) • Applications (for example E-mail servers) Data type: 32-bit integer.

Variables in the Interface directory

Table B- 2 Variables in the Interface directory

Variables	Access rights	Description
ifNumber	Read only	The number of different interfaces available in the component. With a SCALANCE X414-3E, the value 68 is output for this variable (26 physical ports, 42 internal (virtual) ports. With a SCALANCE X408-2, the value 17 is output for this variable (8 physical ports, 9 internal (virtual) ports. With a SCALANCE X-300, the value 21 is output for this variable (10 physical ports, 11 internal (virtual) ports. Data type: 32-bit integer
ifDescr	Read only	A description of and possibly other information on a port. Possible value: string with a maximum of 255 characters.
ifType	Read only	With IE switches, the value ethernet-csmacd(6), gigabitEthernet(117) or fastEther(62) is entered. Data type: Integer
ifSpeed	Read only	Data transfer rate of the Ethernet port in bits per second. With IE switches either 10 Mbps, 100 Mbps, or 1000 Mbps is displayed. Data type: Gauge.
ifOperStatus	Read only	The current operating status of the Ethernet port. The following values are possible: • up(1) • down(2) • testing(3) • unknown(4) • dormant(5) [waits for external action] • notPresent(6) • lowerLayerDown(7) The testing(3) status indicates that no user data is transported. Data type: Integer
ifLastChange	Read only	Length of time for which the selected port has been operating in the current status. The value is shown in hundredths of a second. Data type: TimeTicks

Variables	Access rights	Description
ifInErrors	Read only	Number of received packages that were not forwarded to higher protocol layers because of an error. Data type: Counter
ifOutErrors	Read only	Number of packages that were not sent because of an error. Data type: Counter

Port Indexes

With SNMP, you cannot specify port identifiers in the format "Slot.Port". SNMP addresses the ports with interface indexes. To change the settings of a port over SNMP, use the AG index. Changes made using the CLI or WBM, can be seen over SNMP only on the AG interfaces. If traps are used, remember that due to the architecture, the AP interfaces are specified in the SNMP bindings of, for example, link up traps. The following tables show how the interface indexes are assigned to the ports.

Port tables for SCALANCE X-300, X408-2 and X414-3E

- Example of a port table (applies to SCALANCE X-300 / X408-2 / X-414-3E):
  The "ifOperStatus.51380225" variable determines the operating state (up, down etc.) of port 1 of the IE switch.

Note

The available number of ports is decided by the device version

Ports are available or not depending on the device version, for example on the device X-306-1LD FE, there are only 7 ports available.

Table B- 3 SCALANCE X-300 port table

Interface Index AG / AP	Port	Port name							
		X306-1LD FE	X307-3, X307-3LD, X308-2, X308-2LD, X308-2LH, X308-2LH+, X310, X310FE	X302-7 EEC, X307-2 EEC	X308-2M	X320-1 FE	X320-3LD FE	XR324-4M	XR324-12M
34603009/ 51380225	Port 1	1	1	1	1	1	1	1	1.1
34603010/ 51380226	Port 2	2	2	2	2	2	2	2	1.2
34603011/ 51380227	Port 3	3	3	3	3	3	3	3	2.1
34603012/ 51380228	Port 4	4	4	4	4	4	4	4	2.2
34603013/ 51380229	Port 5	5	5	5	5 / 1.1	5	5	5	3.1
34603014/ 51380230	Port 6	6	6	6	6 / 1.2	6	6	6	3.2
34603015/ 51380231	Port 7	7	7	7	7 / 2.1	7	7	7	4.1
34603016/ 51380232	Port 8	-	8	8	8 / 2.2	8	8	8	4.2
34603017/ 51380233	Port 9	-	9	9	-	9	9	9	5.1
34603018/ 51380234	Port 10	-	10	-	-	10	10	10	5.2
34603019/ 51380235	Port 11	-	-	-	-	11	11	11	6.1
34603020/ 51380236	Port 12	-	-	-	-	12	12	12	6.2
34603021/ 51380237	Port 13	-	-	-	-	13	13	13	7.1
34603022/ 51380238	Port 14	-	-	-	-	14	14	14	7.2
34603023/ 51380239	Port 15	-	-	-	-	15	15	15	8.1
34603024/ 51380240	Port 16	-	-	-	-	16	16	16	8.2
34603025/ 51380241	Port 17	-	-	-	-	17	17	1.1	9.1

Interface Index AG / AP	Port	Port name							
		X306-1LD FE	X307-3, X307-3LD, X308-2, X308-2LD, X308-2LH, X308-2LH+, X310, X310FE	X302-7 EEC, X307-2 EEC	X308-2M	X320-1 FE	X320-3LD FE	XR324-4M	XR324-12M
34603026/ 51380242	Port 18	-	-	-	-	18	18	1.2	9.2
34603027/ 51380243	Port 19	-	-	-	-	19	19	2.1	10.1
34603028/ 51380244	Port 20	-	-	-	-	20	20	2.2	10.2
34603029/ 51380245	Port 21	-	-	-	-	21	21	3.1	11.1
34603030/ 51380246	Port 22	-	-	-	-	-	22	3.2	11.2
34603031/ 51380247	Port 23	-	-	-	-	-	23	4.1	12.1
34603032/ 51380248	Port 24	-	-	-	-	-	-	4.2	12.2

Table B- 4 Port table for SCALANCE X408-2 and X414-3E

Interface Index AG / AP	Port	Port name			
		X408-2	X414-3E		
			without extender	with electrical extender	with optical extender
34603009 / 51380225	Port 1	5.1	5.1	5.1	5.1
34603010 / 51380226	Port 2	5.2	5.2	5.2	5.2
34603011 / 51380227	Port 3	6.1	6.1	6.1	6.1
34603012 / 51380228	Port 4	6.2	6.2	6.2	6.2
34603013 / 51380229	Port 5	8.1	7.1	7.1	7.1
34603014 / 51380230	Port 6	8.2	7.2	7.2	7.2
34603015 / 51380231	Port 7	8.3	9.1	9.1	9.1
34603016 / 51380232	Port 8	8.4	9.2	9.2	9.2
34603017 / 51380233	Port 9	-	9.3	9.3	9.3
34603018 / 51380234	Port 10	-	9.4	9.4	9.4
34603019 / 51380235	Port 11	-	10.1	10.1	10.1
34603020 / 51380236	Port 12	-	10.2	10.2	10.2
34603021 / 51380237	Port 13	-	10.3	10.3	10.3
34603022 / 51380238	Port 14	-	10.4	10.4	10.4
34603023 / 51380239	Port 15	-	11.1	11.1	11.1
34603024 / 51380240	Port 16	-	11.2	11.2	11.2
34603025 / 51380241	Port 17	-	11.3	11.3	11.3
34603026 / 51380242	Port 18	-	11.4	11.4	11.4
34603027 / 51380243	Port 19	-	-	12.1	12.1
34603028 / 51380244	Port 20	-	-	12.2	12.2
34603029 / 51380245	Port 21	-	-	12.3	13.1
34603030 / 51380246	Port 22	-	-	12.4	13.2
34603031 / 51380247	Port 23	-	-	13.1	14.1
34603032 / 51380248	Port 24	-	-	13.2	14.2
34603033 / 51380249	Port 25	-	-	13.3	15.1
34603034 / 51380250	Port 26	-	-	13.4	15.2

Important private MIB variables of an IE Switch

OID

The private MIB variables of the IE switch have the following object identifier:

iso(1).org(3).dod(6).internet(1).private(4).enterprises(1).ad(4196).adProductMibs(1).simaticNet(1).iScalanceX(5).iScalanceX300X400(4)

Table B- 5 Private MIB variables of an IE switch

Variables	Access rights	Description
snX300X400FaultState	Read only	Displays the status of the signaling contact. Possible values: • 1 No error • 2 Error. Data type: Integer
snX300X400ReportFaultIndex	Read only	Errors are assigned an ascending index according to the order in which they occur. This 4-byte variable specifies the index.
snX300X400ReportFaultState	Read only	Contains the error message belonging to an index.
snX300X400RmMode	Read only	The redundancy manager mode: • The IE switch is redundancy manager. • The IE switch is not redundancy manager.
snX300X400RmState	Read only	Indicates whether the redundancy manager is active or passive. Possible values: • The redundancy manager is passive. The IE switch is operating as redundancy manager and has opened the ring; in other words, the line of IE switches connected to it is operating problem-free. The "Passive" status is also shown when the redundancy manager mode is disabled. • The redundancy manager is active. The IE switch is operating as redundancy manager and has closed the ring; in other words, the line of IE switches connected to it is interrupted (fault). The redundancy manager switches through the connection between the ring ports and thus restores a functioning bus configuration. Data type: Integer
snX300X400RmStateChanges	Read only	Indicates how often the redundancy manager was switched to "active". Data type: Counter
snX300X400StandbyMode	Read only	The standby function mode: • The standby function is enabled. • The standby function is disabled.

Variables	Access rights	Description
snX300X400StandbyState	Read only	Displays the standby status: • 1 Device is master and passive. • 3 Device is slave and passive • 5 Device is master and active • 7 Device is slave and active • 257 Device searching for partner for standby connection • 300 The standby function is disabled • Data type: Integer
snX300X400StandbyStateChanges	Read only	Indicates how often the standby status was switched active. Data type: Counter
snBootStrapVersion	Read only	The firmware version of the bootloader in the format *major.minor*.
snHwVersion	Read only	The hardware version of the system in the format *major.minor*.
snSwVersion	Read only	The software version of the system.
snInfoSerialNr	Read only	The serial number of the product.
snMacAddressBase	Read only	The base MAC address of the IE switch.
snX300X400ModuleIdentMLFB	Read only	The MLFB number of the module.
snX300X400Power Supply1State	Read only	The status of power supply input 1.
snX300X400Power Supply2State	Read only	The status of power supply input 2.
snX300X400ReportDigitalInState	Read only	Status belonging to the digital input. (SCALANCE X414-3E)

Appendix C

C

C.1 Tagging frames

Expansion of the Ethernet frames by four bytes

For the functions CoS (Class of Service, frame priority) and port-based 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 an Ethernet frame from 1518 to 1522 bytes. It is necessary to check whether the end nodes on the network can process this length / 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 data packet between the source address and the Ethernet type / length field:

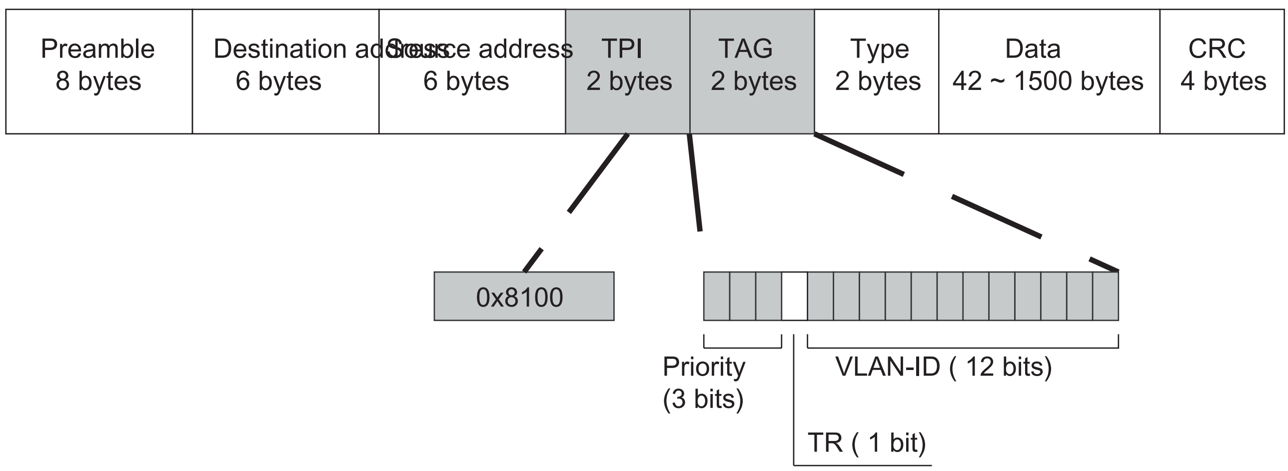


Figure C-1 Structure of a tagged frame

The additional bytes contain the tag protocol identifier field and the tag control information field.

Tag protocol identifier field

The first two bytes form the Tag Protocol Protocol Identifier field (TPI) and always contain the value 0x8100. This value specifies that the data packet contains VLAN information or priority information.

Tag control information field

The 2 bytes of the Tag Control Information field (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 then 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.

An IE switch has four 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

The TR bit is used as an identifier for a Token Ring encapsulation process.

VLAN–ID

With the remaining 12 bits, up to 4095 VLAN-IDs can be formed (VLAN ID 4095 is not permitted). 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.

Appendix D

D

D.1 Error messages of the SCALANCE X300 / X400

Note

If link aggregation is activated, instead of a port number, you can also specify the number of the aggregation (for example AG1).

Messages when an error occurs and following elimination of an error

Error messages assigned to an error status (error LED)
Link down on <port number>. Link up on <port number>.
Non-recoverable ring error on <port number>. Ring error on <port number> recovered.
Second redundancy manager detected ... MAC <MAC address> on <port number>. Second redundancy manager gone ... MAC <MAC address> on <port number>.
<HSR> ring manager activated <HSR> ring manager falls back to client
<HSR> ring manager entered active state. <HSR> ring manager falls back to passive state.
Standby device enters active state. Standby device enters passive state.
Standby is waiting for partner Standby <master or slave> connected to <slave or master> <MAC address>.
Standby <master or slave> lost connection to < slave or master > <MAC address> Standby <master or slave> connected to < slave or master > <MAC address>.
Not supported version <version number> for standby protocol detected. Not supported version <version number> for standby protocol disappeared.
Second observer detected. Details: MAC <MAC address> at <port number>. Second observer gone. Details: MAC <MAC address> at <port number>.
Observer: RM switches frames on isolated port. Observer: RM stopped switching on isolated port.
Unexpected traffic received on observer <port number> Unexpected traffic on observer <port number> gone.
Observer: Timeout for test frames detected on port <port number> while RM signals "passive". Observer: Timeout for test frames on port <port number> is gone.

Error messages assigned to an error status (error LED)
Observer: RM signals active but RM test frames are received on both ring ports. Observer: RM signals right state.
Observer: RM runs incompatible software version <version number>. Observer: RM's incompatible software version <version number> disappeared.
Observer: RM test frame timeout on both ring ports. Observer: RM test frames received.
Observer stopped recovering because of too many (<number of errors>) repeated errors. Observer restarted because of user command.
Standby <partner / observer> conflicts with <active / passive> state. Standby <partner's / observer's> state conflict resolved.
Standby <partner / observer> conflicts with <master / slave> role. Standby <partner / observer> conflicts with <master / slave> role resolved.
Power down on line <ID of the power supply>. Power up on line <ID of the power supply>.
Internal error: <voltage> V power down. Internal error gone: <voltage> V power is back.
Wrong module <module name> on slot <slot number> (ID: <module ID>). Wrong module <module name> on slot <slot number> removed.
C-PLUG not accepted. See System C-PLUG mask for details. C-PLUG accepted.
C-PLUG interface unmounted - restart required. C-PLUG interface mounted.
C-PLUG missing. C-PLUG found.
The media module for ring <port number> is missing. The media module for ring <port number> was detected.
DIP switch <name of switch> changed, restart required. DIP switch <name of switch> set back to original state.
Internal error(s) and/or exception(s) occurred. Internal error(s) and/or exception(s) confirmed.
Device boot up incomplete. Device boot up completed.
RM <MAC address> lost. RM <MAC address> detected.
The media module for standby <port number> is missing. The media module for standby <port number> was detected.
PNIO fault - please use STEP 7 for diagnostics PNIO fault - gone.
PNIO connection established PNIO connection terminated.
Severe module change detected, restart required. Severe module change reverted.
DIP switch settings manipulated ... -> Redundancy will be started after next restart. DIP switch settings reset ... -> Redundancy mode will not change after next restart.
Authentication status on <port number>: FAILED! Reason: <cause of error>" Authentication status on <port number>: o.k. Reason: <cause of error>

Error messages assigned to an error status (error LED)
Standby <master or slave> freezes current state <status> because <slave or master> <MAC address> disappeared. Unfreeze standby state <status> because partner <MAC address> became visible.
Link up on <port number>. Link down on <port number>.
Default route is stored in hardware. Default route no longer in hardware.
Non-recoverable error: RM receives test frames from only one ring port. Non-recoverable error cleared: RM receives test frames from both ring ports.
Non-recoverable error: More than one RM in ring. Non-recoverable error cleared: Single RM in ring.
Last MRP manager in ring won't stop on ring ports <port number> and <port number> (danger of network loops). MRP ring manager may stop now (no danger of network loops anymore).
Redundancy mode transition not completed ! is: <blocked or data transfer possible>, should: < data transfer possible or blocked> Redundancy mode transition to <blocked or data transfer possible> completed.
Erroneous connected ring line on <port number> (should <port number>) Erroneous connected ring line removed on <port number>.
Main Power Usage exceeded Threshold. Main Power Usage fallen below Threshold again.
Unknown SFP module on <port number> (vendor: <vendor name>) Unknown SFP module on <port number> removed
New fault state: <description of the error> Message when the error occurs. Fault state gone: <description of the error> Message after eliminating the error. New fault state (reconfiguration) / Fault state gone (reconfiguration): <description of the error> Message due to changed settings in error monitoring by the user.

Message to inform about an event that occurred

The following messages provide you with information about events that are not directly related to an error status (error LED).

Messages for information
User entry: <user entry>
Unknown command <command> for <protocol name> protocol received.
Device is configured to ring <off | ARD | HSR client | MRP client | HSR manager | MRP manager>.
Standby function <master or slave>.
Observer started.
Observer stopped.
Observer contacted Redundancy Manager <MAC address>.
Standby is waiting for <partner / observer>.
Standby <partner / observer> connected to <master / slave> <MAC address> <port number>.
Standby <partner / observer> lost connection to <master / slave> <MAC address> <port number>.
Port <port number> is isolated ring port.
Port <port number> is static ring port.
No SMTP connection to mail server. Server IP address <IP address> TCP port <TCP port number>.
No SMTP application found. Server IP address <IP address> TCP port <TCP port number>.
SMTP (E-Mail) connection aborted. Server IP address <IP address>.
Unable to send message to syslog server. Please check syslog socket configuration.
Connected to syslog server.
SNMP: Authentification failure.
R)STP: new root bridge detected.
(R)STP: topology change detected.
Unable to send E-Mail(s). Please check IP configuration.
Unable to send trap(s). Please check IP configuration.
Failure reply code <error code> from SMTP server.
Restart requested.
No C-PLUG found. Internal flash memory used.
An empty C-PLUG was found.
C-PLUG format request.
A filled C-PLUG was found.
A corrupted C-PLUG was found.
C-PLUG removed at runtime.
C-PLUG plugged in at runtime.
RMON rising alarm occurred.
RMON falling alarm occurred.
Ring redundancy enabled.
Ring redundancy disabled.
(R)STP protocol enabled.

Messages for information
(R)STP protocol disabled.
Disabled (R)STP because ring redundancy is enabled.
DIP settings taken from C-PLUG. RM=<ON|OFF>, STBY=<ON|OFF>, R1=<ON|OFF>, R2=<ON|OFF>
(R)STP topology change detected while (R)STP is off. Aging time will be reduced to <time in s> sec for at least <time in s> sec.
Set aging time back to original value <time in s> sec.
No connection to SNTP server. Server IP address <IP address>.
Connected to SNTP server. Server IP address <IP address>.
Enabled link status monitoring on ring ports.
Changed port VLAN ID of the ring ports to 1.
Disabled GVRP because ring redundancy is enabled.
Disabled GMRP because ring redundancy is enabled.
Disabled mirroring because monitor port is ring port.
(Re)enabled ring ports (because disabled by user).
Disabled port lock on ring ports.
Warning: ring ports have different static VLAN configuration.
Warning: ring ports have different VLAN port configuration.
Warning: ring ports have different static multicast configuration.
Warning: ring ports have different load limits configuration.
Enter fault state: port <port number> enabled for link status monitoring and link down.
Leave fault state: port <port number> disabled for link status monitoring.
Enter fault state: power line <ID of power supply> enabled for power monitoring and power down.
Leave fault state: power line <ID of power supply> disabled for power monitoring.
<CLI | WBM | SSH>: Authentication failure.
Warning: OSPF consumed too much memory and is shut down.
Duplicate IP address <IP address> sent from <MAC address>
IN <number of the digital input> (<name of the input>) <high or low>
VRRP: Virtual Router <number of the routers> on VLAN <VLAN-ID> transitioned to <Master | Backup | Disabled | Initialize | Invalid> state.
PNIO configuration invalid, conflict with standby.
PNIO configuration invalid, conflict with HSR.
PNIO configuration invalid, conflict in MRP ring ports: <cause of conflict>
PNIO configuration invalid, conflict in alternative redundancy configuration.
PNIO configuration invalid, conflict detected: <description of configuration conflict>

Index

J

L

M

N

O

P

R

S

T

U

V

W