

SIMATIC NET

Industrial Ethernet switches SCALANCE X-200

Configuration Manual




Preface

Recommendations on Network Security	1
IRT communication with X-200	2
Network topologies and media redundancy	3
Assignment of an IP address	4
Configuration using WBM and CLI	5
Menus in the WBM	6
Configuration via SNMP	7
Connection to PROFINET IO	8
Downloading firmware	9
MIBs for X-200	A
Default ring ports	B
Encryption methods used (ciphers)	C

Legal information

Warning notice system

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

 DANGER
indicates that death or severe personal injury will result if proper precautions are not taken.
 WARNING
indicates that death or severe personal injury may result if proper precautions are not taken.
 CAUTION
indicates that minor personal injury can result if proper precautions are not taken.
NOTICE
indicates that property damage can result if proper precautions are not taken.


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

Qualified Personnel

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

Proper use of Siemens products

Note the following:

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

Trademarks

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

Disclaimer of Liability

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

Preface

Purpose of the Configuration Manual

This manual supports you when configuring the SCALANCE X-200 Industrial Ethernet switches. It outlines the technical options provided by a SCALANCE X-200 and describes how to configure with Web Based Management (WBM) and the Command Line Interface (CLI).

Overview of the technical documentation of the IE Switches X-200

The technical documentation of the X-200 product line is divided into hardware and software and can be found in the following documents:

- **PH SCALANCE X-200 configuration manual**
Software description of the X-200 product line
- **SCALANCE X-200 BA Operating Instructions**
Hardware description for all product groups and general information.

You will find the documents here:

- On the data medium that ships with some products:
 - Product CD / product DVD
 - SIMATIC NET Manual Collection
- On the Internet pages of Siemens Industry Online Support (<http://support.automation.siemens.com/WW/view/en/33118791/133300>).

Validity of this configuration manual

This manual is valid for the following firmware versions:

- SCALANCE X-200/XF-200 as of firmware version 5.2.5
- SCALANCE X-200IRT/XF-200IRT as of firmware version 5.5
- SINEC PNI as of version 1.0
- SNMP/OPC server as of version 6.2.1

According to the operating instructions SCALANCE X-200, this manual is valid for the following product lines:

- SCALANCE X-200 and SCALANCE XF-200
- SCALANCE X-200IRT and SCALANCE XF-200IRT

Names of the devices in these operating instructions

Unless mentioned otherwise, the descriptions in these operating instructions refer to all devices of the SCALANCE X-200 product line named above in the section on Validity.

In the remainder of the instructions, these will also be referred to as **IE switches** or also simply as **X-200**.

Further documentation

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

You will find the system manuals on the Internet pages of Siemens Industry Online Support under the following entry IDs:

- 27069465 (<http://support.automation.siemens.com/WW/view/en/27069465>)
Industrial Ethernet / PROFINET Industrial Ethernet System Manual
- 84922825 (<http://support.automation.siemens.com/WW/view/en/84922825>)
Industrial Ethernet / PROFINET - Passive network components System Manual

Finding information

To help orientation, there is not only a table of contents but also an Index in the Appendix.

The SIMATIC NET Glossary also provides additional help, see below.

Audience

These operating instructions are intended for persons involved in commissioning networks in which IE switches are used.

SIMATIC NET Selection Tool

The SIMATIC NET selection tool supports you when selecting Industrial Ethernet switches and components for Industrial Wireless Communication. You will find current information on the Product Support pages under the following entry ID:

39134641 (<http://www.siemens.de/snst>)

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, loop detection, ring redundancy 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 to know how an IP address is structured and which options you have for assigning an IP address to an IE switch.	Assignment of an IP address (Page 37)
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.	Configuration using WBM and CLI (Page 41)
You want to know how to manage an IE switch with SNMP.	Configuration via SNMP (Page 153)
You would like information about the IRT technology with SCALANCE X-200.	IRT communication with X-200 (Page 19)
You want to know how you can use the options of PROFINET IO for a connected IE switch.	Connection to PROFINET IO (Page 155)
You want to update the firmware.	Downloading firmware (Page 173)

Further documentation

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

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

You will find the system manuals here:

- On the data medium that ships with some products:
 - Product CD / product DVD
 - SIMATIC NET Manual Collection
- On the Internet pages of Siemens Industry Online Support:
 - Industrial Ethernet / PROFINET Industrial Ethernet System Manual (<https://support.industry.siemens.com/cs/ww/en/view/27069465>)
 - Industrial Ethernet / PROFINET Passive Network Components System Manual (<https://support.industry.siemens.com/cs/ww/en/view/84922825>)

SIMATIC NET manuals

You will find the SIMATIC NET manuals here:

- On the data medium that ships with some products:
 - Product CD / product DVD
 - SIMATIC NET Manual Collection
- On the Internet pages of Siemens Industry Online Support (<https://support.industry.siemens.com/cs/ww/en/ps/15247>).

SIMATIC NET glossary

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

You will find the SIMATIC NET glossary here:

- SIMATIC NET Manual Collection or product DVD
The DVD ships with certain SIMATIC NET products.
- On the Internet under the following address:
50305045 (<https://support.industry.siemens.com/cs/ww/en/view/50305045>)

Security information

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

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

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

For additional information on industrial security measures that may be implemented, please visit <https://www.siemens.com/industrialsecurity> (<https://www.siemens.com/industrialsecurity>)

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

To stay informed about product updates, subscribe to the Siemens Industrial Security RSS Feed under <https://www.siemens.com/industrialsecurity> (<https://www.siemens.com/industrialsecurity>)

License conditions

Note

Open source software

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

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

- DOC_OSS-SCALANCE-X_74.pdf
- DC_LicenseSummaryScalanceX200_76.pdf
- DC_LicenseSummaryScalanceX200IRT_76.pdf

You will find these documents on the product DVD in the following directory: /Open Source Information

Trademarks

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

SCALANCE, C-PLUG, OLM

Table of contents

	Preface	3
1	Recommendations on Network Security	13
2	IRT communication with X-200.....	19
3	Network topologies and media redundancy	23
3.1	Network topologies.....	23
3.2	Options of media redundancy	29
3.3	Media redundancy in ring topologies.....	29
3.4	MRP	30
3.5	MRPD	32
3.6	HRP	33
3.7	Redundant coupling of network segments.....	34
3.8	Spanning tree, media redundancy and passive listening.....	35
4	Assignment of an IP address.....	37
4.1	Introduction.....	37
4.2	Initial assignment of an IP address	38
5	Configuration using WBM and CLI	41
5.1	Web Based Management.....	42
5.1.1	Principle and requirements.....	42
5.1.2	Starting the WBM and logging in	42
5.1.3	Simulation of the LEDs	44
5.1.4	Operator activities	45
5.2	Command Line Interface	45
6	Menus in the WBM.....	49
6.1	The System menu	49
6.1.1	System	49
6.1.2	I&M	51
6.1.3	Restart & Defaults	52
6.1.4	Save & Load HTTP	53
6.1.5	Save & Load TFTP.....	56
6.1.6	Version Numbers	59
6.1.7	Passwords.....	60
6.1.8	Select/Set Button	62
6.1.9	Event log	63
6.1.10	C-PLUG	64
6.2	The X-200 menu	67
6.2.1	X-200	67

6.2.2	Fault Mask	68
6.2.3	Ring.....	71
6.2.4	Standby	80
6.2.5	Procedure for redundant linking of rings.....	83
6.3	The Agent menu	84
6.3.1	Agent	84
6.3.2	Ping.....	87
6.3.3	SNMP Config	87
6.3.4	SNMP Trap Config	89
6.3.5	SNMP Groups.....	90
6.3.6	SNMP Groups New Entry	92
6.3.7	SNMP Config Users.....	93
6.3.8	SNMP Users New Entry.....	95
6.3.9	Agent Timeout Configuration	96
6.3.10	Event Config	97
6.3.11	E-Mail Config	101
6.3.12	Time Config	102
6.3.13	Daylight Saving Time	107
6.3.14	PNIO Config	112
6.3.15	Management ACL	113
6.4	The Switch menu	116
6.4.1	Switch	116
6.4.2	Ports.....	119
6.4.3	FMP.....	121
6.4.4	Cable tester	128
6.4.5	POF	130
6.4.6	FDB	133
6.4.7	ARP table	135
6.4.8	LLDP	136
6.4.9	DCP	138
6.4.10	Loop Detection Config.....	140
6.5	the Statistics menu	144
6.5.1	Statistics	144
6.5.2	Packet size	145
6.5.3	Packet type	147
6.5.4	Packet Error	149
7	Configuration via SNMP.....	153
8	Connection to PROFINET IO	155
8.1	Configuration of the bus adapters for XF-200IRT	155
8.2	Configuring the interrupts in STEP 7	156
8.3	MRP configuration in STEP 7	157
8.4	Configuring the topology in STEP 7.....	164
8.5	Configuring HRP.....	165
8.6	Structure of the data records	166
8.6.1	Data record 4.....	166
8.6.2	Data record 5.....	167
8.6.3	Data record 0x802A	168

9	Downloading firmware	173
9.1	Regular firmware download	173
9.2	Loading firmware using the boot loader	173
A	MIBs for X-200.....	175
A.1	Important MIB variables	175
A.2	Important private MIB variables.....	176
B	Default ring ports	179
C	Encryption methods used (ciphers).....	181
	Index	183

Recommendations on Network Security

NOTICE

Information security

Connect to the device and change the standard passwords for the users "admin" and "user" before you operate the device. To be able to change passwords you need to be logged in with write access to the configuration data.

To prevent unauthorized access to the device and/or network, observe the following security recommendations.

General

- Check the device regularly to ensure that these recommendations and/or other internal security policies are complied with.
- Evaluate your plant as a whole in terms of security. Use a cell protection concept with suitable products.
- When the internal and external network are disconnected, an attacker cannot access internal data from the outside. Therefore operate the device only within a protected network area.
- No product liability will be accepted for operation in a non-secure infrastructure.
- Use VPN to encrypt and authenticate communication from and to the devices.
- For data transmission via a non-secure network, use an encrypted VPN tunnel (IPsec, OpenVPN).
- Separate connections correctly (WBM, Telnet, SSH etc.).
- Check the user documentation of other Siemens products that are used together with the device for additional security recommendations.
- Using remote logging, ensure that the system protocols are forwarded to a central logging server. Make sure that the server is within the protected network and check the protocols regularly for potential security violations or vulnerabilities.

Physical access

- Restrict physical access to the device to qualified personnel because the plug-in data medium can contain sensitive data.
- Lock unused physical interfaces on the device. Unused interfaces can be used to gain access to the plant without permission.

Software (security functions)

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

Authentication

Note

Accessibility risk - Risk of data loss

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

- Replace the default passwords for all user accounts, access modes and applications (if applicable) before you use the device.
- Define rules for the assignment of passwords.
- Use passwords with a high password strength. Avoid weak passwords, (e.g. password1, 123456789, abcdefgh) or recurring characters (e.g. abcabc). This recommendation also applies to symmetrical passwords/keys configured on the device.
- Make sure that passwords are protected and only disclosed to authorized personnel.
- Do not use the same passwords for multiple user names and systems.
- Store the passwords in a safe location (not online) to have them available if they are lost.
- Regularly change your passwords to increase security.
- A password must be changed if it is known or suspected to be known by unauthorized persons.
- When user authentication is performed via RADIUS, make sure that all communication takes place within the security environment or is protected by a secure channel.
- Watch out for link layer protocols that do not offer their own authentication between endpoints, such as ARP or IPv4. An attacker could use vulnerabilities in these protocols to attack hosts, switches and routers connected to your layer 2 network, for example, through manipulation (poisoning) of the ARP caches of systems in the subnet and subsequent interception of the data traffic. Appropriate security measures must be taken for non-secure layer 2 protocols to prevent unauthorized access to the network. Physical access to the local network can be secured or secure, higher layer protocols can be used, among other things.

Certificates and keys

- As of firmware version V5.2.5, we converted from RSA certificates to certificates for elliptic curves cryptography ("ECDSA certificates"). Only use ECDSA certificates in PEM format that were generated with the following curves:

- secp256r1 (NIST P-256)
- secp384r1 (NIST P-384)
- secp521r1 (NIST P-521)

RSA certificates are no longer supported as of this firmware version. The existing RSA certificates on the device are automatically replaced with self-signed ECDSA certificates.

- On the device there is a preset SSL certificate with the key length 256 bits for the elliptic-curves cryptography. Replace this certificate with a self-made certificate with key. We recommend that you use a certificate signed either by a reliable external or by an internal certification authority.
- Use a certification authority including key revocation and management to sign certificates.
- Make sure that user-defined private keys are protected and inaccessible to unauthorized persons.
- Verify certificates and fingerprints on the server and client to prevent "man in the middle" attacks.
- Change certificates and keys immediately if there is a suspicion of compromise.

Secure/non-secure protocols

- Avoid or disable non-secure protocols, for example Telnet and TFTP. For historical reasons, these protocols are available, however not intended for secure applications. Use non-secure protocols on the device with caution.
- Check whether use of the following protocols and services is necessary:
 - Non authenticated and unencrypted ports
 - MRP, HRP
 - LLDP
 - DHCP Options 66/67

The following protocols provide secure alternatives:

- HTTP → HTTPS
- TFTP → FTPS
- Telnet → SSH
- SNMP → NTP
Check whether use the use of NTP is necessary. NTP is classified as non-secure. Activate Secure NTP when the NTP server supports this protocol and use the authentication and encryption mechanisms of Secure NTP.
- SNMPv1/v2c → SNMPv3
Check whether use of SNMPv1/v2c. is necessary. SNMPv1/v2c are classified as non-secure. Use the option of preventing write access. The device provides you with suitable setting options.
If SNMP is enabled, change the community names. If no unrestricted access is necessary, restrict access with SNMP.
Use the authentication and encryption mechanisms of SNMPv3.
- Use secure protocols when access to the device is not prevented by physical protection measures.
- If you require non-secure protocols and services, operate the device only within a protected network area.
- Restrict the services and protocols available to the outside to a minimum.
- For the DCP function, enable the "DCP read-only" mode after commissioning.

Available protocols

The following list provides you with an overview of the open protocol ports.

The table includes the following columns:

- **Protocol**
- **Port number**
- **Port status**
 - Open
 - Closed

- **Factory setting**
Indicates the state of the port on delivery or after reset to factory settings.
- **Authentication**
Specifies whether the communication partner is authenticated.
- **Encryption**
Specifies whether or not the transfer is encrypted.

Protocol	Port number	Port status	Factory setting	Authentication	Encryption
SSH	TCP/22	Open	Open	Yes	Yes
TELNET	TCP/23	Open (when configured)	Open	Yes	No
HTTP	TCP/80	Open (when configured)	Open	Yes	No
PROFINET IO Service	TCP/84	Open	Open	No	No
HTTPS	TCP/443	Open	Open	Yes	Yes
DHCP	UDP/68	Open (when configured)	Closed	No	No
SNTP	UDP/123	Open (when configured)	Closed	No	No
NTP (secure)					Yes
SNMP	UDP/161	Open (when configured)	Open	Yes	Yes (SNMPv3)
PROFINET IO	UDP/34964 UDP/49152, 49153 *)	Open	Open	No	No

*) These ports are assigned dynamically and can differ from the values specified here.

Decommissioning

Shut down the device properly to prevent unauthorized persons from accessing confidential data in the device memory.

To do this, restore the factory settings on the device.

Also restore the factory settings on the storage medium.

IRT communication with X-200

IRT - Isochronous Real Time

With STEP 7 as of V5.4, you can configure PROFINET devices that support data exchange using IRT. To achieve the best possible synchronization and performance, IRT frames are transferred deterministically via planned communication paths in a specified order.

Note

No port mirroring in IRT mode

Disable the function "Port Mirroring" in SCALANCE X-200IRT devices if you want to operate the device in IRT mode. IRT mode is not possible when the mirroring function is enabled.

Supported devices and firmware versions

Topology-based IRT requires special network components that support planned data transmission. The following devices of the SCALANCE X-200 product line support topology-based IRT:

- X200-4P IRT
- X201-3P IRT
- X201-3P IRT PRO
- X202-2IRT
- X202-2P IRT
- X202-2P IRT PRO
- X204IRT
- X204IRT PRO
- XF204IRT
- XF204-2BA IRT

Note

Firmware versions

In IRT mode, all X-200 IE switches in a plant must either have **firmware version V3.1 or older, or** they must have **firmware version V4.0 or newer**. Operating an IRT plant containing both devices with firmware V3.1 and older and devices with V4.0 and newer is not possible.

Where necessary, install firmware V3.1 on the devices. You will find the firmware on the accompanying CD in the following directory:

\\FW\\SCALANCE X-200IRT Isochronous Real-Time\\

You should remember the following restrictions: The **XF204IRT**, the **XF204-2BA IRT** and the **X201-3P IRT PRO** are **not compatible with firmware V3.1**. This firmware version must therefore not be used for these two modules.

Note

The use of the SCALANCE X-200IRT as a redundant sync master is only permitted for IRT with the "High Performance" option.

Constant bus cycle and isochronous real time also available with PROFINET

The possibilities available for constant bus cycles and isochronous real time with PROFIBUS DP are now available for PROFINET IO.

When using the constant bus cycle functionality in PROFIBUS DP, all nodes are synchronized by a global control signal generated by the DP master. In PROFINET IO with IRT, a sync master generates a signal with which the sync slaves synchronize themselves. The sync master and sync slaves belong to a sync domain that is assigned a name during project engineering. In principle, both an IO controller and an IO device can adopt the role of sync master. A sync domain has exactly one sync master.

Relationship: Sync domain and IO systems

The important point is that sync domains do not need to be restricted to a PROFINET IO system: The devices of several IO systems can be synchronized by a single sync master as long as they are connected to the same Ethernet subnet.

On the other hand: A IO system may only belong to one sync domain.

Signal delays must be taken into account

If you use extremely precise synchronization intervals, the cable lengths and the associated delay times must be taken into account. With the aid of a Topology Editor, you can enter the properties of the cables between the ports of the switches. Based on this information and the other configuration data, STEP 7 calculates the optimized sequence of the IRT communication and the resulting update time.

Keeping network load within limits

To allow you to limit the network load resulting from extremely short update times, update groups are configured for the IRT data. If only a few devices require the shortest update times, these are assigned to the first update group. Each further update group has n times the update time of the previous group, where n can be configured. This means that the data is updated less frequently and the network load is reduced.

In STEP 7 V5.4, only one update group is planned.

IRT runs alongside real-time and TCP/IP communication

Apart from IRT communication for which a fixed bandwidth is reserved within the update time, RT communication and TCP/IP communication are also permitted within the update time.

In RT communication (real-time communication), the cyclic data is transferred between the IO controller and IO device, however, without the best possible synchronicity.

Unsynchronized IO device automatically exchange data using RT communication.

Since TCP/IP communication is also possible, other non real-time data or configuration/ diagnostic data can be transported.

Network topologies and media redundancy

3.1 Network topologies

Switching technology allows extensive networks to be set up with numerous nodes and simplifies network expansion.

Which topologies can be implemented?

Bus, ring, or star topologies can be implemented with the X-200 IE switches.

Note

Make sure that the maximum permitted cable lengths for the relevant devices are not exceeded. You will find information about the permitted cable lengths in the Technical specifications section in the operating instructions.

Bus topology

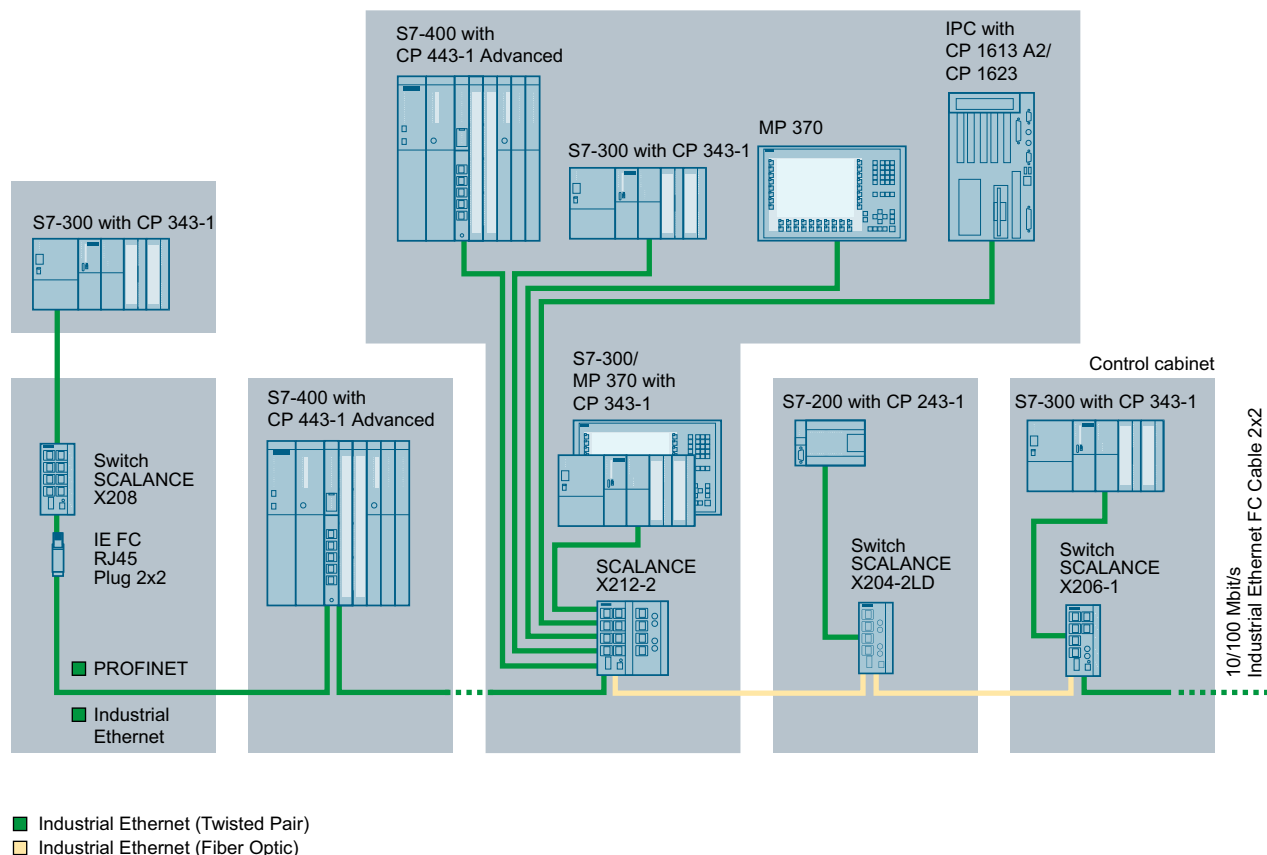
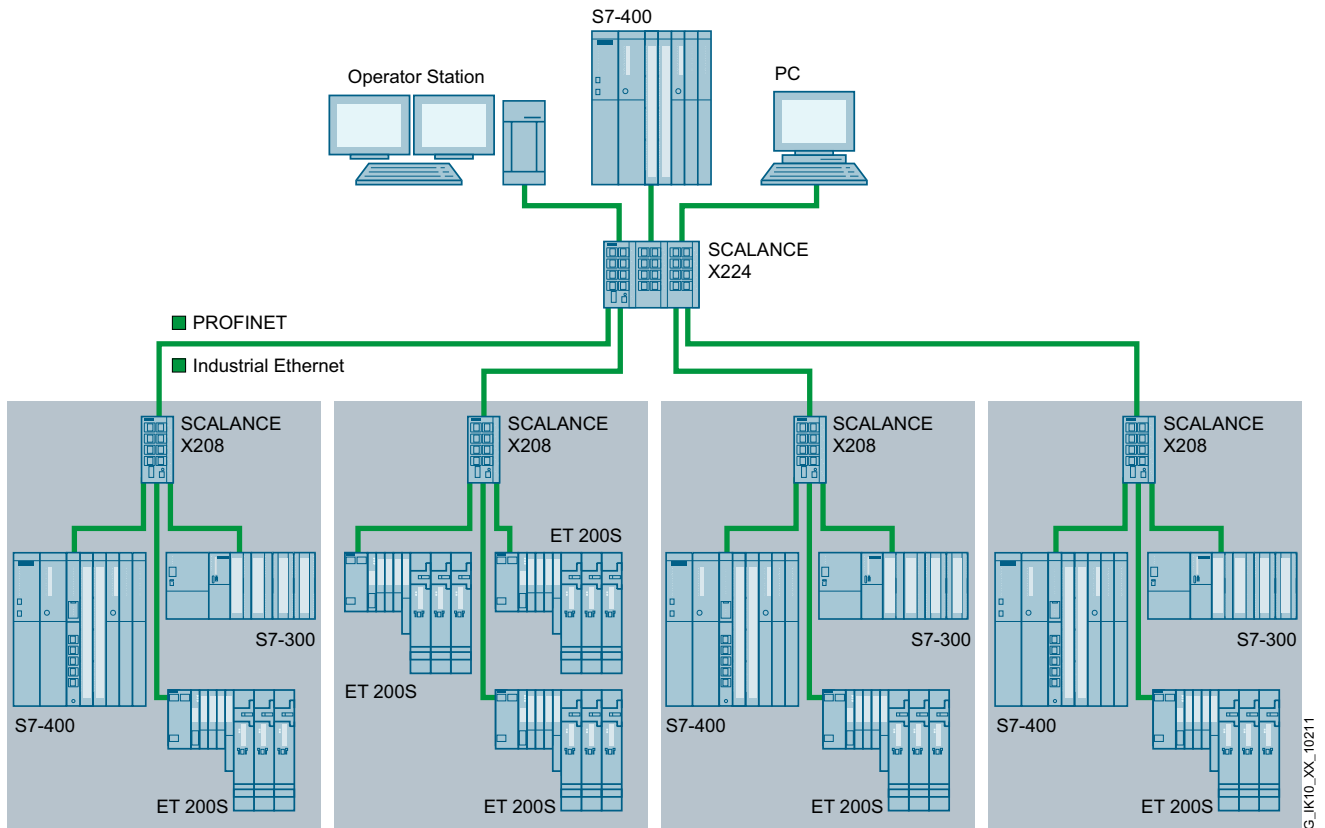


Figure 3-1 Electrical / optical linear topology with X-200

Star topology



G_IK10_XX_10211

Figure 3-2 Star topology with X-200

3.1 Network topologies

Ring topology

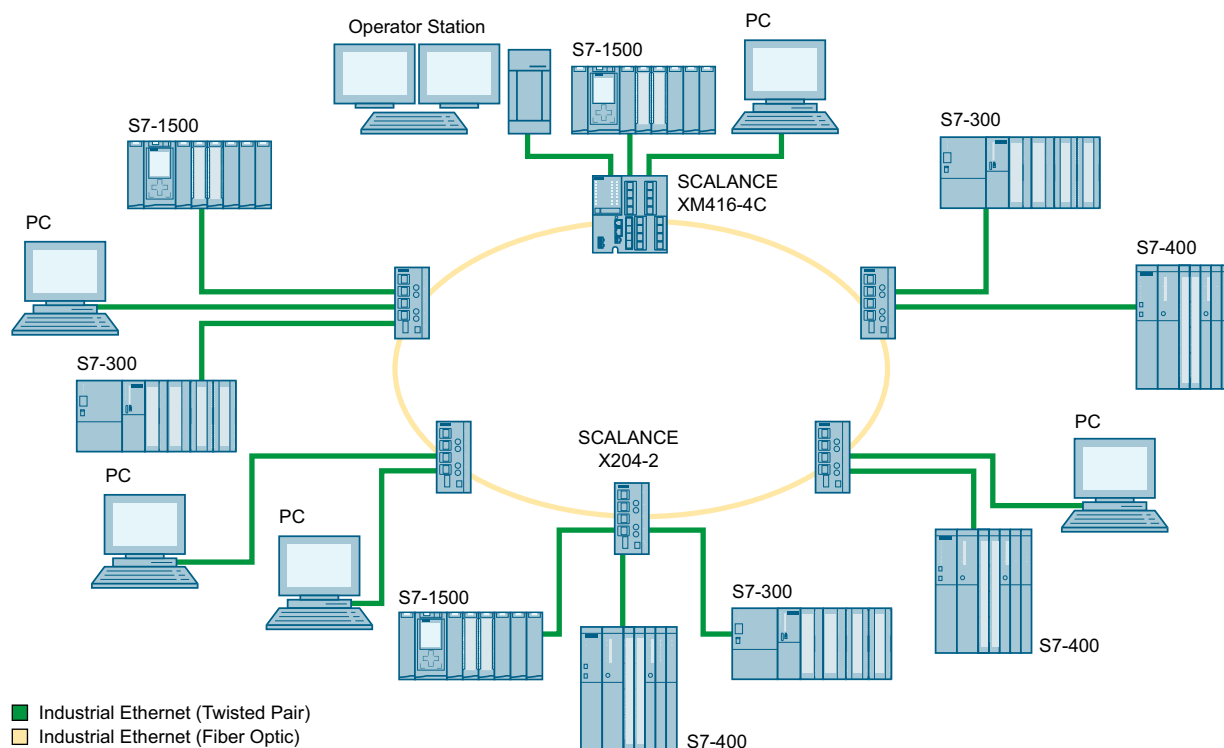


Figure 3-3 Optical ring, example with X-200 or X-400 as redundancy manager

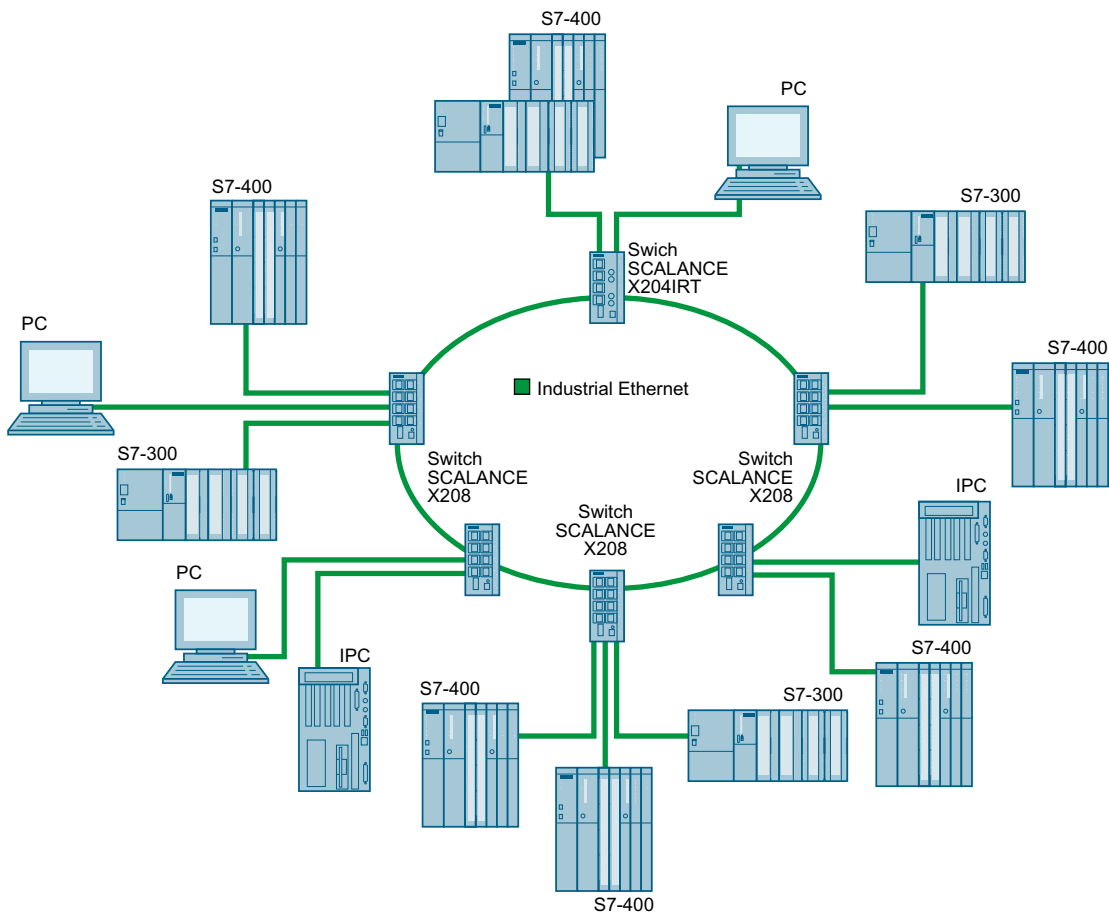


Figure 3-4 Electrical ring, example with X200

3.1 Network topologies

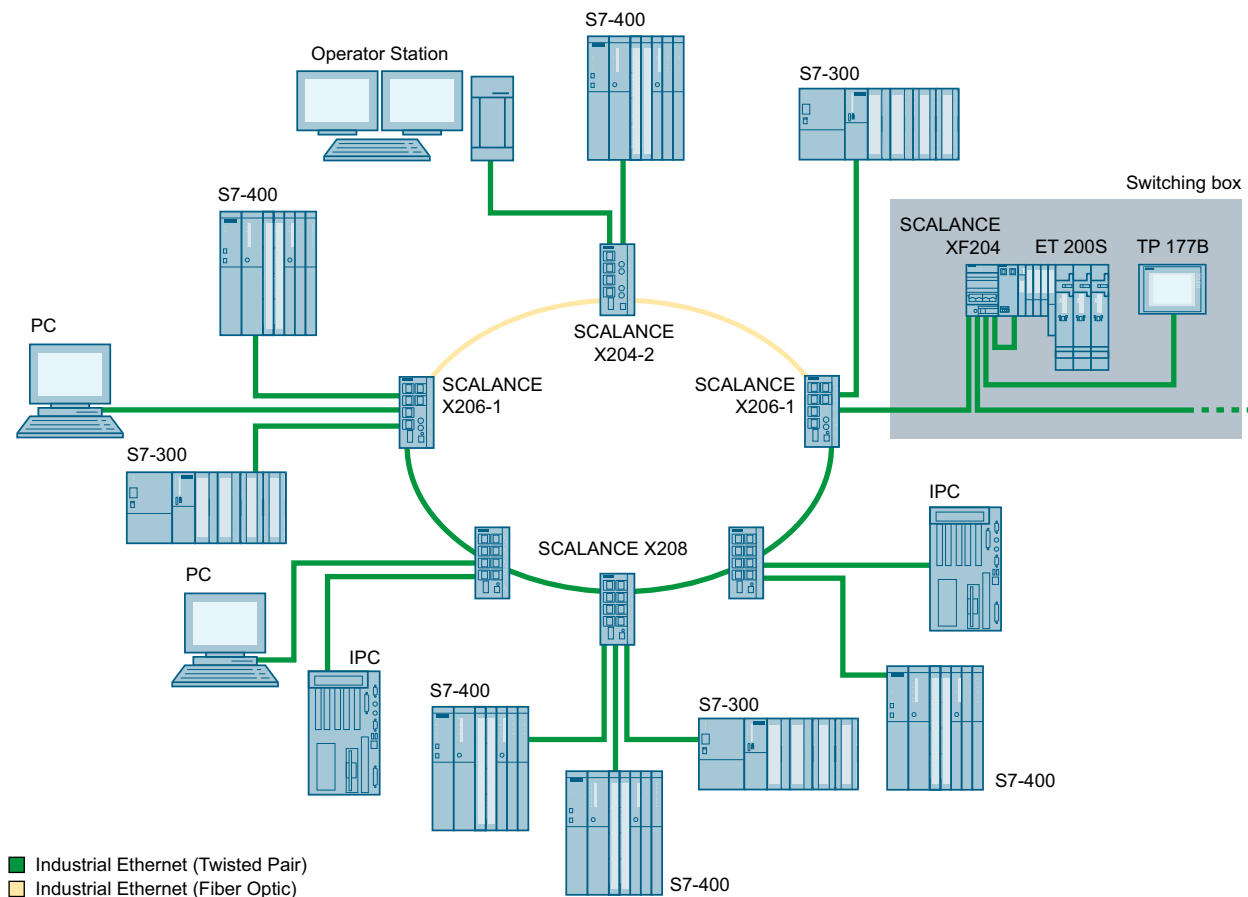


Figure 3-5 Electrical and optical ring sections, example with X206-1, X208 or X204-2 as redundancy manager

To increase availability, optical or electrical bus topologies made up of X-200 IE switches with a redundancy manager can be closed to form a ring. The following IE switches can be configured as the redundancy manager:

- SCALANCE X-200
- SCALANCE X-300
- SCALANCE X-400
- OSM / ESM version 2

The X-200 IE switches are first connected over their ring ports to form a bus. The two ends of the line are closed to form a ring by the switch operating as redundancy manager.

When a switch is used as the redundancy manager, the ring ports are isolated from each other if the network is operating problem-free.

The IE switch operating as redundancy manager monitors the connected bus via its ring ports. If the connected bus is interrupted, it switches the ring ports through; in other words, it re-establishes a functioning bus via this alternative path. Reconfiguration takes place within 0.3 seconds.

As soon as the problem has been eliminated, the original topology is restored; in other words, the ring ports in the redundancy manager are once again disconnected from each other.

3.2 Options of media redundancy

There are various options available to increase the network availability of an Industrial Ethernet network with optical or electrical linear bus topologies:

- Mesh networks
- Parallel connection of transmission paths
- Closing a linear bus topology to form a ring topology

3.3 Media redundancy in ring topologies

Structure of a ring topology

Nodes in a ring topology can be external switches and/or the integrated switches of communications modules.

To set up a ring topology with media redundancy, you bring together the two free ends of a linear bus topology in one device. Closing the linear bus topology to form a ring is achieved with two ports (ring ports) of a device in the ring. This device is the redundancy manager. All other devices in the ring are redundancy clients.

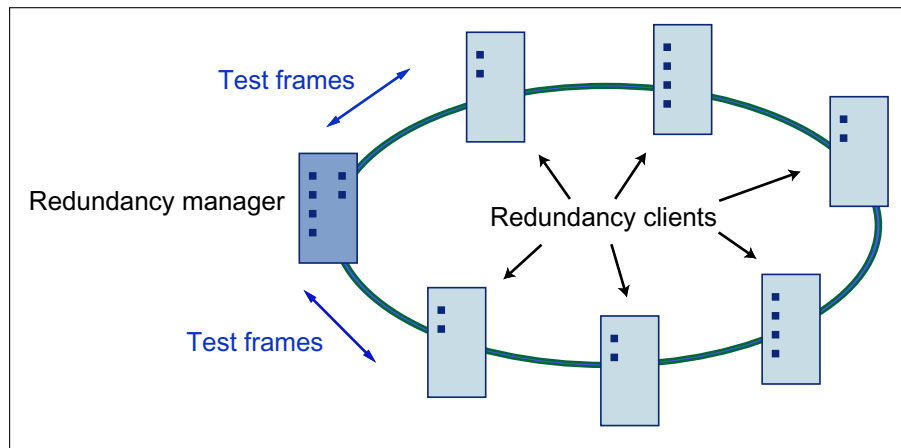


Figure 3-6 Devices in a ring topology with media redundancy

The two ring ports of a device are the ports that establish the connection to the two neighboring devices in the ring topology. The ring ports are selected and set in the configuration of the relevant device. In STEP 7 and on the S7 Ethernet CP modules themselves, the ring ports are indicated by an "R" after the port number.

Note

Before physically closing the ring, download the configuration of your STEP 7 project to the individual devices.

How media redundancy works in a ring topology

When using media redundancy, the data paths between the individual devices are reconfigured if the ring is interrupted at one point. Following reconfiguration of the topology, the devices can once again be reached in the resulting new topology.

In the redundancy manager, the 2 ring ports are disconnected from each other if the network is uninterrupted. This prevents circulating data frames. In terms of data transmission, the ring topology is a linear bus topology. The redundancy manager monitors the ring topology. It does this by sending test frames both from ring port 1 and ring port 2. The test frames run round the ring in both directions until they arrive at the other ring port of the redundancy manager.

An interruption of the ring can be caused by loss of the connection between two devices or by failure of a device in the ring.

If the test frames of the redundancy manager no longer arrive at the other ring port because of an interruption in the ring, the redundancy manager connects its two ring ports. This substitute path once again restores a functioning connection between all remaining devices in the form of a linear bus topology.

As soon as the interruption is eliminated, the original transmission paths are established again, the two ring ports of the redundancy manager are disconnected and the redundancy clients informed of the change. The redundancy clients then use the new paths to the other devices.

The time between the ring interruption and restoration of a functional linear topology is known as the reconfiguration time.

If the redundancy manager fails, the ring becomes a functional linear bus.

Media redundancy methods

The following media redundancy methods are supported by SIMATIC NET products:

- HRP (High Speed Redundancy Protocol)
Reconfiguration time: 0.3 seconds
- MRP (Media Redundancy Protocol)
Reconfiguration time: 0.2 seconds

The mechanisms of these methods are similar. HRP and MRP cannot be used in the ring at the same time.

3.4 MRP

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

IEC 62439-2:2016 Industrial communication networks - High availability automation networks
Part 2: Media Redundancy Protocol (MRP)

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

Topology

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

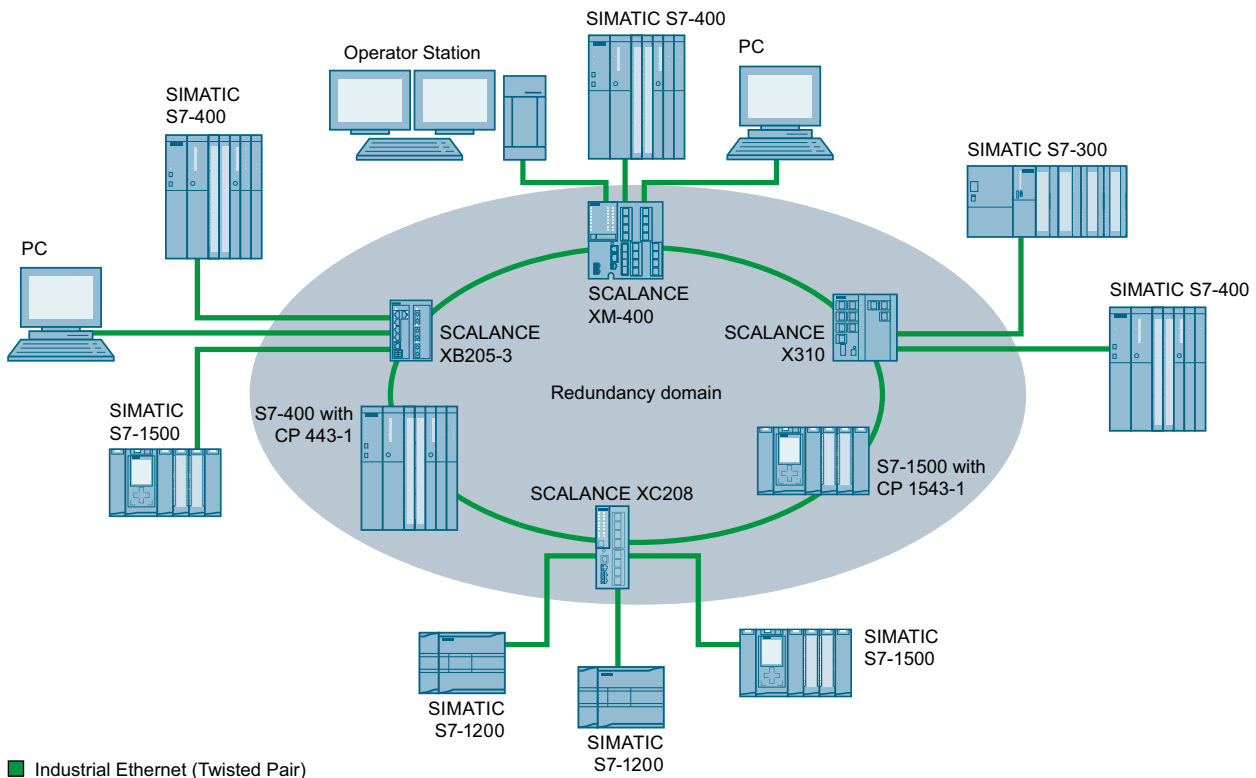


Figure 3-7 Example of a ring topology with the MRP media redundancy protocol

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

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

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

Requirements

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

- MRP is supported in ring topologies with up to 50 devices. Exceeding this number of devices can lead to a loss of data traffic.
- The ring in which you want to use MRP may only consist of devices that support this function. These include, for example, some of the Industrial Ethernet SCALANCE X switches, some of the communications processors (CPs) for SIMATIC S7 and PG/PC or non-Siemens devices that support this function.

3.5 MRPD

- All devices must be interconnected via their ring ports.
Multimode connections up to 3 km and single mode connections up to 26 km between two SCALANCE X IE switches are possible. At greater distances, the specified reconfiguration time may be longer.
- "MRP" must be enabled for all devices in the ring.
- The connection settings (transmission medium / duplex) must be set to full duplex and at least 100 Mbps for all ring ports. Otherwise there may be a loss of data traffic.
 - STEP 7: Set all the ports involved in the ring to "Automatic settings" in the "Options" tab of the properties dialog.
 - WBM: If you configure with Web Based Management, the ring ports are set automatically to autonegotiation.

See also

Ring (Page 71)

Note

Number of devices

Except in PROFINET IO systems, topologies with up to 100 SCALANCE X-200 and SCALANCE X-300 IE switches were tested successfully.

3.5 MRPD

The redundancy method MRPD (Media Redundancy with Path Duplication)

The MRPD procedure is specified in IEC 61158 Parts 5 and 6 type 10 "PROFINET". It allows redundancy for PROFINET IRT.

In MRPD, the cyclic IRT frames are duplicated and sent to the recipient via different paths. The two redundant paths are planned in STEP 7. Two different paths are then available if the entire network or part of it has a ring topology.

Requirements

- All devices involved must support IRT.
- All devices involved must support MRPD.
Among the Industrial Ethernet switches, this means the following devices:
 - SCALANCE X-200IRT as of firmware version 5.0
- STEP 7 as of version V5.5 SP1

Project engineering

MRPD can only be configured in STEP 7 and there are no alternative configuration options.

To prevent loops forming and to ensure redundancy for other types of communication, MRP is always required for MRPD. If you activate MRP in STEP 7, products capable of IRT and MRPD use MRPD automatically.

The "High Performance" version of IRT must be used and the topology of the network must be configured.

3.6 HRP

Note

Name change

The acronym for the media redundancy protocol "High Speed Redundancy Protocol" has been changed from HSR to HRP.

This is only a change of name; the functionality has not been modified. HSR and HRP nodes can be operated together in a ring.

The "HRP" media redundancy method allows a reconfiguration time of 0.3 seconds following an interruption in the ring.

Requirements

The following conditions must be met for problem-free operation with HRP:

- HRP is supported in ring topologies with up to 50 devices.
In topologies with SCALANCE X-200 and SCALANCE X-300 IE switches, up to 100 nodes are supported.
Exceeding this number of devices can lead to a loss of data traffic.
- The ring in which you want to use HRP may only consist of devices that support this function.
This applies, for example, to the following devices: X-400 IE switches, X-300 IE switches, X-200 IE switches and OSM/ESM.
- All devices must be interconnected via their ring ports.
Multimode connections up to 3 km and single mode connections up to 26 km between two IE switches are possible. At greater distances, the specified reconfiguration time may be longer.
- A device in the ring must be configured as redundancy manager by selecting the "HRP Manager" setting. You can do this with the button on the front of the device, Web Based Management, CLI or SNMP.
- On all other devices in the ring, either the "HRP Client" or "Automatic Redundancy Detection" mode must be activated.
You can do this with Web Based Management, CLI or SNMP.
- In the basic status, the "HRP Client" or "Automatic Redundancy Detection" mode is set as default.

3.7 Redundant coupling of network segments

Coupling option

The coupling of two network segments shown here as an example is possible with X-200IRT, X-300 and X-400 IE switches. This requires the standby function of these devices that can be set via Web Based Management or CLI.

If the standby function is enabled, this is signaled on X-200IRT IE switches by the RM LED.

A SCALANCE X-200IRT can be operated either as redundancy manager or in standby mode.

The following figure shows the redundant link of SCALANCE X-200 rings with two SCALANCE X-200IRT devices:

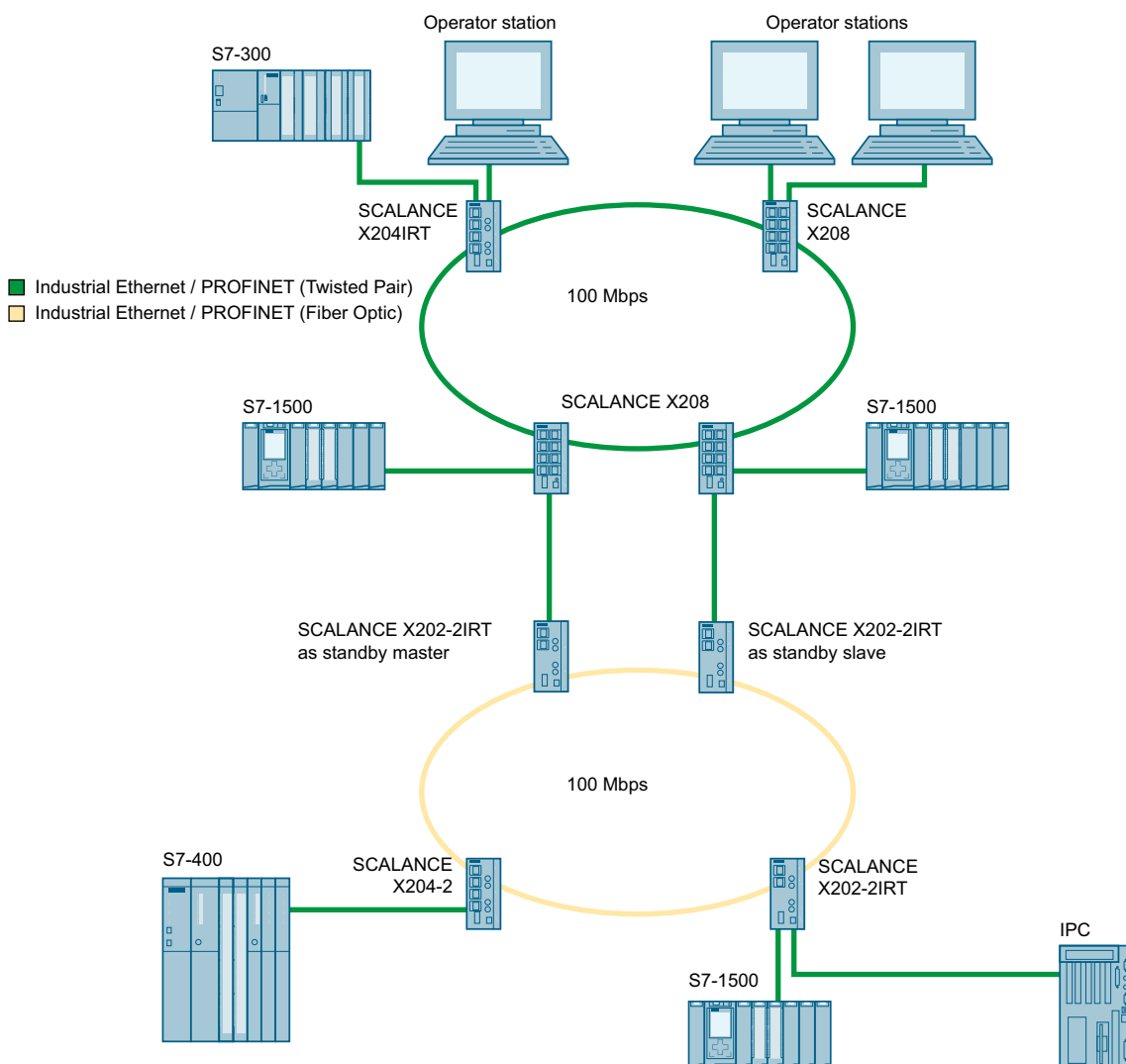


Figure 3-8 Redundant link (X202-2IRT: With activated standby function, left-hand device as master, right-hand device as slave.)

For a redundant link as shown in the figure, two X-200IRT IE switches must be configured within a network segment. This configuration is set in Web Based Management, Command Line

Interface or using SNMP access. For more detailed information, refer to the "Configuration manual "SCALANCE X-200 Industrial Ethernet Switches".

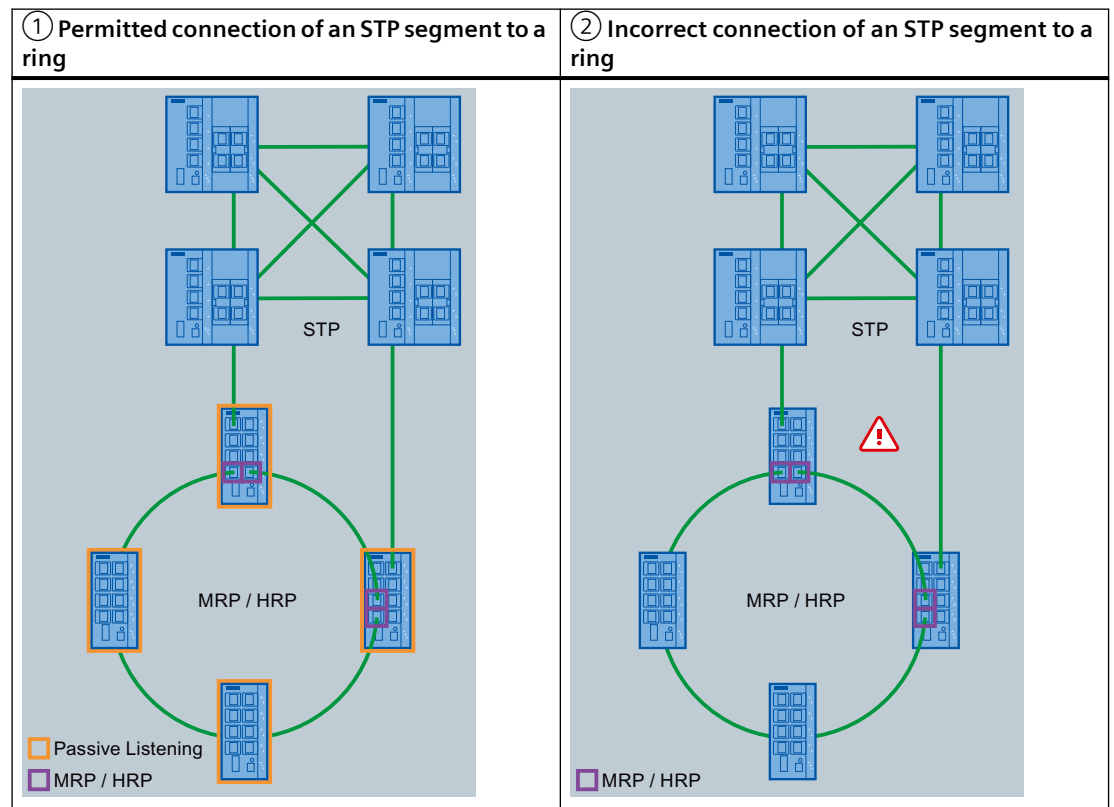
The two X-200IRT IE switches connected in the configuration exchange data frames with each other and in doing so synchronize their operational status. Here, one device adopts the role of standby master, the other the role of standby slave. If there are no problems, only the link from the master to the other network segment is active. If this link fails (for example due to a link-down or a device failure), the slave activates its link as long as the problem persists. Reconfiguration takes place within 0.3 s.

See also

Standby (Page 80)

3.8 Spanning tree, media redundancy and passive listening

If you want to link an STP segment to various devices of an MRP or HRP ring, you will need to enable passive listening on all devices of the ring ①. Since passive listening supports the forwarding of STP BPDUs, there are no circulating frames.



Assignment of an IP address

4.1 Introduction

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.

Note

The initial assignment of an IP address for X-200 IE switches cannot be made with Web Based Management because this configuration tool can only be used if an IP address already exists.

Address classes to RFC 1518 and RFC 1519

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.

IP address range	Max. number of networks	Max. number of hosts/ network	Class	CIDR notation
1.x.x.x to 126.x.x.x	126	16777214	A	/8
128.0.x.x to 191.255.x.x	16383	65534	B	/16
192.0.0.x to 223.255.255.x	2097151	254	C	/24
Multicast groups			D	
Reserved for experiments			E	

Subnet mask

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

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

Example of a class B network:

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

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

Outside the local network, the described division of the end node address has no significance. For packet switching here, only the entire IP address is of interest.

Note

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

4.2 Initial assignment of an IP address

Configuration options

An initial IP address for an IE switch cannot be assigned using Web Based Management or the Command Line Interface 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:

- By DHCP (factory setting)
When the devices ship and after resetting to factory defaults, DHCP is active. 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.
- With the STEP 7 configuration tool

- With the NCM PC configuration tool
- With PNI (SINEC Primary Network Initialization)
This program for initial commissioning of network devices uses the DCP protocol to detect devices in a network and assign an IP address.
For more information, refer to PNI (<https://support.industry.siemens.com/cs/products?mfn=ps&pnid=26672&lc=en-US>)

For more detailed information on using the configuration tools, refer to the relevant manuals.

Configuration using WBM and CLI

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 (CLI), you can configure the IE switches via Telnet or SSH. An Ethernet connection is necessary. You can enable or disable Telnet or SSH using Web Based Management.
- Web Based Management (WBM) accesses the configuration of the IE switches using a Web browser. An Ethernet connection to the IE switch is necessary.

Note

Unauthorized access

Depending on the selected configuration method, the following mechanisms are integrated to prevent unauthorized access to an IE switch:

- CLI via TELNET or SSH
 - A CLI session is interrupted automatically if there is no input for certain length of time. In the factory settings, this is set to 300 seconds. You can increase this period to a maximum of 600 seconds.
- WBM
 - With the WBM, there is an automatic logout after a certain time. In the factory settings, this is set to 15 minutes. You can increase this period to a maximum of 60 minutes.
 - In the top menu bar of the WBM user interface, you will see the "Logout" menu command. To log out manually, click this command.
 - **Always exit a WBM sessions by clicking "Logout". Simply closing the browser you are using does not mean logging out and is therefore not secure.**

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. This ensures that all configuration changes are saved.

Note

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

5.1 Web Based Management

5.1.1 Principle and requirements

Principle

IE switches have an integrated HTTP server for Web Based Management. If an IE switch is addressed over 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

- An IE switch must have an IP address before you can use WBM.
- To use WBM, there must be an Ethernet connection between the IE switch and the client computer.
- We recommend the use of Microsoft Internet Explorer as of version 5.5.
- All the pages of the WBM require JavaScript. You should therefore make sure that Java Script is enabled in your browser settings.
- WBM is HTTP- or HTTPS-based, so you must also allow access to port 80 or 443 if you have a firewall installed.

5.1.2 Starting the WBM and logging in

Browser settings

Note

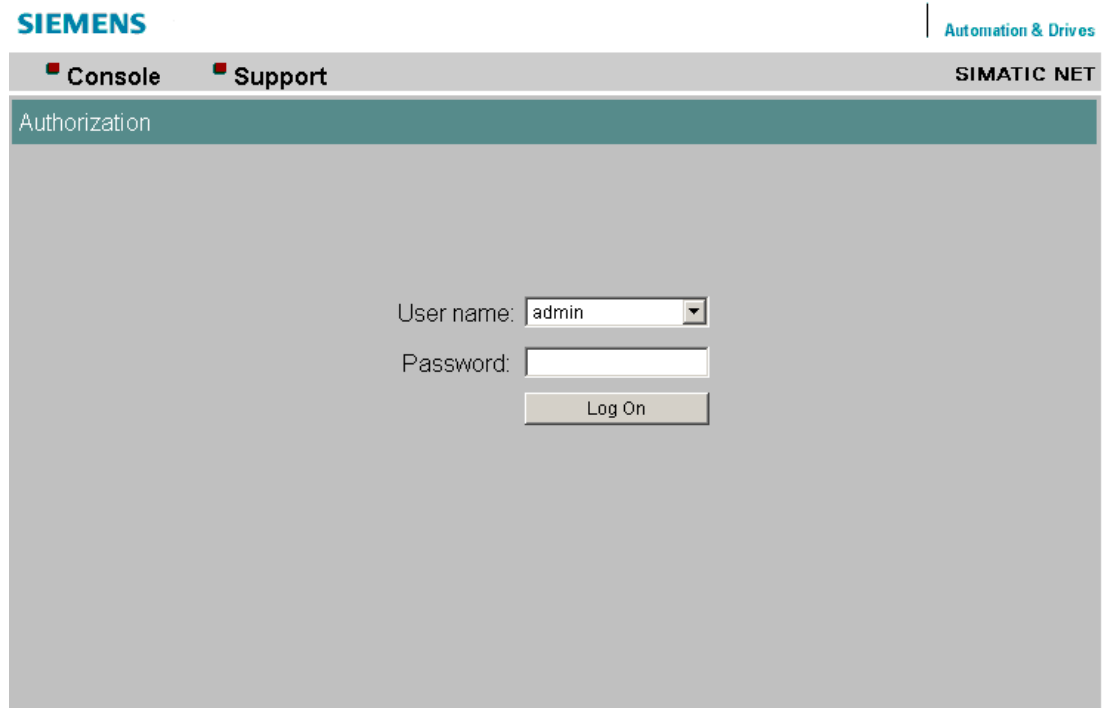
Set your browser so that the page is **not** refreshed with each new access by the server. The updating of the dynamic content of the page is ensured by other mechanisms.

Settings in the Internet Explorer

1. Select "Internet Options" in the "Tools" menu.
The "Internet Options" window opens.
2. Select the "General" tab.
3. In the middle section of the window "Browsing history", click the "Settings" button.
The "Temporary Internet Files and History Settings" window opens.

4. In the "Check for newer versions of stored pages" list, select the "Automatically" option.
5. Save your entry by clicking the "OK" button.

Logging on using the Web browser



The screenshot shows the Siemens SIMATIC NET login interface. At the top, the Siemens logo is on the left, and 'Automation & Drives' is on the right. Below this is a grey navigation bar with 'Console' and 'Support' tabs, and 'SIMATIC NET' on the right. The main area has a teal header labeled 'Authorization'. In the center, there is a login form with 'User name:' followed by a dropdown menu showing 'admin', 'Password:' followed by a text input field, and a 'Log On' button below them.

Figure 5-1 Logon page

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 appears as shown above.
2. Select the required user from the "User name" drop-down list.
 - As the "admin" user, you have write/read access and can change settings of the IE switch.
 - If you select "user" as the user, you only have read access to the configuration data of the IE switch.

5.1 Web Based Management

3. Enter your password.
The factory set passwords are as follows:
 - User name "admin": admin
 - User name "user": user
4. Click "Log On".

Note

Change the factory set password immediately

For security reasons, make sure that you change the original factory-set passwords. The passwords are public knowledge and do not provide any protection.

Resetting the device also resets the passwords to the factory settings.

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

Protection from brute force attacks

During a brute force attack, all possible solutions are tried out systematically until the right one is found. In this case, the correct password.

There is a mechanism implemented in the IE switch that is intended to protect it from such attacks.

If an incorrect password is entered, entries are blocked for a short time. The more often an incorrect password is entered, the longer entries are blocked. After a maximum number of failed attempts, the user or the client IP address is blocked for a certain time.

5.1.3 Simulation of the LEDs

Display of the operating state

IE Switches X-200 have several LEDs that provide information on the operating state of the devices. Depending on its installation location, direct access to the X-200 is not always possible. WBM therefore provides a simulated display of the LEDs.

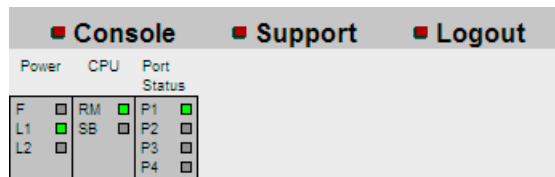


Figure 5-2 Page section with simulation of the LEDs

At the top left of the WBM user interface, there is a schematic representation of the LEDs on your X-200. The traffic display is not shown realistically; in other words the LEDs do not flash.

On the device itself, the power supply and the redundant power supply are displayed by a single LED. In the simulation there is a separate LED for each.

There is also one common LED on the device for the "Redundancy manager" and "Standby" functions. In the WBM, these functions are simulated by two individual LEDs.

5.1.4 Operator activities

Top menu bar

The top menu bar of the WBM contains 3 menu commands:

- Console
If you click this menu command, a console window opens. In this window, you can enter CLI commands. You are then connected to the switch over a TELNET connection. To do this, a standard program must be specified for TELNET connections in your operating system or in your browser.
- Support
If you click this menu command, an Internet connection to the support pages of SIEMENS AG is established. This is only possible when the PC supports an Internet connection.
- Logout
If you click this menu command, you will log out from the WBM of the IE switch.

Updating the display with the "Refresh" button

WBM pages have a "Refresh" button at the lower edge of the page. If you want to request up-to-date information from the IE switch for the current page, click this button.

Storing entries with the "Set Values" button

Note

It is only possible to change the configuration data if you log on with the "admin" user name.

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

Blue text entries are linked

If you click the blue text, you automatically go to the linked page.

5.2 Command Line Interface

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.
2. Enter the "telnet" command followed by the IP address of the IE switch, for example:
C:\>telnet 192.168.200.29

5.2 Command Line Interface

3. When you log in, enter your user name "admin" or "user".
4. Enter your password.

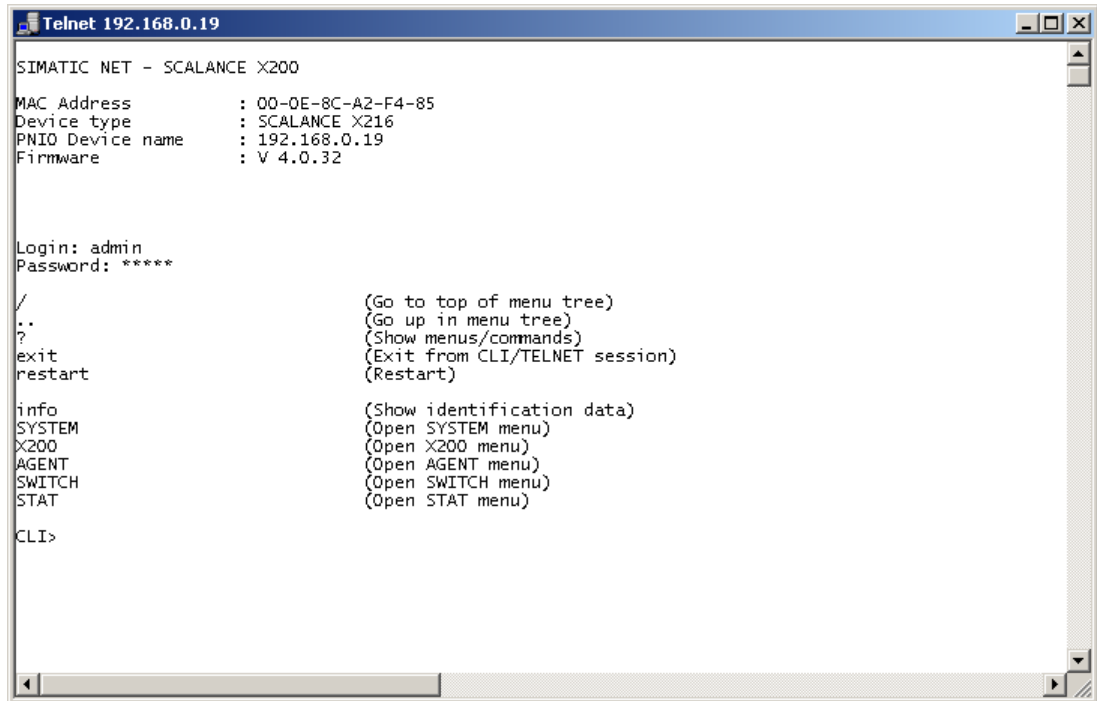


Figure 5-3 CLI via Telnet

Starting the CLI in Web Based Management

Click on the "Console" entry in the upper menu bar of WBM. This automatically opens a Telnet connection in which you can log in. To do this, a standard program must be specified for Telnet connections in your operating system or in your browser.

Shortcuts for commands

As an alternative, instead of entering full CLI commands, you can simply enter the first letters and then press the Tab key. The Command Line Interface then displays a command starting with the 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 and syntax of the CLI commands

Before you can enter a command in the Command Line Interface, you must first open the required menu or submenu.

You will find a description of the CLI syntax at the end of the individual sections under Menus in the WBM (Page 49).

Addressing scheme of the ports

The following addressing scheme is used for the port designations:

- The number relates directly to the port.
The label 2 therefore stands for the second port on the X-200 IE switch.

Symbols for representing CLI commands

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

- **Mandatory parameters** are shown in pointed brackets.
Example: <IP address>
If you omit necessary parameters, most commands output the current value.
- **Optional parameters** are shown in square brackets.
Example: devname [Device Name]
You can assign a new name with the "devname" command by setting the parameter [Device Name]. If the parameter [Device Name] is not set, the current name is displayed.
- **Alternative input values** are separated by the pipe character (|). In this case, you specify one of the listed values as the parameter.
Example: <E|D>
You enter either E or D.
- If a numeric value is required as a mandatory parameter, you can also specify a range of values:
Example: <0 ... 255>
Enter a value between 0 and 255.

Commands not dependent on menus

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

Table 5-1 Command Line Interface - CLI \ ... >

Com-mand	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
Info	Displays information on the current menu item.	Administrator and User

Menus in the WBM

6.1 The System menu

6.1.1 System

System Configuration

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

The first 3 text boxes can only be read and display general information about the device. In the lower 4 boxes, you can specify parameters.

You can change the following entries:

- System Contact
- System Location
- System Name

SIEMENS | Automation & Drives

■ Console ■ Support ■ Logout

SIMATIC NET

Power	CPU	Port	Status
F	RM	P1	<input checked="" type="checkbox"/>
L1		P2	<input checked="" type="checkbox"/>
L2		P3	<input checked="" type="checkbox"/>
		P4	<input checked="" type="checkbox"/>
		P5	<input checked="" type="checkbox"/>
		P6	<input checked="" type="checkbox"/>
		P7	<input checked="" type="checkbox"/>

SIMATIC NET Industrial Ethernet Switch
SCALANCE X206-1
 192.168.200.20

System Configuration

System Up Time: 0 days 00:10:05

Product Name: SIMATIC NET Industrial Ethernet Switch

Device Type: SCALANCE X206-1

System Contact:

System Location:

System Name:

Figure 6-1 System Configuration

System up time

The system up time displays the operating time of the device since the last restart.

Product Name

Displays the product name.

6.1 The System menu

Device Type

Displays the device type.

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.

You apply your settings with Set Values.

Syntax of the Command Line Interface

Table 6-1 System Configuration - CLI\SYSTEM>

Command	Description	Comment
info	Shows the current system information.	
name [sysName]	Sets the "sysName" variable.	Administrator only
contact [sysContact]	Sets the "sysContact" variable.	Administrator only
location [sysLocation]	Sets the "sysLocation" variable.	Administrator only

6.1.2 I&M

System Identification & Maintenance

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

SIEMENS | Automation & Drives

Console **Support** **Logout** **SIMATIC NET**

Power CPU Port Status Port Status

F	RM	P1	P5	P9	P13
L1		P2	P6	P10	P14
L2		P3	P7	P11	P15
		P4	P8	P12	P16

SIMATIC NET Industrial Ethernet Switch
SCALANCE X216
X216-0042

System Identification & Maintenance

I&M 0

Manufacturer ID: 42

Order ID: 6GK5 216-0BA00-2AA3

Serial Number: VPW7052998

Hardware Revision: 3

Software Revision: V 4.0.32

Revision Counter: 0

Revision Date: 0000/00/00 00:00:00

I&M 1

Function Tag:

Location Tag:

Refresh Set Values

Figure 6-2 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 6-2 System Identification & Maintenance - CLI\SYSTEM\IM>

Command	Description	Comment
info	Displays information on the "Identification & Maintenance" menu item.	
revcnt [E D]	Enables/disables the revision counter. The revision counter counts the number of software updates performed.	Administrator only
function [function]	Specifies the function (max. 32 characters).	Administrator only
location [location]	Specifies a location (max. 32 characters).	Administrator only

6.1.3 Restart & Defaults

System Restart & Defaults

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

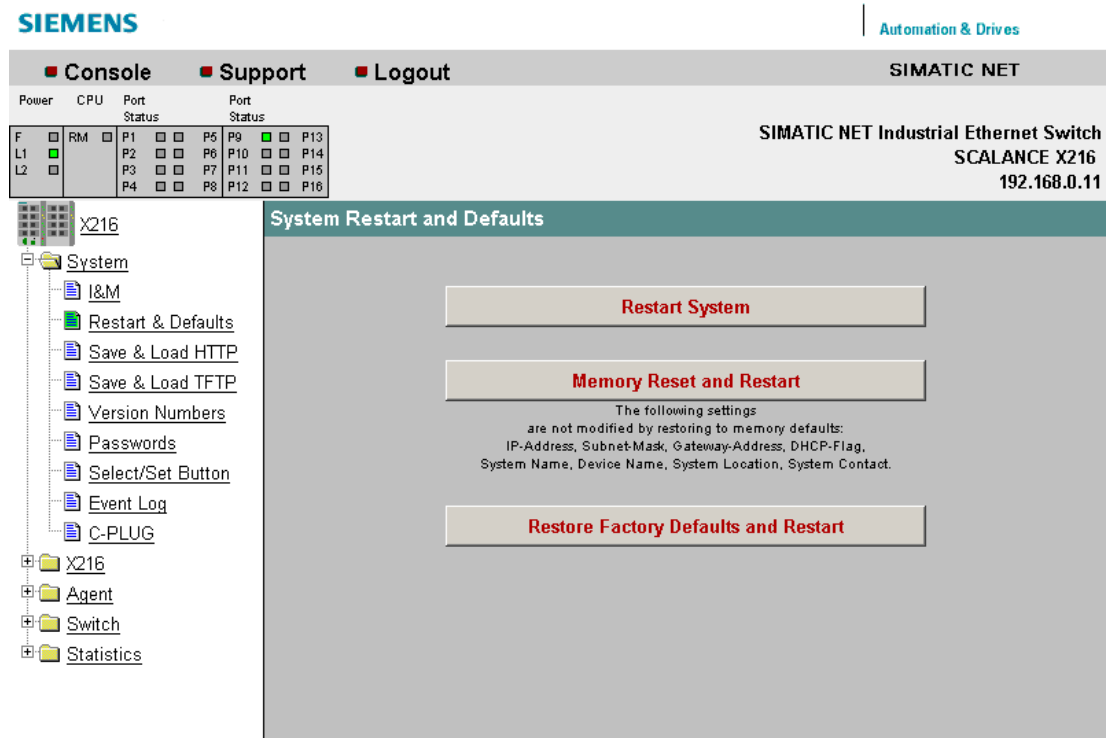


Figure 6-3 Restart and Defaults

Restart System

Click this button to restart the IE Switch X-200. You must confirm the restart in a dialog box. During a restart, the IE Switch X-200 is reinitialized, the internal firmware is reloaded. The learned entries in the address table are deleted. You can leave the browser window open while the IE Switch X-200 restarts.

Memory Reset and Restart

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

- IP address
- Subnet mask
- IP address of the default router
- DHCP flag
- System Name
- System Location
- System Contact
- PNIO Device Name
- System Event Log Table
- Settings for ring redundancy and standby

An automatic restart is triggered. In the user mode, this button is invisible.

Restore Factory Defaults and Restart

Click this button to restore the factory defaults for the configuration. The protected defaults are also reset. In the user mode, this button is invisible.

Note

The IE Switch X-200 must be given a new IP address before it can be accessed again.

Syntax of the Command Line Interface

Table 6-3 System Restart & Defaults - CLI\SYSTEM\RESTARTS>

Command	Description	Comment
memreset	Restores the factory defaults. The protected settings are retained.	Administrator only
defaults	Restores the factory defaults. The protected settings are also reset.	Administrator only

6.1.4 Save & Load 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 the IE Switch X-200.

6.1 The System menu

You can also load new firmware from a file located on your client PC. You can make the entries required for this on the page of the System Save & Load HTTP menu.

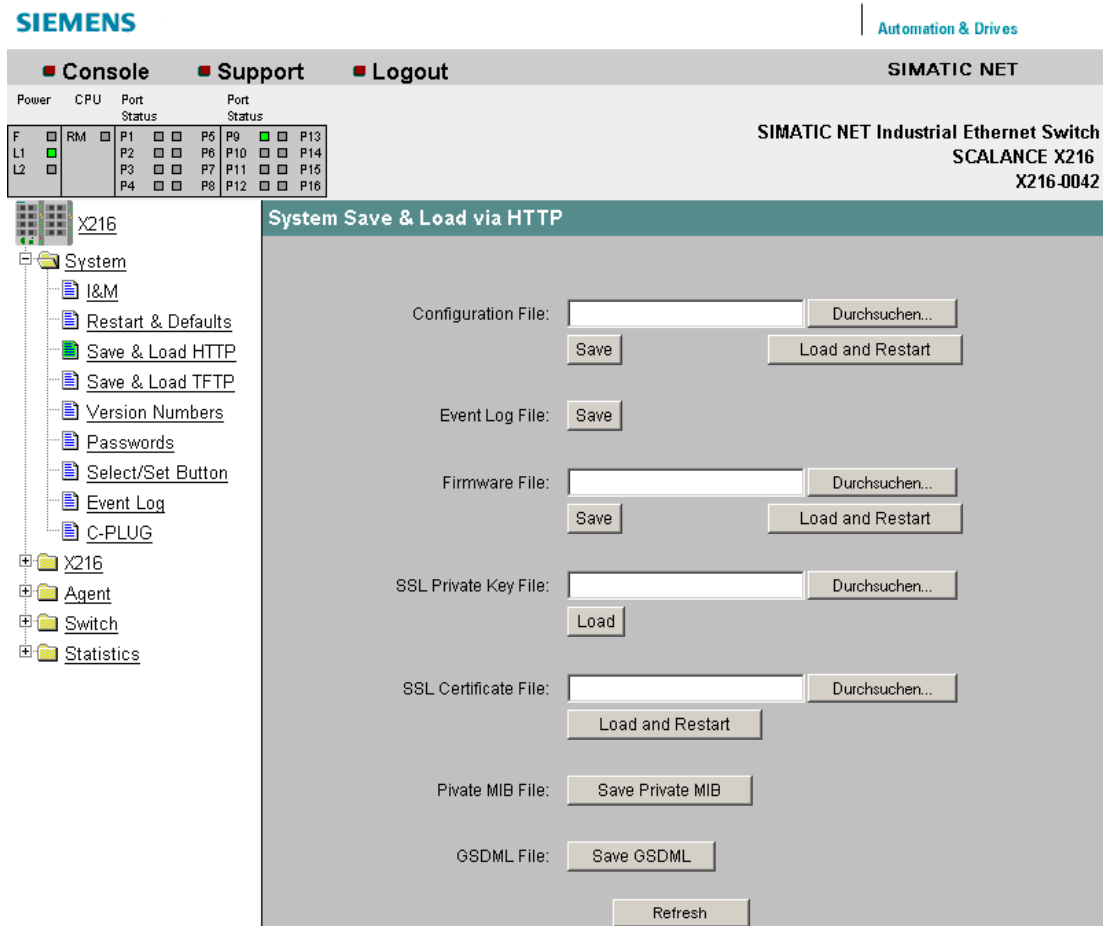


Figure 6-4 System Save and Load via HTTP

Configuration File

Name and possibly also folder path of the configuration file that you want to load on the IE Switch X-200 or where you want to store the current configuration information.

Before you download the configuration file to a device, reset the device to the factory settings, see section "System > Restart & Defaults". There are then no conflicts with existing configurations.

Note

When a configuration file is downloaded, the device type is not checked.

Event Log File

By clicking "Save", you can save the event table (event log file) on the local computer.

Firmware File

Name and, if applicable, directory path of the file from which you want to load the new firmware.

Note

Compatibility of the firmware versions

If you load firmware that is older than the firmware on the device ("Downgrade"), you will have to reset the device to the factory settings after loading the firmware.

Following a downgrade, it may be no longer be possible to access the device via the WBM or via an SSH connection under certain conditions. In this case, use the SET button to reset the device to factory settings. You can also reset the device to factory settings using one of the following programs:

- SINEC PNI ("Device list" menu > "Reset device" button)
- TIA Portal
- STEP 7

If you update the firmware of an IE Switch X-200, make sure that the firmware in use is compatible with the relevant device. If incompatible firmware is downloaded to the device, it will no longer be possible to operate the device. In this case, compatible firmware will have to be loaded again with the boot loader.

Firmware compatibility

Note the following restrictions relating to the compatibility of the firmware versions with the individual devices:

Firmware version	IE switch
at least X-200IRT V5.3	XF204-2BA IRT
at least X-200IRT V4.5	X201-3P IRT PRO
at least X-200IRT V4.1	XF204IRT
at least X-200IRT V3.1	X202-2P IRT PRO X204IRT PRO
at least X-200IRT V2.1	X200-4P IRT X201-3P IRT X202-2P IRT
at least X-200 V4.5	X208PRO
at least X-200 V4.3	X204-2TS
at least X-200 V4.1	XF204 XF204-2 XF206-1 XF208

SSL Private Key File

Name of the file that contains the private key for SSL.

SSL Certificate File

Name of the file that contains the certificate for SSL.

6.1 The System menu

Private MIB File

Here, you can save the private MIB of the IE switch X-200 in a file.

GSDML file

Here, you can save the GSDML file of the IE Switch X-200 in a file.

Note

The private key and the certificate for SSL are required to allow the user to communicate via a secure connection with the Web server on the IE Switch X-200.

The files must be available in PEM format.

6.1.5 Save & Load TFTP

System Save & Load TFTP

The WBM allows you to store configuration information in an external file on a TFTP server or to load such data from an external file from the TFTP server to the IE Switch X-200.

You can also load new firmware from a file located on the TFTP server. You can make the entries required for this on the page of the System Save & Load TFTP menu.

Figure 6-5 System Save and Load via TFTP

TFTP Server IP Address

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

TFTP Server IP 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 using the CLI.

Configuration File

Name and possibly also folder path of the configuration file (maximum 32 characters) that you want to load on the IE Switch X-200 or where you want to store the current configuration information.

Before you download the configuration file to a device, reset the device to the factory settings, see section "System > Restart & Defaults". There are then no conflicts with existing configurations.

Note

When a configuration file is downloaded, the device type is not checked.

Event Log File

By clicking "Save", you can save the event table (event log file) on the local computer.

Firmware File

Name and possibly also folder path of the file (maximum 32 characters) from which you want to load the new firmware.

Note**Compatibility of the firmware versions**

If you load firmware that is older than the firmware on the device ("Downgrade"), you will have to reset the device to the factory settings after loading the firmware.

Following a downgrade, it may be no longer be possible to access the device via the WBM or via an SSH connection under certain conditions. In this case, use the SET button to reset the device to factory settings. You can also reset the device to factory settings using one of the following programs:

- SINEC PNI ("Device list" menu > "Reset device" button)
- TIA Portal
- STEP 7

If you update the firmware of an IE Switch X-200, make sure that the firmware in use is compatible with the relevant device. If incompatible firmware is downloaded to the device, it will no longer be possible to operate the device. In this case, compatible firmware will have to be loaded again with the boot loader.

Firmware compatibility

Note the following restrictions relating to the compatibility of the firmware versions with the individual devices:

Firmware version	IE switch
at least X-200IRT V5.3	XF204-2BA IRT
at least X-200IRT V4.5	X201-3P IRT PRO
at least X-200IRT V4.1	XF204IRT
at least X-200IRT V3.1	X202-2P IRT PRO X204IRT PRO
at least X-200IRT V2.1	X200-4P IRT X201-3P IRT X202-2P IRT
at least X-200 V4.5	X208PRO
at least X-200 V4.3	X204-2TS
at least X-200 V4.1	XF204 XF204-2 XF206-1 XF208

SSL Private Key File

Name of the file that contains the private key for SSL.

SSL Certificate File

Name of the file that contains the certificate for SSL

Note

The private key and the certificate for SSL are required to allow the user to communicate via a secure connection with the Web server on the IE Switch X-200.

The files must be available in PEM format.

System Command Line Interface

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

Command	Description	Comment
info	Displays information on the system.	
server [IP address] [:port]	Specifies the IP address or the port of the TFTP server with which data will be exchanged.	Administrator only
fwname	Specifies the name of the firmware file.	Administrator only
fwload	Loads the firmware from a file.	Administrator only
fwsave	Saves the firmware in a file.	Administrator only
cfgname [file name]	Specifies the name of a file (maximum 255 characters) from which the configuration data will be loaded or in which this data will be saved.	Administrator only

Command	Description	Comment
cfgsave	Saves the configuration data in a file.	Administrator only
cfgload	Loads the configuration data from a file.	Administrator only
logname [file name]	Specifies the name of a file (maximum 255 characters) in which the log table is stored.	Administrator only
logsave	Saves the log table in a file.	
pkname	Specifies the name of the file (maximum 255 characters) that contains the private SSL key.	Administrator only
pkload	Loads the private SSL key from a file.	Administrator only.
ctname	Specifies the name of the file (maximum 255 characters) that contains the SSL certificate.	Administrator only
ctload	Loads the SSL certificate from a file.	Administrator only

6.1.6 Version Numbers

System Version Numbers

This page informs you about the current versions of the boot software, firmware, and hardware.

SIEMENS | Automation & Drives

Console Support Logout SIMATIC NET

Power CPU Port Status Port Status

F	RM	P1	P5	P9	P13
L1		P2	P6	P10	P14
L2		P3	P7	P11	P15
		P4	P8	P12	P16

SIMATIC NET Industrial Ethernet Switch
SCALANCE X216
X216-0042

System Version Numbers

Boot Software: V1.11 24.04.2007

Firmware: V 4.0.32

Hardware Revision: 3

MAC Address: 00-0E-8C-A2-F4-85

MLFB Number: 6GK5 216-0BA00-2AA3

Serial number: VPW7052998

Refresh

Figure 6-6 System Version Numbers

Boot Software

The version of the boot software is displayed here. The boot software is stored permanently on the IE Switch X-200 and is used to load new firmware.

6.1 The System menu

Firmware

The version of the firmware running on the IE Switch X-200.

Hardware Revision

Displays the version of the device.

MAC Address

Displays the MAC address of the device.

MLFB Number

Displays the order number of the device.

Serial number

Displays the serial number of the device.

Syntax of the Command Line Interface

Table 6-5 System Information - CLI\>

Command	Description	Comment
info	Displays the MAC address, MLFB and serial number	

Table 6-6 System Configuration - CLI\SYSTEM>

Command	Description	Comment
versions	Shows versions of firmware, hardware and boot software.	

6.1.7 Passwords

System Passwords

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

You apply your settings with "Set Value".

Note

Default password when supplied

- For Admin: admin
 - For the user: user.
-

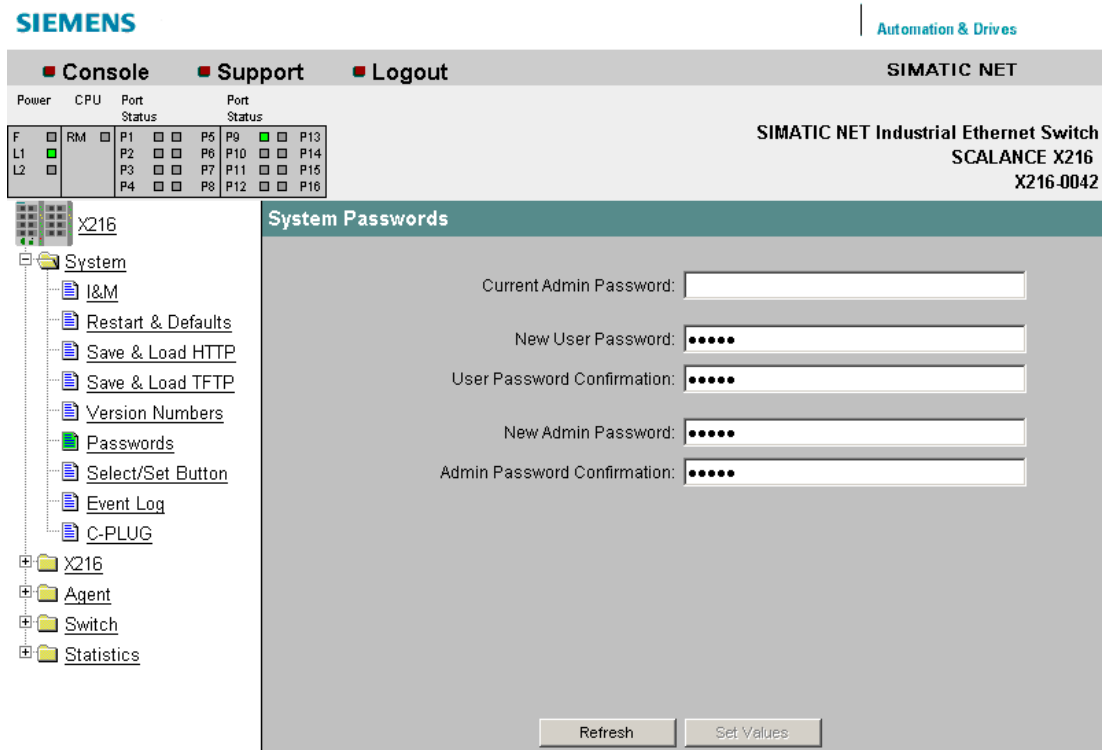


Figure 6-7 System Passwords

Table 6-7 System Passwords - CLI\SYSTEM>

Command	Description	Comment
password <admin user> <password>	Sets a new password for the user or administrator.	Administrator only

6.1.8 Select/Set Button

Select/Set Button Configuration

On this page, you can configure the functions of the SET button.

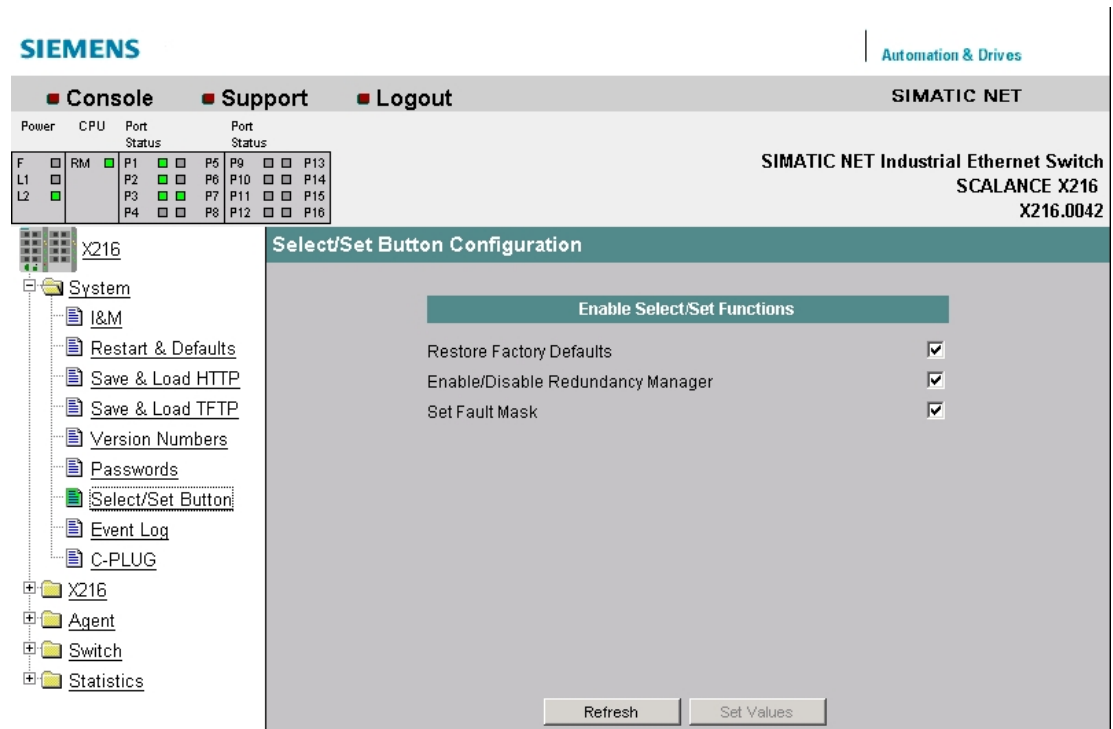


Figure 6-8 Select/Set Button Configuration

Restore Factory Defaults

Here, you decide whether the device is reset to factory defaults when the SET button is pressed.

Enable/Disable Redundancy Manager

Here, you decide whether the redundancy manager can be switched on and off by pressing the SET button.

Set Fault Mask

Here, you decide whether the information of the "Fault Mask" is used when the SET button is pressed.

Syntax of the Command Line Interface

Table 6-8 System Passwords - CLI|SYSTEM|SELSET>

Command	Description	Comment
info	Displays the functionality of the SET button.	
defaults [E D]	Enables/disables the "Restore Factory Defaults" button function.	Administrator only

Command	Description	Comment
rm [E D]	Enables/disables the "Enable/Disable Redundancy Manager" button function.	Administrator only
faultmsk [E D]	Enables/disables the "Set Fault Mask" button function.	Administrator only

6.1.9 Event log


System Event Log Table

This page shows which events occurred and when. You can save the event table using HTTP or TFTP in the System menu.

You specify the events that are to be logged in the "Agent > Event Config" dialog.

Note

Note that events occurring in quick succession are not always displayed in the causal sequence.


Automation & Drives

Console

Support

Logout

Power

CPU

Port Status

F

L1

L2

RM

SB

P1

P2

P3

P4

SIMATIC NET

SIMATIC NET Industrial Ethernet Switch

SCALANCE X202-2IRT

192.168.16.101

X202-2IRT

System

I&M

Restart & Defaults

Save & Load HTTP

Save & Load TFTP

Version Numbers

Passwords

Select/Set Button

Event Log

C-PLUG

X202-2IRT

Agent

Switch

Statistics

System Event Log Table

Restart	Sys. Up Time	Event Text
35	0 days 00:21:20	1987/05/18 09:33:06 Authentication error - Wrong WEB password from 192.168.16.3.
35	0 days 00:20:05	1987/05/18 09:31:51 Fault state: No fault.
35	0 days 00:20:05	1987/05/18 09:31:51 Non-recoverable ring error cleared - no error.
35	0 days 00:19:58	1987/05/18 09:31:44 Link down on port 1
35	0 days 00:19:20	1987/05/18 09:31:06 Fault state: fault (RM Ring error).
35	0 days 00:19:20	1987/05/18 09:31:06 Non-recoverable ring error: RM found one more RM in ring.
35	0 days 00:19:17	1987/05/18 09:31:04 Link up on port 1
35	0 days 00:18:13	1987/05/18 09:30:00 Time was set manually.
35	0 days 00:10:25	Link up on port 2
35	0 days 00:09:42	Link down on port 2
35	0 days 00:04:09	Port Mirroring enabled.
35	0 days 00:02:02	Fault state: No fault.
35	0 days 00:02:00	Fault state: fault (Link down on port 3).

Refresh

Clear Log

Figure 6-9 System Event Log Table

Restart

Specifies the device restart after which the relevant event occurred.

Sys. Up Time

Shows the operating time of the device since the last restart.

Event Text

Displays a brief description of the event that has occurred.

If you have set the system time, the date and time of the event are also displayed.

Syntax of the Command Line Interface

Table 6-9 System Event Log Table- CLI\SYSTEM\LOG>

Command	Description	Comment
info	Displays information on the log table configuration.	
events <show clear>	Indicates or erases expired events in memory.	Administrator only
eventmax [Max count]	Specifies the maximum number of events in the log table. A maximum of 10 to 400 entries can be set.	Administrator only

6.1.10 C-PLUG**C-PLUG Information**

This page tells you whether a C-PLUG is inserted and whether it is valid for the X-200 IE switch.

If a valid C-PLUG is inserted in the device, the page provides information about the IE switch with which the current configuration was saved and C-PLUG itself.

The content of this page cannot be changed.

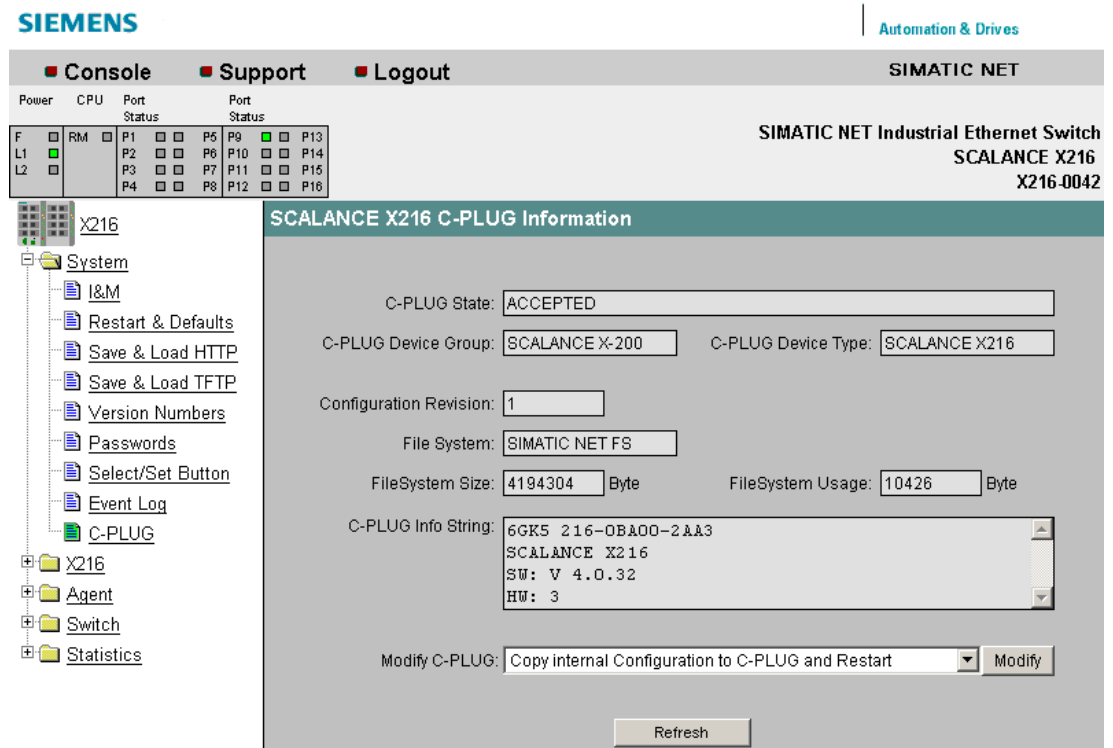


Figure 6-10 C-PLUG Information

C-PLUG State

The status of the C-PLUG is displayed here.

- **ACCEPTED**
There is a C-PLUG with a valid and matching content inserted in the device.
- **NOT ACCEPTED**
No C-PLUG or C-PLUG inserted but invalid or incompatible content. This status is also displayed if 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 X-200.
- **EMPTY**
The inserted C-PLUG is empty.

C-PLUG Device Group

Indicates the SIMATIC NET product line that saved the current configuration on the C-PLUG.

C-PLUG Device Type

Indicates the device type within the product line that saved the current configuration on the C-PLUG.

Configuration Revision

Indicates the version of the configuration structure. This information relates to the configuration options supported by the IE Switch X-200. This does not relate to the actual hardware configuration. The information can change if you update the firmware.

6.1 The System menu

File System

Shows the type of C-PLUG file system.

File System Size

Shows the maximum storage capacity of the C-PLUG file system.

File System Usage

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

C-PLUG Info String

Displays information on the device that saved the current configuration on the C-PLUG, for example order number, type designation, version of hardware and software.

The version relates to the versions that were used on the device when the configuration was saved on C-PLUG. The version changes if you save parameters using a different version. A firmware update or restart of the device does not change the version.

Note

If an empty C-PLUG is inserted in an IE Switch X-200, the next time the device starts up, the configuration stored internally on the basic device is transferred to the C-PLUG.

If you operated an IE Switch X-200 with a C-PLUG inserted, the configuration stored internally on the basic device is no longer modified.

During ongoing operation, changes to the configuration data are stored only on the C-PLUG.

If you remove the C-PLUG later, the configuration stored internally on the basic device becomes valid again. This restores the configuration status prior to inserting the C-PLUG.

Modify C-PLUG, Modify button

If you are logged on as administrator, you can make settings here.

- **Copy internal Configuration to C-PLUG and Restart**
The configuration in the internal flash memory of the switch is copied to the C-PLUG and this is followed by a restart.
Use case:
The X-200 IE switch starts up with a C-PLUG inserted. This contains a configuration that differs from the IE Switch X-200 or a configuration containing errors. With this function, you can overwrite the content of the C-PLUG with the original device configuration.
- **Copy default Configuration to C-PLUG and Restart**
This stores the configuration with all factory default values on the C-PLUG. This is followed by a restart during which the X-200 IE switch restarts with these default values.
- **Clean C-PLUG (Low Level Format, Configuration lost)**
Deletes all data from the C-PLUG and triggers low-level formatting. This is not followed by an automatic restart and the device displays an error. You can clear this error status by restarting or removing the C-PLUG after turning off the basic device. To retain the configuration of the basic device even after deleting the C-PLUG, the configuration data stored on the C-PLUG is transferred to the internal memory of the basic device.
- **Continue without C-PLUG**
If the C-PLUG is removed from a device, an error message is displayed after the device restarts. In this case, you can select the "Continue without C-PLUG" option to change the device to the mode without a C-PLUG.

Your selection is then adopted when you click "Modify".

Syntax of the Command Line Interface

Table 6-10 C-PLUG Information - CLI\SYSTEM\C-PLUG>

Command	Description	Comment
info	Displays the current status (information) of the C-PLUG.	
initdef	Initializes the C-PLUG with the default parameters and restarts the device.	Administrator only
initmem	Initializes the C-PLUG with the MEMORY parameters and restarts the device.	Administrator only
usecplug [D]	If the C-PLUG was removed, the next time you restart the device, an error command is displayed in the Command Line Interface. By entering the usecplug D command, you can change the device to operate in the mode without C-PLUG.	Administrator only
clear	Erases the data on the C-PLUG.	Administrator only

6.2 The X-200 menu

6.2.1 X-200

Status

This page provides information on operating states such as power supply and fault status.
The content of this page cannot be edited.

The screenshot displays the SIMATIC NET interface for the SCALANCE X204-2 Industrial Ethernet Switch. The top navigation bar includes 'Console', 'Support', and 'Logout' buttons, along with the 'SIMATIC NET' logo. The main content area is titled 'SCALANCE X204-2 Status'. It features a status summary on the left with indicators for Power (F, L1, L2), CPU (RM), and Port Status (P1-P8). The central part of the page shows the status of the power supply and fault status. The status is 'up' for both Power Line 1 and Power Line 2, and 'No fault' for the Fault Status. A 'Refresh' button is located at the bottom of the status section.

Figure 6-11 Status

Power Line 1 / Power Line 2

- up
Power supply 1 or 2 is applied.
- down
Power supply 1 or 2 is not applied or is below the permitted voltage.

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.

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.
RM Ring error	<p>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.</p> <p>In the first case, check the configuration of the ring ports:</p> <ul style="list-style-type: none"> • Suitable setting for the operating mode (full duplex/half duplex)? • With fiber-optic cables: Send and receive cables correctly plugged in? <p>In the second case:</p> <p>Reconfigure the second redundancy manager in the ring so that this adopts the suitable client role or remove the device from the ring.</p>
No Fault	The switch has not detected any errors. The signaling contacts do not respond and the error LED does not light up.

6.2.2 Fault Mask**Fault Mask**

The settings on this page allow you to monitor the link status and the redundant power supply. Values are also displayed here that were set with the button configuration.

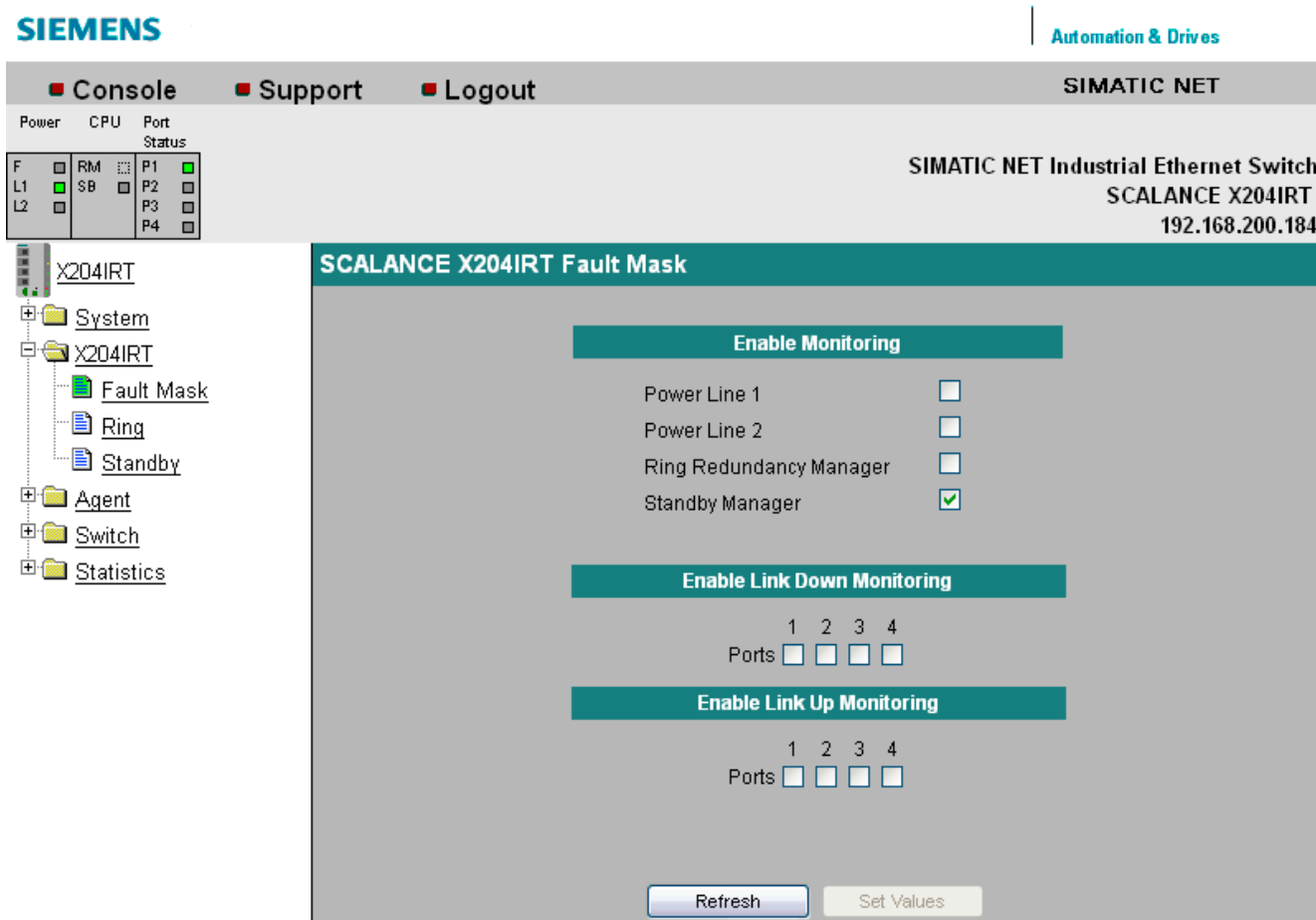


Figure 6-12 Fault Mask

Enable Monitoring

Power Line 1/Power Line 2

Here, you specify which of the two power supplies, Power Line 1 and Power Line 2 will be monitored.

If there is no voltage or the voltage is too low at the monitored connector (Power Line 1 or Power Line 2), an error is signaled by the alarm system.

Note

Bridging power failures

With SCALANCE X-200, IE switches power failures of up to 20 ms can be bridged.

Exception: If you operate a SCALANCE XF-200IRT with two bus adapters BA 2xSCRJ power failures of up to 15 ms can be bridged.

Note

The following devices do not have a redundant power supply:

- SCALANCE X204IRT PRO
- SCALANCE X202-2P IRT PRO
- SCALANCE X201-3P IRT PRO

Ring Redundancy Manager

Here you can choose whether the "active" status of the redundancy manager triggers an error.

Standby Manager (only relevant for IRT devices)

Here, you can choose whether the "master" status and "passive" or "slave" and "active" or partner not found triggers an error.

FMP Event (relevant only for FM devices, refer to the section "FMP (Page 121)")

Here, you can decide whether an error is triggered if the received power or the power loss change to the "Maintenance demanded" status.

Enable Link Down Monitoring

Error message when the status of the port is "Link down". Here, you can enable/disable monitoring of the link status for the individual ports.

Enable Link Up Monitoring

Error message when the status of the port is "Link up". Here, you can enable/disable monitoring of the link status for the individual ports.

Note

Since according to the factory default, neither the monitoring of the ports nor the monitoring of the power supply are activated, none of the check boxes are selected when the device ships.

Syntax of the Command Line Interface

Table 6-11 Fault Mask - CLI/X200>

Command	Description	Comment
info	Displays information on the "X-200" menu item.	
fault	Displays the fault status.	
power [<E D> [lines]]	Specifies a fault mask for the power supplies Power Line 1 and Power Line 2.	Administrator only
others <R S F> <E D>	Specifies the fault mask for: R - Ring Redundancy Manager S - Standby Manager (only relevant for IRT devices) F - FMP Event (only relevant for FM devices)	Administrator only
downmask <1-n> <E D>	Specifies a port mask for the ports for which the monitoring of a link down event is enabled.	Administrator only
upmask <1-n> <E D>	Specifies a port mask for the ports for which the monitoring of a link up event is enabled.	Administrator only

6.2.3 Ring

Ring redundancy

On this page, you can set the ports for media redundancy and the required redundancy mode. You can also configure the Link Check function.

Note

X-200 IE switches as of firmware V4.0 support the media redundancy methods MRP and HRP.

X-200 IE switches with firmware V3.1 and older, X-300 and X-400 IE switches with firmware V2.3 and older and OSMs/ESMs support only the HRP method.

Note

If you want to configure an MRP ring, the devices can be interconnected to form a ring without any extra configuration. In this case, the default ring ports must be used, see Appendix Default ring ports (Page 179). The default role "Automatic Redundancy Detection" automatically configures the ring.

If an HRP ring is configured, exactly one device in the ring must be set to the HRP Manager role. All other devices in the ring must be set to either "Automatic Redundancy Detection" or "HRP Client".

If an HRP ring is configured in which a linear bus is set up in which a device is set to HRP manager and the other devices have the setting "Automatic Redundancy Detection", the error message "other RM in ring" is output. This disappears after connecting the linear bus to form a ring.

Note

As default, a role for automatic ring configuration is enabled. This causes cyclic frame communication at a low transmission speed. If it is not required, disable this redundancy function to avoid unnecessary network load.

SIEMENS Automation & Drives

Console Support Logout SIMATIC NET

Power CPU Port Status

F L1 L2 RM P1 P2 P3 P4 P5 P6

SIMATIC NET Industrial Ethernet Switch
SCALANCE X204-2FM
192.168.16.22

SCALANCE X204-2FM Ring Redundancy

Redundancy Control

Enable Ring Redundancy: ☒

Redundancy Mode: Automatic Redundancy Detection

First Ring Port: 5

Second Ring Port: 6

Redundancy Role: Manager (MRP)

Redundancy Manager State: Active

Number of State Changes: 0

Maximum Delay (ms): 0

Link Check Control

Ring Port	Link Check Enabled	Link Check State	Frames Out	Frames In	Action
First	<input checked="" type="checkbox"/>	running	3673	3673	Reset
Second	<input type="checkbox"/>	disabled	0	0	Reset

Refresh Set Values

Figure 6-13 Ring redundancy

Enable ring redundancy

Here, you can choose whether or not the module is part of a ring.

Redundancy Mode

Here, you can choose the redundancy method and the role of the module within a ring.

- **Automatic Redundancy Detection**
Select this setting to configure the redundant mode automatically.
In "Automatic Redundancy Detection" mode, the IE Switch X-200 automatically detects whether or not there is a device with the role of HRP manager in the ring. If this is the case, the device adopts the role of "HRP Client".
If no HRP manager is found, all devices with the "Automatic Redundancy Detection" or "MRP Auto Manager (Auto)/Client" setting negotiate among themselves to establish which device adopts the role of MRP manager. The other devices automatically set themselves to "MRP Client" role.
- **MRP Client**
Here, you can select the "MRP Client" role.
In an MRP ring, at least one device must be set either to the "Automatic Redundancy Detection" role or to the "MRP Manager (Auto)/Client" role. 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 device automatically adopts the role of MRP manager.
Select the "MRP Client" role if you want to operate the device along with components that do not originate from Siemens in the ring.
- **MRP Manager (Auto)/Client**
Devices with the setting "Automatic Redundancy Detection" or "MRP Manager (Auto)Client" negotiate among themselves which device will adopt the MRP manager role. The device with the lowest MAC address will always become the MRP manager. In contrast to the setting "Automatic Redundancy Detection", the devices cannot detect whether or not an HRP manager is in the ring. This means that they never adopt the role of "HRP Client".
- **HRP Client**
Here, you can select the role "HRP Client".
Select the role "HRP Client" if you want to use the standby functionality of the X-200 IE switch.
- **HRP Manager**
Here, you can select the role HRP Manager. When you configure an HRP ring, exactly one module must be set as HRP manager. All other devices must be configured as HRP clients.

Note

Ring ports after resetting to factory settings

If you reset to factory defaults, the redundancy role Automatic Redundancy Detection (ARD) becomes active. The configuration of the ring ports is also reset to the ports set in the factory.

You will find the default ring ports of the individual X-200 variants in the Appendix Default ring ports (Page 179).

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.

First ring port

Relevant only when the Automatic Redundancy Detection role, MRP client or HRP client is selected and the HRP manager or MRP manager role was adopted.

Here, you select which is the first ring port.

Second ring port

Relevant only when the Automatic Redundancy Detection role, MRP client or HRP client is selected and the HRP manager or MRP manager role was adopted.

Here, you select which is the second ring port.

Static ring port

Relevant only when the HRP Manager role is selected and the HRP manager role was adopted.

The port that is active in the ring is specified here.

Isolated ring port

Relevant only when the HRP Manager role is selected and the HRP manager role was adopted.

The port that closes the ring but via which no communication takes place is specified here.

Redundancy Role

Here, you can see which role the module has actually adopted in the ring.

Redundancy Manager State

Relevant only if the HRP manager or MRP manager role was adopted.

- **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.
- **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 uninterrupted. Error situation. The redundancy manager connects its ring ports through and restores an uninterrupted linear topology.

Number of State Changes

Relevant only when the redundancy role HRP manager or MRP manager was adopted.

This shows how often the redundancy manager switched to the alternative path due to an interruption in the ring since the device was turned on.

Maximum delay (ms)

Relevant only when the HRP manager or MRP manager role was adopted.

This shows how long a test frame was delayed. (Test frames are placed on the ring to detect interruptions in the ring.) For reliable functioning of the network, values < 20 ms are necessary.

Note

The standby function always requires an activated HRP client. If the standby manager is activated, the following message is displayed if an attempt is made to turn off ring redundancy or to change to "Redundancy Manager":

Cannot disable "Redundancy" if "Standby Manager" is enabled.

Note

When the devices ship, the default ring ports are set, see Appendix Default ring ports (Page 179).

Note

Note the following when configuring an HRP ring:

- If no HRP manager has been specified yet, the ring must be interrupted at one point. This avoids circulating frames.
 - If an MRP ring is configured, at least one device must be set to the "Automatic Redundancy Detection" or "MRP Manager (Auto)/Client" role. The role of the redundancy manager is adopted automatically by a device with this setting.
 - If you change an MRP ring in the configuration to create an HRP ring, open the ring while you reconfigure the devices. This avoids circulating frames.
-

Note

Note the following when configuring an MRP ring:

- With devices having more than 8 ports, the selection of the ring ports when using MRP is restricted:
 - With SCALANCE X216 and X224, ports 1 to 8 can be selected as MRP ring ports.
 - With SCALANCE X212-2 and X212-2LD, ports 9 to 14 can be selected as MRP ring ports.
 - The default ring ports are adapted automatically if you select MRP. Make sure that the ring ports are set correctly.
-

Link Check

Note

The Link Check function is not available for X-200IRT IE switches.

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

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

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

Requirements

- You can only enable the Link Check function with optical ring ports of an HRP or MRP ring.
- Link Check must be enabled on two neighboring devices (connection partners) within an HRP or MRP ring.
- The ring ports on which you enable Link Check must be connected.

How Link Check works

- Behavior with an undisturbed connection
If you enable Link Check on two connected ring ports, the two connection partners exchange Link Check frames cyclically on these ports. The frames received by one connection partner are sent back to the other.
When the devices receive back the frames they sent from the connection partner, the connection is prepared for Link Check. The connection partners then increase the send frequency of the Link Check test frames and the actual connection monitoring is active.
- Behavior with a disturbance
When connection monitoring is enabled, you can see the number of sent and received Link Check frames on this page. Based on these statistics you can recognize smaller disturbances for which the disturbance does not yet cause the transmission line to be closed down by Link Check.
Link Check recognizes a connection as being disturbed and closes it down when too many test frames are lost within a given period. Link Check uses several intervals to be able to recognize sudden occurrences of errors as well as a continuous low error rate.
A port that was turned off by Link Check must be reset to be able to communicate again. To do this you have 2 options:
 - Pull out the connecting cable and plug it in again.
 - Reset the function on both connection partners using the "Reset" button. This must be done on both devices within 30 s.

Note

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

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

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

Configuring via a PROFINET IO controller

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

When a new configuration is transferred, Link Check is automatically disabled on all ports that were not configured as ring ports.

Note

Events relating to the Link Check function are not reported by PROFINET IO.

Configuration for the monitoring of the connection**NOTICE**

Make sure that the frames used by Link Check for monitoring the optical connections are not supplanted by an overload of high priority frames in the network.

An overload of high priority frames can, for example, be caused by the following:

- Network loops that can cause duplication of the high priority frames
- Feeding in of high priority load such as spanning tree BPDUs in the ring

Note

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

Note

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

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

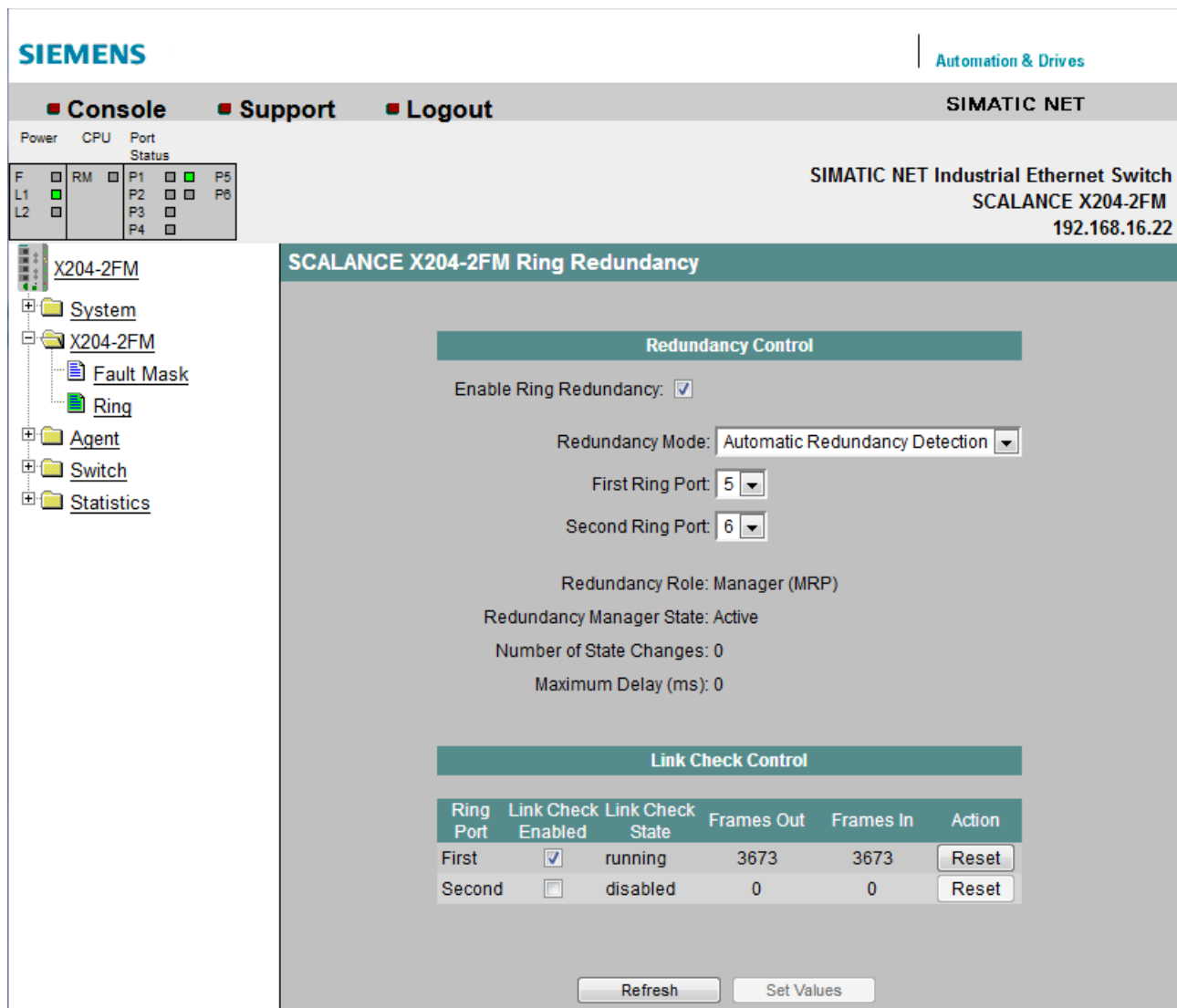


Figure 6-14 Ring redundancy - Link Check

Ring Port

Shows information about the Link Check function for the first or second ring port.

Link Check Enabled

With this check box, you enable or disable the Link Check function for the first or second port.

Link Check State

Shows the status of the Link Check function for the first or second ring port. The following statuses are possible:

- disabled
The function is disabled.
- enabled
The function is enabled. The connection partner has not yet confirmed the monitoring.

- **running**
The function is enabled. The connection monitoring is enabled. The outgoing and incoming test frames are counted and matched up.
- **fault**
The function is enabled. Link Check has detected a fault on the monitored section and turned off the port.

Frames Out

Shows how many Link Check test frames were sent

Frames In

Shows how many Link Check test frames were received.

Action

With the "Reset" button, you reset Link Check on the first or second ring port. After resetting Link Check, the function is restarted on the port and the statistics are reset.

If you use the "Reset" button, the reset must be performed on both connection partners within 30 s.

Note

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

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

Syntax of the Command Line Interface

Table 6-12 Ring Redundancy - CLI\X200\REDUND>

Command	Description	Comment
info	Displays information on the redundancy modules.	
mode [A AM C E D]	Sets the redundancy role: A - Auto: MRP manager or MRP/HRP client AM - Auto: MRP manager or MRP client C - MRP client E - HRP manager D - HRP client	Administrator only
static [n-m]	Specifies the static (fixed) ring port. Note: Only for the HRP manager and HRP client roles: Specifies the static (fixed) ring port in the range n-m.	Administrator only
isolated [n-m]	Specifies the isolated ring port. Note: Only for the HRP manager and HRP client roles: Specifies the static (fixed) ring port in the range n-m.	Administrator only
rports [n-m n-m]	Specifies the two ring ports in the range n-m.	Administrator only
clear	Resets all redundancy counters to the original setting.	Administrator only

6.2 The X-200 menu

Command	Description	Comment
redund [E D]	Enables / disables ring redundancy.	Administrator only
linkchk <E D> [rport1 rport2]	Commands for the Link Check function: <ul style="list-style-type: none"> • E Enables the Link Check function for the specified ring port. • D Disables the Link Check function for the specified ring port. 	Administrator only
reset <All rport1 rport2>	Resets Link Check function for the specified ports. When you use this command, loops can form temporarily resulting in a loss of data traffic. The loop is automatically cleared again If this is not acceptable for your application, reset Link Check by pulling the cable and plugging it in again.	Administrator only

6.2.4 Standby

Redundant linking of rings

X-200IRT IE switches support not only media redundancy in ring topologies but also the redundant linking of HRP rings. These also include interrupted HRP rings; in other words, buses. With a redundant link, two HRP rings are linked together via 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).

You will find further information on Ethernet cabling and the topological positioning of master and slave in the SCALANCE X-200 operating instructions in the section "Network topologies and media redundancy".

Note

- The function is supported only by X-200IRT IE switches.
- To be able to use the function, HRP must be activated.

Standby manager

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

Enable the standby manager for both standby partners and select the port via which the module is connected to the ring you want to link to.

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

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

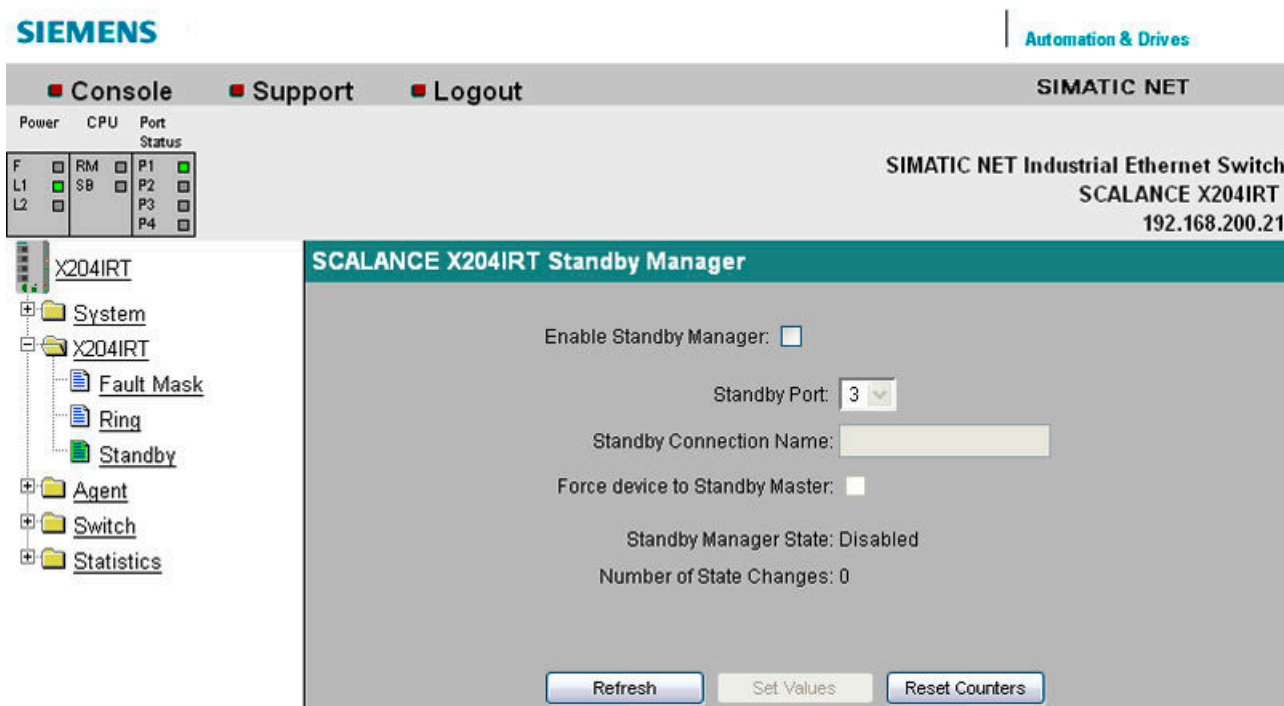


Figure 6-15 Standby manager

Enable Standby Manager

Click the check box to enable or disable the function.

Standby Port

Select a port for the link to the second ring.

The standby port is involved in the redirection of data traffic. In there are no problems, only the standby port of the master is enabled and handles the data traffic into the connected HRP ring or HRP bus.

If the master or the Ethernet connection (link) of one of the standby ports of the master fails, the standby port of the master will be disabled and the standby port of the slave enabled. As a result, a functioning Ethernet connection to the connected network segment (HRP ring or HRP linear bus) is restored.

Standby Connection Name

This name defines the master/slave device pair. Both devices must be located in the same ring.

Here, enter the name for the standby connection. This must be identical to the name entered on the standby partner. You can select any name to suit your purposes, however, you can only use the name for one pair of devices in the entire network.

Force device to Standby Master

If you select this check box, the device is configured as a standby master regardless of its MAC address.

- If this check box is not selected for either of the devices for which the standby master is enabled, then assuming that no error has occurred, the device with the higher MAC address adopts the role of standby master.
- If the option is selected for both devices or if the "Force device to Standby Master" property is supported by only one device, the standby master is also selected based on the MAC address.

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

Note

The standby manager always requires an activated HRP client. If this is not activated, the following error message is displayed:

"Cannot enable Standby manager if redundancy is disabled or not in "HRP Client" mode."

Note

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

Note

The X-200IRT IE switch uses a locally valid Ethernet address for communication in standby mode. This is formed by setting the "universally/locally administered address bit" for the MAC address of the X-200IRT IE switch.

This is the second least significant bit of the first byte of the Ethernet address.

Syntax of the Command Line Interface

Table 6-13 Standby (only for IE Switch X-200IRT) - CLI\X200\STANDBY>

Command	Description	Comment
info	Displays information on the standby module.	
port [1-4]	Specifies the standby port.	Administrator only
partner [Name]	Specifies the name of the standby connection.	Administrator only
clear	Resets all counters to the original setting.	Administrator only
standby [E D]	Enables/disables the standby manager.	Administrator only
force [E D]	Enables/disables the device as standby master.	Administrator only

6.2.5 Procedure for redundant linking of rings

Procedure for redundant linking of rings

Note**Circulating frames and therefore failure of the data traffic**

- The redundant Ethernet connection must not be plugged in until the configuration has been completed.
 - The Ethernet connection must also not be plugged in when the redundant link is deactivated.
 - The redundant Ethernet connection must be plugged into the correct port on both devices; in other words, the configured standby port.
-

Note

The Standby Connection Name (for a device pair) may only be used once in the network.

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

1. Plan which device in the ring adopts the role of standby master and which adopts the role of standby slave.
2. You should also plan the port of the standby master and standby slave to which the Ethernet connections to the other rings is 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.
3. For both master and slave, specify which port is the standby port under "Standby Port".
4. Specify a name for the standby connection. Enter this name for the master and slave device.
5. Select the "Enable Standby Manager" option both on the master and on the slave.
6. Confirm the configuration by clicking on the "Set Values" button for the master and slave.
7. **Now**, you can plug in the redundant Ethernet connection.

6.3 The Agent menu

6.3.1 Agent

Agent Configuration

This menu command provides you with options for the IP address. Here, you can specify whether you will assign a fixed address for the X-200 IE switches or whether the IP address will be obtained dynamically. You can also enable options for accessing X-200 IE switches, for example TELNET.

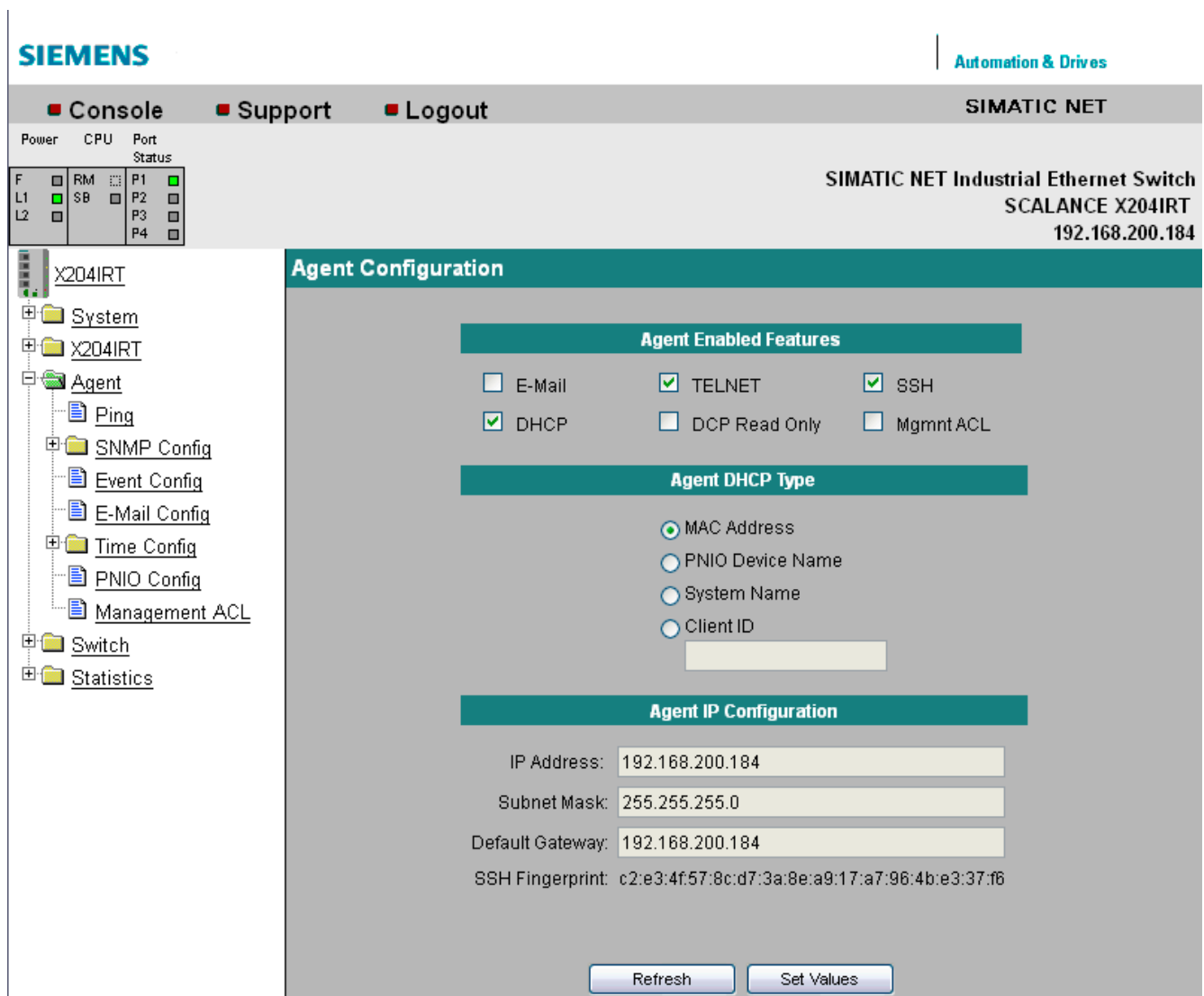


Figure 6-16 Agent Configuration

Note

When supplied, SSH and TELNET are activated.

When supplied, DHCP (identification via MAC address) is enabled.

When the device ships, Mgmnt ACL is disabled.

Settings for X-200 IE switches

Agent Enabled Features

E-Mail

Enables/disables E-mail functionality.

TELNET

Enables/disables the availability of the IE Switch X-200 over TELNET.

SSH

Enables / disables the SSH protocol.

DHCP

Enables/disables the search by the IE switch X-200 for a DHCP server when it starts up. The IP parameters of the X-200 are configured according to the data supplied by this server.

If DHCP is enabled, the "Agent DHCP Type" section is available. Select one of the options for identifying the IE switch X-200 in the configuration of the DHCP server.

DCP Read Only

The configuration of an X-200 can be read and edited via DCP (SINEC PNI and STEP 7).

If you enable the "DCP Read Only" option, the configuration data can only be read via DCP.

Mgmnt ACL

Note**Note the following before you enable "Mgmnt ACL"**

A bad configuration on the "Management ACL" page can result in you being unable to access your device. You should therefore configure an access rule that allows access to the management before you enable the function.

Enable/disable the rules for accessing the management of the IE switch.

The access rules are managed on the "Management ACL" page, see section "Management ACL (Page 113)".

Agent IP Configuration

IP Address

The IP address of the X-200 IE switch. If you make a change here, the WBM loses the connection to the IE Switch X-200. Enter the new IP address in the Internet browser to restore the connection.

Subnet Mask

6.3 The Agent menu

Here, you enter the subnet mask of the X-200 IE switch.

Note

You can configure the following subnet masks via WBM and CLI; however, these subnet masks are not permissible in operation with PROFINET or SINEC PNI (DCP):

- 128.0.0.0
- 192.0.0.0
- 224.0.0.0

Default gateway

If the PC with the Internet browser is not in the same subnet as the IE Switch X-200, you must enter the IP address of the default gateway here.

Syntax of the Command Line Interface

Table 6-14 Agent Configuration - CLI\AGENT>

Command	Description	Comment
info	Displays information on the agent settings.	-
telnet [E D]	Enables/disables the TELNET function	Administrator only
ssh [E D]	Enables/disables the SSH function.	Administrator only
mail [E D]	Enables/disables the mailing function.	Administrator only
dcp [RO RW]	DCP is activated in the mode <ul style="list-style-type: none"> • RO = Read Only or • RW = Read and Write 	Administrator only
mgmntacl [E D]	Enables / disables management ACL.	Administrator only
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.	-

Table 6-15 Agent Configuration - CLI\AGENT\IP>

Command	Description	Comment
info	Displays information on the IP settings.	-
ip [IP address]	Specifies the IP address. DHCP is disabled.	Administrator only
subnet [subnet mask]	Specifies the subnet mask.	Administrator only
gateway [IP address]	Specifies the IP address of the default IP gateway.	Administrator only
dhcp [E D]	Enables / disables DHCP.	Administrator only

Command	Description	Comment
dhcptype [M N C D]	Sets the DHCP parameters: - M MAC address - N system name - C client ID - D PNIO device name	Administrator only
clientid [client ID]	Specifies the DHCP client ID.	Administrator only

6.3.2 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.

Ping

IP address: Repeat:

Ping Output:

Figure 6-17 Ping

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.

6.3.3 SNMP Config

Note

On X-200IRT IE switches with firmware versions V4.0 and lower only the SNMPv1/v2 mode is possible.

Agent SNMP Configuration - Configuration of SNMP for an IE Switch X-200

On the SNMP Agent Configuration page, you make basic settings for SNMP. For detailed settings (traps, groups, users), there are separate menu commands in WBM.

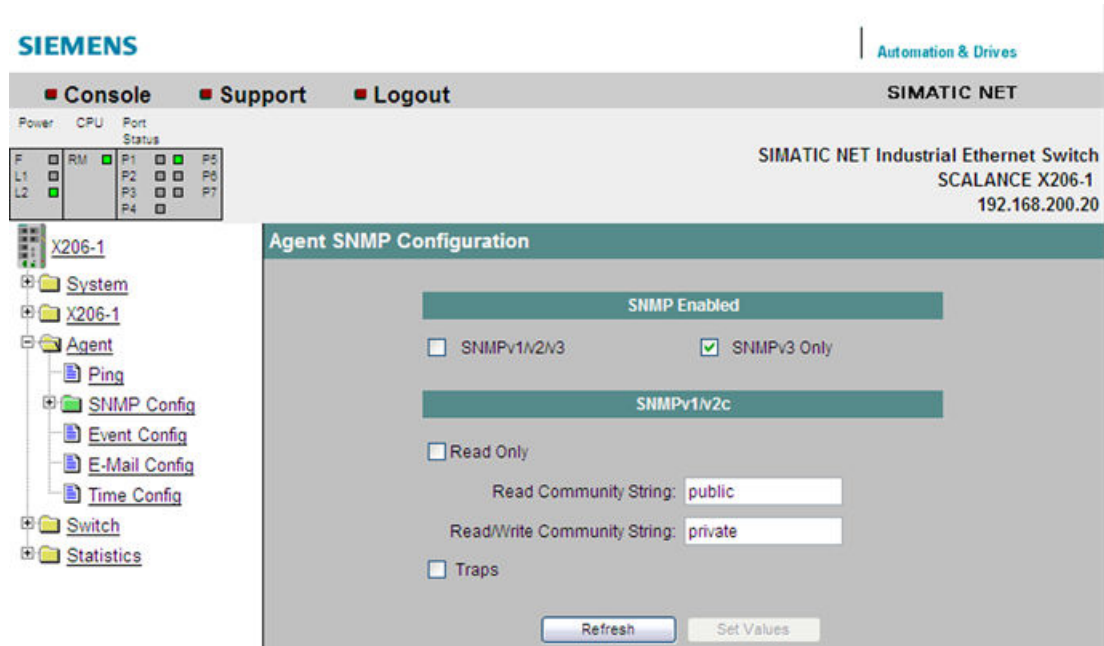


Figure 6-18 Agent SNMP Configuration

SNMP enabled

Here, you can decide whether only SNMPv3 or also SNMPv1/v2 can be used.

SNMP Read Only

Enables/disables write protection for SNMP variables.

SNMP Community Strings

Read Community String

Displays the user name for read access to SNMP variables.

Write Community String

Displays the user name for write access to SNMP variables. Here, changes can only be made, when write protection (SNMP read only) has been disabled.

Traps

Here, you can enable or disable the sending of SNMP traps.

Syntax of the Command Line Interface

Table 6-16 Agent SNMP Configuration - CLIAGENT\SNMP>

Command	Description	Comment
info	Displays information on SNMP.	
snmp [A 3 D]	Enables either [A] all SNMP versions or [3] only SNMPv3 or [D] disables SNMP.	Administrator only

Command	Description	Comment
readonly	Enables / disables SNMPv1 read only mode.	Administrator only
getcomm [string]	Specifies the Read Community string.	Administrator only
setcomm [string]	Specifies the Write Community string.	Administrator only
traps [E D]	Enables / disables SNMPv1 traps.	Administrator only.

6.3.4 SNMP Trap Config

Agent Trap Configuration - SNMP Traps for Alarm Events

If an alarm event occurs, the IE Switch X-200 can send traps (alarm frames) to up to two different (network management) stations at the same time. Traps are sent only for events specified in the Agent Event Configuration menu.

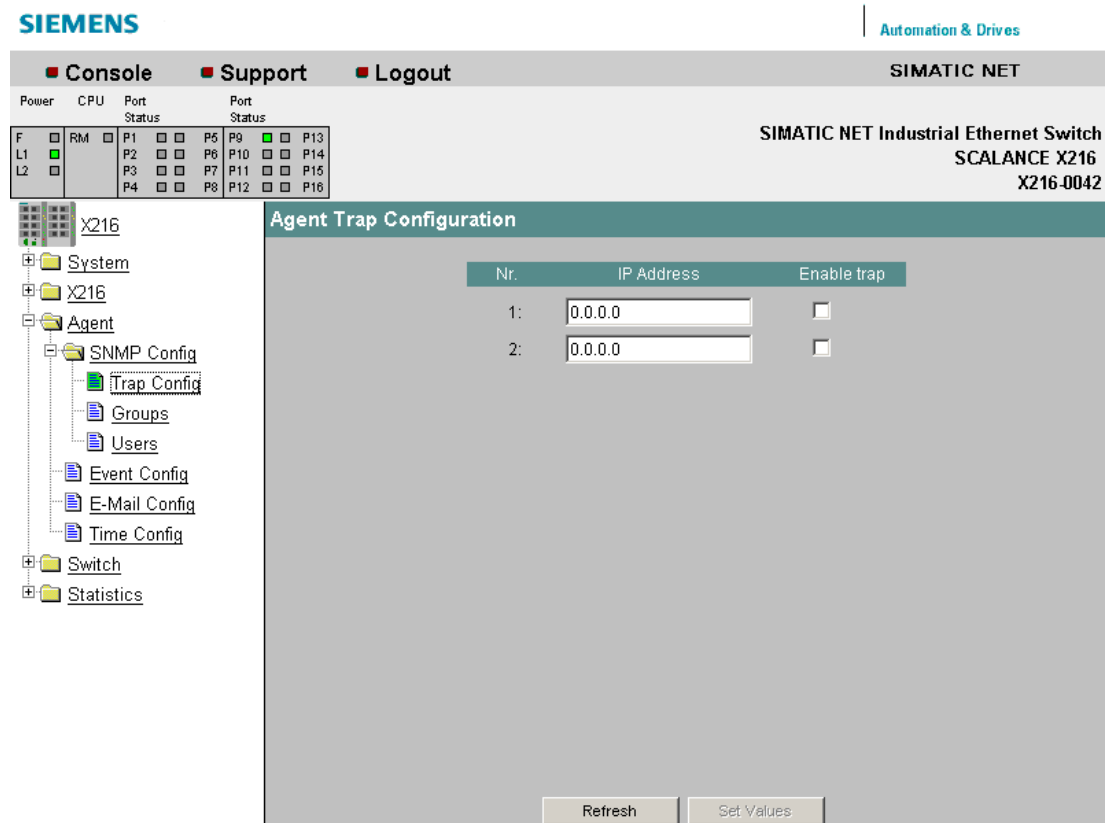


Figure 6-19 Agent Trap Configuration

IP Address

Here, you enter the addresses of the stations to which the IE Switch X-200 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 6-17 Agent Trap Configuration - CLIAGENT\TRAP>

Command	Description	Comment
info	Shows the trap configuration table.	
traps [E D]	Enables / disables traps.	Administrator only
settrap <entry> <IP> <E D>	Enables / disables the trap IP address to be specified.	Administrator only

6.3.5 SNMP Groups

SNMP Configuration Groups

On this page, you create or delete user groups for device access using SNMPv3. You can decide whether or not members of a group need to authenticate themselves, whether they communicate with encryption and whether they have read and write permissions.

The screenshot displays the SIMATIC NET configuration interface for a SCALANCE X204-2LD Industrial Ethernet Switch. The interface includes a top navigation bar with 'Console', 'Support', and 'Logout' options. A left sidebar shows a tree view of the configuration hierarchy: X204-2LD > System > X204-2LD > Agent > SNMP Config > Groups. The main area is titled 'SNMP Group Table' and contains a table with the following data:

Group Name	Auth	Priv	Read	Write
SCALANCE_Admins	x	x	x	x
SCALANCE_Users	x	-	x	x

At the bottom of the main area, there are two buttons: 'New Entry' and 'Refresh'.

Figure 6-20 SNMP Configuration Groups

Syntax of the Command Line Interface

Table 6-18 Agent SNMP Configuration Groups - CLI\AGENT\SNMP\GROUP>

Command	Description	Comment
info	Displays a list of all created SNMPv3 user groups.	
add <Name> [NOAUTH AUTH PRIV] [R W]	Adds an SNMPv3 user group.	Administrator only
edit <index> [NOAUTH AUTH PRIV] [RE RD WE WD]	Changes the properties of an SNMPv3 group. The index of the group to be modified must be obtained with the "Info" command.	Administrator only
delete <index>	Deletes an SNMPv3 group. The index of the group to be deleted must be obtained with the "Info" command.	Administrator only
clearall	Deletes all the SNMPv3 groups that have been created.	Administrator only

6.3.6 SNMP Groups New Entry

SNMP Group Table - new user group

Click the "New Entry" button on the SNMP Group Table page. The page shown below appears. Here, you can create a new SNMPv3 user group:

SIEMENS | Automation & Drives

■ Console ■ Support ■ Logout **SIMATIC NET**

Power CPU Port Status Port Status

F	RM	P1	P2	P3	P4	P5	P6	P7	P8	P9	P10	P11	P12	P13	P14	P15	P16
L1	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
L2	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

SIMATIC NET Industrial Ethernet Switch
SCALANCE X216
X216-0042

SNMP Group Table

Group Name:

Security Level:

Access: ☒ Read ☒ Write

Current Entries Refresh Set Values

Figure 6-21 SNMP Group Table - entry of a new user group

Group Name

Enter the name of the SNMPv3 group you want to create here.

Security Level

Here, you set the required security level for the group you are creating.

No Auth/No Priv	The members of the group do not need to authenticate themselves when accessing the IE Switch X-200 and communicate without encryption.
Auth/No Priv	The members of the group need to authenticate themselves for SNMP access to the IE Switch X-200 but nevertheless communicate without encryption.
Auth/Priv	The members of the group need to authenticate themselves and communicate via an encrypted SNMP connection.

Access

Here, you decide whether the members of the group have read and write permissions.

6.3.7 SNMP Config Users

SNMP User Table

Here, you can create or remove users for access via SNMPv3.

When you create a new user, you need to assign this user to a group. You also need to set the required passwords and the authentication algorithm.

The factory setting is made so that the password corresponds to the relevant user name.

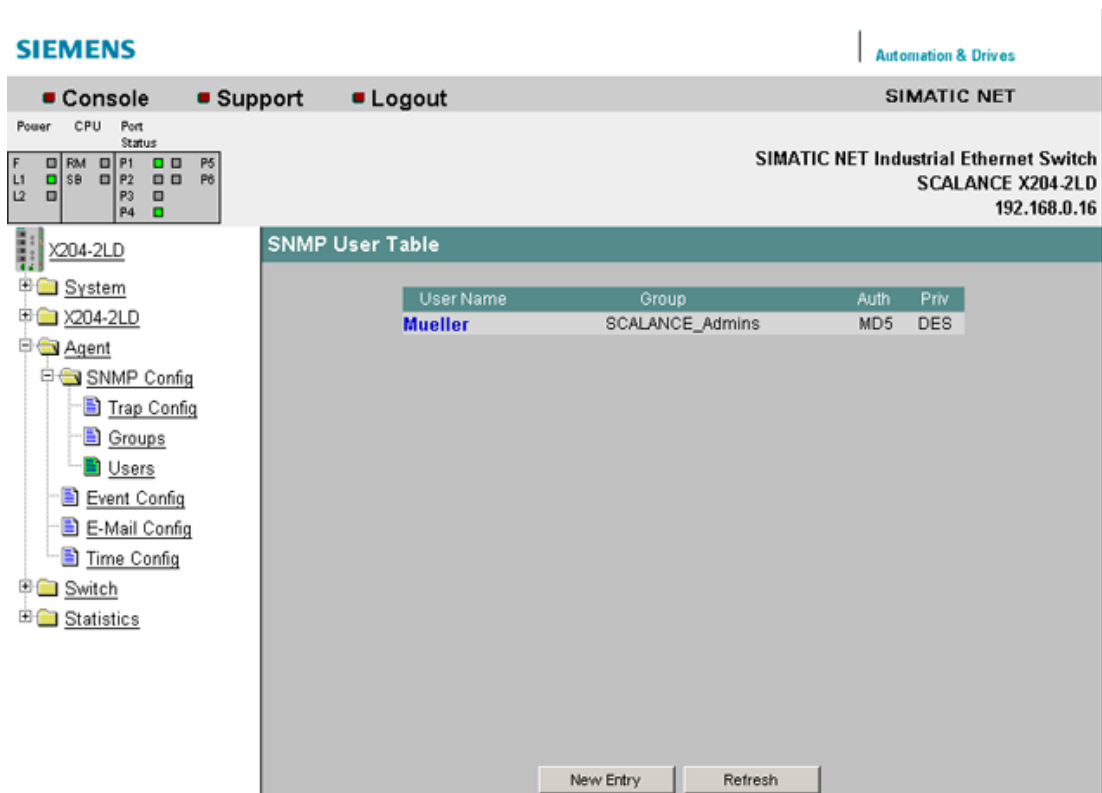


Figure 6-22 Agent SNMP Config Users screen

Syntax of the Command Line Interface

Table 6-19 Agent SNMP Configuration Users - CLIAGENT\SNMP\USER>

Command	Description	Comment
info	Displays a list of all created SNMPv3 users.	
add <user> <group> [NONE MD5 SHA] [Authpass] [Privpass]	Adds a new SNMPv3 user to a user group.	Administrator only
edit <index>[NONE MD5 SHA] [AuthPass][PrivPass])	Changes the properties of an SNMPv3 user. The index of the user to be modified must be obtained with the "Info" command.	Administrator only
delete <index>	Deletes an SNMPv3 user. The index of the user to be deleted must be obtained with the "Info" command.	Administrator only
clearall	Deletes all SNMPv3 users that have been created.	Administrator only

6.3.8 SNMP Users New Entry

Agent SNMP Configuration User Table

Click the "New Entry" button on the SNMP User Table page. The page shown below appears. Here, you can create a new SNMPv3 user:

Figure 6-23 SNMP User Table - new entry

User Name

Enter the name of the user you want to create here.

Group Name

Here, you select the SNMPv3 user group to which the user you are creating will be assigned.

Authentication Algorithm

Here, you select the authentication method that the user will use.

Authentication Password/Password Confirmation

Here, you enter the password with which the user you are creating will log on with the IE switch for SNMPv3 communication.

Privacy Password/Password Confirmation

Here, you specify the password that the user will use for encryption of SNMPv3 communication.

6.3.9 Agent Timeout Configuration

Agent Timeout Configuration

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

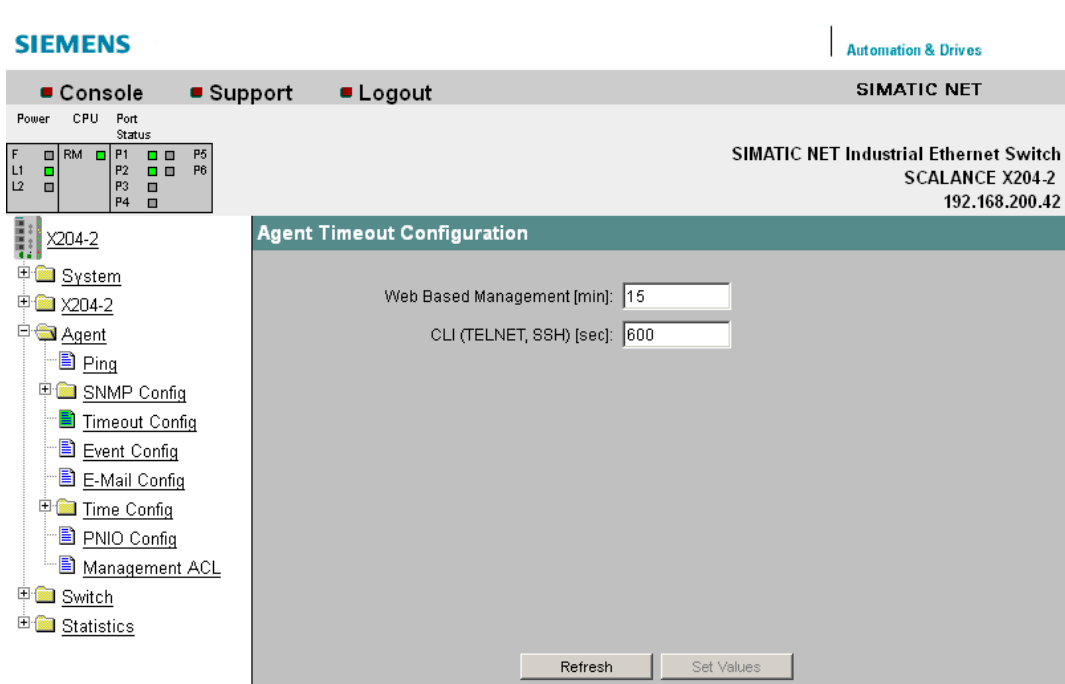


Figure 6-24 Agent Timeout Configuration

Web Based Management [min]

Set the WBM timeout.

Permitted values for the WBM timeout: 0 to 999 minutes

0 means: There is no automatic logout.

CLI (TELNET, SSH, Serial) [sec]

Set the CLI timeout.

Permitted values for the CLI timeout: 60 to 600 seconds

0 means: There is no automatic logout.

Syntax of the Command Line Interface

Table 6-20 Agent Configuration - CLI\AGENT>

Command	Description	Comment
timeout [E D Timeout]	Enable, disable or set the timeout for SSH, TELNET or serial connections. When specifying the value, a range of 60 to 600 seconds is possible.	Administrator only
wbmtime [minutes]	Displays or specifies the time limit after which a WBM connection is reset. A maximum value of 999 minutes can be set. The value 0 disables the time limit.	Administrator only

6.3.10 Event Config

Agent Event Configuration

On this page, you specify how the X-200 IE switch reacts to system events. By selecting the corresponding check boxes, you specify how the X-200 IE switch reacts to the various events. The following options are available:

- The IE Switch X-200 sends an e-mail.
- The IE Switch X-200 triggers an SNMP trap.
- The IE Switch X-200IRT saves the relevant event in the event table.

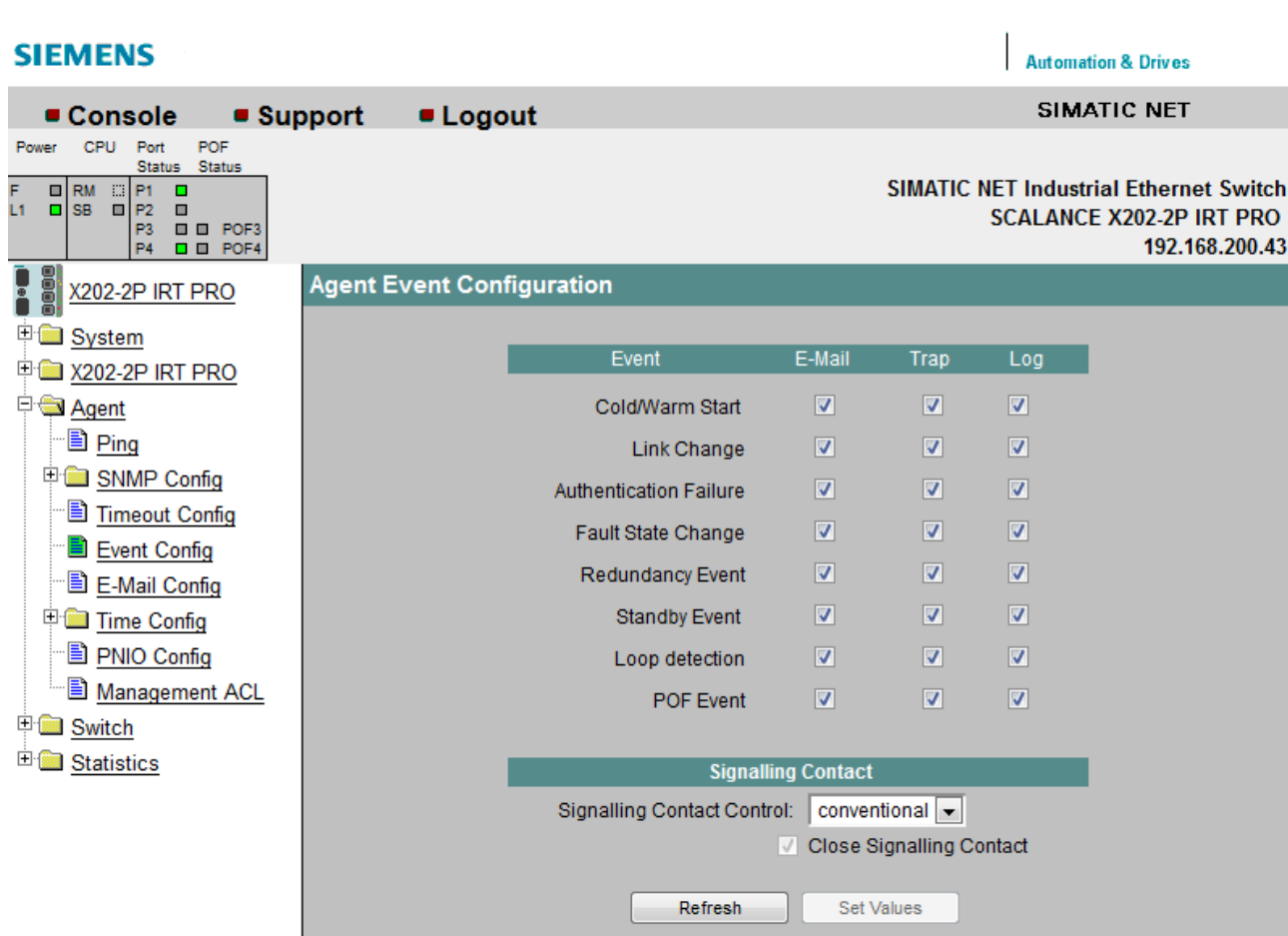


Figure 6-25 Agent Event Configuration

You can configure the reaction of the IE Switch X-200 to the following events:

Cold/Warm Start

The IE Switch X-200 was turned on or reset 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 or Web Based Management access with a bad password or inadequate access rights (refer also to the section "Agent SNMP Configuration").

Power Change (only relevant for devices with a redundant power supply)

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

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.

Redundancy Event

A redundancy event is triggered:

- When the redundant connection is opened or closed
- When a second ring manager is identified.

Standby Event (relevant for IRT devices only)

A standby event is triggered

- When the standby connection is opened or closed
- When the standby partner is lost or returns.

Loop detection

A loop was detected in the network.

FMP Event (only relevant for FM devices, refer to the section "FMP (Page 121)")

The value of the received power or the power loss has exceeded a certain limit.

POF Event (only relevant for devices with POF functionality, refer to the section "POF (Page 130)")

The value of the received power or the power loss has fallen below a certain limit.

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 6-21 Agent Event Configuration - CLI\AGENT\EVENT>

Command	Description	Comment
info	Shows the current event configuration.	
scontrol [C A]	Selects how the signaling contact works: <ul style="list-style-type: none">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, if this in "aligned" mode: <ul style="list-style-type: none">Yes The contact is closed.No: The contact is opened	Administrator only.
setec <Event Index> <E D> <E D> <E D>	Specifies how an IE switch reacts to system events. You can enter the following values for the <Event> parameter:	
	CW	Cold/Warm Start
	LC	Link Change
	AF	Authentication Failure
	PM	Power M12 Change
	FC	Fault State Change
	RD	Redundancy Event
	SB	Standby Event
	LD	Loop Detection
	FM	FMP Event
	PO	POF Event
	<p>If an event is specified, the configured actions are formed for each event.</p> <p>With the two parameters <E> or <D>, you configure the reactions of the IE switch in the order:</p> <ul style="list-style-type: none">E-mailTrapEntry in the log table <p>Example: If you only want to send an e-mail when there is a Link Change, enter the following command: setec LC E D D</p>	

6.3.11 E-Mail Config

Agent E-Mail Configuration - Network monitoring with E-mails

An X-200 IE switch provides you with the option of automatically sending an E-mail (for example to a network administrator) if an alarm event occurs. 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 with the time since the device started up. 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 X-200 and the E-mail address of the recipient is configured.
- the E-mail function is enabled for the relevant event.
- there is an SMTP server in your network that can be reached by the IE Switch X-200.
- the IP address of the SMTP server is entered on the IE Switch X-200.

SIEMENS | Automation & Drives

Console **Support** **Logout** **SIMATIC NET**

Power	CPU	Port Status	Port Status
F	RM	P1	P5
L1		P2	P6
L2		P3	P7
		P4	P8
		P9	P13
		P10	P14
		P11	P15
		P12	P16

SIMATIC NET Industrial Ethernet Switch
SCALANCE X216
X216-0042

Agent E-Mail Configuration

E-Mail Address:

SMTP Server IP Address:

SMTP Server IP Port:

From-Field:

Figure 6-26 E-Mail Configuration

E-Mail Address

Here, you enter the E-mail address to which the IE Switch X-200 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 IP Port

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

"From" Field

You can enter a text that appears in the "From" field of the E-mail.

Send Test E-Mail

Sends an E-mail with the selected parameters.

Syntax of the Command Line Interface

Table 6-22 Agent E-Mail Configuration - CLI\AGENT\EMAIL>

Command	Description	Comment
info	Shows the E-mail configuration.	
mail [E : D]	Enables/disables the mailing function.	Administrator only
smtp [IP address] [:port]	Specifies the IP address and the port number of the SMTP server.	Administrator only
from [address]	Specifies a text that will be entered in the "From" field of the E-mail.	Administrator only
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
testmail <test E-mail comment>	Sends an E-mail for testing.	Administrator only

6.3.12 Time Config**Agent Time Client Configuration**

The time-of-day protocols are set on this page.

Note

The content of this page depends on the selection in the "Time Client Type" box.

Note**Time-of-day synchronization**

SCALANCE X-200 IE switches do not have a quartz clock for their internal time of day. This means that the speed of the clock can vary by more than 1 second a day between two different devices.

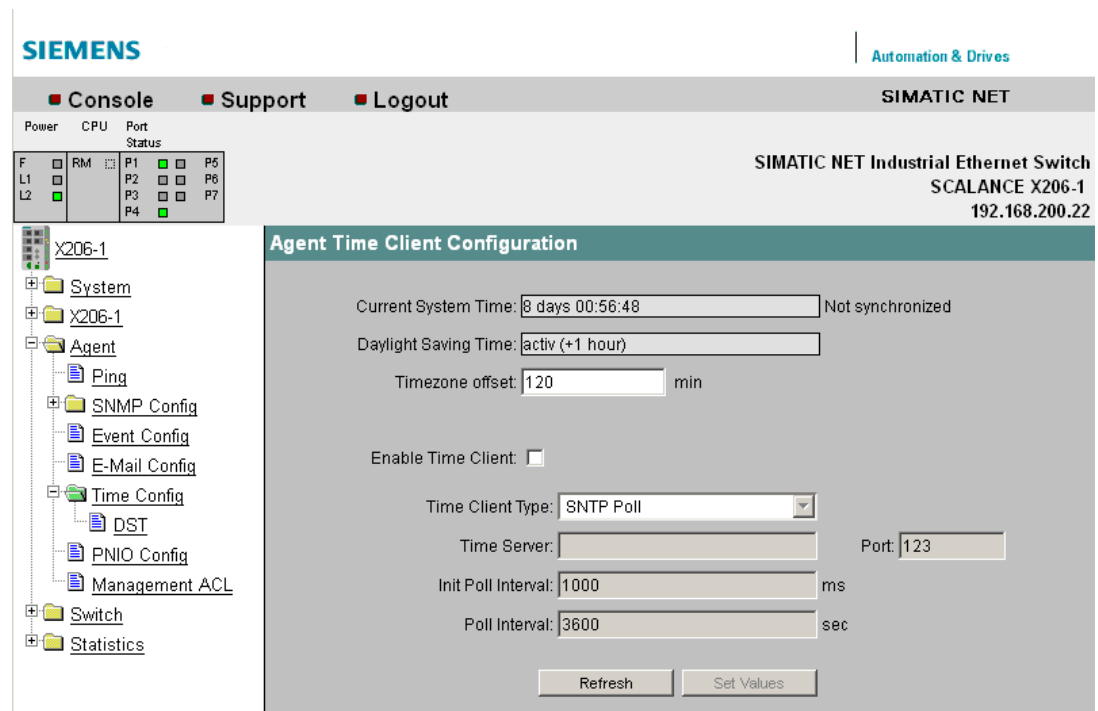


Figure 6-27 Agent Time Client Configuration - "SNTP Poll" selected

Current System Time

Here, either the time since the last restart or the current time is shown. If "Not synchronized" is displayed, the time was set manually. "Not synchronized" is also displayed if SNTP Poll is enabled and if no connection could be established to the server with the last poll.

Daylight Saving Time

Shows whether the daylight saving time changeover is active:

- active (+1 hour)
The time in the "Current System Time" is daylight saving time.
- inactive (+0 hours)
The time in the "Current System Time" is not daylight saving time.

Timezone Offset

Enter the deviation between your time zone and coordinated universal time (UTC) in minutes.

Enable Time Client

The time function can be enabled and disabled here.

Time Client Type

You can choose from four different protocol types here:

- SNTP Poll
If you choose this protocol type, you have to make further settings: Timezone offset, Time server, Init poll interval, Poll interval.
- SNTP Listen
No further settings are possible in this mode.

- **SIMATIC Time**
If you use the SIMATIC time transmitter, you do not need to make any further settings.
- **Manual**
If you have selected this protocol type, the "Set Time" input box is displayed. Enter the current values for day, month, year and time in the "Set Time" input box.
When turning off or resetting the device, this information is lost and must be set again.
- **NTP**
With this setting, time synchronization uses the Network Time Protocol according to RFC 958.
The additional settings are described below.

Time Server

Enter the Internet address of the server with which the system time will be synchronized.

Port

Enter the number of the UDP port being used. As default, the SNTP protocol uses UDP port 123.

Init Poll Interval

Here, you can enter the interval at which the X-200 IE switch repeats the initial poll for the system time if this was not successful the first time.

Range of values: 1000 - 100000

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.

Range of values: 10 - 100000

Additional settings if "NTP" is selected:

SIEMENS Automation & Drives

Console Support Logout SIMATIC NET

Power CPU Port Status

F L1 L2 RM P1 P2 P3 P4 P5 P6

X204-2

System

X204-2

Agent

Ping

SNMP Config

Event Config

E-Mail Config

Time Config

DST

PNIO Config

Management ACL

Switch

Statistics

Agent Time Client Configuration

Current System Time: 2013/07/07 13:13:05 Not synchronized

Daylight Saving Time: activ (+1 hour)

Timezone offset: 120 min

Enable Time Client: ☒

Time Client Type: NTP

NTP Server Addresses

No.	IP Address	Auth	Key ID	Key
1:	192.168.200.20	MD5	1111	****
2:	0.0.0.0	MD5	1111	****
3:	0.0.0.0	MD5	1111	****
4:	0.0.0.0	MD5	1111	****

Enable Secure NTP: ☐

NTP Client Configuration

Poll Interval: 20 sec

Init Poll Interval: 1000 msec

Refresh Set Values

Figure 6-28 Agent Time Client Configuration - "NTP" selected

IP address

Enter the IP address of the NTP server with which the client will synchronize its time-of-day. You can specify up to four different NTP servers.

Auth

Select how the frames for time-of-day synchronization will be signed. You have the two options: MD5 and SHA.

Key ID

Enter the key ID to be used for signing.
Permitted values for the key ID: 1-65534.

Key

Enter the key to be used for signing.

6.3 The Agent menu

Permitted values for the key: an ASCII string with up to 11 characters or a hexadecimal string with up to 40 characters.

Enable Secure NTP

Select this function to check the signing of the frames.

Syntax of the Command Line Interface

Table 6-23 Agent Time Client Configuration - CLI\AGENT\TIME>

Command	Description	Comment
info	Displays information on the time settings of the IE switch.	
timec [E D]	Enables / disables the time settings of the IE switch.	Administrator only
server [IP address] [:port]	Sets the IP address and the port of the server.	Administrator only
tinitpoll [1000 - 100000ms]	Specifies the time during two time polls if no time information has yet been received. You can enter a value between 1000 and 100000 milliseconds.	Administrator only
tpoll [10 - 100000sec]	Specifies the time between two time polls. You can enter a value between 10 and 100000 seconds.	Administrator only
ttype [P L S N M]	Specifies how the time is set: - P SNTP Poll - L SNTP Listen - S Siemens - N NTP - M Manual.	Administrator only
time [date] [time]	If no parameters are set, this command shows the time. By entering a time in the format MM/DD/YYYY hh:mm:ss You set the time.	Administrator only
offset [+/-] <offset>	Specifies the deviation between coordinated universal time (UTC) in minutes.	Administrator only

Table 6-24 Agent Time Client Configuration - CLI\AGENT\TIME\NTP>

Command	Description	Comment
server <number> <IP>	Specifies the IP address of the NTP server indicated by "number". You can specify IP addresses for a maximum of four NTP servers.	Administrator only
initint [1 ... 10000]	Specifies the time between two NTP polls if no time information has yet been received. You can enter a value between 1 and 10000 milliseconds.	Administrator only
interval [1 ... 160]	Specifies the interval between two NTP polls. You can enter a value between 1 and 160 seconds.	Administrator only

Command	Description	Comment
secure <server no.> <Key-ID> <MD5 SHA> <key>	Specifies the key ID, the hash algorithm and the key for secure communication with the NTP server.	Administrator only
security [E D]	Enables / disables checking the signature for communication with the NTP server.	Administrator only

6.3.13 Daylight Saving Time

Daylight Saving Time Table

On this page, you can control the daylight saving time changeover so that the system time is correctly set for the local time zone.

You can define a rule for the daylight saving time changeover or specify a fixed date.

The screenshot shows the Siemens SIMATIC NET configuration interface. The top bar includes the Siemens logo, 'Automation & Drives', and navigation links for Console, Support, and Logout. The main header identifies the device as 'SIMATIC NET Industrial Ethernet Switch SCALANCE X204-2' with IP address '192.168.200.42'. A status bar at the top left shows Power, CPU, and Port Status indicators.

The left sidebar displays a tree view of the configuration hierarchy: X204-2 > System > X204-2 > Agent. Under the Agent menu, various configuration options are listed: Ping, SNMP Config, Event Config, E-Mail Config, Time Config, DST, PNIO Config, and Management ACL. The 'Time Config' option is currently selected.

The main content area is titled 'Daylight Saving Time Table'. It contains a table with the following data:

Nr.	Year	Start	End	Rec
1	2013	02\23 02h	02\25 23h	x
2	2013	03\12 02h	06\12 02h	-

At the bottom of the table, there are three buttons: 'New Entry', 'Refresh', and 'Set Values'.

Figure 6-29 Daylight Saving Time Table

The table shows you an overview of the existing entries for the daylight saving time changeover. As soon as the end date of an entry is exceeded, if a rule is defined, the data for the next changeover is displayed. With fixed entries, the row is deleted.

Nr.

Shows the number of the entry.

If you create a new entry, a new row is created with a unique number.

Year

Shows the year for which the entry was created.

Start

Shows the month, day and time for the start of daylight saving time.

End

Shows the month, day and time for the end of daylight saving time.

Rec

Shows whether or not a rule was defined for the daylight saving time changeover:

- x
A rule was defined for the daylight saving time changeover.
- -
A fixed date was entered for the daylight saving time changeover.

Daylight Saving Time Table New Entry

Click the "New Entry" button on the "Daylight Saving Time Table" page.

Note

The content of this page depends on the selection in the "Type" box.

Type

Select how the daylight saving time changeover is made:

- **Recurring**
You can define a rule for the daylight saving time changeover.
This setting is suitable for regions in which the daylight saving time always begins or ends on a particular weekday.
- **Date**
You can define a fixed date for the daylight saving time changeover.
This setting is suitable for regions in which there is no rule governing the daylight saving time changeover.

Settings with "Recurring" selected

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

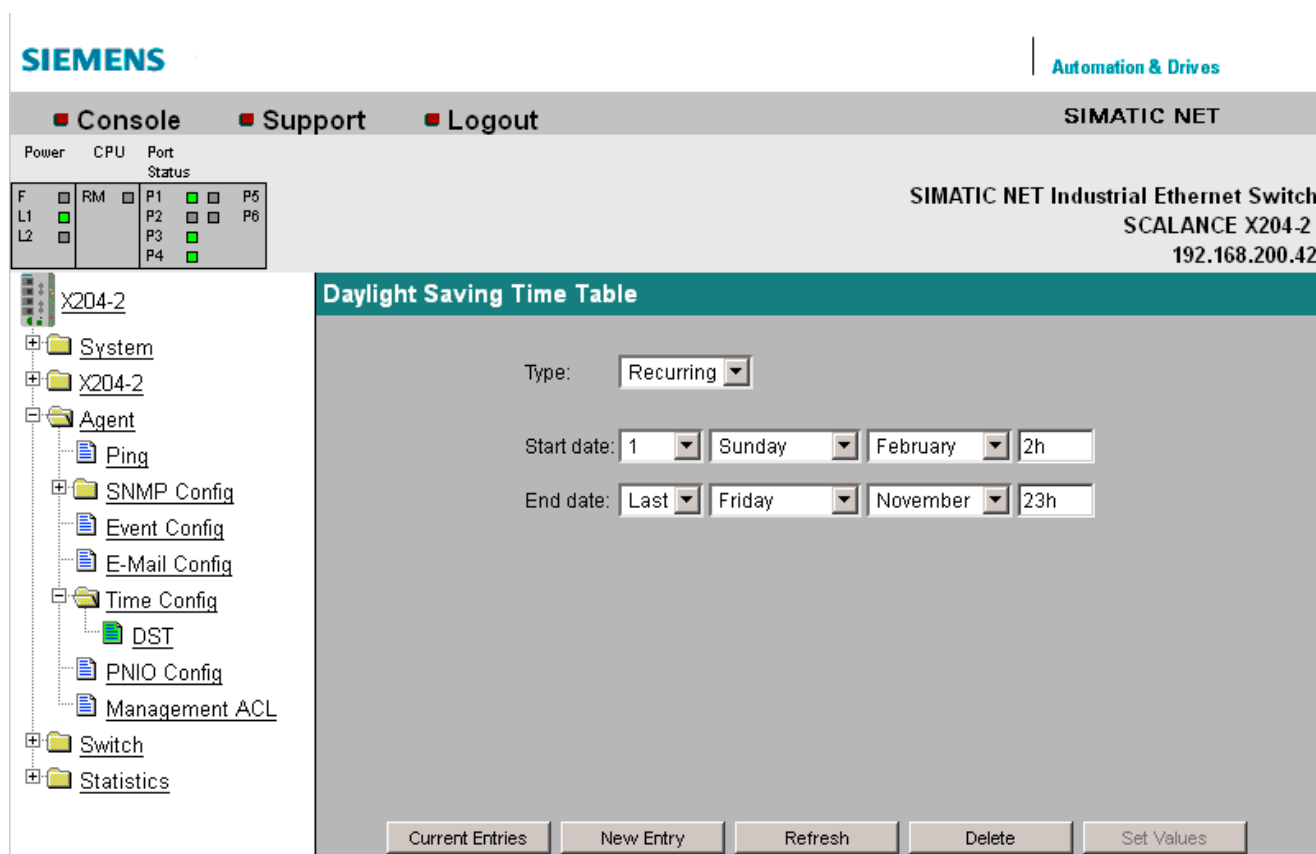


Figure 6-30 Daylight Saving Time Table - new entry "Recurring"

Start date

Enter the following values for the start of daylight saving time:

- Week of the month
You can select the 1st to 5th or the last week of the month.
- Weekday
- Month
- Time of day in hours

End date

Enter the following values for the end of daylight saving time:

- Week of the month
You can select the 1st to 5th or the last week of the month.
- Weekday
- Month
- Time of day in hours

Settings with "Date" selected

You can set a fixed date for the start and end of daylight saving time.

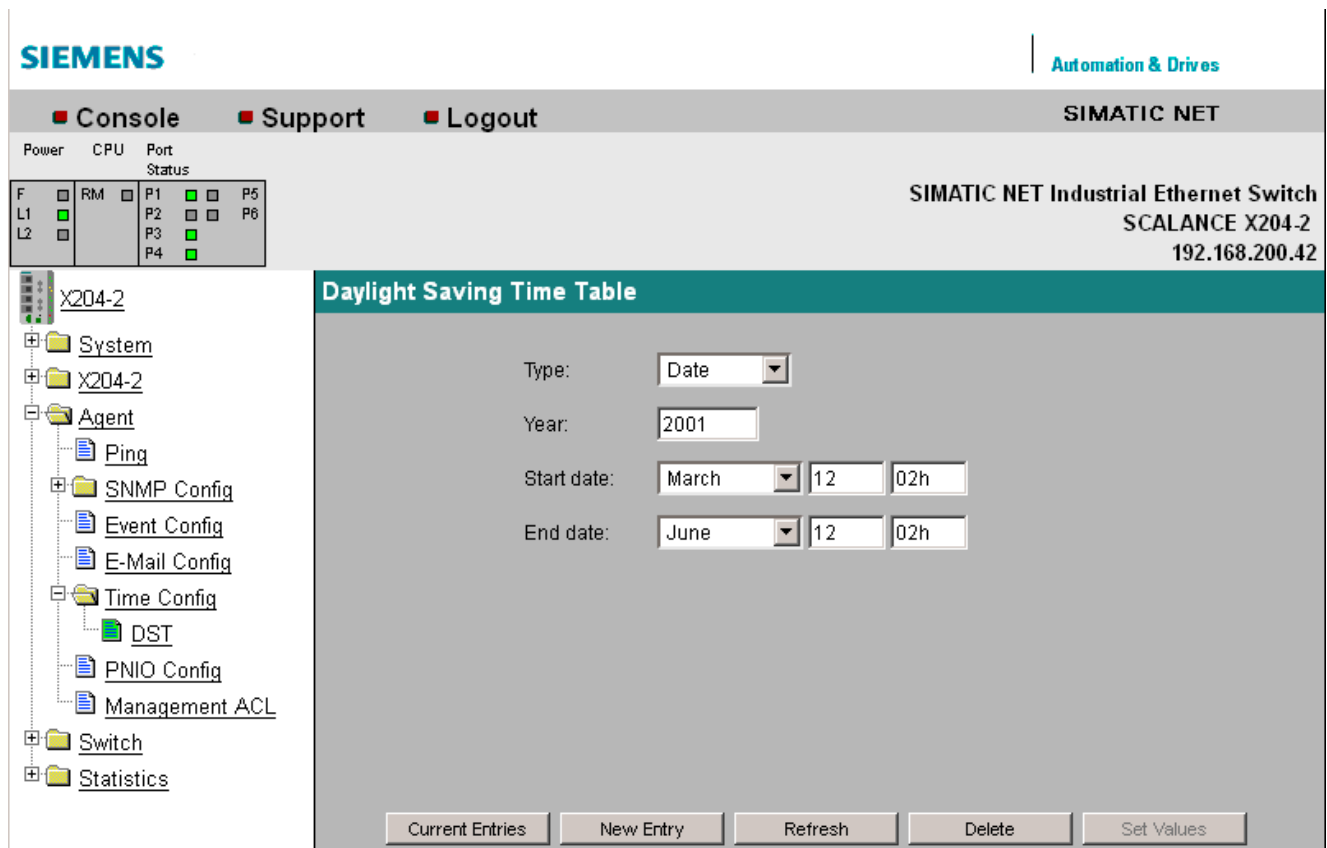


Figure 6-31 Daylight Saving Time Table - new entry "Date"

Year

Enter the year for the daylight saving time changeover.

Start date

Enter the following values for the start of daylight saving time:

- Month
- Day
- Time of day in hours

End date

Enter the following values for the end of daylight saving time:

- Month
- Day
- Time of day in hours

Syntax of the Command Line Interface

Table 6-25 Daylight Saving Time Table - CLI\AGENT\TIME\DST>

Command	Description	Comment
info	Shows information about the time zone and the daylight saving time changeover.	
recurring <start date> <end date>	Creates an entry of the type "Recurring". You need to enter the following information for the <start date > and <end date >: <ul style="list-style-type: none"> • 1-5 or Last • Weekday • Month • Hour 	Administrator only Example: recurring last sunday march 02 last sunday october 03
date <yyyy> <start date> <end date>	Creates an entry of the type "Date". For the <start date> and <end date> parameters, enter the month, day and hour in the following form: <ul style="list-style-type: none"> • mmddhh 	Administrator only Example: date 2010 040102 100103
delete <index>	Deletes an entry. The index of the entry to be deleted must be obtained with the "info" command.	Administrator only

6.3.14 PNIO Config

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.

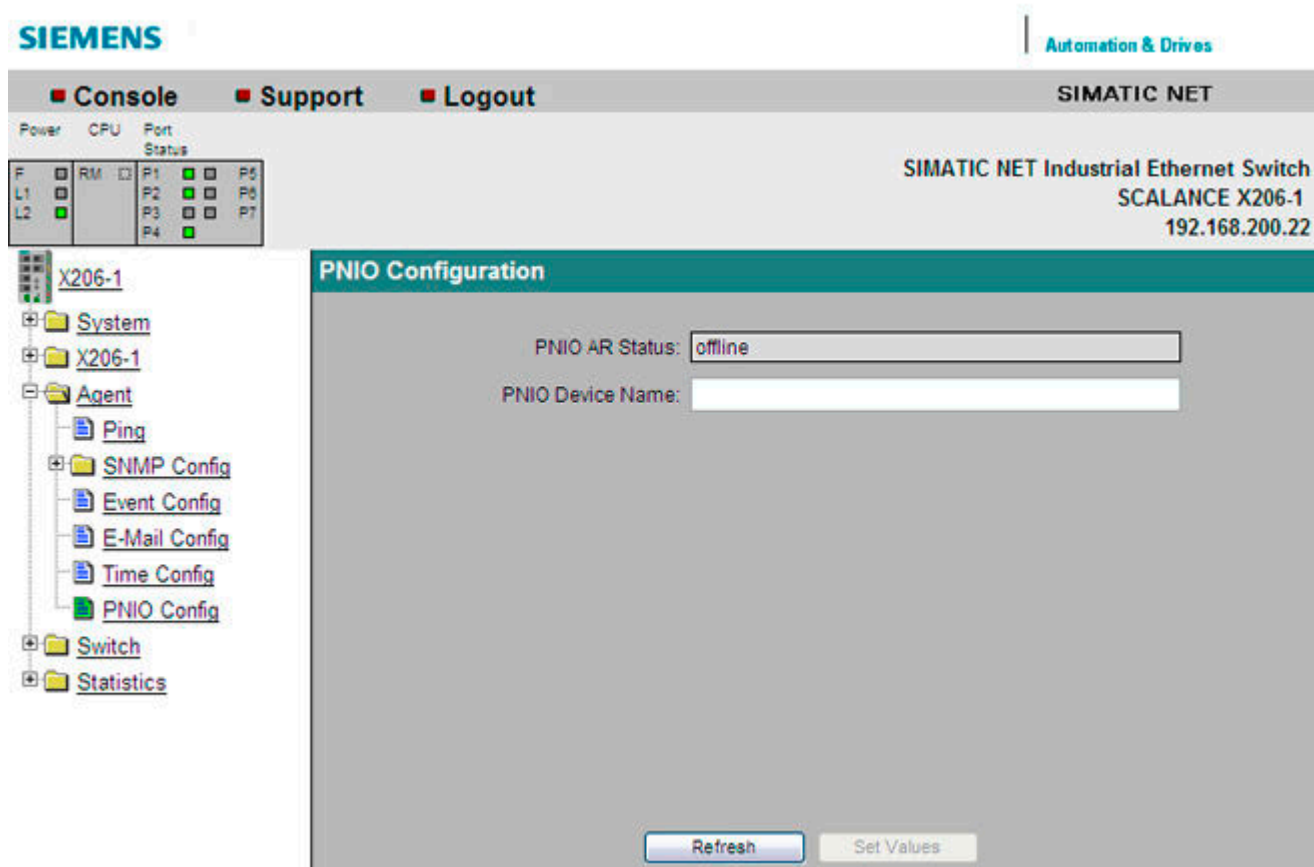


Figure 6-32 PNIO Configuration

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.

Syntax of the Command Line Interface

Table 6-26 PNIO Configuration - CLI\AGENT\PNIOCONF>

Command	Description	Comment
info	Shows the current PROFINET IO configuration	-
devname [string]	Sets the PROFINET IO device name.	Administrator only.

6.3.15 Management ACL

Management ACL

On this page you can define rules for access to the management of your IE switch.

Note

A bad configuration may mean that you can no longer access your device. You should therefore configure an access rule that allows access to the management before you enable the function, see section Agent (Page 84).

Note

The configured access rules are only taken into account when the function is enabled.

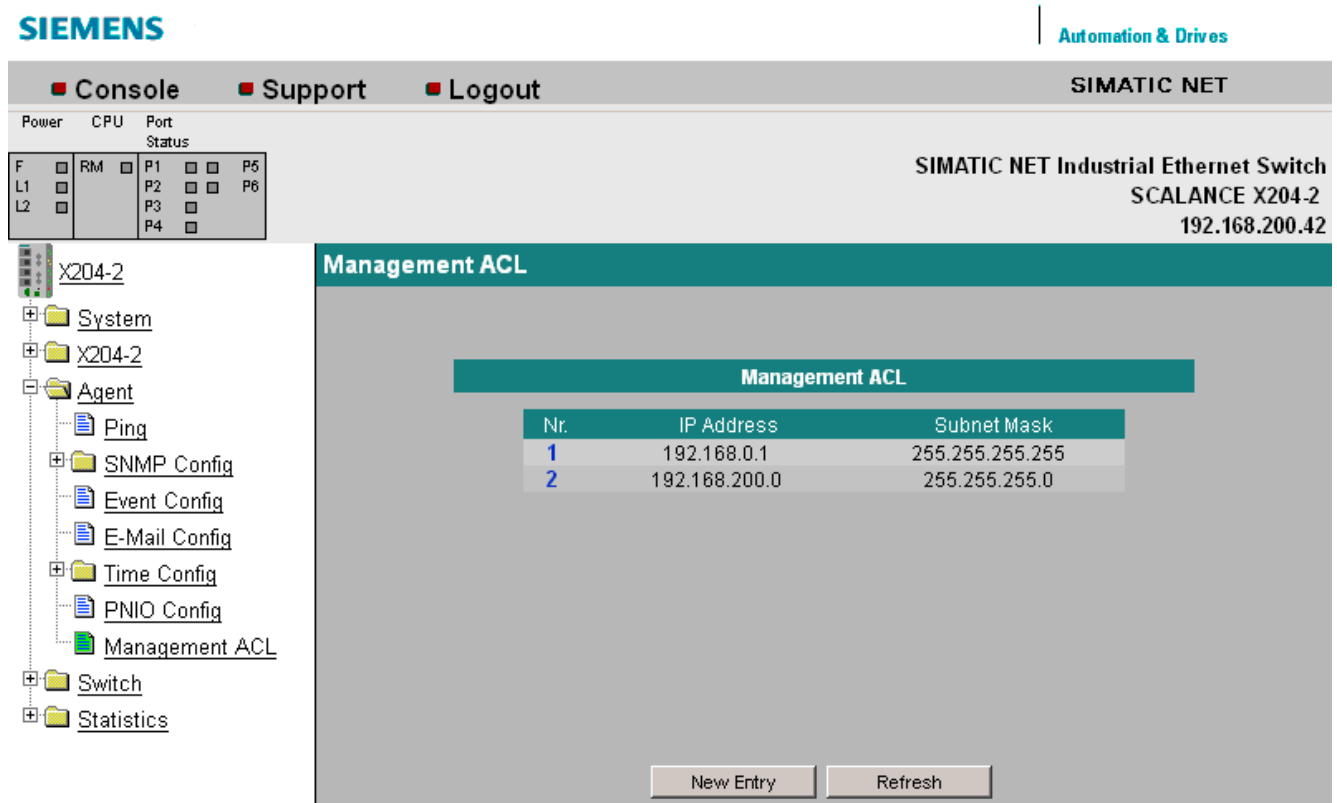


Figure 6-33 Management ACL

Nr.

Shows the number of the access rule.
If you define a new access rule, a new row with a unique number is created.

IP Address

Shows the IP address to which the access rule applies.

Subnet Mask

Shows the subnet mask to which the access rule applies.

Management ACL New Entry

Click the "New Entry" button on the "Management ACL" page. The page shown below appears. Here, you can create a new access rule.

SIEMENS | Automation & Drives

Console Support Logout SIMATIC NET

Power CPU Port Status

F	RM	P1	P5
L1		P2	P6
L2		P3	
		P4	

SIMATIC NET Industrial Ethernet Switch
SCALANCE X204-2
192.168.200.42

Management ACL

IP address: 192.168.200.0

Subnet mask: 255.255.255.0

Services

SNMP: <input checked="" type="checkbox"/>	TELNET: <input type="checkbox"/>	HTTP: <input checked="" type="checkbox"/>
HTTPS: <input type="checkbox"/>	SSH: <input checked="" type="checkbox"/>	ICMP: <input type="checkbox"/>

Ports

Port 1	<input checked="" type="checkbox"/>	Port 5	<input type="checkbox"/>
Port 2	<input type="checkbox"/>	Port 6	<input type="checkbox"/>
Port 3	<input type="checkbox"/>		
Port 4	<input type="checkbox"/>		

Current Entries Refresh Set Values

Figure 6-34 Management ACL - new entry

IP Address

Enter the IP address to which the access rule applies.
If you use the IP address 0.0.0.0, the settings apply to all IP addresses.

Subnet Mask

Enter the subnet mask to which the access rule applies.
The subnet mask 255.255.255.255 is for a specific IP address. The subnet mask 0.0.0.0 applies to all subnets. If you want to allow a specific subnet, for example a C subnet, enter 255.255.255.0.

Services

Enable the services via which the device may be accessed.

Ports

Enable the ports via which the device may be accessed.

Syntax of the Command Line Interface

Table 6-27 Management ACL - CLIAGENT\MACL>

Command	Description	Comment
info	Displays the current settings of the management ACL.	
add [IP address] [Subnet Mask]	Creates a new entry in the management ACL.	Administrator only
delete [IP address] [Subnet Mask]	Removes an entry from the management ACL.	Administrator only
ports [IP address] [Subnet Mask] <E D> [port]	Specifies the ports via which the device may be accessed.	Administrator only
services [IP address] [Subnet Mask] <E D> [service]	Specifies the protocols that can be used to access the device.	Administrator only

6.4 The Switch menu

6.4.1 Switch

Port Mirroring

Note

valid for all SCALANCE X-200IRT modules

Disable the function "Port Mirroring" if you want to operate the device in IRT mode. IRT mode is not possible when the mirroring function is enabled.

At this point, you can enable or disable port mirroring; in other words, mirroring the data traffic from the mirror port to the monitor port.

Apart from the device be monitored, no other communication node should be connected to the monitor port.

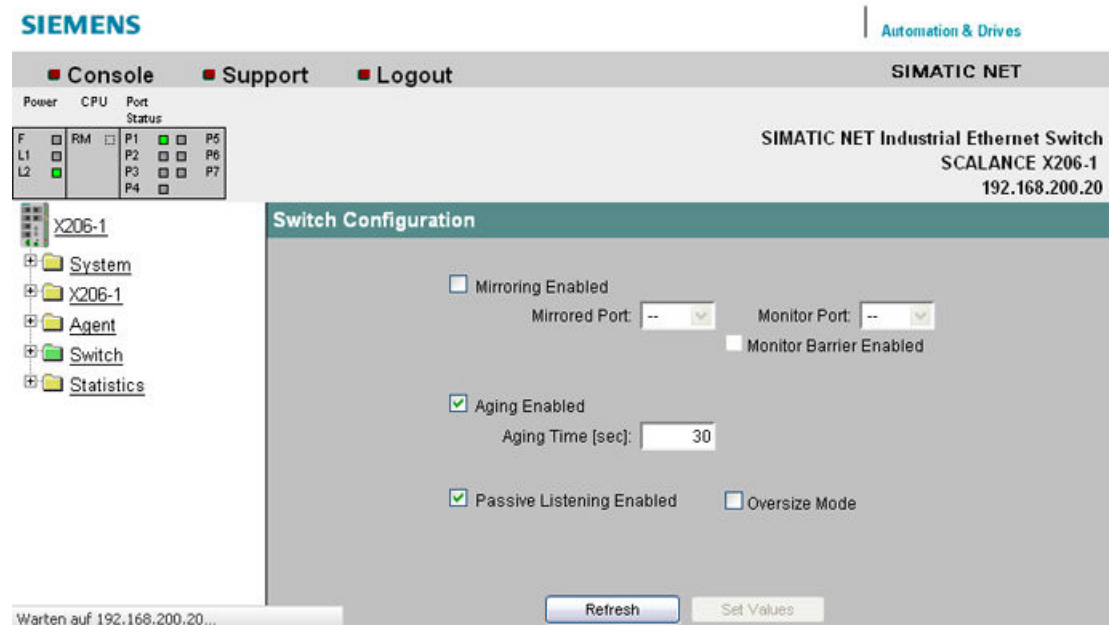


Figure 6-35 Switch Configuration (Port Mirroring)

Mirroring Enabled

Clicking this check box enables or disables the mirroring function.

Mirrored Port

Under mirrored port, enter the port to be monitored.

Monitor Port

Under monitor port, enter the port to be monitored.

Monitor Barrier Enabled

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

Passive Listening Enabled

With this check box, you enable/disable the "Passive Listening" function. If "Passive listening" is enabled, the IE switch deletes its MAC address table when it receives an STP topology change frame. The IE switch also forwards STP BPDUs. If "Passive Listening" is disabled, all received STP frames are discarded.

Note

When an STP Topology Change frame is received, the MAC address table on the X-200 is deleted within 1 second.

With IRT devices, the time needed for the delete action depends on the number of entries.

See also section "Spanning tree, media redundancy and passive listening (Page 35)".

Oversize Mode

Only relevant for devices **without** the IRT function.

If you select this check box, frames with a size up to 1,632 bytes instead of 1,532 bytes are permitted.

Aging

Clicking the check box here disables the aging function. The aging time can be set in seconds.

Note

If the aging function is disabled, communication problems will occur when connected nodes are plugged into different ports. In normal mode, the aging function should therefore remain enabled.

Note

Note the following for all X-200IRT IE switches:

With the "Port Mirroring" function and cyclic PROFINET data traffic, the mirror port (monitor port) only shows the frames received at the monitored port (mirrored port). Non-cyclic frames mean that PROFINET communication is not involved and, in this case therefore, both sent and received packets are shown at the mirror port (monitor port).

Syntax of the Command Line Interface

Table 6-28 Switch Configuration (Ports Mirroring) - CLI\SWITCH>

Command	Description	Comment
info	Displays information on the IE switch configuration.	
mirrored [port]	Specifies the port for mirroring.	Administrator only
monitor [Port]	Specifies the port for the protocol monitor.	Administrator only
mirroring [E D]	Enables / disables mirroring.	Administrator only
barrier [E D]	Enables/disables communication via the mirror port.	Administrator only
plisten [E D]	Enables/disables passive listening	Administrator only
oversize [E D] *)	Enables/disables the oversize mode function	Administrator only
aging [E D] Aging time]	Enables/disables whether or not the aging time of the switch can be set.	Administrator only

*) Only relevant for devices **without** the IRT function.

6.4.2 Ports

Switch Ports

This page informs you about the current status of the ports. You can also make various port settings.

SIEMENS | Automation & Drives

Console Support Logout SIMATIC NET

Power CPU Port Status Port Status

SIMATIC NET Industrial Ethernet Switch
SCALANCE X216
X216-0042

Switch Ports Status

Port	Type	Mode current	Mode must be	Status current	Status must be	Link
1	TP 100 TX	10M HD	AutoNeg	forwarding	Enabled	down
2	TP 100 TX	10M HD	AutoNeg	forwarding	Enabled	down
3	TP 100 TX	10M HD	AutoNeg	forwarding	Enabled	down
4	TP 100 TX	10M HD	AutoNeg	forwarding	Enabled	down
5	TP 100 TX	10M HD	AutoNeg	forwarding	Enabled	down
6	TP 100 TX	10M HD	AutoNeg	forwarding	Enabled	down
7	TP 100 TX	10M HD	AutoNeg	forwarding	Enabled	down
8	TP 100 TX	10M HD	AutoNeg	forwarding	Enabled	down
9	TP 100 TX	100M FD	AutoNeg	forwarding	Enabled	up
10	TP 100 TX	10M HD	AutoNeg	forwarding	Enabled	down
11	TP 100 TX	10M HD	AutoNeg	forwarding	Enabled	down
12	TP 100 TX	10M HD	AutoNeg	forwarding	Enabled	down
13	TP 100 TX	10M HD	AutoNeg	forwarding	Enabled	down
14	TP 100 TX	10M HD	AutoNeg	forwarding	Enabled	down
15	TP 100 TX	10M HD	AutoNeg	forwarding	Enabled	down
16	TP 100 TX	10M HD	AutoNeg	forwarding	Enabled	down

Refresh Set Values

Figure 6-36 Switch Ports Status

Port

Shows the port number.

Type

Displays the type of port.

The following port types are available with the IE Switch X-200 modules:

- TP 10 TX
- TP 100 TX
- FO 100 FX

Mode

Shows transmission rate (10 or 100 Mbps) and the transmission mode (full duplex (FD) or half duplex (HD)).

Negotiation

Indicates whether autonegotiation is enabled or disabled.

Status

Indicates that the port is enabled.

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.

Note

With X-200 IE switches, that are not IRT-compliant, it is not possible to disable ports in PROFINET mode!

If a port of such a device is disabled by Web Based Management, the disabled setting is overwritten when a PROFINET configuration is downloaded. In PROFINET mode, all ports of a non IRT-compliant X-200 IE switch are automatically enabled.

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.

If an IE switch port is set permanently to full duplex, the connected partner device must also be set to full duplex.

If the autonegotiation function is disabled, the MDI/MDI-X autocrossover function is also inactive. This means it may be necessary to use a crossover cable.

Syntax of the Command Line Interface

Table 6-29 Switch Port Status - CLI|SWITCH>

Command	Description	Comment
ports	Displays the port status.	Administrator only

Table 6-30 Switch Ports Status - CLI|SWITCH|SETPORT>

Command	Description	Comment
info	Displays the current port settings.	
enable <port> [D E]	Enables / disables the specified port.	Administrator only

Command	Description	Comment
speed <port> [10 100 A]	Specifies the port speed: <ul style="list-style-type: none">• 10 - 10 Mbps• 100 - 100 Mbps• A - Autonegotiation. If autonegotiation is set, the setting applies for speed and duplicity.	Administrator only.
duplex <port> [H F A]	Specifies the port duplexity: <ul style="list-style-type: none">• H - half• F - full• A - autonegotiation If autonegotiation is set, the setting applies for speed and duplicity.	Administrator only

6.4.3 FMP

Requirements

- You can only use fiber monitoring with transceivers capable of diagnostics. Devices and modules with transceivers capable of diagnostics have the supplement "FM" in the name. Note the documentation of the devices.
- To be able to use the Fiber Monitoring (FM) function, enable LLDP. The FM information is appended to the LLDP packets.

Monitoring optical links

With Fiber Monitoring, you can monitor the received power and the loss of power on optical links between two switches.

If you enable fiber monitoring on an optical port, the device sends the current transmit power of the port to its connection partner using LLDP packets. In addition to sending, the device also checks whether corresponding information is received from the connection partner.

Regardless of whether the IE switch receives diagnostics information, it monitors the received power measured at the optical port for the set limit values.

If fiber monitoring is enabled on the connection partner, the connection partner transfers the current value for the transmit power of the port to the device. The device compares the value it has received for the transmit power with the actually received power. The difference between the received power and the transmit power represents the power loss on the link. The calculated power loss is also monitored for the set limit values.

If the value of the received power or the power loss falls below or exceeds the set limit values, an event is triggered. You can set limit values in two stages. In "Agent > Event Configuration", you can specify how the IE switch indicates the event. In "X-200 > Fault Mask", you can also specify whether or not an error should be signaled.

SIEMENS Automation & Drives

Console Support Logout SIMATIC NET

Power CPU Port Status

F L1 L2 RM P1 P2 P3 P4 P5 P6

X204-2FM

System

X204-2FM

Agent

Switch

Ports

FMP

Cable Tester

FDB

ARP Table

LLDP

DCP

Loop Detection

Statistics

Fiber Monitoring Protocol

Port	Rx Power Maintenance [1/10 dBm]		Power loss Maintenance [1/10 dB]	
	required	demand	required	demand
5	-230	-270	-100	-130
6	-230	-270	-100	-130

Port	State	Rx Power State	Rx Power [dBm]	Power loss State	Power loss [dB]
5	enabled	ok	-18.9	ok	-5
6	enabled	maintenance required	-25.2	idle	0

Refresh Set Values

Figure 6-37 Fiber Monitoring Protocol

Setting the power limits

In the first table, you can set the limits for the received power and the power loss for the available ports.

Port

Shows the available optical ports.

Rx Power Maintenance [1/10 dBm]

- required**
 Enter the value at which you want to be informed of deterioration of the received power the first time.
 If you enter the value 0, the received power is not monitored.
- demand**
 Enter the value at which you want to be informed of deterioration of the received power the second time.
 If you enter the value 0, the received power is not monitored.

Power loss Maintenance [1/10 dB]

- **required**
Enter the value at which you want to be informed about the power loss of the connection the first time.
If you enter the value 0, the power loss is not monitored.
- **demanded**
Enter the value at which you want to be informed about the power loss of the connection the second time.
If you enter the value 0, the power loss is not monitored.

Setting and status of the ports

In the second table, you can enable or disable Fiber Monitoring for the available ports and monitor the status of the ports.

Port

Shows the available optical ports.

State

Enable or disable FM.

Rx Power State

- **disabled**
FM is disabled.
- **ok**
The value for the received power of the optical link is OK.
- **maintenance required**
Check the link.
An event is triggered.
- **maintenance demanded**
The link needs to be checked.
An event is triggered and the fault LED is lit yellow.
- **link down**
The connection is interrupted.

Rx Power [dBm]

Shows the current value of the received power.

The value can have a tolerance of +/- 3 dB.

Power loss State

To be able to monitor the power loss of the connection, the port requires a link to another port with FM enabled.

- **disabled**
FM is disabled.
- **ok**
The value for the power loss of the optical link is OK.

6.4 The Switch menu

- **maintenance required**
Check the link.
An event is triggered.
- **maintenance demanded**
The link needs to be checked.
An event is triggered and the fault LED is lit yellow.
- **idle**
The port has no connection to another port with FM enabled.
If no diagnostics information has been received for 5 cycles, the connection counts as being interrupted. A cycle lasts 5 seconds.

Power loss [dB]

Shows the current value of the power loss.

The value can have a tolerance of +/- 3 dB.

Syntax of the Command Line Interface

Table 6-31 Fiber Monitoring Protocol - CLI\SWITCH\FMP>

Command	Description	Comment
info	Shows the FM configuration.	
limit [rx loss] [req dem] [<port>] [<limit>]	Specifies the limits for the received power and the power loss per port: <ul style="list-style-type: none"> • rx Received power • loss Power loss • req First notification • dem Second notification • port Port for which the settings apply • limit Value for the limit in 1/10 dBm (received power) or 1/10 dB (power loss) 	Administrator only If you enter the value 0, the received power or power loss is not monitored.
enable <D E> [<Port>]	Enables / disables FM for the specified port.	Administrator only

Table 6-32 Fiber Monitoring - CLI\SWITCH\FM>

Command	Description	Comment
info	Shows general information about the transceivers, for example model, serial number and current values, e.g. received and transmit power.	

Diagnostics of the received power

The diagnostics page shown below appears if you click on the value of the received power. It shows the values of the received power over time.

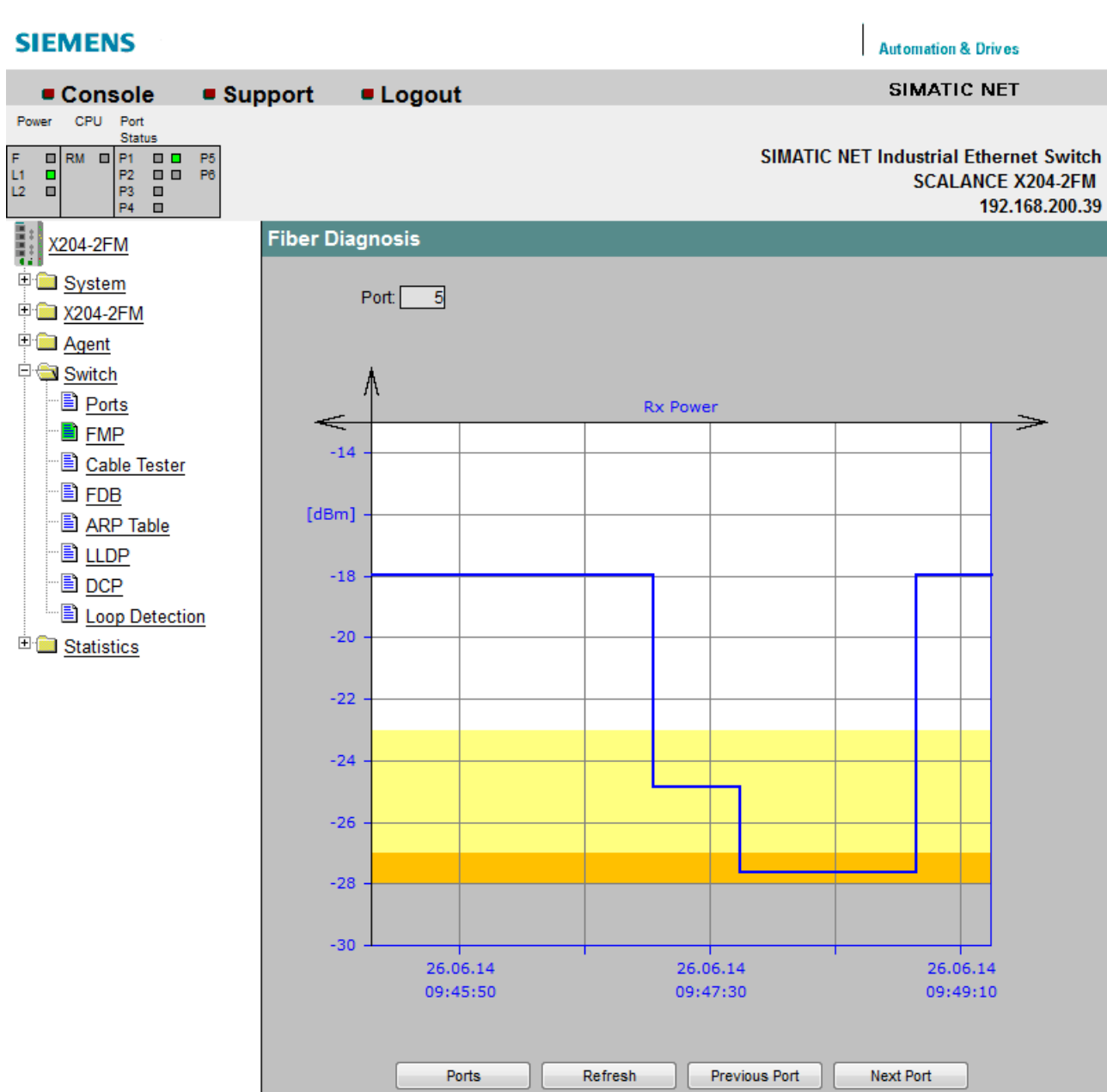


Figure 6-38 Diagnostics of the received power

The vertical axis shows the received power in dBm.

The horizontal axis shows the time since the IE switch started up relative to the current time of day and the current date. Date and time information are adopted from the PC on which the Web browser in use is running.

The diagram itself is divided into the following areas:

- **White**
The value for the received power of the optical link is OK.
- **Yellow**
If the received power enters the yellow range, maintenance is required. The limit value between the white and yellow area corresponds to the setting for "Rx Power Maintenance required".
- **Orange**
If the received power enters the orange range, urgent maintenance is necessary. The limit value between the yellow and orange area corresponds to the setting for "Rx Power Maintenance demanded".

Diagnostics of power loss

The diagnostics page shown below appears if you click on the value of the power loss. It shows the values of the power loss over time.

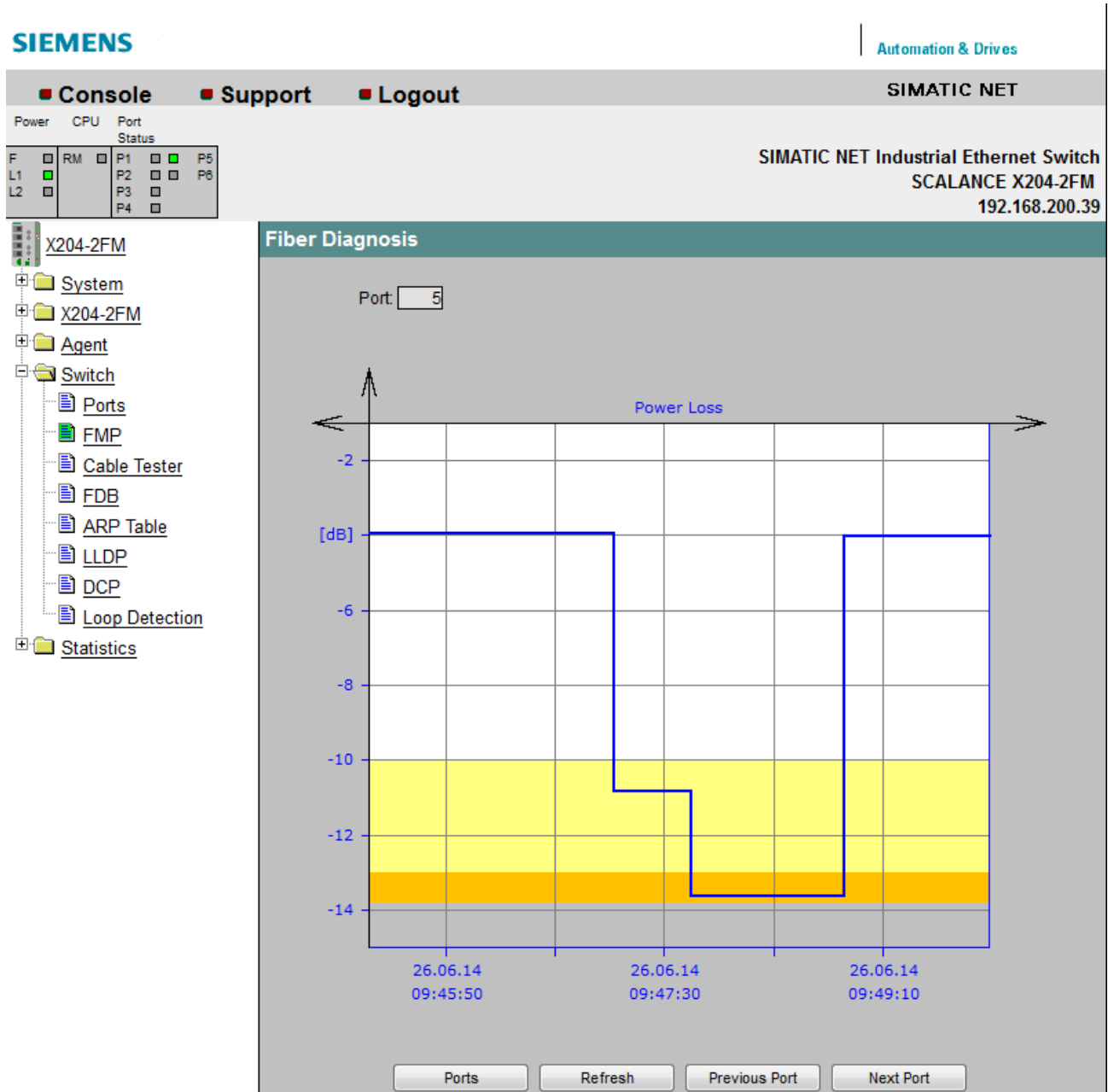


Figure 6-39 diagnostics power loss

The vertical axis shows the power loss in dB.

The horizontal axis shows the time since the IE switch started up relative to the current time of day and the current date. Date and time information are adopted from the PC on which the Web browser in use is running.

The diagram itself is divided into the following areas:

- **White**
The value for the power loss of the optical link is OK.
- **Yellow**
If the power loss enters the yellow range, maintenance is required. The limit value between the white and yellow area corresponds to the setting for "Power loss Maintenance required".
- **Orange**
If the power loss enters the orange range, urgent maintenance is necessary. The limit value between the yellow and orange area corresponds to the setting for "Power loss Maintenance demanded".

6.4.4 Cable tester

Cable fault diagnostics

You can run fault diagnostics for the cables at each individual electrical Ethernet port. This makes it possible to localize short-circuits and cable breaks.

This function is not possible with IRT devices.

To be able to run the fault diagnostics, the Ethernet cable must be plugged into the X-200. There must, however, been no physical connection (link) to another network component.

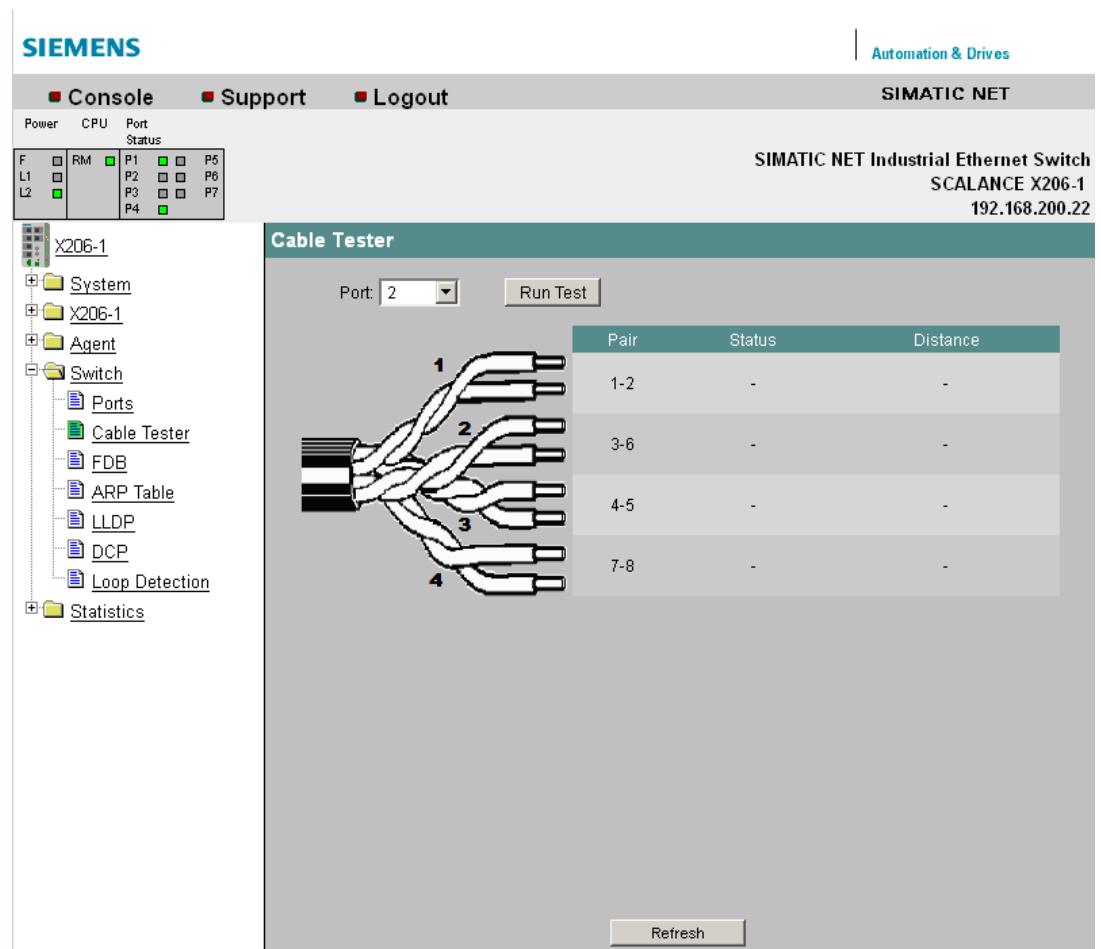


Figure 6-40 Switch Port Diagnostics

Port

Select the port to which the cable you are testing is connected.

Run Test

This button activates the error diagnostics.

Pair

Displays the pair of wires in the cable.

Pairs 4-5 and 7-8 are not used.

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 6-33 Switch Port Diagnostics - CLI|SWITCH>

Command	Description	Comment
test <n>	Starts the "Switch Port Diagnostics" function for an individual port.	

6.4.5 POF

Requirement

The page for diagnostics of fiber-optic cable only shows correct link power margins when plastic optical fiber (POF) is used. If polymer cladded fiber (PCF) is used, diagnostics is not possible.

The following X-200 IE switches use Plastic Optical Fiber (POF) as the transmission medium:

- X200-4P IRT
- X201-3P IRT
- X201-3P IRT PRO
- X202-2P IRT
- X202-2P IRT PRO

Plastic Optical Fiber Management

This page shows the diagnostics data for interfaces with plastic FO cables.

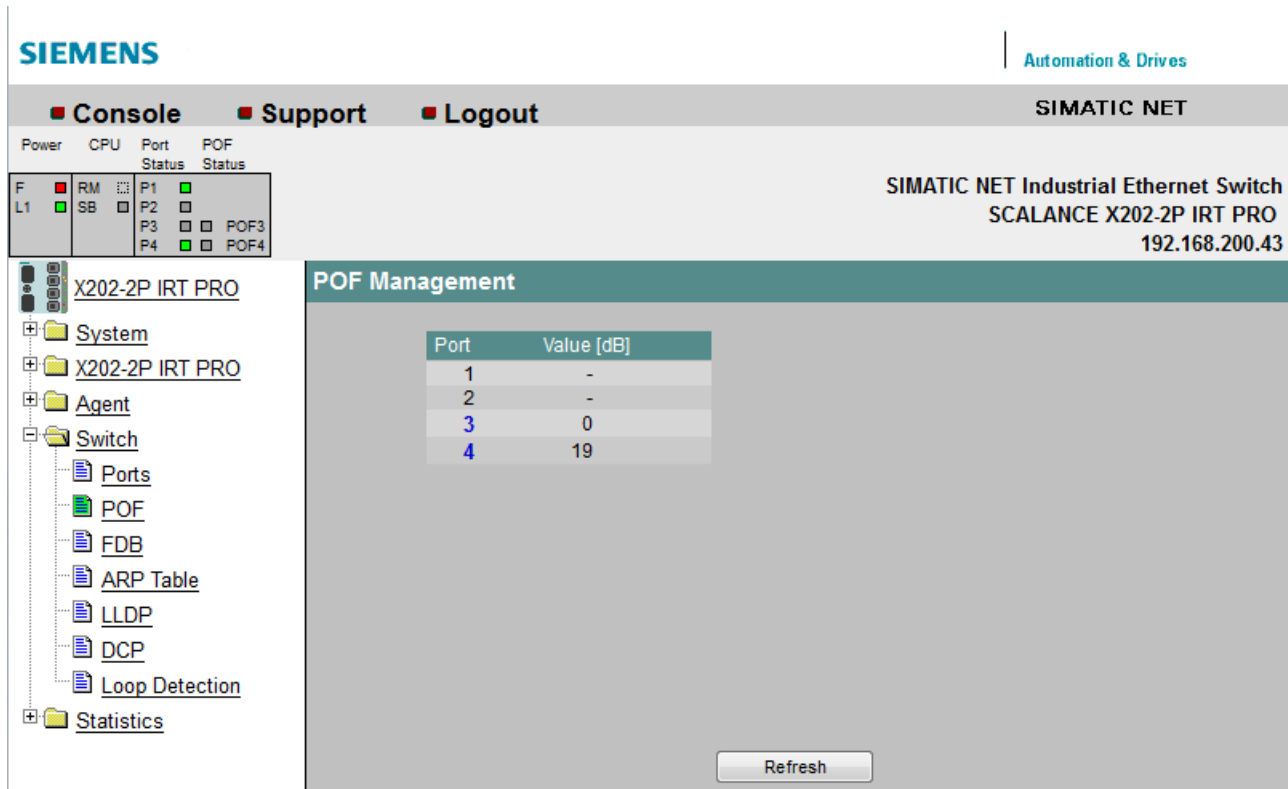


Figure 6-41 POF Management

Here, you can see the currently available link power margin as a numerical value for each POF port.

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

The diagnostics page shown below appears if you click on one of the displayed ports. It displays information on the available link power margin over time.

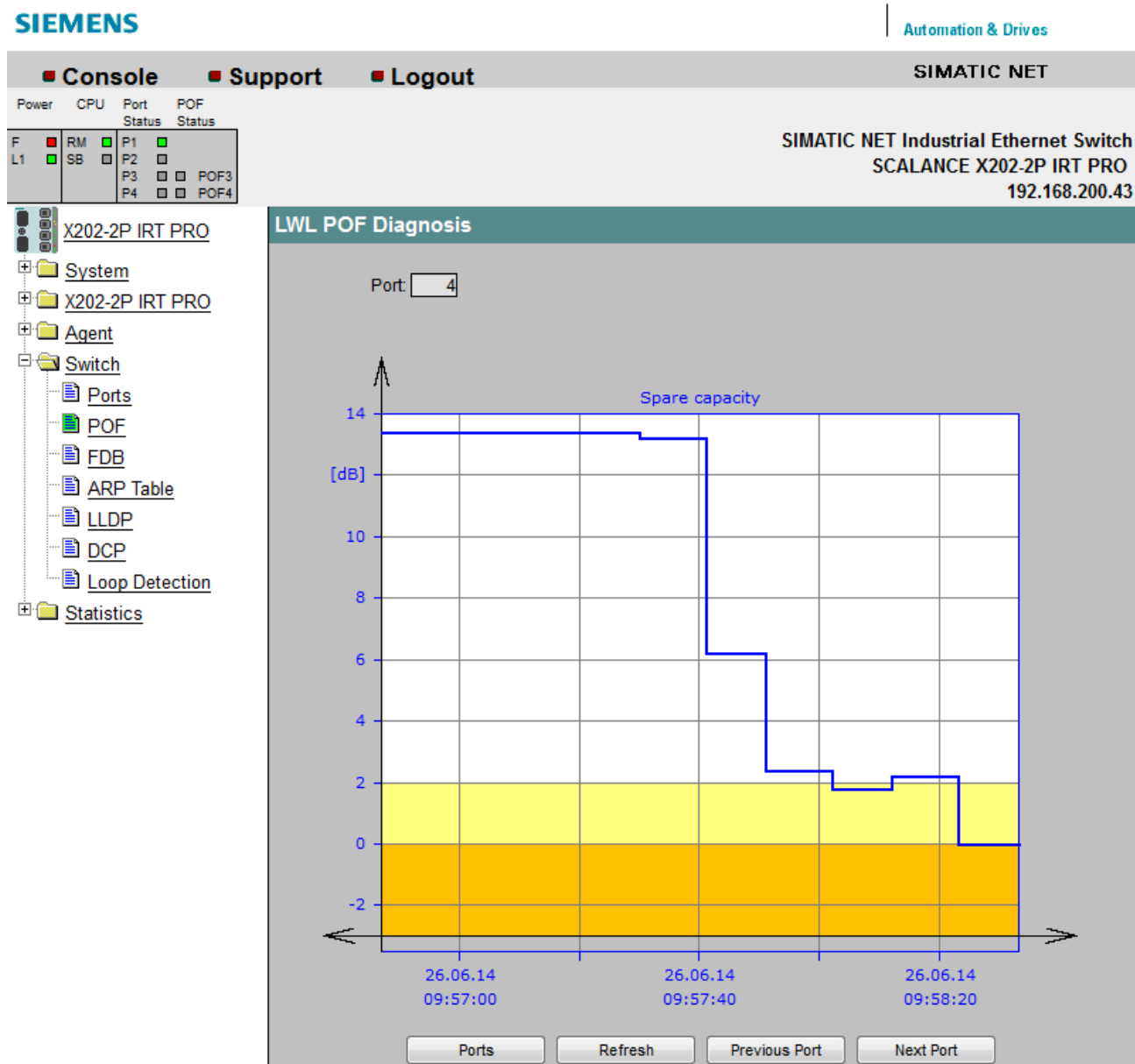


Figure 6-42 POF fiber-optic diagnostics

The vertical axis shows the available link power margin in dB. The measured values only have the required accuracy to be able to show the existing link power margin correctly in the range from 0 dB to 6 dB.

The horizontal axis shows the time since the IE switch started up relative to the current time of day and the current date. Date and time information are adopted from the PC on which the Web browser in use is running.

The diagram itself is divided into the following areas:

- **White**
There is an adequate link power margin for problem-free operation. When the X-200 IE switch is installed, the link power margin should be in this range.
- **Yellow**
If the link power margin enters this range, maintenance is necessary. The boundary of the yellow area is at a link power margin of 2 dB. To ensure long-term functionality of the system, the maintenance should be performed. If the link power margin is in the yellow area, an event is triggered.
- **Orange**
If the link power margin enters the orange range, urgent maintenance is necessary. The boundary of the orange area is at a link power margin of 0 dB. If the link power margin is in the orange range, an event is triggered and the FO LED of the relevant port lights up.

6.4.6 FDB

Switch Forwarding Database

This page shows which MAC addresses are currently reachable via which port.
The FDB is renewed when the aging time elapses.

The screenshot shows the SIMATIC NET web interface for a SCALANCE X202-2IRT switch. The top navigation bar includes 'Console', 'Support', and 'Logout' buttons. The left sidebar shows a tree structure with 'System', 'X202-2IRT', 'Agent', 'Switch', 'Ports', 'FDB', 'ARP Table', 'LLDP', 'DCP', 'Loop Detection', and 'Statistics'.

The main content area displays the 'Switch Forwarding Database' table:

MAC Address	Ports	Status
00-1B-1B-0F-62-95	2	dynamic
01-0E-CF-00-00-00	C 1 2 3 4	dcp
01-0E-CF-00-00-01	C 1 2 3 4	dcp
09-00-06-01-FF-EF	C 1 2 3 4	si-time
68-05-CA-19-40-BB	1	static

A 'Refresh' button is located at the bottom of the table.

Figure 6-43 Switch Forwarding Database

MAC Address

Shows the MAC addresses of the nodes that the IE switch has learned or the user has created.

Ports

Shows the ports via which the MAC address is reachable.

The internal interface of the X-200 IE switch is called "C" in the FDB.

Status

Shows how the entry was created. The following values are possible:

- static
The user created the entry.
Static addresses are stored permanently; in other words, they are not deleted when the aging time expires or when the IE switch is restarted.
- dynamic
The IE switch learned the entry.
When the aging time elapses or during a restart, dynamic entries are deleted again.
- dcp
The entry was created for DCP.
In the factory settings, DCP is enabled on all ports.
- si-time
The entry was created for SIMATIC Time.
In the factory settings, SIMATIC Time is disabled.

Syntax of the Command Line Interface

Table 6-34 Switch Forwarding Database - CLI|SWITCH\FDB>

Command	Description	Comment
info	Shows the current switch forwarding database.	
add <MAC addr><port>	<p>Adds a static MAC address.</p> <p>If you enter a multicast address statically, you can specify several ports. Separate the ports with commas.</p> <p>Example: The command "add 01-08-00-99-99-99 1,2,3" enters the MAC address 01-08-00-99-99-99 for ports 1, 2 and 3 in the FDB.</p>	Administrator only
delete [<MAC addr> D S B]	<p>Deletes an entry:</p> <ul style="list-style-type: none"> • <MAC addr> Deletes the entry for a MAC address. • D Deletes all dynamic entries. • S Deletes all static entries. • B Deletes all dynamic and static entries. 	Administrator only

Note

With SCALANCE X-200, the MAC address table is deleted within 1s.

Note

SCALANCE X-200IRT IE switches can learn up to 4000 Ethernet addresses, the other SCALANCE X-200 IE switches up to 8000 Ethernet addresses. The entry of a learned Ethernet address in the address table is made by the storage system which may reduce the actual number of addresses that can be learned.

6.4.7 ARP table

Switch ARP (Address Resolution Protocol)Table

This dialog shows which MAC address is assigned to which IP address.

The screenshot displays the SIMATIC NET configuration interface for a SCALANCE X216 switch. The top navigation bar includes 'Console', 'Support', and 'Logout' buttons. The main title is 'SIMATIC NET Industrial Ethernet Switch SCALANCE X216 X216-0042'. On the left, a tree view shows the configuration hierarchy: System, X216, Agent, Switch, Ports, Port Diags, FDB, ARP Table (selected), LLDP, DCP, and Statistics. The 'Switch ARP Table' dialog is open, showing a table with the following data:

Index	MAC Address	IP Address	Type
1	00-1B-21-07-69-C9	192.168.0.4	dynamic

A 'Refresh' button is located at the bottom right of the table.

Figure 6-44 Switch ARP Table

Syntax of the Command Line Interface

Table 6-35 Switch ARP Table - CLI\SWITCH>

Command	Description	Comment
arp	Displays the ARP table.	

6.4.8 LLDP

Configuring frames of the Link Layer Discovery Protocol

On this page, you can configure the handling of frames of the Link Layer Discovery Protocol (LLDP) per port.

The LLDP protocol is used to exchange information between neighboring devices. An X-200 IE switch sends LLDP frames to all ports at regular intervals. The LLDP frames received from neighboring devices are not forwarded; only the information they contain about neighboring devices is stored. This information can be read from a central location and used to identify the network topology.

To structure a network logically, the sending and receipt of LLDP frames can be configured per port.

Note

The LLDP protocol can be disabled in STEP 7 using the "End of topology discovery" function.

Note

With the SCALANCE X202-2IRT (6GK5 202-2BB00-2BA3) and X204IRT (6GK5 204-0BA00-2BA3) with a product version lower than or equal to 003, the following port-specific sender addresses are used for LLDP frames:

- Port 1: 08:00:06:9D:38:40
- Port 2: 08:00:06:9D:38:41
- Port 3: 08:00:06:9D:38:42
- Port 4: 08:00:06:9D:38:43

With all other X-200 IE switches, MAC addresses are used as the sender address for LLDP frames that are both device and port-specific.

The MAC address for a specific port is formed by adding the index of this port to the MAC address of the X-200 IE switch.

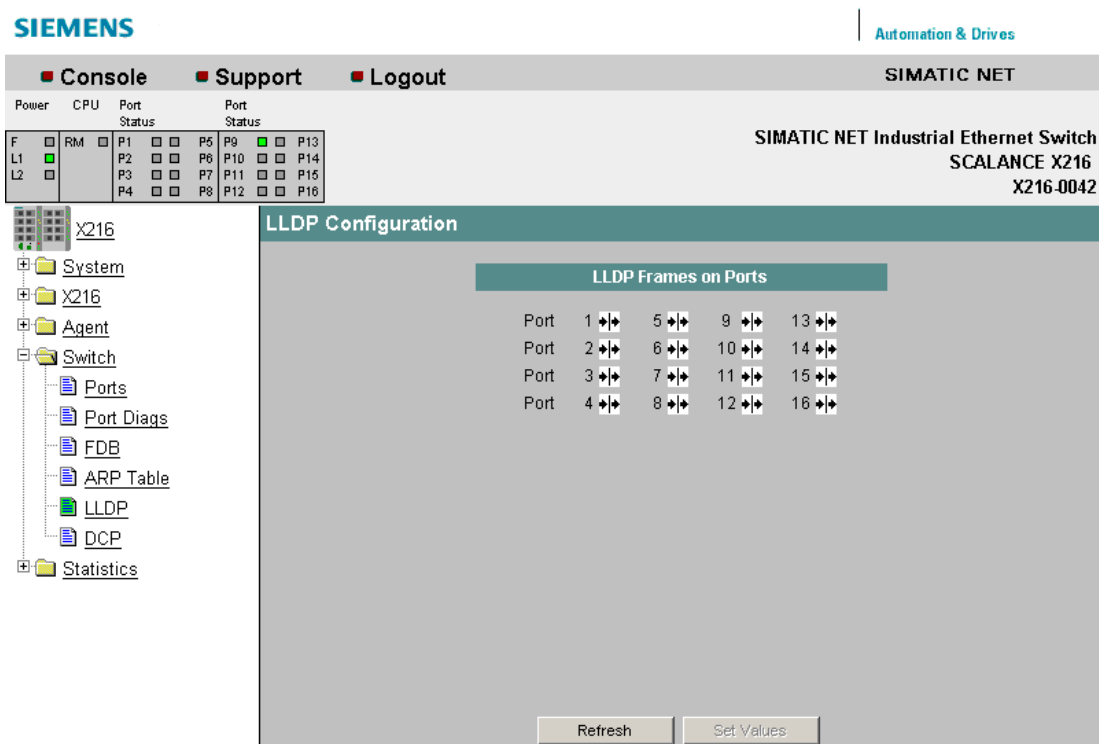


Figure 6-45 LLDP switch

The following settings can be made for the displayed ports:

Symbol	Meaning
	Port sends and receives LLDP frames.
	LLDP frames are neither sent nor received. (not with X-200IRT IE switches)
	LLDP frames are sent but not received.
	LLDP frames are received but not sent. (not with X-200IRT IE switches)

Syntax of the Command Line Interface

Table 6-36 Switch LLDP - CLI|SWITCH|LLDP>

Command	Description	Comment
info	Displays the current LLDP settings.	
lldpport [ports] <mode>	<p>Changes the LLDP settings for one or more ports. The <mode> parameter can have the following values:</p> <ul style="list-style-type: none"> • RX - receive only • TX - send only • TX RX - send and receive • D - disables sending and receiving. <p>Example: The command "lldpport 1,2,3 rx" specifies that LLDP frames are only received on ports 1-3.</p>	Administrator only

Note

With X-200IRT IE switches, only the following settings are possible:

- Port sends and receives LLDP frames.
- LLDP frames are sent but not received.

6.4.9 DCP

DCP Configuration

On this page, you can configure the handling of frames of the Discovery and basic Configuration Protocol (DCP) per port.

The DCP protocol is used to detect nodes in a network and to assign basic parameters such as the IP address, system name etc. to them.

To allow the logical structuring of networks, the sending of DCP multicast frames can be enabled or disabled port-oriented on an X-200 IE switch.

Note

The sending of DCP frames can be disabled in STEP 7 using the "End of detection of accessible nodes" function.

Note

If DCP is switched off, it is possible that not all switches can be configured with SINEC PNI.

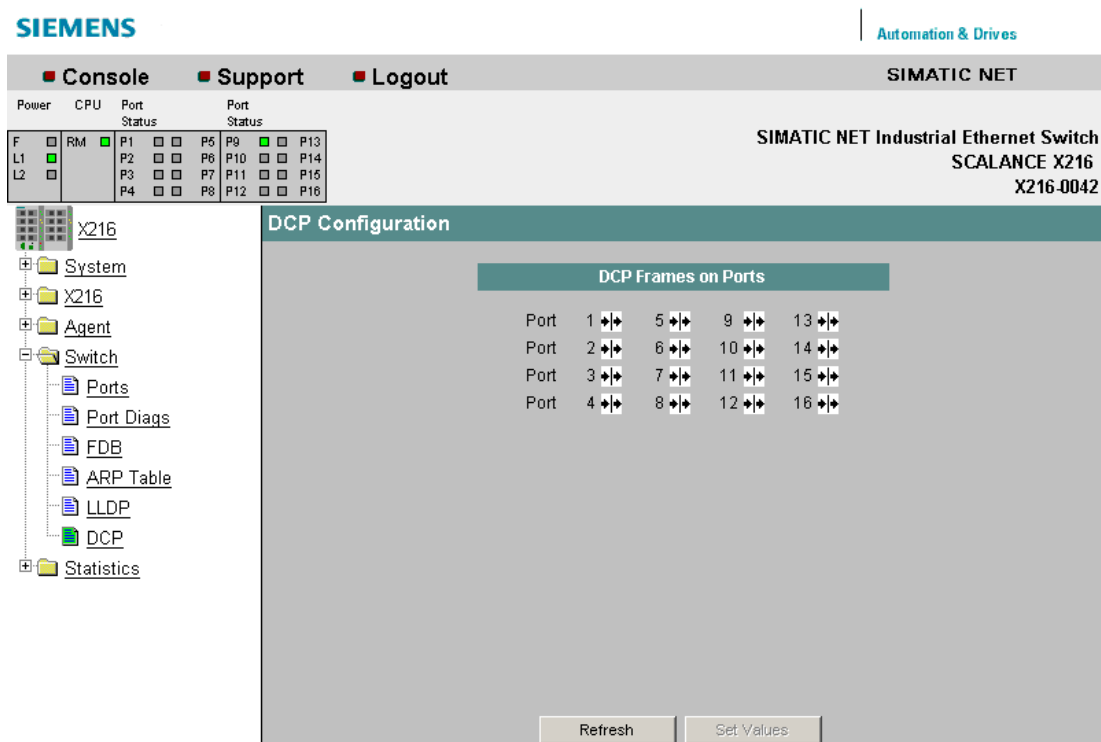


Figure 6-46 DCP switch

The following settings can be made for the displayed ports:

Symbol	Meaning
	The port sends and receives all DCP frames.
	The port does not send any DCP multicast frames. The DCP communication using unicasts is not filtered.

Syntax of the Command Line Interface

Table 6-37 Switch DCP - CLI\SWITCH\DCP>

Command	Description	Comment
info	Displays the current DCP settings.	-
dcpport [ports] <enabled disabled>	<p>Enables or disables the sending of DCP frames on one or more ports.</p> <ul style="list-style-type: none">• enabled The port receives and sends all DCP frames.• disabled The port receives all DCP frames, but only forwards DCP unicast frames. <p>Example: The command "dcpport 1,2,3 disabled" specifies that all DCP frames are received on ports 1-3, however only DCP unicast frames are forwarded.</p>	Administrator only

6.4.10 Loop Detection Config

Loop Detection Configuration

On this page, you specify for the ports for which loop detection will be activated. These ports send test frames. If these frames are sent back to the device, there is a Loop.

Note

Note that the functions of the "Loop Detection Configuration" WBM menu are not available for X-200IRT.

If the frames are received again at another port of the same device, there is a "Local Loop" involving this device.

If the sent frames are received again at the same port, there is a "Remote Loop" involving other network components.

Note

Note that loop detection is only possible at ports that were not configured as ring ports.

Loop Detection Configuration

Loop Detection Control

Loop Detection Enabled: ☒

Rx Threshold (All Ports):

Remote Loop Reaction (All Ports):

Local Loop Reaction (All Ports):

Loop Detection Port Control

Port	Setting	Rx Threshold	Remote Loop Reaction	Local Loop Reaction	State	Source Port	Action
1	<input type="text" value="Forwarder"/>	<input type="text" value="2"/>	<input type="text" value="Disable"/>	<input type="text" value="Disable"/>	deactivated	-	<input type="button" value="Reset"/>
2	<input type="text" value="Forwarder"/>	<input type="text" value="2"/>	<input type="text" value="Disable"/>	<input type="text" value="Disable"/>	deactivated	-	<input type="button" value="Reset"/>
3	<input type="text" value="Sender"/>	<input type="text" value="2"/>	<input type="text" value="Disable"/>	<input type="text" value="Disable"/>	active	-	<input type="button" value="Reset"/>
4	<input type="text" value="Sender"/>	<input type="text" value="2"/>	<input type="text" value="Disable"/>	<input type="text" value="Disable"/>	local loop	5	<input type="button" value="Reset"/>
5	<input type="text" value="Sender"/>	<input type="text" value="2"/>	<input type="text" value="No Action"/>	<input type="text" value="Disable"/>	remote loop	5	<input type="button" value="Reset"/>
6	<input type="text" value="Forwarder"/>	<input type="text" value="2"/>	<input type="text" value="Disable"/>	<input type="text" value="Disable"/>	deactivated	-	<input type="button" value="Reset"/>
7	<input type="text" value="Forwarder"/>	<input type="text" value="2"/>	<input type="text" value="Disable"/>	<input type="text" value="Disable"/>	deactivated	-	<input type="button" value="Reset"/>
8	<input type="text" value="Forwarder"/>	<input type="text" value="2"/>	<input type="text" value="Disable"/>	<input type="text" value="Disable"/>	deactivated	-	<input type="button" value="Reset"/>
9	<input type="text" value="Forwarder"/>	<input type="text" value="2"/>	<input type="text" value="Disable"/>	<input type="text" value="Disable"/>	deactivated	-	<input type="button" value="Reset"/>
10	<input type="text" value="Forwarder"/>	<input type="text" value="2"/>	<input type="text" value="Disable"/>	<input type="text" value="Disable"/>	deactivated	-	<input type="button" value="Reset"/>
11	<input type="text" value="Forwarder"/>	<input type="text" value="2"/>	<input type="text" value="Disable"/>	<input type="text" value="Disable"/>	deactivated	-	<input type="button" value="Reset"/>
12	<input type="text" value="Forwarder"/>	<input type="text" value="2"/>	<input type="text" value="Disable"/>	<input type="text" value="Disable"/>	deactivated	-	<input type="button" value="Reset"/>
13	<input type="text" value="Forwarder"/>	<input type="text" value="2"/>	<input type="text" value="Disable"/>	<input type="text" value="Disable"/>	deactivated	-	<input type="button" value="Reset"/>
14	<input type="text" value="Blocked"/>	<input type="text" value="2"/>	<input type="text" value="Disable"/>	<input type="text" value="Disable"/>	deactivated	-	<input type="button" value="Reset"/>

Figure 6-47 Loop Detection Configuration

Loop Detection Control

The following settings are available:

- "Loop Detection enabled" check box
Here you can enable loop detection for this switch. If loop detection is disabled, loop detection frames of other devices are forwarded.
- "Rx-Threshold (All Ports)" input box
Here, you can enter the number of received frames after which a loop is assumed. If a port-specific setting was made "Variant" is displayed.
- "Remote Loop Reaction (All Ports)" drop-down list
Here you can specify for all ports whether a port is activated or deactivated if a remote loop is detected. If a port-specific setting was made "Variant" is displayed.
- "Local Loop Reaction (All Ports)" drop-down list
Here you can specify for all ports whether a port is activated or deactivated if a local loop is detected. If a port-specific setting was made "Variant" is displayed.

Loop Detection Port Control

Meaning of the column entries:

- "Port" display box
The relevant port is listed here.
- "Setting" drop-down list
In this area, you define the behavior of the port. You can choose from the following options:
 - "Sender"
If this option is set, loop detection frames are sent and forwarded.
 - "Forwarder"
If this option is set, loop detection frames of other devices are forwarded.
 - "Blocked"
If you select this option, the forwarding of loop detection frames is blocked.
- "Rx-Threshold" input box
Here, you can specify the number of received frames after which a loop is assumed.
- "Remote Loop Reaction" drop-down list
Here, you can activate or deactivate a port if a remote loop is detected.
- "Local Loop Reaction" drop-down list
Here, you can activate or deactivate a port if a local loop is detected.
- "State" display box
Shows the status of the loop detection for the corresponding port.
- "Source Port" display box
Shows the port that received the frame that triggered the last reaction.
- "Action" button
After the loop in the network has been eliminated, you can use this button to reset the port again.

Note

A loop is an error in the network structure that needs to be eliminated. The loop detection can help to find the errors more quickly but does not eliminate them. The loop detection is not suitable for increasing network availability by deliberately including loops.

Note

Loops can only be detected between devices that forward loop detection frames. Loops via network components whose ports are set to "blocked" are not detected.

Note

Test frames create additional network load. We recommend that you only configure individual switches, for example at branch points of the ring, as "senders" and the others as "forwarders".

Syntax of the Command Line Interface

Table 6-38 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: <ul style="list-style-type: none"> "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

6.5 the Statistics menu

6.5.1 Statistics

Statistics - counting and evaluation of received and sent frames

The X-200 IE switches have internal statistics counters (RMON (Remote Monitoring) counters) with which they counts the number of received frames according to the following criteria:

- Frame length
- Frame type
- Bad frames

This information provides you with an overview of the data traffic and any problems on the network.

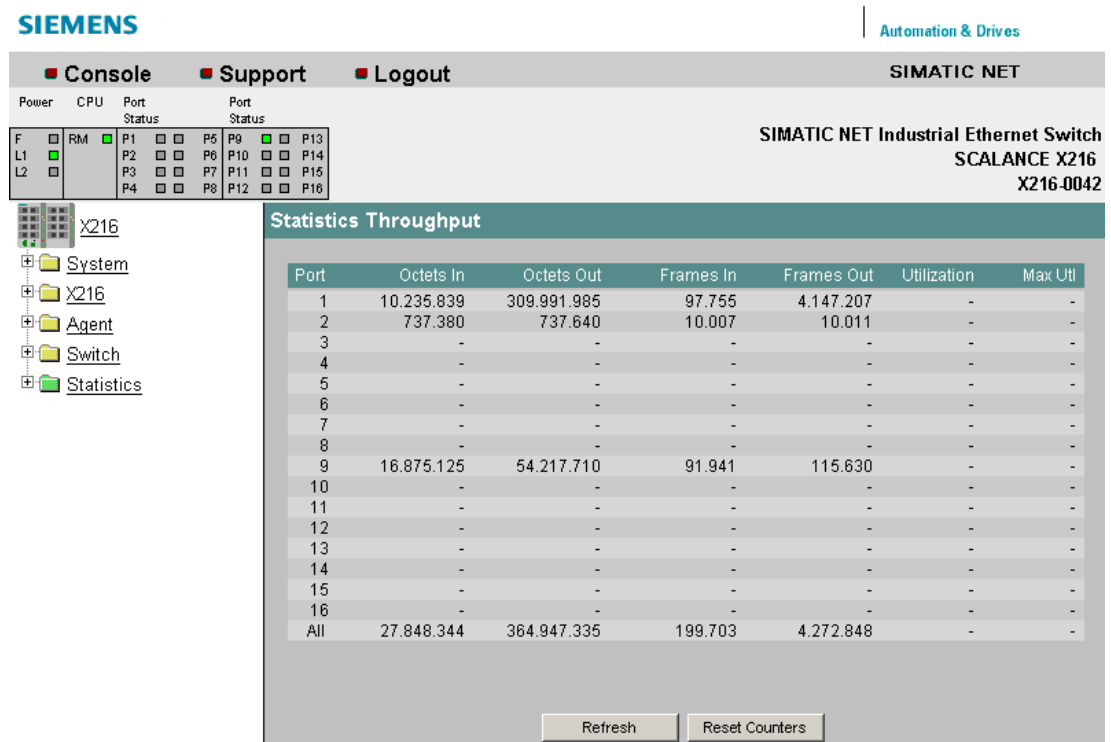


Figure 6-48 Statistics Throughput

Octets In

Displays the number of received bytes.

Octets Out

Displays the number of sent bytes.

Frames In

Displays the number of received frames.

Frames Out

Displays the number of sent frames.

Utilization

Displays the port utilization as a percentage (%). If the bus utilization is less than 1%, nothing is displayed. Depending on the frame length (system dependent), the display can deviate by up to 20% since the proportion of pauses between frames increases the shorter the frame.

Max. Utilization

Displays the peak value of port utilization as a percentage (%).

Note

The Utilization value is calculated from the incoming frames. Here, both correct and bad frames are relevant. Outgoing frames are not taken into account in the calculation of this value.

Syntax of the Command Line Interface

Table 6-39 Statistic - CLI\STAT>

Command	Description	Comment
info	Shows statistical information on sent and received frames.	
types	Displays information on the type of the sent and received frames.	
sizes	Displays information on the length of the sent and received frames.	
errors	Displays information on bad sent and received frames.	

6.5.2 Packet size

Packet Size Statistics - received packets sorted according to length

The Statistics Packet Size 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.

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 graphical representation of the counter value.

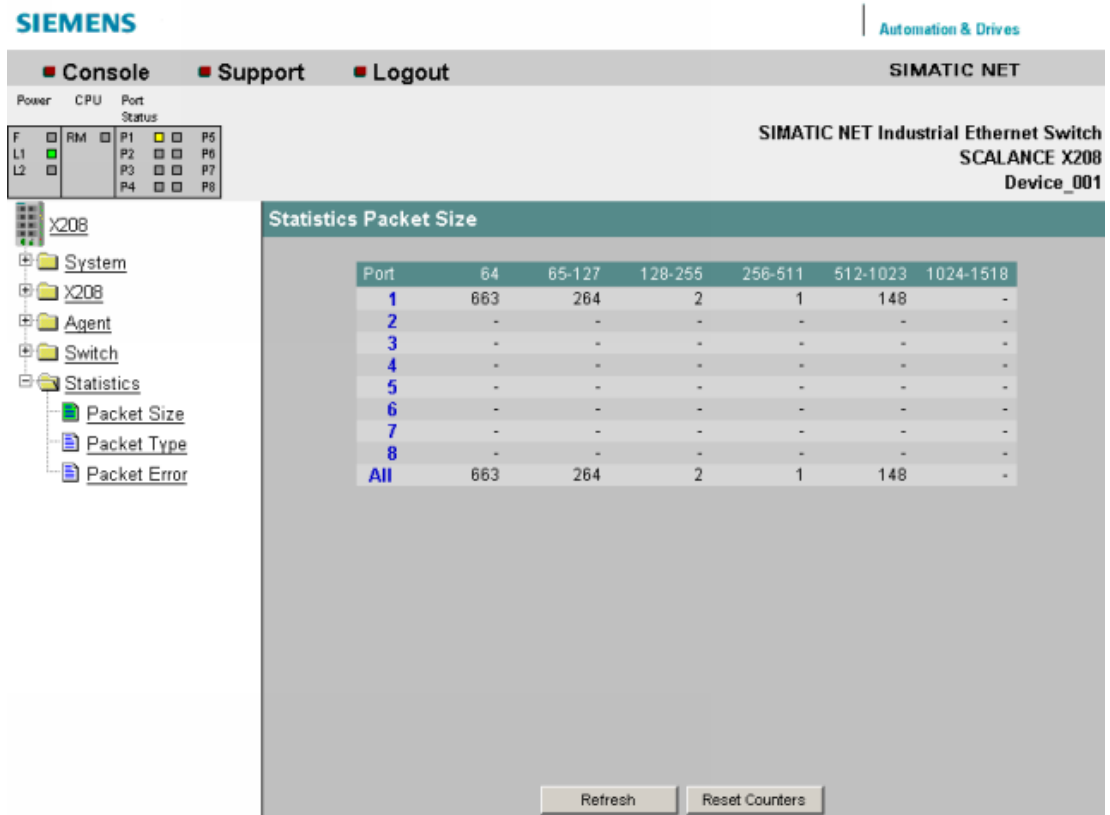


Figure 6-49 Statistics Packet Size

64

Displays the number of packets with a length of 64 bytes.

65-127

Displays the number of packets with a length of 65-127 bytes.

128-255

Displays the number of packets with a length of 128-255 bytes.

256-511

Displays the number of packets with a length of 256-511 bytes.

512-1023

Displays the number of packets with a length of 512-1023 bytes.

1024-1518

Displays the number of packets with a length of 1024-1518 bytes.

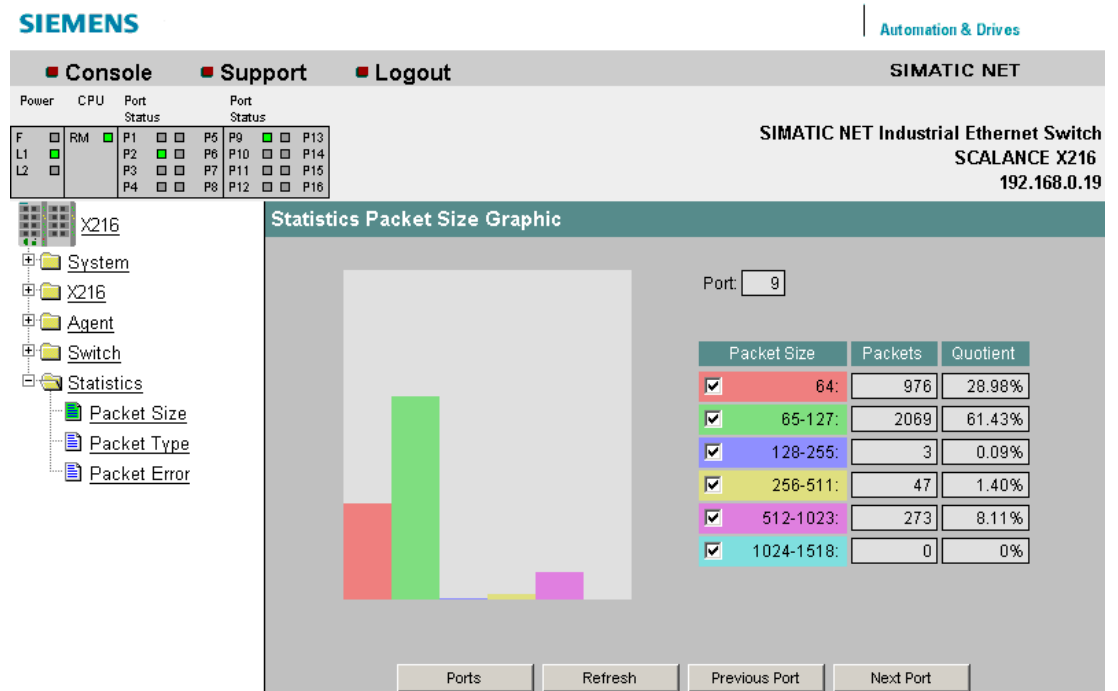


Figure 6-50 Statistics Packet Size Graphic

Syntax of the Command Line Interface

Table 6-40 Statistic Packet Size - CLI\INFORM>

Command	Description	Comment
sizes	Shows statistical information broken down according to frame length.	

6.5.3 Packet type

Packet Type Statistics - received packets sorted according to type

The Statistics Packet Type 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.

If you click on an entry in the Port column, the Statistics Packet Type Graphic is displayed for the selected port. You then see a graphical representation of the counter value.

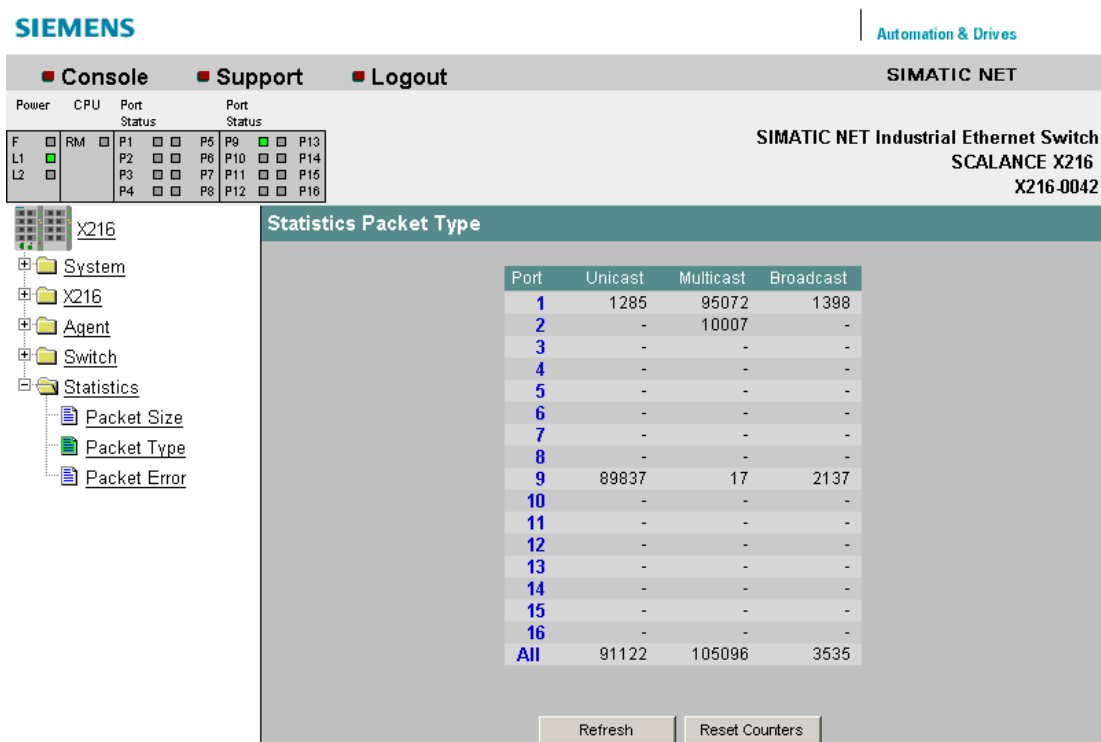


Figure 6-51 Statistics Packet Type

Unicast

Displays the number of packets to the unicast recipient address.

Multicast

Displays the number of packets to the multicast recipient address.

Broadcast

Displays the number of packets to the broadcast recipient address.

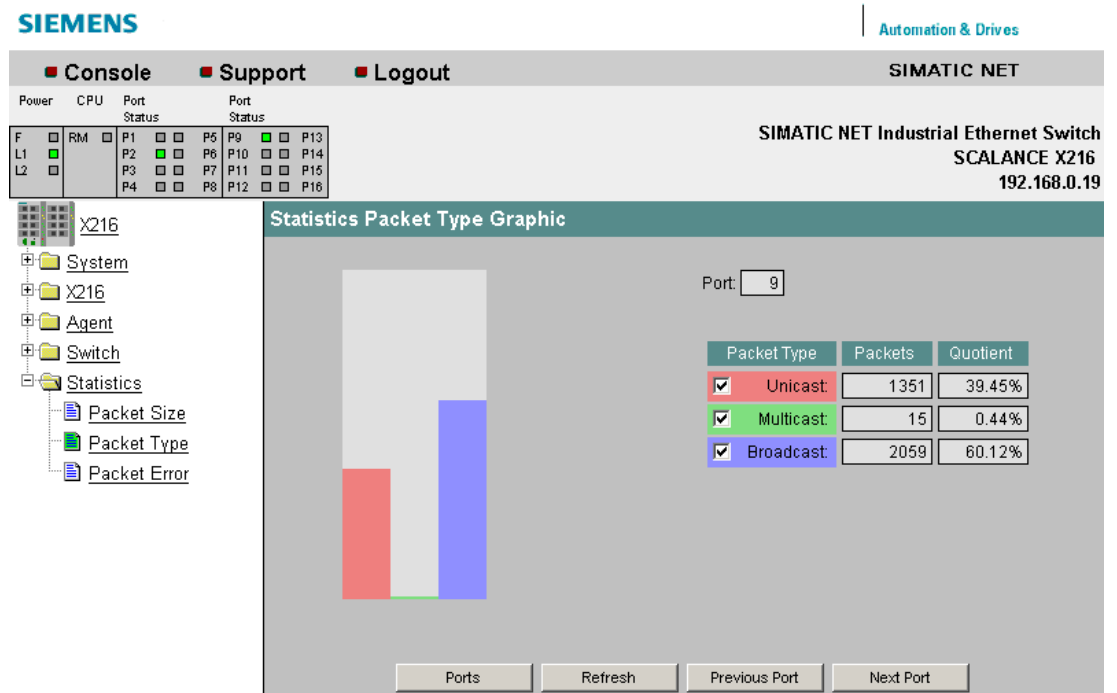


Figure 6-52 Statistics Packet Type Graphic

Syntax of the Command Line Interface

Table 6-41 Statistic Packet Type - CLIINFORM>

Command	Description	Comment
types	Shows statistical information broken down according to frame type.	

6.5.4 Packet Error

Statistics Packet Error - Counting and evaluation of transmission errors

This page shows information on any errors that may have occurred and allows diagnostics for the port on which the error occurred. You can reset the error counters with the "Reset Counters" button.

If you click on an entry in the Port column, the Statistics Packet Error Graphic is displayed for the selected port. You then see a graphical representation of the counter value.

Statistics Packet Error

Port	CRC	Undersize	Oversize	Fragmented	Jabbers	Collisions
1	-	-	-	-	-	-
2	-	-	-	-	-	-
3	-	-	-	-	-	-
4	-	-	-	-	-	-
5	-	-	-	-	-	-
6	-	-	-	-	-	-
7	-	-	-	-	-	-
All	-	-	-	-	-	-

Refresh Reset Counters

Figure 6-53 Statistics Packet Error (The "Fragmented" column is only present with devices **without** the IRT function.)

The following errors can be detected:

CRC

Packets with a valid length but bad checksum.

Undersize

Packets too short with valid checksum.

Oversize

Packets too long with valid checksum.

Fragmented (Only with devices **without** the IRT function.)

Packets with a length less than 64 bytes and a bad CRC checksum.

Jabbers

Packets too long without valid checksum.

Collisions

Indicates the number of collisions that have occurred.

Note

X-200IRT IE switches work in the cut-through mode.

If a frame is received with a bad checksum, the forwarding of the frame is aborted prematurely and the frame is therefore shortened. The counter for CRC errors is incremented.

If the frame involved is a frame with a length of 64 bytes, the counter for undersize errors is also incremented due to the shortening of the frame

Syntax of the Command Line Interface

Table 6-42 Statistic Packet Error - CLI\INFORM>

Command	Description	Comment
errors	Displays statistical information on received errors.	

Configuration via SNMP

Configuration of an IE switch using SNMP

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 on the node with which the management station exchanges data using Get and Set requests. The X-200 IE switches support SNMPv1, SNMPv2 and SNMPv3.

The configurable data is stored on the IE switch in a database known as the MIB (Management Information Base) and this can be accessed by the management station or by Web Based Management.

Note

Only the settings possible via WBM and CLI are approved

In contrast to configuration via WBM or CLI, only a limited plausibility and consistency check, or none at all, of the device configuration takes place with configuration via SNMP. An incorrect device configuration can lead to data loss and an impairment of the entire network.

Only the configuration settings that you can make via WBM or CLI have been tested and approved.

SIMATIC NET SNMP OPC Server

The SNMP OPC server makes the SNMP information from TCP/IP networks with SNMP available on the OPC interface. With the aid of the SNMP OPC server, any OPC client systems (such as WinCC) can now access diagnostics and parameter data of SNMP-compliant components.

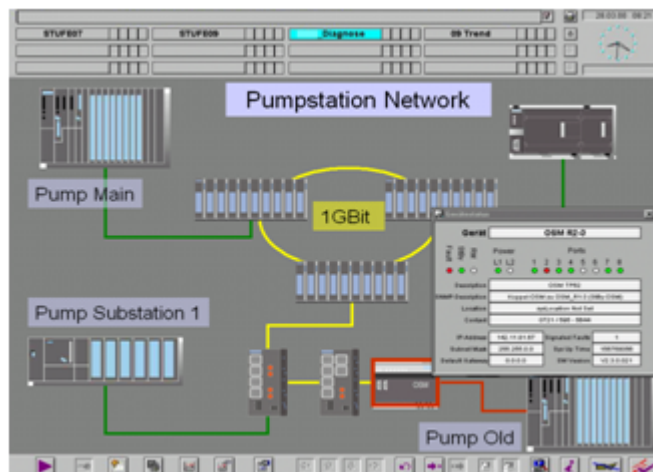


Figure 7-1 WinCC example of network diagnostics with the SIMATIC NET SNMP OPC server

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.

With STEP 7 or alternatively NCM PC, you configure which devices are monitored by the SNMP OPC server.

You will find further information about the SNMP OPC server from SIMATIC NET with the following link:

SNMP OPC server (<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 completed device profile can be found on the Product Support pages under the following entry ID:

22015045 (<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 X-200 IE switch supports the following MIBs:

- RFC 1213: MIB II (all groups except egp and transmission)
- RFC 1286, RFC 1493: Bridge MIB (dot1dBase and dot1dStp)
- Private MIBs

For information on the MIB variables of the IE switch, refer to Appendix MIBs for X-200 (Page 175) of this manual.

Access to the private MIB file of an IE switch

To access the private MIB file of an IE switch, follow the steps below:

1. Open Web Based Management.
2. Select the System -> Save & Load HTTP menu item.
3. Click the "Save Private MIB" button.
4. Follow the instructions in the window that opens.

Connection to PROFINET IO

connection via STEP 7

The SCALANCE X-200 IE switches are also suitable for use in a network with PROFINET IO. The devices must be linked into PROFINET IO using STEP 7.

How this connection is achieved is not covered in these operating instructions but is explained in the STEP 7 help.

Configuring interrupts in STEP 7 V5

The configuration of the "C-PLUG error" and "Redundant power supply" interrupts is a special feature among the SIMATIC net devices. For this reason, you will not find any information in the STEP 7 help relating to configuration of these two interrupts.

The configuration of these interrupts is described in the following section.

Further information about PROFINET IO

The system manual PROFINET System Description provides an overview of the PROFINET communications system. You will find this manual on the Product Support pages under the following entry ID:

19292127 (<http://support.automation.siemens.com/WW/view/en/19292127>)

Note

If an X-200 that was previously configured via PROFINET IO needs to be operated without PROFINET functionality, you will need to reset the device to its factory defaults. For more detailed information, refer to section "The System > Restart & Defaults (Page 52) menu".

8.1 Configuration of the bus adapters for XF-200IRT

Note

If you wish to operate a SCALANCE XF204-2BA IRT with just one BusAdapter, insert the BusAdapter in the left-hand slot, ports P1 and P2.

If only one BusAdapter is plugged in the right-hand slot (ports P3 and P4), communication via all ports of the SCALANCE XF204-2BA IRT is blocked.

8.2 Configuring the interrupts in STEP 7

Configure the ports of the bus adapters in STEP 7 in the same way as the bus adapters actually plugged into the device. If the configuration in STEP 7 does not correspond to the actually plugged in bus adapters, the status of the device is displayed as being disrupted.

The following table contains the names of the ports according to the hardware catalog in STEP 7.

Component	Port 1 or port 3	Description
	Port 2 or port 4	
BA 2×RJ45	RJ45	PROFINET bus adapter with Ethernet socket for standard RJ-45 plugs
	RJ45	
BA 2×RJ45 (Coated)	RJ45 coated	PROFINET bus adapter with Ethernet socket for standard RJ-45 plugs, with printed circuit boards with conformal coating.
	RJ45 coated	
BA 2×FC	FC	PROFINET bus adapter with FastConnect Ethernet connector for direct connection of the bus cable
	FC	
BA 2×FC (Coated)	FC coated	PROFINET bus adapter with FastConnect Ethernet connector for direct connection of the bus cable with printed circuit boards with conformal coating.
	FC coated	
BA 2xSCRJ	SC RJ	PROFINET bus adapter with fiber-optic connector POF/PCF
	SC RJ	
BA 2xSCRJ (Coated)	SC RJ coated	PROFINET bus adapter with FO connector POF/PCF with printed circuit boards with conformal coating.
	SC RJ coated	
BA SCRJ/RJ45	SC RJ	Media converter, PROFINET bus adapter with fiber-optic connector POF/PCF ↔ standard RJ-45 plug
	RJ45	
BA SCRJ/FC	SC RJ	Media converter, PROFINET bus adapter with fiber-optic connector POF/PCF ↔ direct connection of the bus cable
	FC	

8.2 Configuring the interrupts in STEP 7

Configuration of the "C-PLUG error" and "Redundant power supply" interrupts

The configuration of the "C-PLUG error" and "Redundant power supply" interrupts of the SCALANCE X-200 IE switches is a special feature among the SIMATIC net devices. For this reason, you will not find any information in the STEP 7 help relating to configuration of these two interrupts.

How to configure the interrupts of an X-200 in STEP 7 V5 is described below:

1. Select the device you want to configure.
In the lower part of the station window you will see the detailed view of the selected device.
2. Open the page with the general settings.
Here you will find the settings that are valid for the entire device.
3. Double-click on the "0" entry in the "Slot" column.
The "Properties - SCALANCE X-200" window opens.
4. Select the "Parameter" tab.

5. Open the "Alarm setting" folder.
6. Select one of the following options from the possible settings:
 - Under the "Redundant power supply" entry:
 - Monitored
If one of the two sources of power fails, an interrupt is generated.
 - Not monitored
No interrupt is generated if one of the two sources of power fails.
 - Under the "C-PLUG error" entry:
 - Monitored
If a C-PLUG fault occurs, an interrupt is generated.
 - Not monitored
No interrupt is generated if a C-PLUG error occurs.

8.3 MRP configuration in STEP 7

Configuration in STEP 7

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

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

- Domain
- Role
- Ring port
- Diagnostic interrupts

These settings are described below.

Note

Valid MRP configuration

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

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

Note

Note factory settings

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

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

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

Note

Reconfiguration only when the ring is open

First open the ring before you

- change the MRP role or
 - reconfigure ring ports
-

Note

Starting up and restarting

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

Note

Prioritized startup

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

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

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

Domain

Single MRP rings

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

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

Multiple MRP rings

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

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

Note

Suitable devices for MRP multiple rings

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

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

Note

Suitable devices for MRP Interconnection

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

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

Role

Note

Reconfiguration only when the ring is open!

The choice of role depends on the following use cases.

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

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

Note

Role after resetting to factory settings

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

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

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

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

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

Ring port 1 / ring port 2

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

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

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

NOTICE

Ring ports after resetting to factory settings

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

Note

Reconfiguration only when the ring is open

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

Diagnostic interrupts

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

The following diagnostic interrupts can be generated:

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

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

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

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

Note

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

Changing the configuration of an existing HRP manager

The configuration of a device in the role as redundancy manager with the HRP redundancy method cannot be changed to the redundancy method MRP using STEP 7.

The only way to change the redundancy mode is to use manual parameter assignment methods such as WBM, CLI or SNMP and to activate the "MRP Manager (Auto)/Client" or "Automatic Redundancy Detection" role.

X-200IRT: No change to the MRP configuration during PROFINET IO operation

With X-200IRT, media redundancy cannot be set during PROFINET IO operation. Set the X-200IRT to the factory settings to configure MRP using an alternative method (WBM, CLI, SNMP). After saving the settings on the device using the alternative method, you can create or modify the MRP configuration in STEP 7.

Information on the ring ports

You will find a list of the default ring ports of the individual device variants in the Appendix Default ring ports (Page 179).

8.4 Configuring the topology in STEP 7

Procedure

1. Call the dialog box with port-specific settings. To open the dialog, select the device whose settings you want to change. In the lower half of the station window, there is a detailed view of the selected device.
2. Double-click on the required port to open its properties dialog. As an alternative, the properties dialog can also be opened by right-clicking on the relevant port and selecting the "Object Properties" entry from the context menu.
3. Then select the "Topology" tab.

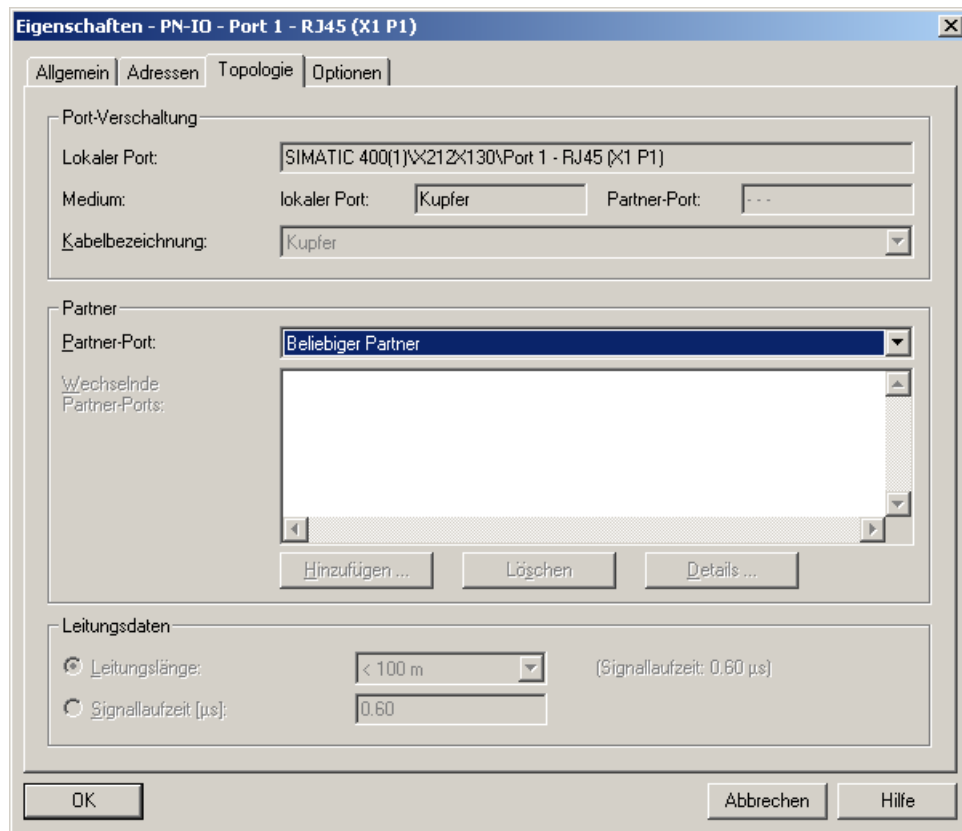


Figure 8-1 STEP 7 HW Config dialog box, "Topology" tab

Partners

- Partner port
Here you can configure the topology that will be monitored. To do this, select the port of another device that is connected to the currently selected port in the "Partner Port" drop-down list:
 - "Alternating partner port"
Select this option if you want alternating ports to be monitored.
 - "Any partner"
Select this setting, if you do not want the topology be monitored.
This is the default setting.
- Changing partner ports
Here, select all ports to be monitored when ports alternate.

8.5 Configuring HRP

HRP configuration - not with STEP 7

HRP cannot be configured with STEP 7.

We recommend that you use MRP instead of HRP if you want to use the X-200 with PROFINET IO.

HRP with PROFINET IO

Note the following information if you nevertheless want to use HRP with PROFINET IO:

- Select the firmware version V3.0 for all modules in HRP mode in STEP 7 HW Config. If a firmware version V4.0 or higher is selected in HW Config, the parameters for the redundancy function are always set by STEP 7. STEP 7, however, supports only MRP mode. This behavior only occurs up to STEP 7 V5.4. With STEP 7 V5.5, the setting "Parameter assignment of the redundancy is not set by STEP 7" was introduced.
- If the default setting for the ring ports is used, only one device in the ring needs to be configured as HRP manager. No further parameter assignment is necessary for the other nodes.

Note

Create the configuration of the module with Web Based Management, CLI or SNMP before it establishes a connection to the controller. As soon as there is a connection to the controller, the redundancy settings can no longer be changed.

Note

Compatibility of the firmware versions

If you load firmware that is older than the firmware on the device, you will have to reset the device to the factory defaults after loading the firmware.

If you update the firmware of an IE Switch X-200, make sure that the firmware in use is compatible with the relevant device.

If incompatible firmware is downloaded to the device, it will no longer be possible to operate the device. In this case, compatible firmware will have to be loaded again with the boot loader.

Firmware compatibility

Note the following restrictions relating to the compatibility of the firmware versions with the individual devices:

Firmware version	IE switch
at least X-200IRT V4.5	X201-3P IRT PRO
at least X-200IRT V4.1	XF204IRT
at least X-200IRT V3.1	X202-2P IRT PRO X204IRT PRO
at least X-200IRT V2.1	X200-4P IRT X201-3P IRT X202-2P IRT
at least X-200 V4.5	X208PRO
at least X-200 V4.3	X204-2TS
at least X-200 V4.1	XF204 XF204-2 XF206-1 XF208

8.6 Structure of the data records

Data records 4, 5 and 0x802A

The structure of the data records 4, 5 and 0x802A is described below.

8.6.1 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

Alarm_enable:

This bit list specifies what is to be monitored. If a bit is set, this alarm source is enabled.

Reserved Bits 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.

8.6.2 Data record 5

Data record 5 supplies the current alarm setting for this port

Access: Read-only

```
typedef struct {
    Word BlockType;
    Word BlockLength;
    Byte BlockVersionHigh;
```

8.6 Structure of the data records

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 compo- nent 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 about the current error status 0: Fault line passive 1: Fault line active	This bit provides informa- tion about the redundant power supply 0: not redundant 1: redundant

8.6.3 Data record 0x802A

Structure:

```
typedef 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 designation.

SubslotNumber

Subslot designation

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

Designation 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

Value (hexadecimal)	Meaning
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	100BASEPXFHD
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 to 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
0x03	Wireless communication
0x04 – 0xFFFFFFFF	Reserved

Note

You will find further information on the IEC data record in IEC 61158.

Downloading firmware

9.1 Regular firmware download

Options for downloading firmware

The X-200 IE switches provide the following options for updating the firmware:

- Download using HTTP / HTTPS
- Download with TFTP
- If an error occurred: Loading using the boot loader

Download using HTTP / HTTPS

How a regular update is performed using HTTP / HTTPS is explained in the description of the WBM menu in the section Save & Load HTTP (Page 53).

Download with TFTP

How a regular update is performed using TFTP is explained in the description of the WBM menu in the section Save & Load TFTP (Page 56).

Loading with the boot loader if a fault occurs

You will find more detailed information on updating the firmware if a fault occurs in the section Loading firmware using the boot loader (Page 173).

9.2 Loading firmware using the boot loader

Firmware update if a fault occurs

If an error occurs when updating the firmware or if an IE Switch X200 was updated with incompatible firmware, it is possible that the firmware of the device will not start correctly.

In this case, the boot loader is active after the device has started up. This status is signaled by a flashing fault LED.

9.2 Loading firmware using the boot loader

The boot loader can also be activated when the device is turned on by holding down the SET button until the fault LEDs starts to flash.

Note

When a boot loader is active, all ports of the device are active.

If you operate the device in an MRP/HRP ring as redundancy manager, note the following before you start the boot loader.

First open the ring by disconnecting a ring port so that there are no circulating frames.

Procedure

To load new firmware on the X-200 IE switch, follow the steps below with the boot loader activated:

1. Assign an IP address to the device. Use SINEC PNI for this.
Once you have assigned the IP address, you can communicate with the FTP server integrated in the boot loader.
2. Send a firmware file to the IE Switch X-200 using FTP. You can use any FTP client to do this.
Use the following connection settings for FTP access:
 - User name: siemens
 - Password: siemens
 - Transmission mode: Binary

Once it receives the file, the device updates the firmware and restarts automatically.

MIBs for X-200

A.1 Important MIB variables

Important MIB 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

Variables	Access rights	Description
sysDescr	Read only	A string with up to 255 characters is used. This value contains the manufacturer's device ID.
sysObjectID	Read only	The address (object identifier) used to access device-specific SNMP variables is output here: 1.3.6.1.4.1.4196.1.1.5.2.nnn.mmm
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
sysLocation	Read and write.	The device location can be entered here (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: <ol style="list-style-type: none"> 1. Physical (for example repeater) 2. Datalink/subnet (for example bridges, switches) 3. Internet (for example IP gateways, routers) 4. End to end (for example IP hosts) 5. - 6. - 7. Applications (for example e-mail servers), data type: 32-bit integer

Variables in the Interface directory

Variables	Access rights	Description
ifNumber	Read only	The number of different interfaces available in the component. Possible values: 4...8.
ifDescr	Read only	A description and possibly additional information for a port. Possible value: string with a maximum of 255 characters
ifType	Read only	The value ethernet-csmacd(6) or optical(65) is entered for SCALANCE X-200.
ifSpeed	Read only	Data transfer rate of the Ethernet port in bits per second. With SCALANCE X-200 devices, this is either 10 Mbps or 100 Mbps.

A.2 Important private MIB variables

Variables	Access rights	Description
ifOperStatus	Read only	The current operating status of the Ethernet port. The following values are possible: <ul style="list-style-type: none"> up(1) down(2)
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.
ifInErrors	Read only	Number of received packages that were not forwarded to higher protocol layers because of an error.
ifOutErrors	Read only	Number of packages that were not sent because of an error.

A.2 Important private MIB variables

Important private MIB variables

The private MIB variables of the IE Switch X-200 have the following object identifier (OID):

iso(1).org(3).dod(6).internet(1).private(4).enterprises(1).
ad(4196).adProductMibs(1).simaticNet(1).iScalanceX(5).iScalanceX200(2)

Variables	Access rights	Description
snX200FaultState	Read and write.	Displays the error status of the device. Possible values: <ul style="list-style-type: none"> 1 No error 2 Error
snX200ReportFaultIndex	Read only	Errors are assigned an ascending index according to the order in which they occur. This 4-byte variable specifies the index.
snX200ReportFaultState	Read only	Contains the error message belonging to an index.
snX200FaultValue	Read only	This 4-byte long variable provides the current error statuses of the device bit-coded.
snX200RmState	Read only	Indicates whether the redundancy manager is active or passive. Possible values: <ul style="list-style-type: none"> 1: The redundancy manager is passive. The IE Switch X-200 is operating as redundancy manager and has opened the ring. In other words, the bus with the IE Switches X-200 connected to it is operating correctly. The "Passive" status is also shown when the redundancy manager mode is disabled. 2: The redundancy manager is active. The IE Switch X-200 is operating as redundancy manager and has closed the ring. In other words, the line of X-200 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.
snX200RmStateChanges	Read only	Indicates how often the redundancy manager was switched to "active".
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.
snInfoSerialNr	Read only	The serial number of the product.
snMacAddressBase	Read only	The MAC address of the X-200 IE switch.
snSwVersion	Read only	The software version of the system.
snInfoMLFB	Read only	The MLFB number of the device.

A.2 Important private MIB variables

Variables	Access rights	Description
snX200PowerSupplyState	Read only	<p>State of the redundant power supply:</p> <ul style="list-style-type: none"> 1: redundant supply 2: no redundant supply <p>Note: The following devices do not have a redundant power supply:</p> <ul style="list-style-type: none"> SCALANCE X204IRT PRO SCALANCE X201-3P IRT PRO SCALANCE X202-2P IRT PRO
snX200HsrRmMode	Read and write.	<p>Redundancy manager mode in an HRP ring</p> <ul style="list-style-type: none"> 1: The X-200 IE switch is a redundancy manager. 2: The X-200 IE switch is not a redundancy manager.
snX200MrpRmMode	Read and write.	<p>Redundancy manager mode in an MRP ring</p> <ul style="list-style-type: none"> 1: The X-200 IE switch is a redundancy manager. 2: The X-200 IE switch is not a redundancy manager.

Default ring ports

Default ring ports of the IE switches SCALANCE X-200

SCALANCE X200 and SCALANCE XF200	
Product name:	Default ring ports:
X208	P1 and P2
X208PRO	P1 and P2
X216	P1 and P2
X224	P1 and P2
X204-2	P5 and P6
X204-2TS	P5 and P6
X206-1	P1 and P2
X212-2	P13 and P14
X204-2LD	P5 and P6
X206-1LD	P1 and P2
X212-2LD	P13 and P14
Flat design:	
XF204	P1 and P2
XF208	P1 and P2
XF204-2	P5 and P6
XF206-1	P1 and P2

SCALANCE X200IRT and XF200IRT	
Product name:	Default ring ports:
X204IRT	P1 and P2
X204IRT PRO	P1 and P2
X200-4P IRT	P3 and P4
X201-3P IRT	P3 and P4
X201-3P IRT PRO	P3 and P4
X202-2IRT	P3 and P4
X202-2P IRT	P3 and P4
X202-2P IRT PRO	P3 and P4
Flat design:	
XF204IRT	P1 and P2
XF204-2BA IRT	P1 and P2

Encryption methods used (ciphers)

The following tables list the encryption methods (ciphers) that use SCALANCE X-200.

SSL

Name of the service	HTTPs WBM
Port	443
Client/Server	Server

Category	Official name	Hexadecimal value	Enabled by default
Encryption suite	TLS_ECDHE_ECD-SA_WITH_AES_256_GCM_SHA384	c02c	Yes
Encryption suite	TLS_ECDHE_ECD-SA_WITH_AES_256_CBC_SHA384	c024	Yes
Encryption suite	TLS_ECDHE_ECDSA_WITH_AES_256_CCM	c0ad	Yes
Encryption suite	TLS_ECDHE_ECD-SA_WITH_AES_128_GCM_SHA256	c02b	Yes
Encryption suite	TLS_ECDHE_ECD-SA_WITH_AES_128_CBC_SHA256	c023	Yes
Encryption suite	TLS_ECDHE_ECDSA_WITH_AES_128_CCM	c0ac	Yes
Protocol version	TLSv1.2	-	Yes

SSH

Name of the service	SSH CLI
Port	22
Client/Server	Server

Category	Official name	Hexadecimal value	Enabled by default
Encryption method (enc)	aes128-ctr	Not available	Yes
Encryption method (enc)	aes192-ctr	Not available	Yes
Encryption method (enc)	aes256-ctr	Not available	Yes
Host key	ecdsa-sha2-nistp256	Not available	Yes
Key exchange (kex)	curve25519-sha256	Not available	Yes
Key exchange (kex)	curve25519-sha256@libssh.org	Not available	Yes

Category	Official name	Hexadecimal value	Enabled by default
Key exchange (kex)	ecdh-sha2-nistp256	Not available	Yes
Key exchange (kex)	ecdh-sha2-nistp384	Not available	Yes
Key exchange (kex)	ecdh-sha2-nistp521	Not available	Yes
MAC	hmac-sha2-256	Not available	Yes
MAC	hmac-sha2-512	Not available	Yes
Protocol version	SSHv2.0	Not available	Yes

SNMP

Name of the service	SNMP
Port	161
Client/Server	Server

Category	Official name	Hexadecimal value	Enabled by default
Authentication	HMAC-MD5-96	Not available	No
Authentication	HMAC-SHA-96	Not available	No
Encryption	des-cbc	Not available	No

Index

A

Addressing the ports, 47

B

Bus topology, 24

C

CLI

Syntax, 46

CLI command

Shortcuts for commands, 46

Symbolic representation, 47

Compatibility

Firmware, 55, 57, 166

Configuration Manual, 3

Console, 45

D

DHCP, 38

F

Firmware

Compatibility, 55, 57, 166

G

Glossary, 6

H

HRP, 33

I

IP address, 38

Configuration options, 38

Isochronous Real-time Ethernet, 19

L

LEDs, 44

M

Media redundancy methods, 33

MIB, 153

N

NCM PC, 39

O

Object Identifier

OID, 176

OID

Object Identifier, 176

Operating instructions, 3

P

Passwords

Factory default, 44

R

RFC

RFC 1518, 37

RFC 1519, 37

Ring topology, 26

S

Selection Tool, 4

SIMATIC NET glossary, 6

SIMATIC NET manual, 5

SIMATIC NET Selection Tool, 4

SNMP

supported versions, 153

Star topology, 25

STEP 7, 38

Subnet mask, 38

Support, 45

Syntax

CLI, 46

System manual, 4, 5