SIPROTEC 4

Ethernet Module EN100 for IEC 61850 with electrical/optical 100 MBit Interface

Manual

Edition: June 2012

C53000-G1140-C167-10

Disclaimer of Liability

We have checked the text of this manual against the hardware and software described. However, since deviations cannot be ruled out entirely, we do not accept liability for complete conformity or for any any errors or omissions.

The information given in this document is reviewed regularly and any necessary corrections will be included in subsequent editions. We appreciate any suggested improvements.

Subject to technical modifications without notice.

Document version: 01.09.00

Registered Trademarks

SIPROTEC, SINAUT, SICAM and DIGSI are registered trademarks of Siemens AG. Other designations in this manual may be trademarks that if used by third parties for their own purposes may violate the rights of the owner.

Siemens Aktiengesellschaft

C53000-G1140-C167-10

Preface

Content of this manual

This manual describes the EN100-Module, protocol version IEC 61850, which can be used in all SIPROTEC 4 units.

It is divided into the following sections:

- Introduction → Chapter 1
- Design of the Ethernet Modules → Chapter 2
- Commissioning in the Device → Chapter 3
- Integration Into Networks → Chapter 4
- IEC 61850 Conformance Statements → Chapter 5
- Parameterization → Chapter 6
- Additional Information → Chapter 7
- Troubleshooting Hints → Chapter 8
- Diagnostic Functions → Chapter 9
- Technical Data → Chapter 10
- Checklist for Commissioning → Chapter 11
- Appendix → Chapter 12

For general information on the operation, installation, commissioning, and configuration of SIPROTEC 4 units, please refer to the SIPROTEC 4 System Description (Order No.: E50417-H1140-C151).

EN100-Module Specification

The specification of the EN100-Module conforms to international standard IEC 61850. The most relevant part is Part 8:

- ❑ IEC 57/617
  "IEC 61850-8-1: Communication networks and systems in substations - Part 8-1: Specific communication service mapping (SCSM) - Mappings to MMS (SISOI/ IEC 9506 Part 1 and Part 2) and to ISO/IEC 8802-3"

Applicability of this manual

This manual is valid for SIPROTEC 4 units:

- IEC 61850 (device firmware version 4.60 and later) with
- EN100 communication module, version 02.00.05 and later

The following must be used for device parameterization:

- DIGSI, version 4.60 and later
- EN100-Module device basic profiles (device-specific XML description to be found in DIGSI)

Edition 2 of IEC 61850

Edition 2 of IEC 61850 is supported by EN100 firmware version 4.20 and higher, together with the DIGSI 4 version 4.86 and higher. Both firmware versions are a prerequisite for the use of Edition 2.

Additional support

For any questions concerning the SIPROTEC 4 system, please contact your Siemens representative or support hotline.

Training courses

For individual courses being offered, please refer to our Training Catalog, or ask our training center in Nuremberg.

Target audience

Protection engineers, commissioning engineers, personnel concerned with adjustment, checking, and service of selective protective equipment, automatic and control facilities, and personnel of electrical facilities and power plants.

Safety Information

This manual is not a complete index of all safety measures required for operation of the equipment (module, device). However, it comprises important information that must be noted for purposes of personal safety, as well as in order to avoid material damage. Information is highlighted and illustrated as follows according to the degree of danger:

DANGER

DANGER means that death or severe injury **will** result if the measures specified are not taken.

- Comply with all instructions, in order to avoid death or severe injuries.

WARNING

WARNING means that death or severe injury **may** result if the measures specified are not taken.

- Comply with all instructions, in order to avoid death or severe injuries.

CAUTION

CAUTION means that or medium-severe or slight injuries **can** occur if the specified measures are not taken.

- Comply with all instructions, in order to avoid moderate or minor injuries.

NOTICE

NOTICE means that property damage **can** result if the measures specified are not taken.

- Comply with all instructions, in order to avoid property damage.

NOTE

Important information about the product, product handling or a certain section of the documentation, which must be given particular attention.

Qualified Electrical Engineering Personnel

Only qualified electrical engineering personnel may commission and operate the equipment (module, device) described in this document. Qualified electrical engineering personnel in the sense of this manual are people who can demonstrate technical qualifications as electrical technicians. These persons may commission, isolate, ground and label devices, systems and circuits according to the standards of safety engineering.

Typographic and symbol conventions

The following text formats are used when information from the device or for the device appears verbatim in the text flow:

`Parameter names`, i.e. designators of configuration or function parameters that may appear word-for-word on the display of the device or on the screen of a personal computer (with DIGSI), are marked in bold letters of a monospace type style. The same goes for the titles of menus.

`Parameter options`, i.e. possible settings of text parameters that may appear word-for-word on the display of the device or on the screen of a personal computer (with DIGSI), are written both in italics and in bold letters of a monospace type style. The same goes for the options in menus.

`"Annunciations"`, i.e. designators for information, which may be output by the device or required from other devices or switchgear, are marked in a monospace type style in quotation marks.

The above conventions may not be followed in drawings when the type of designator is obvious from the illustration.

Change Log

List of the changes between both versions of this manual:

Modified Chapter/ Pages	Version	Reason for the change
_	1.0	First edition Order No.: C53000-B1174-C167-1 8.7.2004
Chapter 7	1.1	Revision and addition in chapter 7 Order No.: C53000-G1140-C167-2
Chapter 5	1.2	Corrections in chapter 5, Conformance Statement Order No.: C53000-G1140-C167-3
Chapter 5.2 Chapter 7.1	1.3	Corrections in chapter 5.2, Conformance Statement and Chapter 7.1, Time synchronisation Order No.: C53000-G1140-C167-4
	1.4	Extension for the die optical interface Order No.: C53000-G1140-C167-5
Chapter 3 Chapter 4 Chapter 7.2 Chapter 7.3 Chapter 9 Chapter 11 Chapter 12	1.5	Correction in relation to RSTP-Parameter settings Extension for the Configuration information Information for the switching command has been adapted. Description for the RSTP has been extended. FEC-Page has been added including the description of the information value Checkliste has been new created Technical Appendix has been new created Order No.: C53000-G1140-C167-6
Chapter 3.4.2 Chapter 4 Chapter 5.2.1 Chapter 6.2 Chapter 6.3 Chapter 6.4 Chapter 7.1 Chapter 7.1.3 Chapter 7.3 Chapter 7.4.4 Chapter 9 Chapter 11 Chapter 12 Appendix	1.6	Preconfigured Report Control Block Corrections on partial texts Time accuracy and resolution of Time Sync Definition Measurement threshold Memory management New chapter: Communication with the IEC61850 client Extensions Time synchronisation (redundant time server) New chapter: Function of redundant time server Extensions Module information display / module information homepage New: Display of RSTP information using Bridge MIB Update Module Homepage Changing of some screenshots / Supplementary texts Marginal textual changes New chapter: System versions vs. functionality Order No.: C53000-G1140-C167-7

Modified Chapter/ Pages	Version	Reason for the change
Chapter 2.1 Chapter 3 Chapter 4 Chapter 7 Chapter 9 Chapter 11	1.7	Upgrading IP Address Description Upgrading RSTP Upgrading Module Homepage Description of the new module Order No.: C53000-G1140-C167-8
Chapter 4 Chapter 9 Glossary	1.8	Upgrading PRP Order No.: C53000-G1140-C167-9
Chapter 3 Chapter 4 Chapter 6 Chapter 7 Chapter 9 Glossary	1.9	Description of the new modules EN100-E+ and EN100-O+ (The old EN100-E and EN100-O modules will no longer be described) Upgrading HSR Description of IEC 61850, Edition 2 New Chapter 7.3: GOOSE-Stop Order No.: C53000-G1140-C167-10

Contents

Introduction

1

This chapter provides an introduction to EN100-Module, the IEC 61850 protocol implemented in it, and its use in conjunction with SIPROTEC 4.

1.1 How the Protocol Came About

A little history

Use of protection equipment in electrical installations developed as part of the general development of electrical engineering. It was initially electro-mechanical and then electronic.

This development was accompanied by extensive advances in telecontrol. Telecontrol is the control of electrical installations over large distances. This necessitated the definition of telecontrol protocols. These protocols were and, to some extent, still are very specialized in their application, and scope and handling of information.

The first digital protection devices over 20 years ago resulted in both more complex protection algorithms and vast data volumes. These data permit considerably enhanced and optimized power system management and provide very high-quality fault reports enabling comprehensive clarification even of complicated faults.

Substation and power control panel also developed rapidly using digital technology. This made it possible to acquire data volumes locally, i.e. in the electrical installation, to visualize them, and make them available for further processing. Today, such large volumes of power system data are usually processed on personal computers.

One problem that remained, however, was the variety of transmission protocols, often specific to one region. Moreover, lossless conversion from one protocol to another is not always possible because the scope and handling of information differs from one protocol to another.

Given the increasing concentration of control of electric power equipment, even across borders, this variety of protocols has become a great obstacle and, above all, a cost factor. This has led to a number of international standardization processes.

These processes aim at the use of Ethernet-based protocols and procedures, such as are encountered in office communications and PC networking. The reason for this focus was the widespread use of Ethernet in office automation, which means that a low-cost range of products is already available.

The results of these developments and experience was the IEC 61850[1] protocol. It has the advantage of being based on an international standard, permitting cross-border transmission of data from electrical installations. The most important element is the definition of data in the form of objects with a unique name and defined behavior. This ensures interoperability between devices from different manufacturers.

1. UCA was developed before this protocol. However, this protocol, which is also Ethernet-based, is essentially restricted to the American continent.and had never become an international standard.

1.2 Use in SIPROTEC 4 Units

EN100-Modules can be used in all SIPROTEC 4 units

The IEC 61850 protocol is implemented on an Ethernet EN100-module. There are also other protocols[1] and modules for SIPROTEC 4 units. The Ethernet module is installed in Port B (system interface) of the unit.

The modules are available with 2 RJ45 connectors or with 2 Duplex LC interfaces to be connected to an fiber-optic cable.

The physical interface is always duplicated to permit redundant structures.

The fiber-optic (FO) version of the module comprises the entire functionality of the module with the electrical interface, i.e. it can be used for an analog connection provided that the connecting switch is equipped with an optical interface. Moreover, these modules are provided with an integrated switch functionality which allows to establish redundant optical ring structures without external switches[2]. In this operation mode both switches are active.

The modules themselves are integrated into the DIGSI parameterization system as the IEC 61850 protocol, so that the necessary settings can be made there.

To integrate SIPROTEC 4 units into a network, the entire network must be appropriately parameterized. This parameterization is performed using the System Configurator, which is part of DIGSI.

1. For the SIPROTEC 4 units, the IEC 60870-5-103, PROFIBUS FMS, PROFIBUS-DP, MODBUS, and DNP3.0 protocols are also available.
2. An external switch is required for the connection/disconnection of control systems etc. without an integrated switch function..

Design of the Ethernet Modules

2

This chapter describes the mechanical design of the EN100-Module, including the design of the interfaces.

2.1 Mechanical Design

Module with RJ45 interface for flush mounting

Fig. 2-1 shows the mechanical design of the EN100-module with electrical interfaces. This module is installed in the system interface slot (port B) of the device CPU and is screwed to the device backplane. Both Ethernet connectors are accessible from the rear of the device, where they are connected to the network via a RJ45 connector.

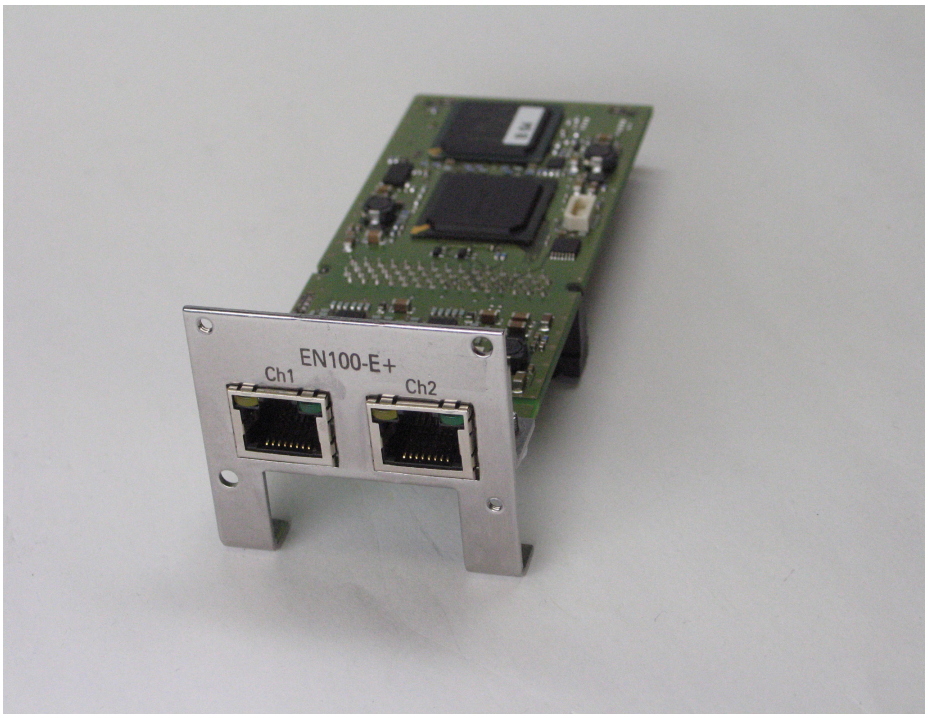


Fig. 2-1 Ethernet module EN100-E+ with RJ45 interfaces for flush mounting

Module with electrical interface for the surface-mounting housing

The module for the surface-mounting housing is connected to an IEC 61850 network via the console top unit shown in Fig. 2-2. The Ethernet cables are connected to the RJ45 interfaces of the console top unit. The connection is the same as in the module with electrical interface for flush mounting.

NOTE

Any upgrades of mounting devices with Ethernet function must be performed by Siemens AG.

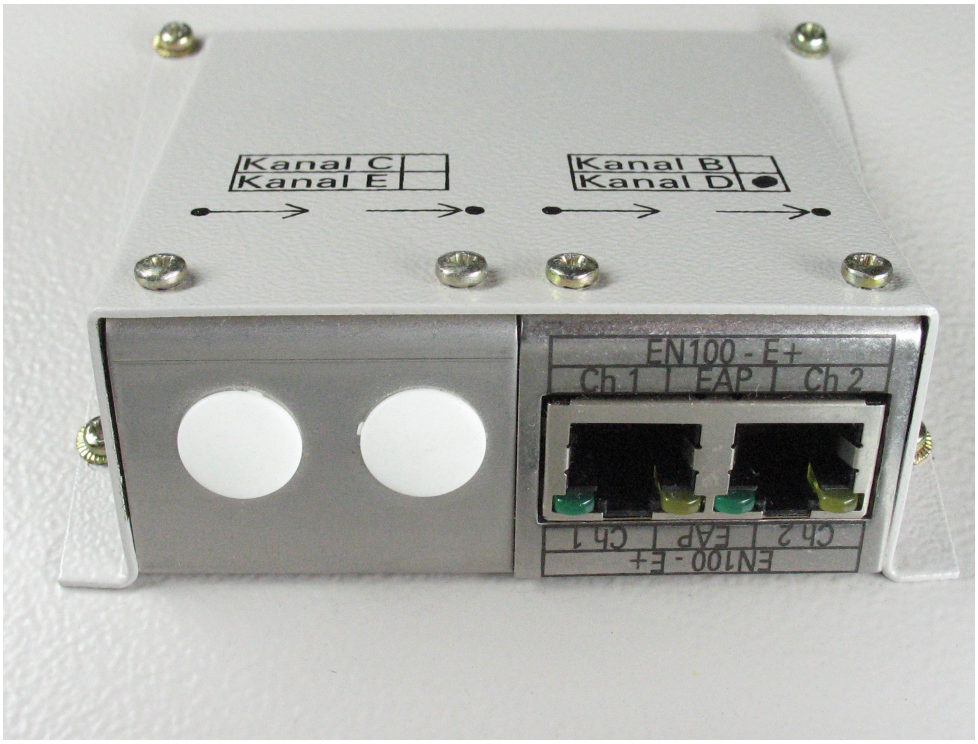


Fig. 2-2 Ethernet module EN100-E+ with electrical interface in the console top unit for surface-mounting housing

Module with optical interface

The design of the module with 2 optical interfaces is shown in Fig. 2-3. The module can be used like an electrical module with both optical interfaces. It also allows to build up ring structures. Telegrams received are not displayed on the module but on a display in the device.

This module is not available for devices in surface-mounting housing.

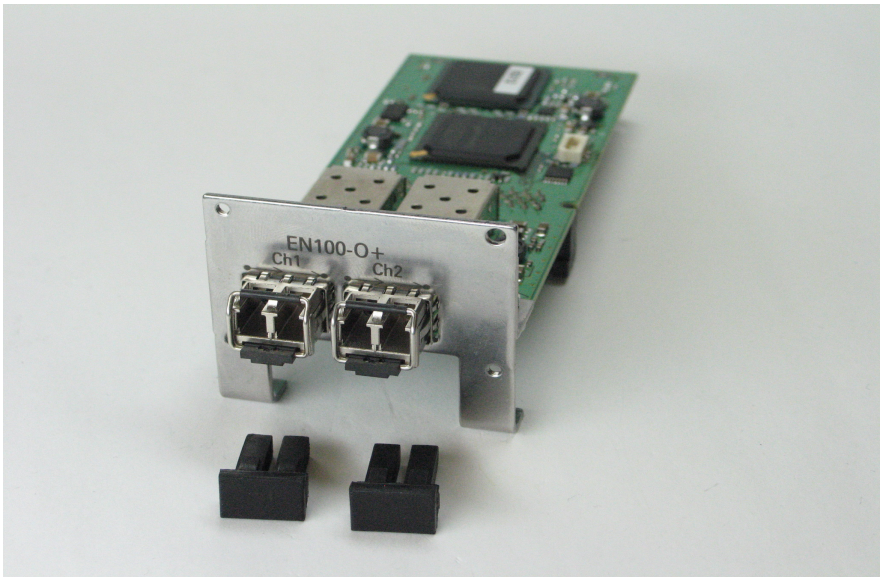


Fig. 2-3 Ethernet module EN100-O+ with Duplex LC interfaces

Components of all modules

The interfaces are available after installation of the module. However, aside from the actual module hardware, further conditions must be met before use. These conditions are:

- Device firmware, version V4.60 and later.
  The devices already contains the firmware on delivery. The firmware ensures compatibility between the device and the EN100-module. Devices with an older firmware version can be updated to make the functionality of the EN100-module available in existing devices.
- Module firmware.
  The device already contains the firmware on delivery. The firmware implements the IEC 61850 function, including interface control. The module firmware is also updatable. Updating is done using the firmware update program. Module firmware version 4.03 (on demand 3.09) and later is required for proper functioning of the device.
- DIGSI parameterization software, version V4.60 and later.
  This software is required both to set the module and to set parameters the IEC 61850 users with the System Configurator. Other power system components such as switches are not set with DIGSI/System Configurator.

No other components are required for the module to operate.

NOTE

If you use the EN100 firmware version 4.20 and higher with an old EN100-O module (with ST connectors), you cannot configure PRP and HSR (refer also to chapter 4.2).

2.1.1 Connector Design

Connectors for electrical interface on the version for flush mounting

The module can be recognized by its front cover, i.e. by the 2 RJ45 sockets as per IEEE 802.3 for 100Base-T connection on the rear of the device. Fig. 2-4 shows a view of the installed module, as seen from the rear of the device

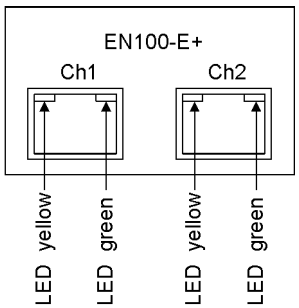


Fig. 2-4 View of an EN100-E+ module with RJ45 interfaces

Function of the LED

The socket of each of the 2 channels Ch1 and Ch2 has one yellow and one green LED to indicate the status of the channel. The yellow LED signals the link status. If the yellow LED lights up, there is a connection at link level. The green LED signals data communication. The flashing of a green LED means that data is being sent or received.

Connectors for electrical interface on version for surface mounting

The console top unit of the top assembly housing has the same connectors as the module for flush mounting, as shown in Fig. 2-4; the LED display, too, is in principle the same as in Fig. 2-4.

Connectors for optical interface on the version for flush mounting

The module with optical interface has the interfaces shown in Fig. 2-5. The interface design conforms with IEEE 802.3, 100Base-FX. It provides 2 channels, each with one transmitter and one receiver. The interface is supplied in Duplex LC. LEDs for display are not available. Corresponding information can be visualized on the device display or on the module homepage.

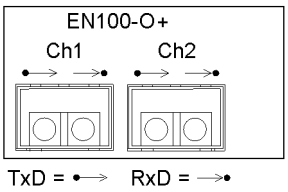


Fig. 2-5 View of the EN100-O+ module with Duplex LC interfaces

Commissioning in the Device

3

This chapter describes commissioning the EN100-module:

3.1 Getting Started

At a normal ordering process the customer will be delivered with the SIPROTEC 4 device including the Ethernet module and the suitable firmware installed. If devices are to be retrofitted with the EN100-module, the following installation procedure must be observed:

Software preparations

1. The module works directly with the device. It is necessary to ensure the device firmware is up to date before installing the module. Otherwise, the device may be inoperable after installation of the module. If this happens, uninstall the module and update the firmware.

Unpacking the module

2. The module is supplied in packaging from which you must remove it. Follow the instructions for handling electronic modules while you do so.

The device firmware must be version 4.60 or later, otherwise malfunctioning with the module cannot be ruled out. If this happens, remove the module, load the new firmware, and install the module again.

NOTE

An important part of the software preparations is ensuring that the device firmware, which supports operation and parameterization of the module, is up to date (version 4.60 or later) before installing the module.

Installing the module

Before starting to install the module, always disconnect the device from the power supply. Failing to do so endangers both your own safety and the device functions, such as the display.

Always use appropriate ESD equipment for work inside the device. Here are the instructions for installing the modules when upgrading existing devices. You will find detailed instructions on installing communication modules in SIPROTEC 4 units in the Internet under *http://www.siprotec.de* ⇨ *Devices* ⇨ *General information*.

Housing for flush mounting

The Ethernet module with electrical interface is produced in 2 variations: one for the housing for flush mounting housing and one for the housing for surface mounting. The module with optical interface is only produced for use in the housing for flush mounting. The installation of the module with optical interface is the same as for the module with electrical interface for flush mounting.

1. First open the front cover on the device. This is done be loosening the 4 screws - or six screws on 1/1 housings unavailable behind covers in the corners of the front cover. These are captive screws. Remove the front cover with care because it is connected to the CPU inside the device via a bus ribbon cable. Detach this cable. Attention: Press the latches sideways before pulling off the cable. This presses the cable out of the connector and prevents damage.
2. The next step is to detach the 2nd ribbon cable from the CPU, following the above instructions.

3. Before you can remove the CPU from the device in the next step, undo further screw connections on the rear of the device of any Non-Siemens protocol modules that may be installed. Otherwise damage may occur. In the case of the 6MD66, 7SD52, and 7SA522 units, the interface (D-sub socket) for time synchronization is also screwed to the backplane and must be detached.
4. Now the module can be inserted into the correct slot. It is then fixed to the CPU with 2 screws.
5. The device is re-assembled in reverse order of disassembly as explained above. Attention: The 2 ribbon cables must also be re-attached!
6. The last step is to fix the module to the rear of the device with 2 screws. Refasten any further screw fixtures for modules in other slots and the interface of the time synchronization input.

This completes installation of the module. The device is now in the as-delivered state with the Ethernet module.

Housing for surface mounting

Installation of a module in a housing for surface mounting is much more difficult and should not be performed by the customer or service technicians. Upgrading in the factory is recommended.

Module with optical interface

The installation of the module with optical interface is the same as for the module with electrical interface for flush mounting **(Important: the modules with optical interface are not available for devices with surface-mounting housing!)**

Loading the protocol software (IEC 61850)

If a module without module firmware[1] is installed in the device, the appropriate firmware must be loaded into it. The module firmware for this can be obtained in the internetworking under *http://www.siprotec.com*. Loading the firmware is similar to the device firmware update via the front interface.

From version 3.0 onward, the protocol software is the same for all module designs; i.e. there is no difference between modules with electrical and optical interface.

Update the firmware using the Ethernet interface with the module-firmware version 4.08 and higher (from July 2011).

Device settings

A SIPROTEC 4 unit is delivered with a parameter set and the front serial interface is active by default. The Ethernet module has already been routed an MAC address but no network settings have been made except that the module is DHCP-enabled.

If a device is integrated into a network with a DHCP server[2] in this state, i.e. an interface is connected to the network, it will automatically be accessed via the Ethernet interface. Reparameterization of the device using DIGSI is also possible. The full DIGSI functionality, with the exception of initialization, is supported. Initialization must be carried out via the front interface.

1. Modules normally come with the module firmware readily installed, so that this situation is not likely to occur; reloading the software should only be necessary after an update.
2. A DHCP server automatically assigns IP addresses. In that case, explicit setting is not required. The device is accessible as it is.

However, most substation networks do not contain a DHCP server. So it is necessary to set the network parameters using DIGSI. See Chapter 3.2.

Once the network parameters of the device have been set using DIGSI, the device must be initialized via the front interface before it can be accessed via Ethernet!

NOTE

Once the device is parameterized, the new parameter set will automatically be used That also applies to the Ethernet interface! If the Ethernet interface is incorrectly parameterized, the Ethernet interface may no longer function. Access is then only possible via the front interface!

Once the device has been parameterized and is in process operation in the network, the IP settings can be viewed but not changed on the display. If you do have to make a change, you will have to use DIGSI.

Direct link with DIGSI (electrical interface)

The device can be directly connected via the rear Ethernet interface to a PC with an installation of DIGSI. This requires a crossover cable. Module EN100-E+ offers auto-crossover functionality. Crossover cables are not needed for the connection to a PC. This enables direct contact with the PC without having to interpose a switch or hub.

Direct link with DIGSI (optical interface)

The device can be directly connected via the optical interface to a PC with an installation of DIGSI. This requires a standard optical/electrical interface converter since optical interfaces are normally not available on PC.

The optical interface knows the ’Line’ operating mode, which corresponds to the operating mode of the electrical module. No further settings are required for this.

The 'Switch' operating mode allows to build up ring structures. Such structures are always redundant. OSM[1] and RSTP[2] can be set as modes. OSM is a proprietary mode, which only works when combined with Siemens OSM switches.

Once the device is connected and started, the transmit and receive output can be read on the display if the connection works properly. For more information please refer to Chapter 7.3.

Link with the network

The link with the network is defined by the existing network. A distinction must be made between purely electrical power systems and networks which are equipped with optical components.

1. OSM, **O**ptical **S**witch **M**odule. This is a proprietary procedure of the Siemens AG
2. RSTP, **R**apid **S**panning **T**ree **P**rotocol, IEEE 802.1w is an international standard which is used world-wide.

Network with electrical components

This type of network usually consists of switches and devices with an Ethernet interface. The switches are the actual nodes in the network to which each device is connected.

Communication problems might occur if crossover cables[1] are used for the coupling between a switch and a PC. It is permitted to connect protection devices to a switch or to a PC with crossover cables.

The Ethernet module has 2 connectors as shown in Fig. 2-1. The link must be established according to the network topology of the project, i.e. to a switch or, in the case of redundancy, to 2 or more switches. Where a network structure contains 2 or more switches, they are normally interconnected.

Selecting the active channel

After power-on, the EN100-module attempts to establish a link on a channel. It is unimportant which channel is connected to a switch or PC. Alternate attempts are made to connect starting with channel Ch1. If both channels are connected and their switches are active, it is not possible to predict which channel will take the link. Correct operation of the interfaces is logged in the device's message buffer, and visualized on the device display.

If you operate the module in the redundancy type RSTP, PRP or HSR, the 2 channels are always active.

Special features of the optical module

The module with optical interface shown in Fig. 2-5 has basically 2 operating modes. It can be directly connected to the ports of an external switch, where it will work just like a module with electrical interface. The second operating mode is the 'Switch' mode of the module, which allows to build up ring structures in which the device interfaces are interconnected. In this structure the correct setting of the operating mode for the project using DIGSI is of prime importance. A wrong setting could lead to an overload of the network or to an interruption of the ring structure. For more information please refer to Chapter 7.3.

Cables for the electrical interface

In order to meet the specified immunity of the protection device, use at least cables of the CAT5 S/FTP type. This cable type offers a braided shield in the sheath. Strand pairs are provided with a foil shield.

Siemens recommends a maximum cable length of 20 m.

Cables for the optical interface

Use multimode fiber-optic cables (G50/125 µm or G62.5/125 µm) with Duplex-LC connectors. The maximum length of the multimode fiber-optic cable is specified at 2 km. The interface works with light whose wavelength is 1.310 nm.

1. Where switches with a so-called auto-cross function are used, any cables may be used.

Network with optical component

Such networks always have a redundancy feature, except in cases where the devices are connected via an optical link with a port of an external switch. This scenario would be equivalent to a network with electrical components, and will not be dealt with here.

The redundancy capability of optical networks is based on certain procedures; of these, RSTP, PRP, HSR and OSM are implemented in the EN100-module. The great advantage of the EN100-module with optical interface is that the modules can be directly connected with one another. Only one external switch is required for connection with the control center. The connections run in a ring from transmitter to receiver etc. In combination with the integrated switch of the optical modules, they allow to build up redundant connections. The structure is shown in Fig. 3-1.

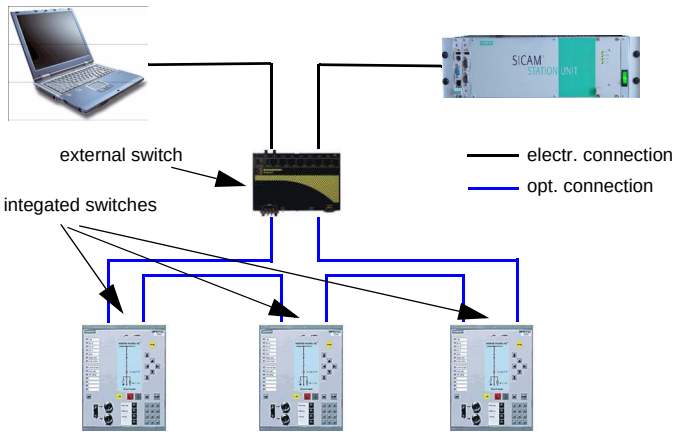


Fig. 3-1 Structure of an optical ring

3.2 Parameter Settings in DIGSI

The previous section explained how to install a module. Installing the module permits connection via Ethernet. However, there are still settings to be made concerning the connection with the device and the network or network applications.

Preparing DIGSI

Before setting the parameters, you should make sure that the device catalog of your DIGSI parameterization software contains the device to be parameterized in the required version. If it does not, the correct device driver must be obtained and installed.

Preparing the device

The devices of a substation are inserted from a device catalog in the station manager of DIGSI and parameterized with DIGSI. This includes making the correct settings for the interfaces. This gives you a view of the substation in which you can select the device and access the settings via *Device* ⇨ *Object Properties* as shown in Fig. 3-2. DIGSI is offline for the following steps, i.e. there is not active serial link to the device.

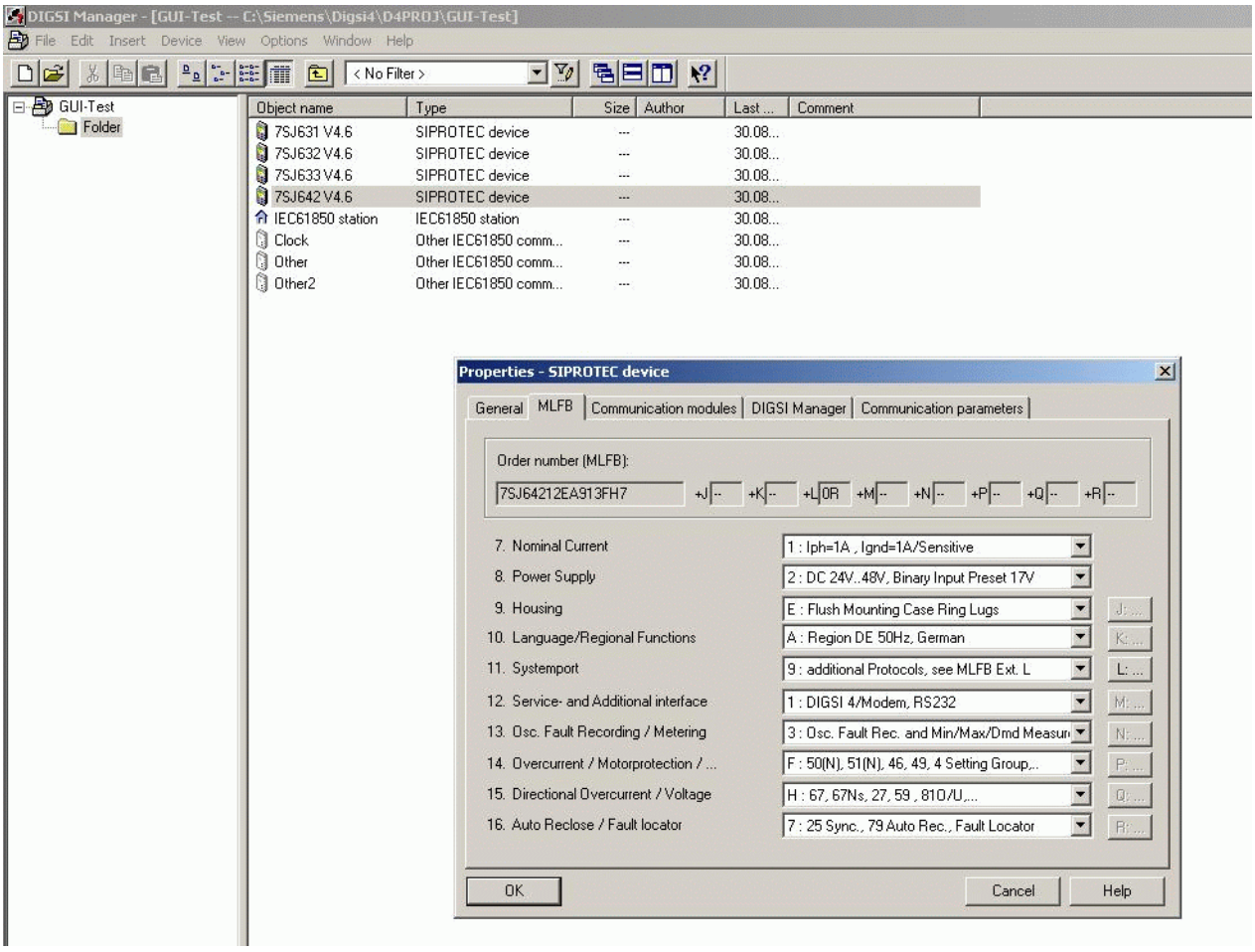


Fig. 3-2 Settings according to the order number (MLFB) of the device

Selecting the system interface

Set setting 11, system interface to *9:additional protocols* in the MLFB sheet. In a dialog that then opens (not shown here), set the IEC 61850 protocol for the interface. For the electrical Ethernet interface, select *L0R*. For the optical interface, select *L0S*.

Setting communication parameters

The communication parameter setting is made in a similar way to the MLFB setting and is shown in Fig. 3-3

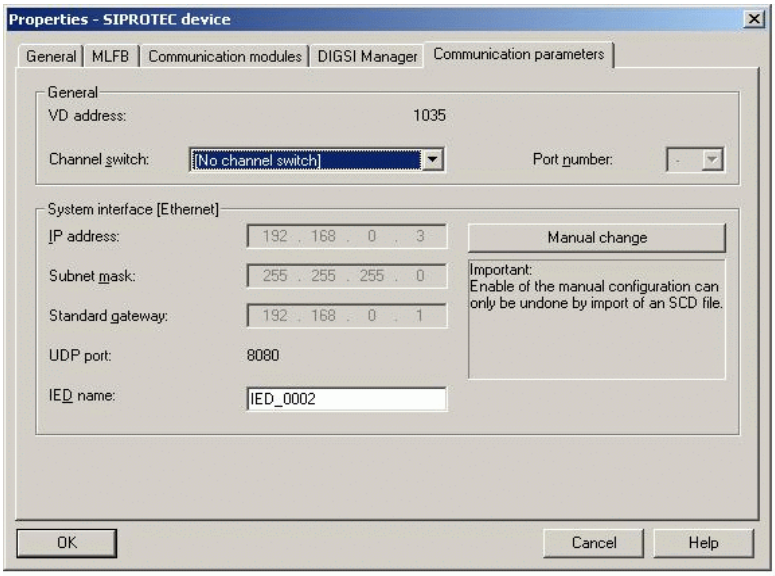


Fig. 3-3 Communication parameter setting

IED name

Set the IED name of the device first. The name can be freely selected. The only condition is that it must not start with a numerical digit and must not have more than 13 characters. It is then used as an identifier for the device in the system configurator in the IEC 61850 station in Chapter 3.3. The device names must not be duplicated.

Manual changes

By clicking the *Manual change* button, you can make network settings manually. That is necessary if you do not want to set the devices using the System Configurator and they will not be used in a station network parameterized in that way.

Addresses set for the system interface will be reassigned if an SCD file is created or imported. These addresses are then assigned as part of network parameterization and overwrite the individual settings.

Selection of the IEC 61850 Edition

It is possible to select between IEC 61850 Edition 1 and 2 in each SIPROTEC 4 device. It is possible to select the edition using the IEC 61850 object properties of the device. This setting is only possible if the device has not been assigned to any station.

It is possible to select the edition using the IEC 61850 object properties of the station. The setting is valid for all devices assigned to the station.

NOTE

If the edition of a device or a station is switched to Edition 2, the setting can no longer be changed. Siemens recommends archiving the DIGSI project before switching the edition.

NOTE

A SIPROTEC device can only be added to a station if the SIPROTEC device has the same edition as the station. Exceptions are not SIPROTEC-devices such as SICAM-PAS Client, SNTP Server, etc.

Setting IEC time synchronization

After setting the communication parameters, the selected device must be initialized as shown in Fig. 3-2. Fig. 3-4 shows the setting of the IEC 61850 time synchronization. If an Ethernet module exists in the device, time synchronization via SNTP is offered. If selected, time synchronization would be performed via the Ethernet network; this option is available both for electrical and optical interfaces. The settings for the SNTP server itself are made via the System Configurator and are not shown here. Redundant time servers are supported as of module firmware V3.09.

After these settings, the device must be saved and closed, because otherwise no ICD file is generated. This file is the precondition for work in the System Configurator, which is based on these files. The ICD files describe the communication properties of the device according to IEC 61850.

NOTE

Always close and save the device when you have changed a parameter. Otherwise no ICD file will be generated. An ICD file (a mapping of the device in a standard-compliant file) is required for further work with the device in the System Configurator.

Configure the ICD file in accordance with the edition settings.

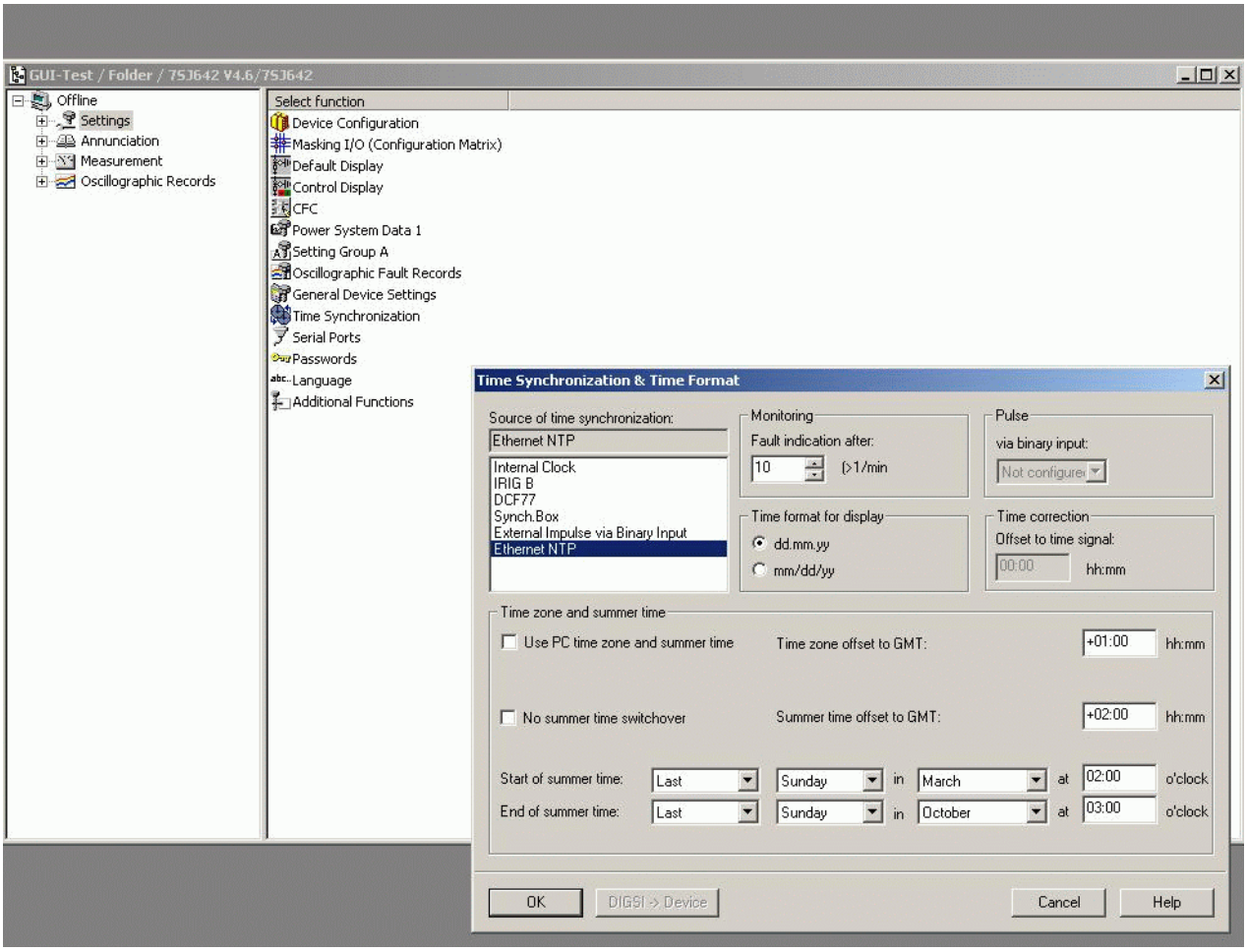


Fig. 3-4 Time synchronization setting via Ethernet and SNTP server

Setting the IEC Interface parameters

Setting the interface parameters includes setting the Ethernet interface, which can be operated not only as a purely electrical interface but also as a switch in various redundancy protocols.

For more details about these settings see Fig. 3-5.

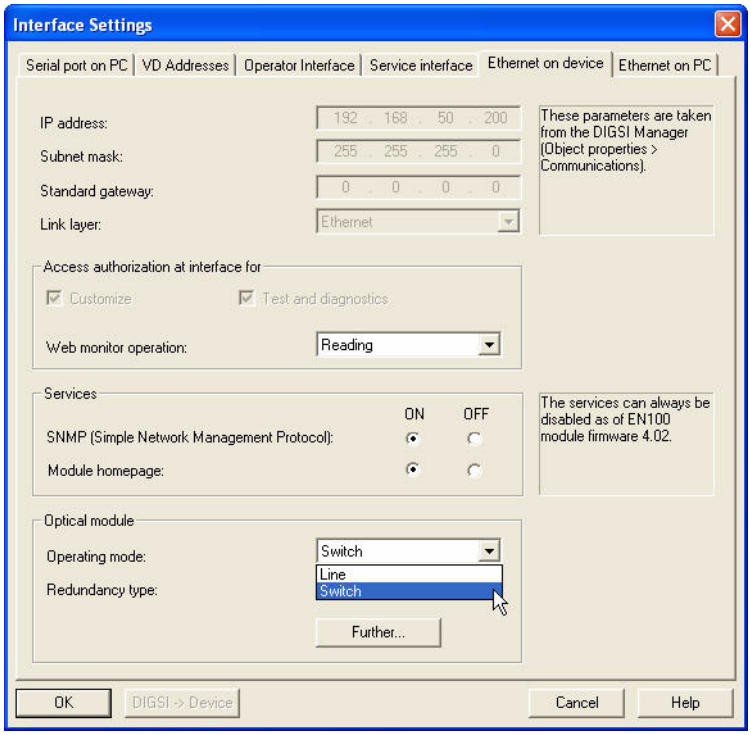


Fig. 3-5 Setting the operating mode of the optical module

Setting the operating mode of the optical module

The operating mode can be set to “line” or “switch”. The setting “switch” corresponds to the functionality of a switch with 3 ports. One is linked directly to the device and the other 2 ports are to form a ring structure (see also chapter 4.2. Network Structures).

Setting the redundancy type

If switch mode has been selected, the redundancy type must be set next. Available redundancy types are RSTP, PRP, HSR and OSM. The redundancy type depends on the network.

Redundancy type OSM

Redundancy type OSM is a proprietary procedure of the Siemens AG, and can only be used in combination with at least one external switch that is capable of this type of redundancy. One of the external switches has to be set as master.

Siemens does not recommend the redundancy type OSM in new station networks.

Redundancy type RSTP

This procedure is used world-wide, and is supported by nearly all switches. Fig. 3-6 shows the setting of the redundancy type.

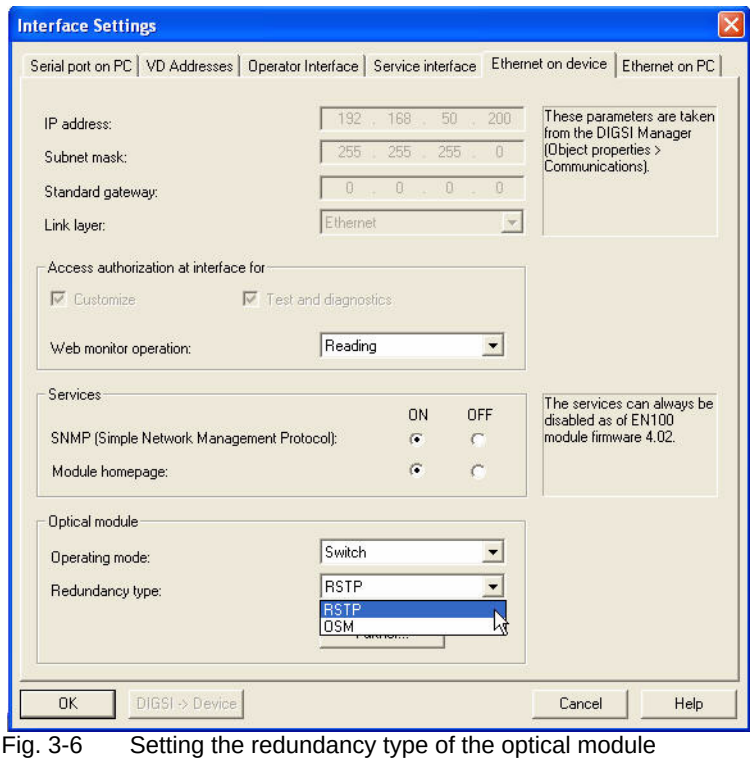


Fig. 3-6 Setting the redundancy type of the optical module

RSTP parameters

If redundancy type RSTP has been set, a number of other settings is possible. These settings are accessible by clicking the *More...* button; they are shown in Fig. 3-7.

NOTE

The RSTP parameter settings should only be changed if this is absolutely necessary. **In particular, the settings recommended in this manual (see Fig. 3-7) must be used.** The DIGSI default settings must be adapted accordingly. They will be harmonized in a future DIGSI version. For more details see Chapter 4.7 and Chapter 7.3.

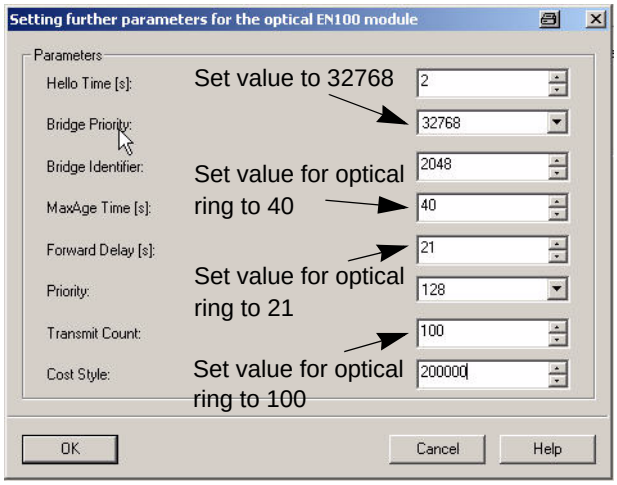


Fig. 3-7 Recommended setting of the RSTP parameters in DIGSI

Redundancy type PRP

The redundancy type PRP is a seamless procedure for parallel network according to IEC 62439-3:2012. If the parameter set of the device does not support this parameter, it is possible to select PRP by parameterization with RSTP. For this purpose, set the parameter **Cost Style** to ***-1*** and the parameter **Hello Time** to ***1***. The other parameters are not relevant for the setting of this operating mode. A prerequisite is that the EN100 firmware version is equal to 4.20 or higher.

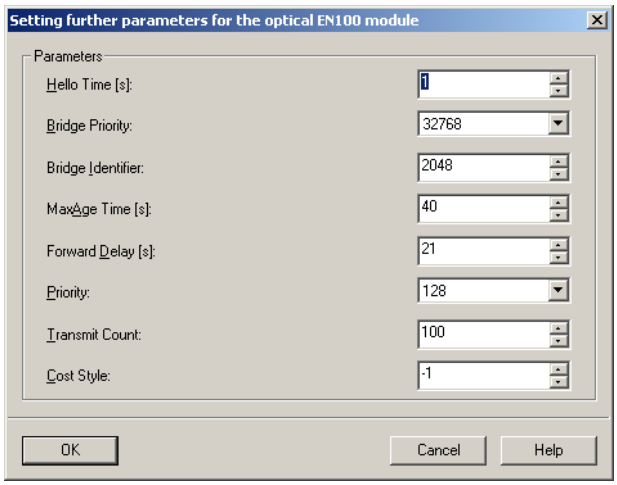


Fig. 3-8 Recommended setting of the PRP parameters in DIGSI

Redundancy type HSR

The redundancy type HSR is a seamless procedure for ring networks according to IEC 62439-3:2012. If the device's parameter set does not support this parameter, it is possible to select HSR by parameterization with RSTP. For this purpose, set the parameter **Cost Style** to ***-1*** and the parameter **Hello Time** to ***2***. The other parameters are not relevant for the setting of this operating mode. A prerequisite is that the EN100 firmware version is equal to 4.20 or higher.

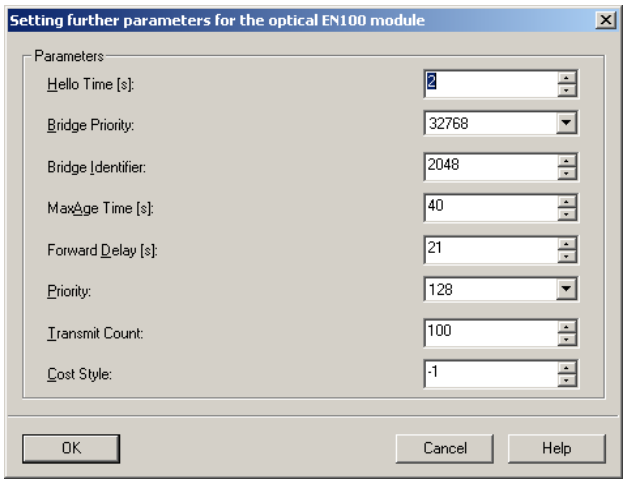


Fig. 3-9 Recommended setting of the HSR parameters in DIGSI

NOTE

Always close and save all device parameters, even when no parameters have been changed. Otherwise the parameter set will not be generated for EN100.

3.3 Setting on IEC 61850 Station in DIGSI

The assignment of the devices of a station with Ethernet interface according to IEC 61850 is made in the IEC 61850 manager by calling the System Configurator (IEC 61850 station).

The help system of the System Configurator in DIGSI provides a detailed description with an example. The following chapter provides an overview of the System Configurator and how it works. The point of departure is Fig. 3-2.

Inserting a station

The first step is to insert a IEC 61850 station. This station is parameterized in the following steps. This parameterization is the complete network-wide parameterization.

Inserting devices into the station

In the same way as the devices, the IEC 61850 station is selected and opened via Properties in the context menu. Fig. 3-10 shows the Properties sheet. Under the *Communicator* tab, the devices are added to the IEC 61850 Station.

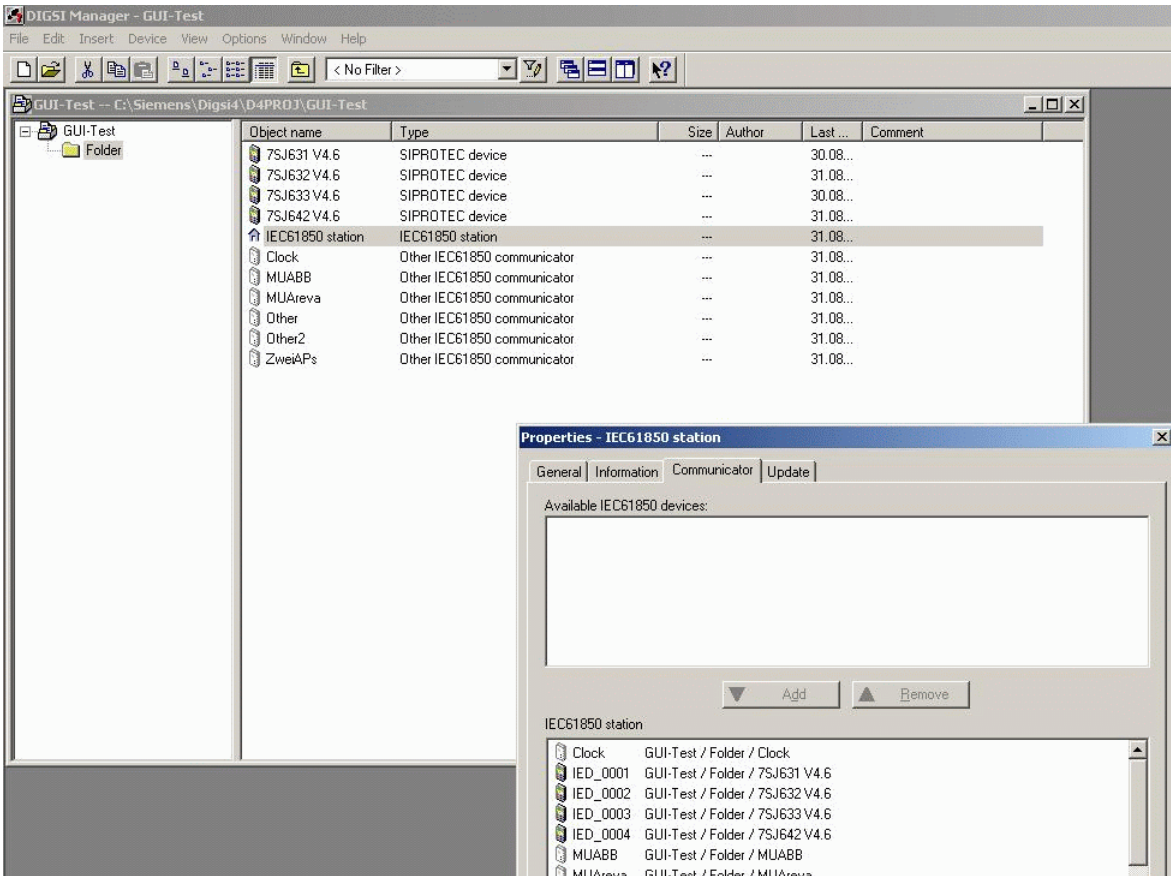


Fig. 3-10 IEC 61850 station, inserting devices

The Properties sheet lists the available IEC 61850 devices which can be selected. The available IEC devices are those for which a corresponding ICD file exists or that were generated by DIGSI (see item 3.2). This section is empty in Fig. 3-10 because all existing devices have been integrated into the station.

The lower part of the Properties sheet lists all devices that have been integrated into the station. This is done be dragging with the mouse devices from the upper to the lower part of the Properties sheet or by clicking the *Add* button.

The names of the devices correspond to those that were assigned to the devices as an IED name when setting the communication parameters in Fig. 3-3.

3.4 System Configurator

Work with the System Configurator now starts with a double-click on the station to be parameterized (unlike in the properties sheet that only permits assignment of devices to the station). The System Configurator is for implementing network settings and setting links between devices.

3.4.1 Network Settings

Fig. 3-11 shows the network settings. This is the user interface of the System Configurator when it first starts.

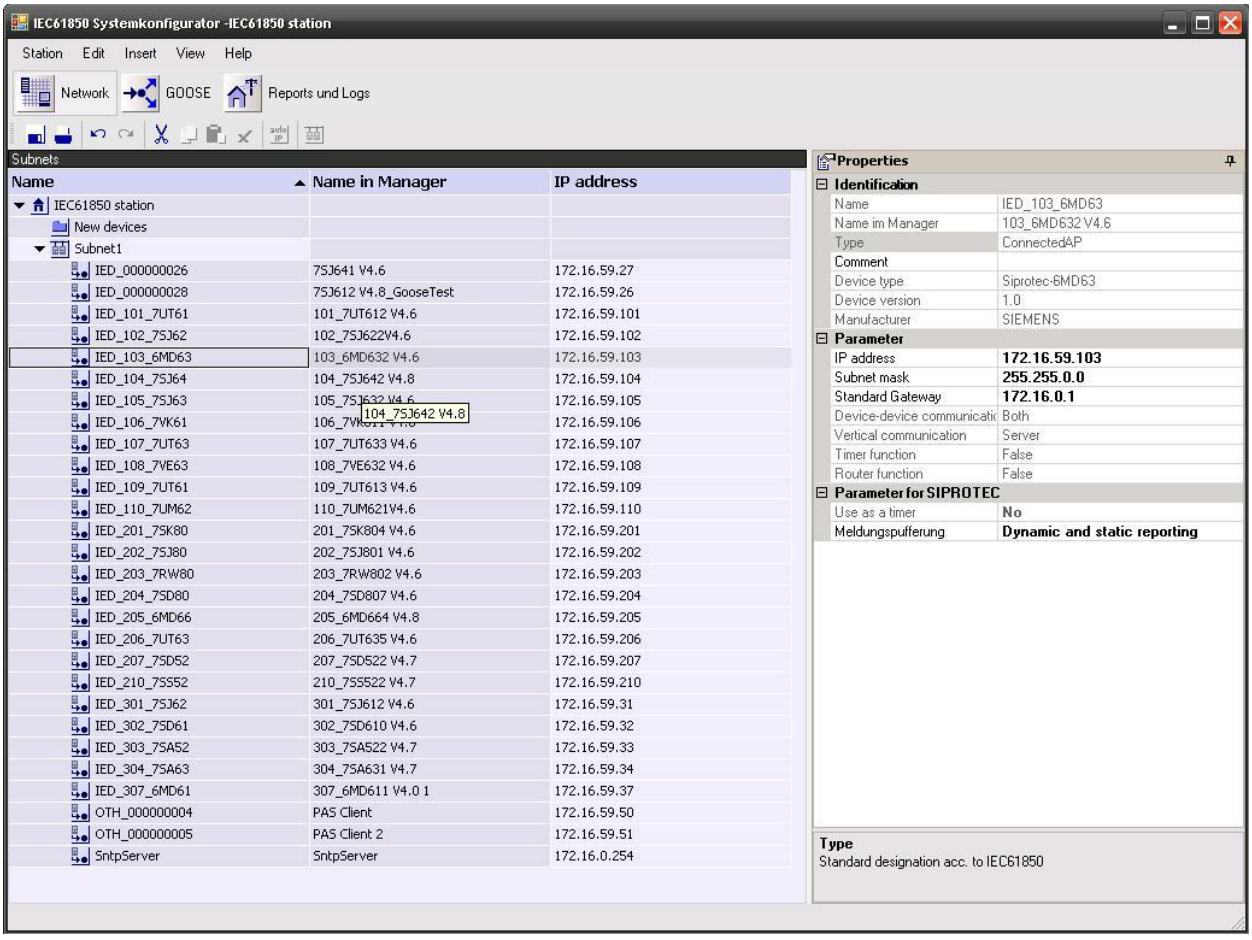


Fig. 3-11 System Configurator network settings

Display of the devices

This Explorer view shows the station that was opened at the top level. The subnets (if there are any) are below the station. The individual devices with their IED names can be seen below these networks. The devices can be selected with a bar and further properties are then shown on the right.

The upper part shows a description of the device to which comment can be added.

Network settings

The lower part is assigned to the network settings. The IP settings must be made there. The other information are further features that are supported and may be accessible via interconnections.

IP-addressing

For the IP addressing the typical operation of private addresses is recommanded. Varied address spaces are available.

Class A: 10.0.0.0 to 10.255.255.255 (max. 16 million participants)

Class B: 172.16.0.0 to 172.31.255.255 (max. 65000 participants)

Class C: 192.168.0.0 to 192.168.255.255 (max. 255 participants)

For small networks a Class B address is recommanded, that avoids possible bottlenecks for an extension of the network. Also a logical structure is represented by the IP addresses.

The IP stack used on the module doesn't allows a Class B subnet mask (255.255.0.0) for Class C addresses, but for a class B address a Class C subnet mask (255.255.0.0) could use. This means that a network with an 192.168.x.x address is limited to 255 participants.

Continuing network parameterization

You can add a device to a project in which part of the station has already been parameterized, as described in item 3.3. First find the device in the **New devices** subnet after opening the System Configurator and then integrate it into an existing subnet by dragging it with the mouse device.

IP-address Scheme

Think about a logical structure within your substation, for example, every device in substation 1 has IP-address 172.16.1.x, reserve an IP-address range for the Ethernet switches, for example, 1-10, so the 1st switch in every substation has address 172.16.x.1, for the 1st SIPROTEC ring reserve 11-40, for a second 41-70, etc.; so you know that 172.16.3.16 is the IP-address of the 6th SIPROTEC device in the 3rd substation.

Also reserve an IP-address range for your devices in the control center room, etc.

Such kind of logical scheme makes your life much easier in case of maintenance or fault clearance.

NTP clock server

The NTP servers are integrated as '*Other IEC 61850 communicators*' via an ICD File which is included in the DIGSI4 CD. 2 NTP servers are supported. The primary server is the preferential server. The secondary server uses as redundancy.

3.4.2 Interconnections

One advantage of IEC 61850 is that data traffic between devices can be parameterized to link applications on the devices. Fig. 3-12 shows the user interface implemented in the System Configurator.

Function and interconnection information

The upper half contains information that is either part of the device description (see left section with the node names), or that arises during further processing (center section showing the interconnection list created), or it contains further information about the application (right section).

Creating an interconnection

Interconnections are defined by a source and a destination. The source and destination are on different devices and possibly different nodes. They are shown in the lower half of the System Configurator in the Explorer view. They show all devices of the station that have such interconnections.

The devices are opened up to the required end point of source/destination. The required row and the opened source and destination points are activated with a double-click in the interconnection table, i.e. they are entered in the source and destination of the selected row. This completes the interconnection. This process is repeated until all interconnections required in the project have been completed.

GOOSE performance

Behind interconnections are multicast circuits in which GOOSE telegrams are routed.The performance of these connections depends on the *BufTim* set in the client for his Report Control Blocks (Buftim). For high-performance connections, the setting should not be less than 100 ms.

Preconfigured Report Control Block

The Report Control Block controls the procedures that are required for reporting values of data to the clients. The data can be buffered for transmission, such as data values are not lost due to transport flow control constraints or loss of connection. 2 Buffered Report Control Blocks are available for each logical device. Each report control block can serve only one client.

After completion of all work, close the System Configurator.

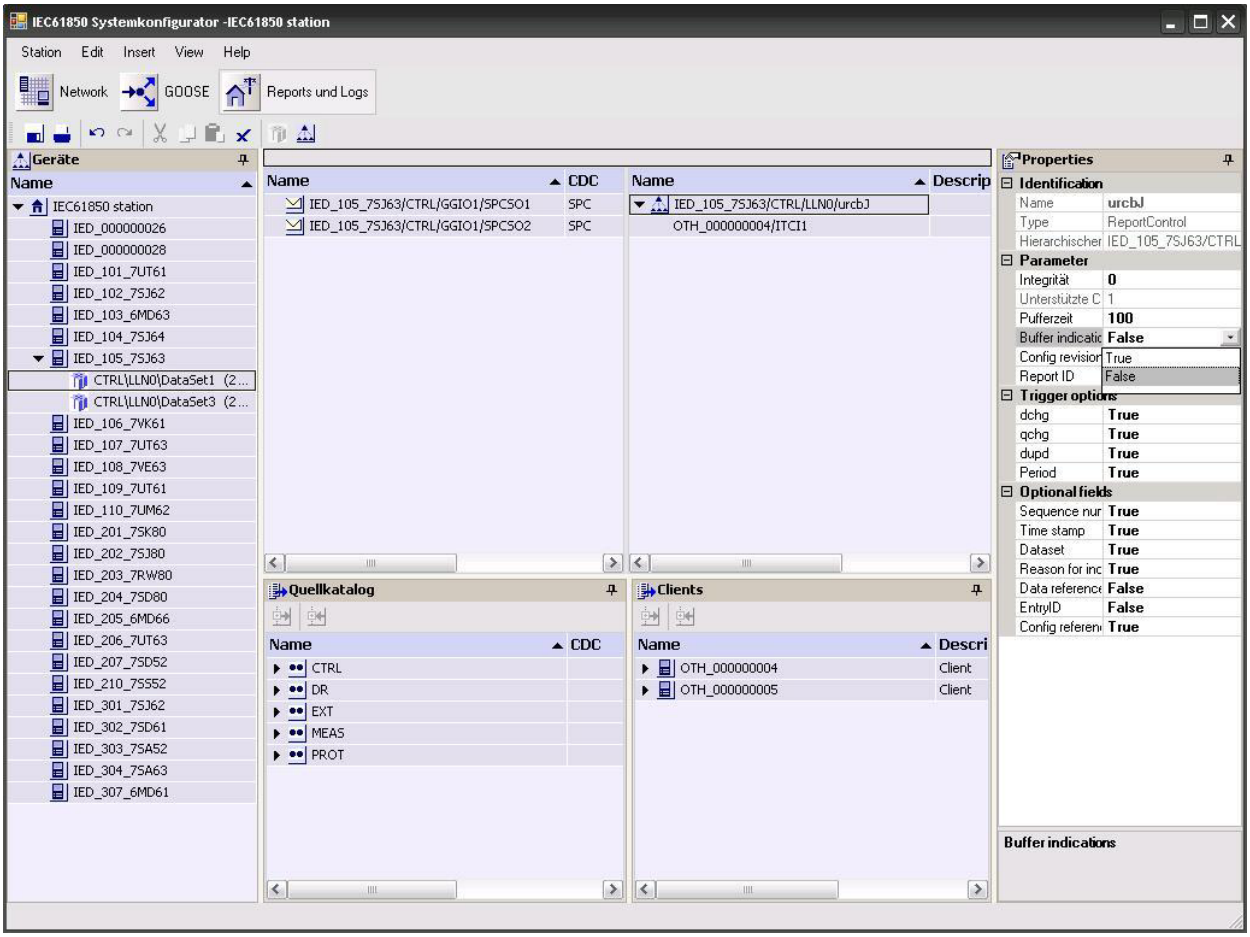


Fig. 3-12 System Configurator interconnections

3.4.3 Finishing Off the Configuration

To complete all work, both the device ICD files must be updated and the SCD file for all stations must be generated or regenerated. This is done on the Properties sheet of the station, as shown in Fig. 3-13.

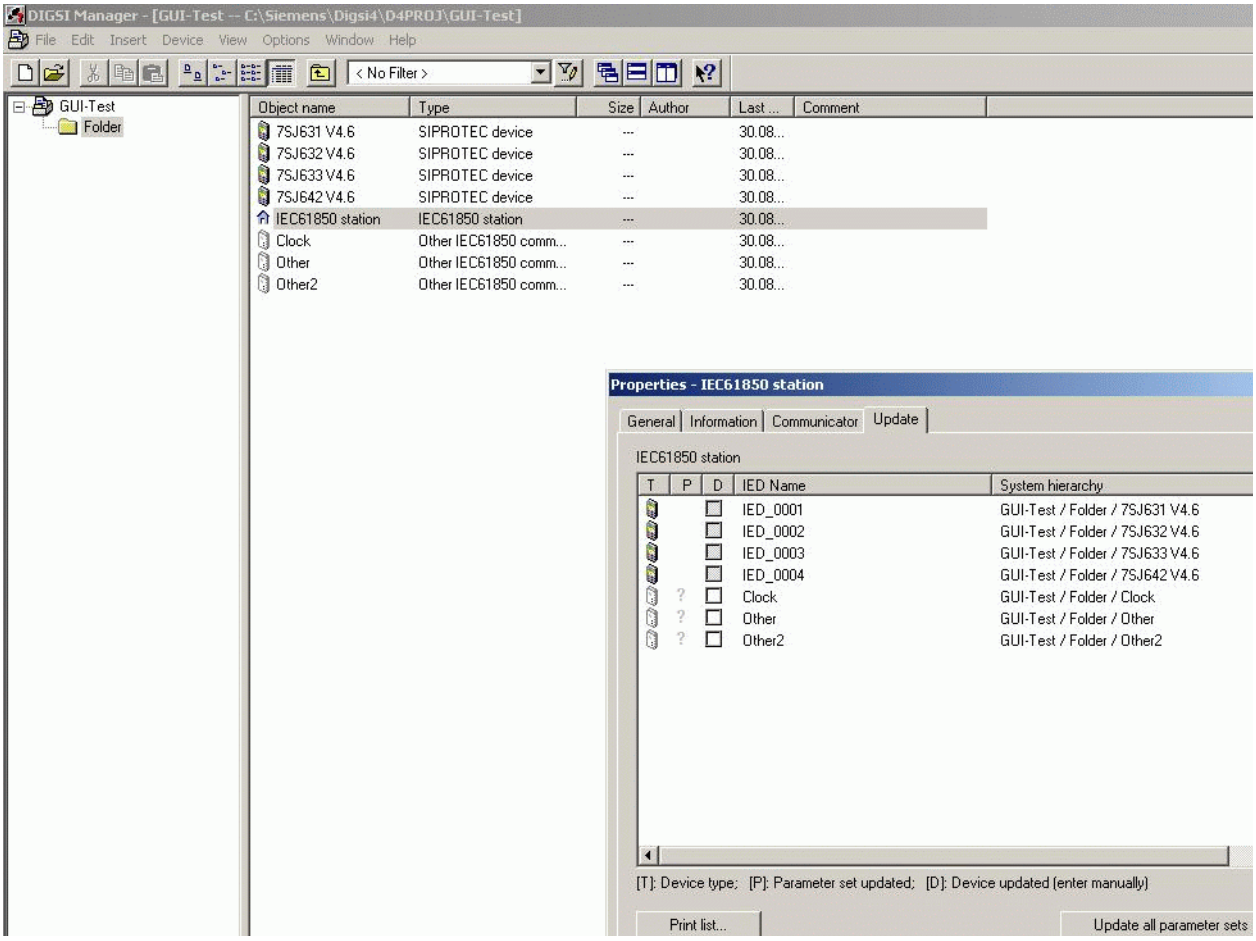


Fig. 3-13 Saving an ICD/SCD file

The Update tab is activated on the Properties sheet. All devices are listed there. The *Update all parameter sets* button updates all configuration files and parameterization in the System Configurator is completed. After this step, the SIPROTEC 4 devices can be connected with DIGSI online and new parameter sets assigned. Only if this is done is consistency of the entire network ensured. Updating the parameter sets does not automatically load the (changed) parameters into the devices!

NOTE

After completion of the work, it is necessary to load the device parameter sets into the devices to ensure system-wide consistency in the network. You can find further information in the online help of the System Configurator in DIGSI.

In projects involving interoperability with devices from other manufacturers, the operating programs of the manufacturer must be used to load the parameter sets into these devices.

Integration Into Networks

4

This chapter describes integration of the devices into a network. It describes special aspects of networks, address selection, switch positions, etc. in detail.

4.1 Network Parameters

MAC address

The MAC address is a transparent address that is permanently stored in the module. It is a worldwide unique identifier for the module. That means the devices can be integrated into any network. The user can only read the MAC address but not change it.

IP address

The IP address is also a unique identifier for a TCP/IP link. It is a 32-bit-wide number.

The IP address is assigned during configuration of a network in a station. It can be set via DIGSI during device parameterization and can also be set in the System Configurator. One exception to this is operation in a network with a DHCP server.

Subnet mask

This mask must be set according to the addressing scheme of the network.

SNTP address

This address is also a TCP/IP address with which the time server can be accessed in the network to ensure precise time synchronization of all devices.

Multicast addresse(s)

These addresses are required in connection with the GOOSE protocol to form multicast recipient lists and define links from one to several other devices. They are automatically assigned during network parameterization in the System Configurator depending on the interconnections made and are completely transparent for the user. They cannot be set on the device itself. GOOSE telegrams uses virtual MAC addresses only as target address. A real MAC address of a SIPROTEC device will never be used as target address. In consequence of a wide acceptance of GOOSE communications, large networks and numerous usage of GOOSE telegrams DIGSI supports a larger address range from 01:0C:CD:01:00:00 to 01:0C:CD:01:FF:FF.

Gateway address

This is the IP address of the gateway. It is required whenever an address outside the LAN of the station is to be accessed. It can only be set via DIGSI.

DHCP

DHCP is used to avoid having to set the above parameters individually. If DHCP is activated, the settings are provided by a DHCP server in the network. The only exceptions are the MAC address and multicast addresses. This function requires that a DHCP server be accessible in the network.

NOTE

To be able to work with DHCP, this feature must be activated in the device. It is activated in the as-delivered condition of the device. The IP addresses, subnet mask, and gateway are then set to zero.

SNMP V2

This protocol has been implemented in order to have access to information in a network in which other units, such as external switches, are administered as well. On the basis of this protocol, the accessible information can be invoked with any MIB browser. The MIB descriptions required for this are available in the internetworking at http://www.siprotec.com or http://www.siprotec.de. In particular, the statuses of the 2 lines are readable via SNMP using a MIB browser. This protocol is implemented in all modules. For more details please refer to Chapter 7.5.

4.1.1 Display of Network Parameters

Display on the device

The parameters of the interfaces can be viewed on the device display. This is done by entering the operating menu from the initial display via the menu key. There, displays are accessible via *Parameter* → *Setup/Extras* → *IP-Configuration* → *System-SST (Port B)*. The display includes:

- IP address
- Subnet mask
- Gateway
- Rights
- Link type

This shows the settings with which the device is working and that constitute the device parameter set. The settings can only be changed via the DIGSI parameterization system.

Please note the following special case. If address assignment via DHCP is activated via DIGSI/System Configurator, address 0.0.0.0 will be shown for the IP address, subnet mask, and gateway. In this case, DIGSI does not store an address in the parameter set. It is assigned by the DHCP server. In that case the System Configurator cannot be used because it works only with fixed addresses. IEC 61850 stations do not use this mode but works with fixed IP addresses.

Parameter display via browser

The above displays are accessible via the Ethernet interface if the device is selected with a browser. In that case, a front view of the device appears on the right side of the browser window. Using the mouse device, you can operate the device in a similar way to the real hardware.

The left side of the browser window shows further information made directly accessible from the protection unit. It is not explained here, as the page is self-explanatory and may differ from device to device. Please refer to the relevant device manual.

Not all devices feature parameter display via a browser. For further information, see chapter 9 and/or the relevant device manual.

4.2 Network Structures

The communication modules are available with the electrical and optical interfaces, with the optical interface providing an integrated switch functionality. This allows to integrate the IEC 61850 devices into nearly all network structures.

The communication module supports several operating modes. The following table shows which operating mode is available from which module firmware version on.

Table 4-1

Hardware	Connectors	Operating mode					Comment	Minimum EN100 Firmware versions*	FPGA versions*
			Integrated switch						
		Line	RSTP	PRP	HSR	OSM†			
EN100-E	RJ45	Yes	No	No	No	No	-	3.09	None (no FPGA)
EN100-O	ST	Yes	Yes	No	No	Yes	Discontinuated since 2010, replaced by EN100-O with LC connectors	3.09	408
EN100-O	LC	Yes	Yes	Yes‡	Yes**	Yes	-	4.02	503 (RSTP) 555 (only PRP) 515 (RSTP, PRP, HSR)
EN100-E+	RJ45	Yes	No	Yes††	No	No	Successor of EN100-E	4.20	604
EN100-O+	LC	Yes	Yes	Yes	Yes	Yes	Successor of EN100-O	4.20	704

*Siemens always recommends using the latest version
†OSM not recommended, only supported for backwards compatiblity
‡From firmware version 4.20 and FPGA version 515 (also in EN100 firmware version 4.10 and FPGA version 555)
**From firmware version 4.20 and FPGA version 515
†† If PRP- parameter is provided by the specific device.

Simple structure

Such a structure always requires so-called switches. A switch is a device to which devices are connected via 2 or more connections. It forms the hub at the center of a star topology. Switches can be interconnected to produce networks of different sizes.

.

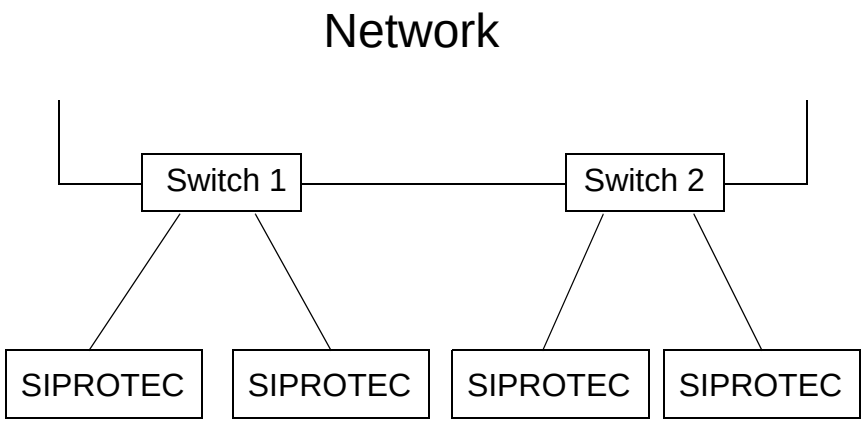


Fig. 4-1 SIPROTEC 4 units connected via a link

As is shown in Fig. 4-1, one SIPROTEC 4 unit is connected to each port of a switch. The link shown is an Ethernet link. The modules have 2 connectors of which only one is active at any one time. The connector selection is detected automatically by the module. This type of structure can be realized with all module types. A module with optical interface must be set to 'Line' mode.

“Line” mode

EN100-modules have generally 2 interfaces which are designed for either electrical or optical interfacing. This means that they can communicate via 2 Ethernet cables, but not simultaneously. The second channel is a standby. This results in the network structures shown in Fig. 4-2 illustrating connection of 2 links to different switch ports. A module with optical interface must be set to 'Line' mode.

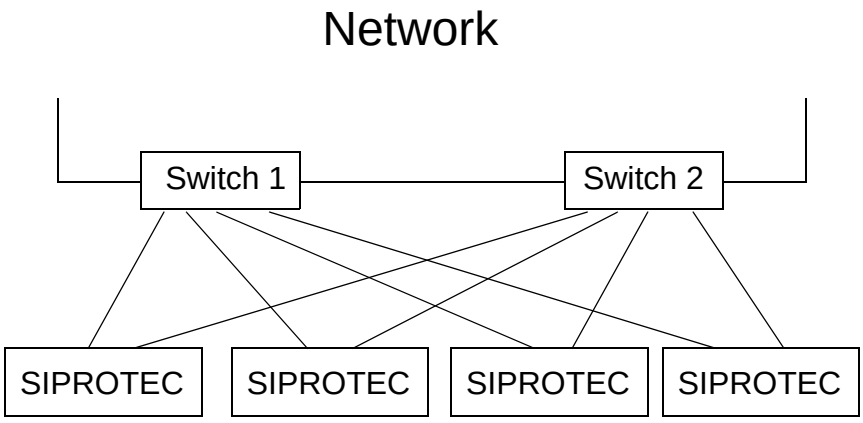


Fig. 4-2 SIPROTEC 4 units connected via 2 links

The 2 physical links are monitored for their connection. This enables generation and output of a message if a link is broken. This message is to be found in the message buffer and can be routed to contacts, LED, or in the logic editor (CFC).

PRP-structure

The PRP structure (Parallel Redundancy Protocol according to IEC62439-3:2012) provides communication over 2 independent networks (LAN A and LAN B) simultaneously. As shown in the following picture both networks may under no circumstances be connected to one another. Siemens recommends building both networks identically. Connect LAN A with channel 1 and LAN B with channel 2.

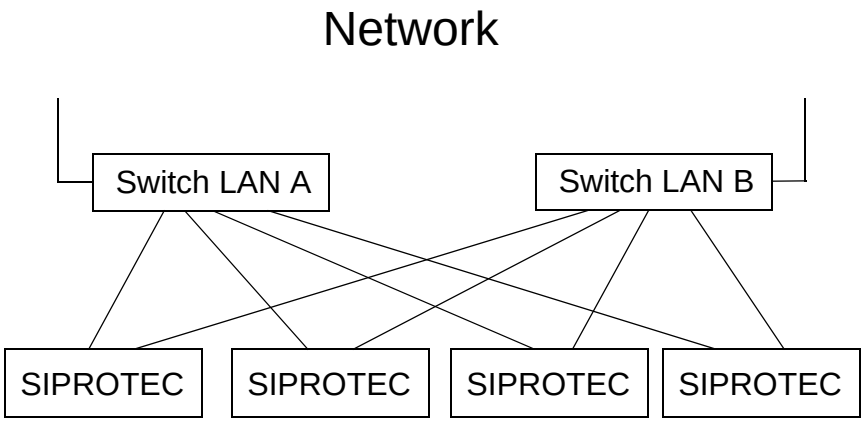


Fig. 4-3 SIPROTEC 4 devices connected via 2 independent networks (LAN A & LAN B)

In case of an interrupted network communication the device switches seamlessly. Only the optical EN100-module with LC connectors and application from version 4.1x supports PRP. RSTP and Line mode cannot be activated with version 4.1x of the application. Configuring the redundancy method via DIGSI is not possible.

Channel switchover in “Line” mode

If the active link, i.e. the link transmitting data between the device and the external switch, is broken, the interruption is detected and signaled as stated above. When an interruption is detected, switch to the second channel is performed immediately so that data exchange can continue almost without interruption. The interruption signal is then transmitted via the standby channel.

Failure of the external switch

If both links are connected to ports in different switches, failure of one external switch does not interrupt the connection with the master. All devices with an active link via the failed switch switchover to their second link that is connected to another switch, and operation can continue. The external switches are normally connected via a ring structure, so that they realize their own redundancy between themselves.

Ring structure

Ring structures mean that all devices are connected in a ring, as shown in Fig. 4-5. However, this operating mode requires 2 ports which actively transmit data. This includes an appropriate network control system. The prerequisite for such a structure is a switch functionality, which is only provided in the module with optical interface.

Switch function (internal switch)

The switch function provides the connection with the device, as well as a connection with the 2 other ports which then implement a ring structure. This 3-port switch is controlled so that only those telegrams which are intended for the device are actually routed to it. Telegrams transmitted by the device are fed into the data stream on the ring. The basic structure of such an integrated switch is shown in Fig. 4-4.

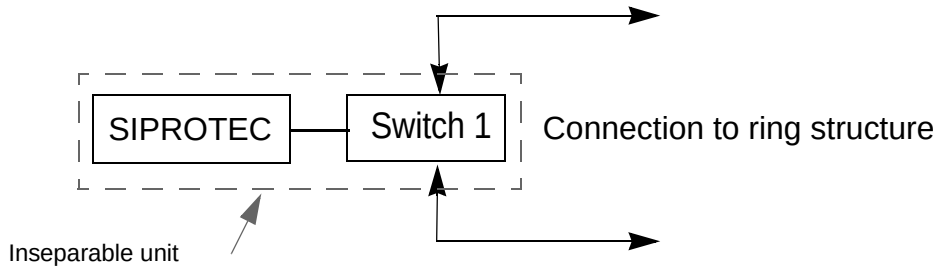


Fig. 4-4 Principle of an integrated switch

Special features of the optical module

The module with the optical interface has 2 operating modes: “Line” and “Switch”. One of the 2 operating modes is active immediately after power-up and has to match the network configuration.

Operating mode RSTP

This operating mode allows the kind of structure shown in Fig. 4-5. Its characteristic feature is that all devices are arranged in a ring; one or more external switches must be integrated into this ring for the output of data, e.g. for display or for transmission into a different network.

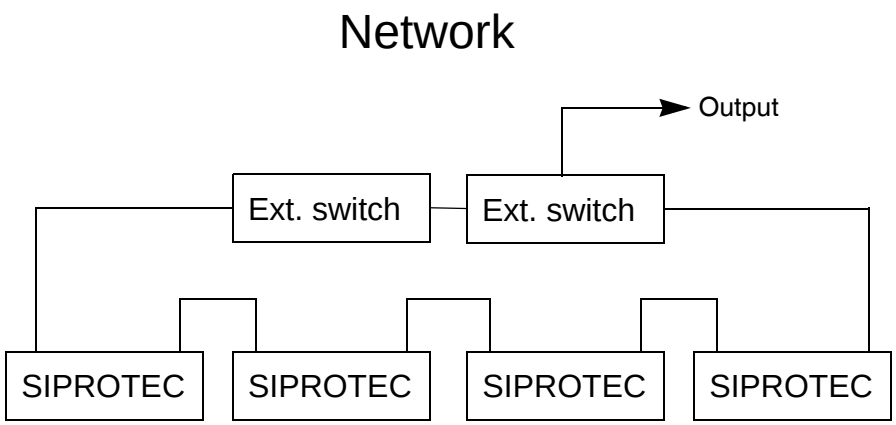


Fig. 4-5 SIPROTEC 4 devices with integrated switch

If the ring which includes the devices and the switch is broken, the ring becomes a line, and the functionality is maintained almost without interruption. If the ring is broken in a second place, the structure cannot handle the resulting double error any more, and one part of the line will be disconnected. This means that only single errors resulting from a broken ring can be handled.

HSR Structure

The devices are arranged in rings in the HSR structure (**H**igh-availability **S**eamless **R**edundancy according to IEC 62439-3:2012) shown in the following figure. The procedure does not have parameters of its own.

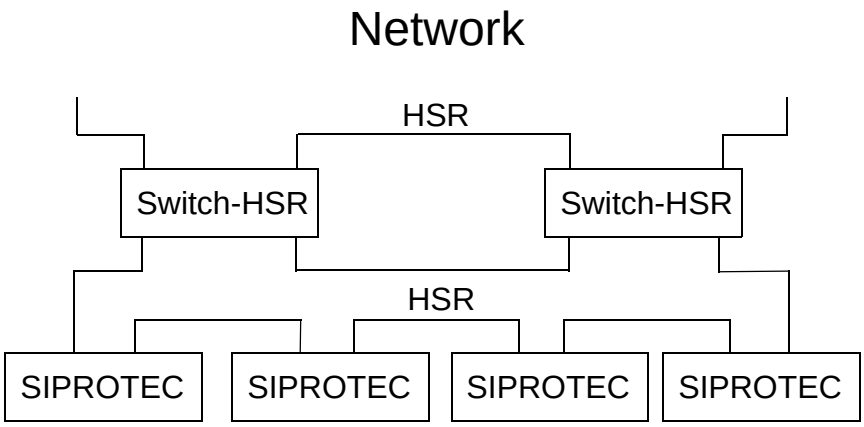


Fig. 4-6 SIPROTEC 4 diveces arranged in rings

A seamless switchover will take place if an interruption in communication occurs in a network. All components in HSR rings must support HSR. If you do not want to connect HSR-enabled devices, use special switches that support HRR.

4.3 Time Synchronization

Time synchronization via SNTP

The SIPROTEC 4 units require time synchronization to permit correct chronological recording of events. Devices equipped with the IEC 61850 protocol are capable of time synchronization via the network. The SNTP protocol is supported, as prescribed by the standard (see Chapter 3.2). The time interrogation of 2 time servers is supported as of module firmware version 3.09 and DIGSI 4.8.

Time server in the network

To be able to use time synchronization via Ethernet according to SNTP, there must be a time server in the network that can service the various time requests of the devices, as defined in the SNTP protocol. Time servers are accessible via an IP address. This must be set during parameterization in DIGSI using the System Configurator. If there is no time server, time synchronization must be ensured in a different way.

Other time synchronization options

In addition to this synchronization protocol, other features of the SIPROTEC 4 units may also be used. Activation is performed with the DIGSI parameterization system. If such a method has been activated, time synchronization via the Ethernet network is not performed and each device must be set for the selected time synchronization method. The necessary time information for the IEC 61850 protocol itself, is then supplied by the device to the communication module.

4.4 Use of External Switches

Switches are used to build Ethernet networks and are necessary to use the SIPROTEC 4 units with the IEC 61850 protocol. This is shown in Fig. 4-1 and Fig. 4-2. This chapter only deals with the external switches.

4.4.1 Characteristics of Switches

Switches are actually nodes in the network, i.e. several devices are connected to one node to intercommunicate. The link from each device to the hub is always a point-to-point link. It is up to the switch to manage the raising and cleared messages.

Switches have the same structure. They have several ports for connecting network cables. The ports are designed for different media depending on the manufacturer and type, some even with mixed electrical and optical interfaces. That not only affects the connectors but also basic implementation as an optical or electrical port.

The switches usually have a further serial management interface that can be used to make special internal switch positions. A switch is accessible not only via this interface but also via any Ethernet port. A switch own IP address is set via this special interface.

Switches can be 'managed' and 'unmanaged' switches. Only 'managed' switches of layer 2 should be used in IEC 61850 networks. A prerequisite for interoperability is complete conformity with IEEE 802.3 and IEEE 802.3u of the Ethernet standard.

4.4.2 Switch Positions

Follow the instructions provided in the documentation of the manufacturer in order to configure the switches.

4.5 Redundancy Settings

4.5.1 How It Works

Module with electrical interface

Redundancy is important for the reliability of an entire communications system. The basic principle with the EN100-module with electrical interface is that both RJ45 interfaces of the module are connected with the ports of 2 different switches. Connecting them to the ports of one switch only achieves line redundancy.

One channel is activated and operated as the active channel by the module, the second is monitored for connection. If the link of the active channel is interrupted, switchover to the other interface is automatic. This process is completely transparent to the user. The active channel can only be seen in the message buffer. A relevant message is generated on switchover.

Module with optical interface

In 'Line' mode, these modules behave in the same way as the modules with electrical interface. In switch mode, both channels are active, and connected in a ring as shown in Fig. 4-5. Special settings are accessible via DIGSI; they concern only the settings of the redundancy functionality.

4.6 Device-Internal Switches

4.6.1 How It Works (simplified)

As shown already in Chapter 4.2, EN100-modules with optical interface have an integrated switch which allows to build up ring structures. The function principle of this switch is that of a switch with 3 ports, one of which is permanently connected with the MAC[1] of the processor. Consequently, the 2 other ports also have fixed functions assigned to them, namely to establish a ring structure. The result of this fixed assignment is a much less complex control structure (see Fig. 4-7)

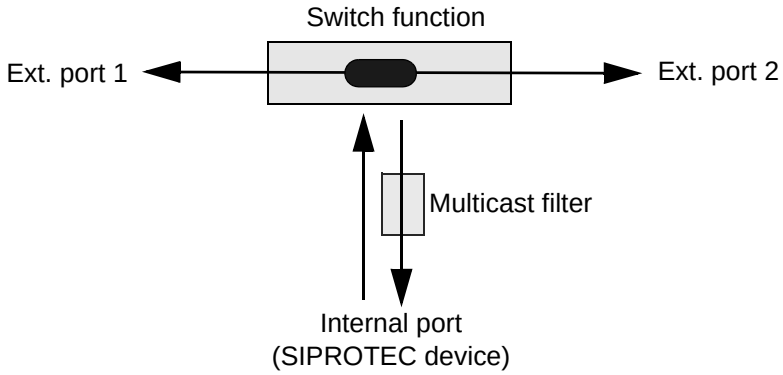


Fig. 4-7 Principle of an internal switch

The network is connected with the 2 external ports, and thus forms a ring structure; this means that all telegrams of the network pass at least once by one of the external ports. Unicast, multicast and broadcast telegrams circulate in the network. They are handled in different ways:

Unicast telegrams

Unicast telegrams are intended for one specific SIPROTEC 4 device. These telegrams, regardless of the external port from which they come, are only forwarded to the internal port - i.e. to the device - if they are intended for that device; otherwise they are passed on to another external port. If the unicast telegram is not addressed to the device, it will be forwarded to the other external port.

Unicast telegrams to an external port which are transmitted from an internal port are removed from the telegram traffic.

Unicast telegrams which are transmitted by the device are passed on to both ports, and fed into the data stream. These telegrams are treated with higher priority than those carried in the network.

1. MAC, Medium Access Controller, function block which controls the access to the medium.

Multicast telegrams

Multicast telegrams are transmitted as MAC multicast telegrams. These telegrams are addressed to 2 or more devices in the network, and are generated by a transmitter. When such telegrams are detected at the external port, they are forwarded to both the other external and the internal port. Multicast telegrams are used for implementation of the GOOSE protocol for extra-fast data transmission. If no status change is carried out, the message will transmit cyclically, e.g. in the distance of a second. A spontaneous transmission (e.g. 1 ms) is immediately carried out at a status change which is repeated in distances being longer until the cyclical distance is reached again. Their essential feature is that they are transmitted several times immediately after the event, at an interval of 1 ms, and therefore constitute a high load for the receiver. This is why a multicast filter is integrated in the receive direction of the internal port. This filter blocks all multicast telegrams which are not intended for the internal port. The filter itself is a 'genuine' filter[1], which allows only those telegrams to pass to which it is set[2]. Software filtering is normally excluded because of performance requirements.

Broadcast telegrams

These telegrams, when received, are forwarded both to the external port and the internal port. Here again, broadcast telegrams generated by the internal port are removed when they are received by an external port.

Port addresses

Switches are normally equipped with a function which assigns one (or more) fixed MAC address(es) to each port. This address is entered in a table and stored there as soon as the first telegram is received at the port. The purpose of this function is that in a multiport switch Unicast telegrams can only be transmitted to the target port. It is combined with special aging timer which initiate that addresses are forgotten and learned again when the connection is broken, or during long periods without data traffic.

Because of the fixed assignment of the ports in an internal switch such a function is not necessary.

1. Such a filter is also included in the modules with electrical interface.
2. Ethernet controllers are always equipped with filters; however, they filter only in 64 groups, so that overlaps may occur, especially when they are integrated in third-party plants in the course of extensions.

4.7 Configuration Information

In the previous sections, details of the network structures and of internal and external switches have been described. This section deals with the RSTP-structure and the special features of ring structures.

Special features of RSTP

It is possible to use multiport switches[1] in different topologies together with SIPROTEC devices. The maximum size of a ring is limited to 40 users (see section “Number of devices in the ring").

In contrast to PRP or HSR, RSTP does not work free of interruptions in the case of a failure.

Siemens recommends that a multiport switch always plays the special role of the root switch in an RSTP ring structure. In order to prevent the endless circulation of telegrams, the RSTP algorithm locates one user in the ring (alternate) that causes the logic break point.

Priorities

The RSTP algorithm always defines a root switch based on the priority (set with the parameter Bridge Priority). Siemens recommends the parameterization of a multiport switch with the priority 0 to ensure that this switch takes the role of the root switch. If this switch fails, the parameterized priority will be used for the search for a new root switch. Therefore Siemens recommends the parameterization of an additional multiport switch of the ring with the priority value of 4096. Set the other multiport switches with the parameter Bridge Priorities higher than 4096 (usually 8192) and smaller than the parameterization of the SIPROTEC devices (default setting = 32768). This ensures that multiport switches will always step in as root switches before a SIPROTEC device takes over this function.

Number of devices in the ring

The maximum number of RSTP users in a ring is limited by the parameter *MaxAge*. According to IEEE 802.1D-2004, the parameter *MaxAge* can be set to a value from 6 to 40. At any time, the distance (Hop) to the respective root switch may not be higher than the parameterized value.

The following formula applies to simple RSTP ring structures with SIPROTEC devices:

Number of SIPROTEC devices + number of multiport switches < MaxAge

Siemens recommends RSTP settings as shown in Fig. 3-7 in order to support this number.

The number of users in the smallest ring of each device must be smaller than the parameterized value of *MaxAge*. This ring must also contain the root switch and the backup switch. The following example (see Fig. 4-8) shows the calculation method. The value is equal to 10 for the highlighted device.

1. Siemens recommends using RuggedCom, Hirschmann and Siemens Scalance switches. Detailed tests have been performed for these switches

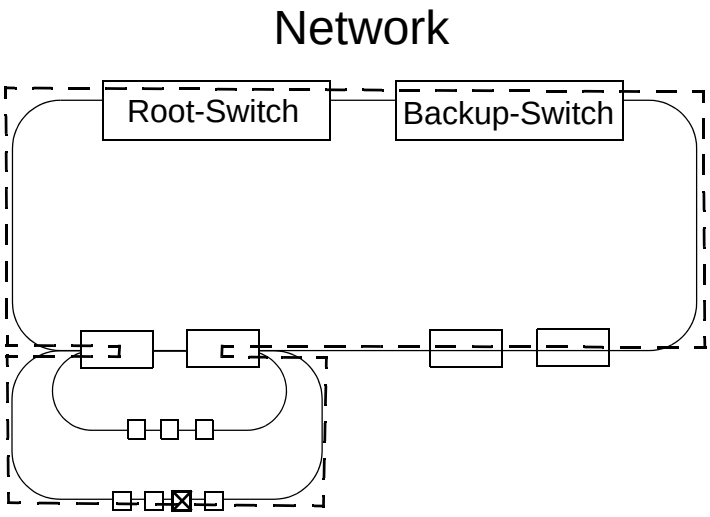


Fig. 4-8 Calculation method of the number of users in complex RSTP ring structures

Simple ring structure

A simple structure consists of multiport switches and a ring of SIPROTEC devices.

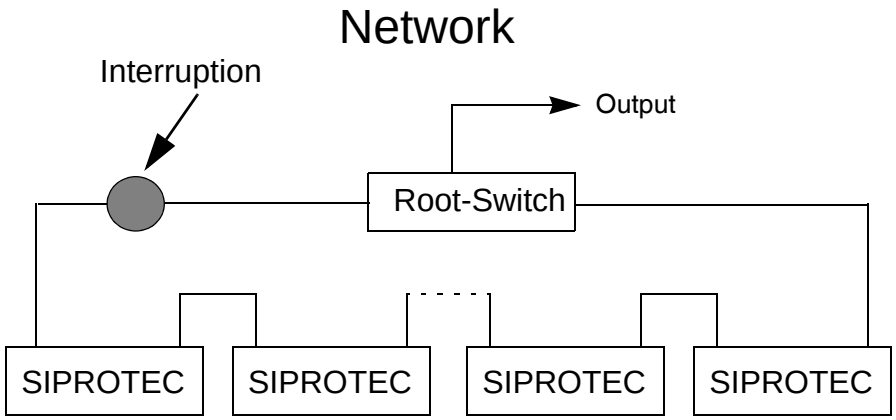


Fig. 4-9 Interruption in a simple ring structure

The worst case of an interruption in this structure is shown in Fig. 4-9. The interruption creates not more than one chain, consisting of the multiport switches and the devices. They are treated properly as long as the maximum number of RSTP users is taken into account.

A line always appears when a ring structure is interrupted in a different place. The multiport switch is located on this line. Both chains then get fewer and fewer users compared to the maximum number of RSTP users.

If the multiport switch fails, it is no longer possible to communicate with SIPROTEC devices from the outside, i.e., via the multiport switch. Inter-device communication carried out via GOOSE is not affected.

Several rings at interconnected multiport switches

Where 2 switches are used, they should have an additional connection with one another, as shown in Fig. 4-10.

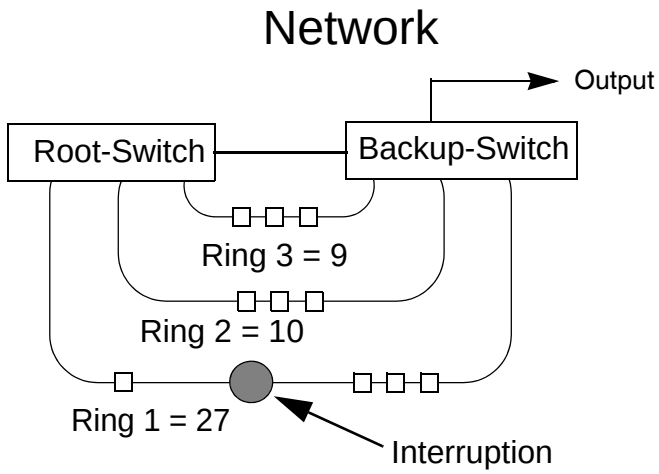


Fig. 4-10 Directly connected witches

The advantage of this structure is that in case of an interruption of the ring the root switch can be accessed directly through the backup switch, so that it is not necessary to pass through devices of another ring.

NOTE

Whenever possible, Siemens recommends the interconnection of multiport switches.

Summing up

All the above can be summed up as follows:

1. Position the root switch and the backup switches so that they form rings as small as possible.
2. In case of failure, physically separate the root switch and the backup switches from all or as many networks as possible.
3. Give preference to simple structures. Keep the nesting level low.
4. Use the formula given in the chapter to determine the maximum number of devices in a RSTP ring. The maximum number does not change even if several rings are connected to a multiport switch.
5. If 2 mulitport switches are used, Siemens recommends connecting them to each other several times.
6. Information output becomes redundant with the use of 2 multiport switches, i.e., if a switch fails, every piece of information is still available.
7. If 2 or more multiport switches are in use, Siemens recommends connecting the rings at 2 different multiport switches.
8. Siemens recommends connecting the ring ends always to 2 multiport switches connected to each other.

IEC 61850 Conformance Statements

5

This chapter describes conformity with IEC 61850. It does not describe the entire standard but only parts in which there is a choice in the services.

5.1 Definitions of the ISO/OSI Reference Model

To achieve stable data exchange, all communication is based on the OSI Reference Model (OSI/IEC 7498-1) for a multi-layer communication function. Fig. 5-1 shows the seven layers defined there.

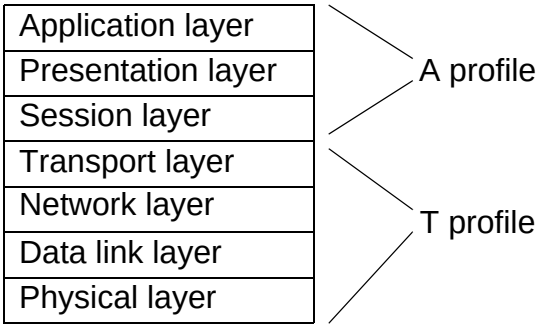


Fig. 5-1 OSI reference model and profiles

This section on using the ISO application (application profile) and transport profiles (T profile) describes the various stack profiles. An ISO application profile is a set of specifications and declarations regarding the top 3 layers of the ISO/OSI reference model (i.e. the application, presentation, and session layers). The T profile is a set of specifications and declarations regarding the lower 4 layers (i.e. transport, network, data link, and physical layers).

A and T profiles can be combined in various ways to form different types of services and information items that can be exchanged. The services specified in Part 7-2 of the IEC 61850 standard are mapped onto 4 different combinations of the profiles. These 4 combinations are used for

- Client/server services,
- GOOSE/GSE management services,
- GSSE services,
- Time synchronization,
- Services for measured value sampling.

5.2 Definition of the Communication Services Acc. to Standard (PICS)

The tables in the sections below appear in the same sequence as in standard IEC 61850, Part 8-1, Section 24.

The tables refer to Part 7 of the standard and the corresponding information must be contained in the PICS.

This section describes the conformance statements. The standard groups them together under the term Protocol Implementation Conformance Statement (PICS).

Mandatory services

Please note that a number of services are prescribed and must be implemented to comply with the standard. Only the optional services and protocols are listed here because they constitute freedom of implementation. None of the mandatory services is explicitly explained here. Please refer to the standard IEC 61850, Part 8-1.

The descriptions below refer to implementation in the SIPROTEC 4 device range.

The tables give the names stated in the standard.

5.2.1 Profile Compliance

Application profile support

Profile		Client	Server	Comments
A1	Client/server	N	Y	
A2	GOOSE/GSE Management	Y	Y	Only GOOSE, not GSE management
A3	GSSE	N	N	
A4	Time sync	Y	N	Time accuracy: 1 ms (performance class T1) Time resolution: approx. 0.9 ms

T profile support

Profile		Client	Server	Comments
T1	TCP/IP profile	N	Y	
T2	OSI T profile	N	N	
T3	GOOSE/GSE T profile	Y	Y	Only GOOSE, not GSE
T4	GSSE T profile	N	N	
T5	Time sync T profile	Y	N	

Please refer to the services of Part 7 to see whether these profiles are supported. No distinction is made between A and T profiles there because the definition only refers to the application.

Client/server services supported

IEC 61850-7-2 model	IEC 61850-7-2 services	Implemented (Y/N)
Server	GetServerDirectory	Y
Association	Associate	Y
	Cancel	Y
	Release	Y
Logical Device	GetLogicalDeviceDirectory	Y
Logical Node	GetLogicalNodeDirectory	Y
	GetAllDataValues	Y
Data	GetDataValues	Y
	SetDataValues	Y
	GetDataDirectory	Y
	GetDataDefinition	Y
Dataset	GetDataSetValues	Y
	SetDataSetValues	N
	CreateDataSet	Y
	DeleteDataSet	Y
	GetDataSetDirectory	Y
Substitution	GetDataValues	N
	SetDataValues	N
Settings group ControlBlock	SelectActiveSG	Y
	SelectEditSG	N
	SetSGValues	N
	ConfirmEditSGValues	N
	GetSGValues	N
	GetSGCBValues	N
Report Control Block	Report	Y
	GetBRCBValues	N[a] / Y[b]
	SetBRCBValues	N[a] / Y[b]
	GetURCBValues	Y
	SetURCBValues	Y
Log Control Block	GETLCBValues	N
	SETLCBValues	N
	GetLogStatusValues	N
	QueryLogByTime	N
	QueryLogAfter	N
GOOSE	GetCoCBValues	Y
	SetGoCBValues	N
GSSE	GetGsCBValues	N
	SetGsCBValues	N

IEC 61850-7-2 model	IEC 61850-7-2 services	Implemented (Y/N)
Control	Select	N
	SelectWithValue	Y
	Cancel	Y
	Operate	Y
	Command termination	Y
	TimeActivatedOperate	N
File transfer	GetFile	Y
	SetFile	N
	DeleteFile	N
	GetFileAttributeValues	N

a) Until version V4 of the module firmware
b) Additional from version V4 of the module firmware up

Services and protocols for client/ server, application profile

These services are all identified as mandatory and are therefore implemented in compliance with the standard.

Services and protocols for client/ server, TCP/IP profile

Services and protocols must be provided in compliance with the standard. There is no choice about implementation. _KEEPALIVE was permanently set to 3[1] seconds although not recommended by the standard.

5.2.2 MMS Conformance

Parts of the services of the IEC 61850 protocol are based on the MMS[2] stack. This provides the relevant MMS services. The MMS services implemented are listed below. Some services whose implementation isn't mandatory are not shown. Please refer to the standard IEC 61850 for more information (see IEC 61850 Part 8-1).

MMS Initiate request general Parameters

MMS Service Supported CBB	Client-CR		Server-CR	
	realized	value/ range	realized	value/ range
status			Y	
getNameList			Y	
identify			Y	
rename			N	
read			Y	

1. The standard permits setting in the range 1 to 20 seconds. The 3 second permanent setting was selected to achieve the same response as with T103
2. MMS. Manufacturing Message Specification, is defined in standard ISO 9506 and was defined for industrial automation systems ranging from simple to complex.

MMS Service Supported CBB	Client-CR		Server-CR	
	realized	value/ range	realized	value/ range
write			Y	
getVariableAccessAttributes			Y	
defineNamedVariable			N	
defineScatteredAccess			N	
getScatteredAccessAttributes			N	
deleteVariableAccess			N	
defineNamedVariableList			Y	
getNamedVariableListAttributes			Y	
deleteNamedVariableList			Y	
defineNamedType			N	
getNamedTypeAttributes			N	
deleteNamedType			N	
input			N	
output			N	
takeControl			N	
relinquishControl			N	
defineSemaphore			N	
deleteSemaphore			N	
reportPoolSemaphoreStatus			N	
reportSemaphoreStatus			N	
initiateDownloadSequence			N	
downloadSegment			N	
terminateDownloadSequence			N	
initiateUploadSequence			N	
uploadSegment			N	
terminateUploadSequence			N	
requestDomainDownload			N	
requestDomainUpload			N	
loadDomainContent			N	
storeDomainContent			N	
deleteDomain			N	
getDomainAttributes			Y	
createProgramInvocation			N	
deleteProgramInvocation			N	
start			N	
stop			N	
resume			N	

MMS Service Supported CBB	Client-CR		Server-CR	
	realized	value/ range	realized	value/ range
reset			N	
kill			N	
getProgramInvocationAttributes			N	
obtainFile			N	
devineEventCondition			N	
deleteEventCondition			N	
getEventConditionAttributes			N	
getEventConditionStatus			N	
getEventConditionMonitoring			N	
triggerEvent			N	
defineEventAction			N	
deleteEventAction			N	
alterEventEnrollment			N	
reportEventEnrollmentstatus			N	
getEventEnrollmentAttributes			N	
acknowledgeEventNotification			N	
getAlarmSummary			N	
getAlarmEnrollmentSummary			N	
readJournal			N	
writeJournal			N	
initializeJournal			N	
reportJournalStatus			N	
createJournal			N	
deleteJournal			N	
fileOpen			Y	
fileRead			Y	
fileClose			Y	
fileRename			N	
fileDelete			N	
fileDirectory			Y	
unsolicitedStatus			N	
informationReport			Y	
eventNotification			N	
attachToEventCondition			N	
attachToSemaphore			N	
conclude			Y	
cancel			Y	

MMS Service Supported CBB	Client-CR		Server-CR	
	realized	value/ range	realized	value/ range
getDataExchangeAttributes			N	
exchangeData			N	
defineAccessControlList			N	
getAccessControlListAttributes			N	
reportAccessControlledObjects			N	
deleteAccessControlList			N	
alterAccessControl			N	
reconfigureProgramInvocation			N	

MMS Parameter Conformance Building Block (CBB)

MMS Service Supported CBB	Client-CR		Server-CR	
	realized	value/ ranged	realized	value/ range
STR1			Y	
STR2			Y	
VNAM			Y	
VALT			Y	
VADR			Y	
VSCA			N	
TPY			Y	
VLIS			Y	
REAL			N	
CEI			N	

Alternate AccessSelection Conformance Statement

AlternateAccessSelection	Client-CR		Server-CR	
	realized	value/ ranged	realized	value/ ranged
accessSelection			N	
component			N	
index			N	
indexRange			N	
allElements			N	
alternateAccess			Y	
selectAccess			N	
component			N	

AlternateAccessSelection	Client-CR		Server-CR	
	realized	value/ ranged	realized	value/ ranged
index			N	
indexRange			N	
allElements			N	

Variable Access Conformance Statement

VariableAccessSpecification	Client-CR		Server-CR	
	realized	value/ range	realized	value/ range
listOfVariable			Y	
variableSpecification			Y	
alternateAccess			Y	
variableListName			Y	

Variable Conformance Statement

VariableSpecification	Client-RC		Server-CR	
	realized	value/ range	realized	value/ range
name			Y	
address			N	
variableDescription			Y	
scatteredAccessDescription			N	
invalidated			N	

Read Conformance Statement

Read	Client-CR		Server-CR	
	realized	value/ range	realized	value/ range
Request				
specificationWithResult			Y	
variableAccessSpecification			Y	
Response				
variableAccessSpecification			Y	
listOfAccessResult			Y	

GetVariableAccess Attributes Conformance statement

GetVariableAccessAttributes	Client-CR		Server-CR	
	realized	value/ range	realized	value/ range
Request				
name			Y	
address			N	
Response				
mmsDeletable			Y	
address			N	
typeSpecification			Y	

DefineVariableAccessAttributes Conformance Statement

DefineVariableAccessAttributes	Client-CR		Server-CR	
	realized	value/ range	realized	value/ range
Request				
variableListName			Y	
listOfVariable			Y	
variableSpecification			Y	
alternateAccess			N	
Response			Y	

GetNamedVariable ListAttributes Conformance Statement

GetNamedVariableListAttributes	Client-CR		Server-CR	
	realized	value/ range	realized	value/ range
Request				
IObjectName			Y	
Respose				
mmsDeletable			Y	
listOfVariable			Y	
variableSpecification			Y	
alternateAccess			N	

DeleteNamedVariableList Conformance Statement

DeleteNamedVariableList	Client-CR		Server-CR	
	realized	value/ range	realized	value/ range
Request				
Scope			Y	
listOfVariableListName			Y	
domainName			Y	

DeleteNamedVariableList	Client-CR		Server-CR	
	realized	value/ range	realized	value/ range
Response				
numberMatched			Y	
numberDeleted			Y	
DeleteNamedVariableList-Error			Y	

GOOSE Conformance Statement

GOOSE	Participants	Publisher	Value/Comment
GOOSE Services	Y	Y	
SendGOOSEMessage	Y	Y	
GetGoReference	N	N	
GetGOOSEElementNumber	N	N	
GetGoCBValue	N	N	
SetGoCBValue	N	N	
GSENotSupported	N	N	
GOOSE Control Block	N	Y	ReadOnly

5.3 Protocol Implementation Extra Information for Testing (PIXIT)

The extra protocol implementation information for testing is to be found in a supplementary, device-specific document, which is provided via internetworking as a PDF-file. This description is available specifically for each device as a PDF file in the Internet under *http://www.siprotec.de* or *http://www.siprotec.com*. There you find the descriptions for Edition 1 and Edition 2.

5.4 Model Implementation Conformance Statement (MICS)

Content of the statement

This statement contains the description of all objects that are provided by a device and is especially important if devices are connected to a central system that supplies data to certain applications via the objects provided by the device.

In the case of SIPROTEC 4, this document depends on both the device type and the defined user objects and can therefore not be a permanent part of the manual. It is therefore generated from DIGSI.

Generation in DIGSI

Generation is selected in the device processing via menu items *File* → *Export* → *IEC 61850 System Interface for Documentation (PDF)*. The dialog that opens let you enter a device-related, editable filename under which the MICS document to be generated will be stored.

The document is generated with the correct version and device type data. It shows the assignment lists SIPROTEC 4 to IEC 61850 and vice versa. The whole document is shown in a hyperlinked table of contents. The MICS is a readable form of the current mapping of a device on IEC 61850.

In addition to the MICS, an ICD file (XML file) is created which describes the mapping of a device. This ICD file is used by the System Configurator, or can be imported into the system configurators of other manufacturers, in order to integrate these devices into the communication.

Parameterization

6

The subject of this chapter is parameterizing the modules. The basics of module-related device parameterization, parameterization in DIGSI, and in the System Configurator are described without going in to detail.

For more detailed explanations, please refer to the DIGSI manuals and the online help in DIGSI, especially, that of the System Configurator, which provides very detailed information.

6.1 Points of Departure for Parameterization

The IEC 61850 modules must be provided with special information for parameterization. This information is stored in the parameter set of the device and is made available to the module.

Storage of the parameter set

The parameter set within the device is stored in 2 parts. Unlike the other additional protocols, storage of the module parameters is only performed on the module. A reference to the consistency check is contained in the device parameter set that is stored in the device.

During device start-up, the parameter set of the device is first activated for the IEC 61850 modules and then the module is started. During module start-up, a consistency check is made. If this is successfully completed, the module is correctly started and provides the interface.

Information in the parameter set

The parameter set contains extensive information, such as the individual objects fo the SIPROTEC 4 devices to which the objects of the IEC 61850 protocol must be mapped. The user has no part in this mapping. The user may view it but not change it. However, devices with different function scope and type have different mappings.

The second large group of parameters concerns settings provided by DIGSI. They are made in connection with the "Additional protocols" parameterization block.

A further group of parameters concerns the settings that can be directly changed on the device. These may not be stored in the parameter set but taken from the device's internal non-volatile memory. However, it is usually unnecessary to set these parameters on the device because they are usually contained in the parameter set and are automatically stored in the memory of the device.

Network parameterization

This block of parameters describes settings that concern the entire IEC 61850 network within a substation. These settings are especially relevant for parameterization of peer-to-peer data traffic using GOOSE. The parameters themselves are unavailable to the user. The parameterization of the network is performed with the System Configurator whose online help can be used to obtain detailed information.

IEC object description via ICD file

The IEC 61850 protocol represents the necessary objects of the SIPROTEC 4 units externally. These objects are contained in an ICD file in compliance with the standard. This file is contained in the DIGSI parameterization system and is essential for integrating devices into a network. The same goes for devices of other manufacturers. For these, too, a description must be exist in an ICD file if they are to be integrated into a network. ICD files can be imported and exported by DIGSI, which is necessary for integration of devices from other manufacturers and of SIPROTEC 4 units in Non-Siemens networks.

Station description via SCD file

A complete station is formed by several devices. They may also include a master unit. These components have various communication connections between them that must be parameterized. The description of all devices, and their settings and interrelations are grouped together in the station description file. The file itself is created and processed using the System Configurator. The System Configurator is started from the station manager of DIGSI and is integrated into the DIGSI parameterization system. SCD files can also be imported and exported there.

Device parameterization

Parameterization of a complete substation secondary equipment is performed in several steps. The first step is to set parameters of the devices with DIGSI, as is familiar from devices without interfaces and the "traditional" protocols. This parameterization includes setting the protection parameters and routing of signals to the system interface. The logic block charts are also parameterized here. At the end of this step, you have a fully parameterized protection unit.

System parameterization

System parameterization is only performed after parameterization of the device. A System Configurator is used to do this. This is included in the DIGSI parameterization system.

As part of system parameterization, the ICD files of each device are imported and the complete station is assembled using the information they contain. Distribution of the IP and multicast addresses as well as subnet masks is performed in the System Configurator. It is also used to produce and parameterize the inter-device communication, i.e. the link from objects of one device to those of other devices. This defines and routes direct flows of information between devices.

Only after completion of system parameterization is the parameter sets generated for the individual devices. These now contain the links with other devices in the network and only then is the complete station fully functional. The station-wide parameterization information can be exported in an SCD file.

6.2 Parameterization Using DIGSI

Device parameterization of the SIPROTEC 4 units is performed with the DIGSI parameterization system. In addition, a System Configurator is integrated into the DIGSI that allows you to make the settings concerning the network.

Working in the DIGSI station manager

Here, the devices of a station are inserted as required for the project. On inserting a device from the device catalog, the device must be configured according to its order code. For example, the Ethernet interface must be selected.

Properties dialog

These settings are made in the properties dialog, which must be opened. In it, it is possible to activate the IEC 61850 interface via *System interface* → *Further protocols* → *Advanced*. There you can make settings concerning the IP address, subnet mask, etc. These settings remain valid until they are overwritten by work with the System Configurator.

Routing matrix

The device is now opened and you continue work in the parameter dialog. The routing matrix is adjusted depending on the situation. Here, the IEC 61850 objects are already connected to the internal objects according to device type. The IEC 61850 objects can be changed in the properties dialog. The suffix and prefix can be changed. Please note that the system interface can be the destination if the device objects in the monitoring direction are mapped onto the IEC 61850 objects. In the command direction, IEC 61850 objects are mapped onto internal device objects.

Measurement threshold

The measurement threshold is used to decide when a data change of the measured value has to be reported to the client, or sent via GOOSE. The parameterization of the measurement thresholds data attribute db - deadBand - in accordance to IEC 61850 can be processed from DIGSI 4.8 on with Service Pack 2.

Object ID

All SIPROTEC objects (e.g. indications, commands, measured values, etc.) can be mapped one-to-one onto the standard-compliant object GGIO. That way, the user has access to all SIPROTEC information items, even those that are not mapped onto logical nodes. By displaying the SIPROTEC texts and the standard texts assigned to them in the System Configurator, these objects can be uniquely identified and evaluated by the substation secondary equipment. That way, all objects of a device are available, including those that are not defined in the standard but that the user has previously used with SIPROTEC 4. As far as functions go, therefore,
IEC 61850 has no disadvantages for the user over the previous parameterization for the substation control and protection (e.g. IEC 60870-5-103 and PROFIBUS FMS).

IEC 61850 Edition

The setting of the IEC 61850 Edition is described in Chapter 3.2. With the activation, the IEC 61850 module of a SIPROTEC 4 device is either in accordance with Edition 1 or Edition 2. The exported description fils ICD and SCD are in accordance with the selected edition.

Time synchronization

Time synchronization is set in a separate dialog. The dialog has the extra item Ethernet NTP. Selecting it activates time synchronization via a time server in the network.

This selection is connected with further settings for time zones and daylight-saving/ standard time. The settings must be made to activate correct time management in the devices.

Creating an IEC 61850 station

The devices are created as explained above and their properties set to meet the conditions for use in a network. The final step is to create a IEC 61850 station in the properties dialog. During generation, the individual SIPROTEC 4 units of the station can now be assigned. On completion of this step, the station structure is complete. The following steps for parameterization of the station must be performed using the System Configurator.

6.3 Parameterization in the System Configurator

Parameterization with the System Configurator is the subject of this chapter. The System Configurator itself is not described but only the settings important for parameterization that have to be made.

Opening the System Configurator

The System Configurator is opened directly from the DIGSI station manager by double-clicking on the icon of the IEC 61850 station. The network settings are shown by default.

Network settings

The network is shown as a tree. The root of the tree is the station to which subnets are assigned that then contain devices.

The station, devices, and subnets can be assigned a comment or description text.

Subnets

The start address, subnet mask, and standard gateway can be set for subnets. The baud rate of the network and type of network are also displayed. It is not necessary to change them.

The start address is only important for automatic assignment of the network addresses of the devices. In this case, addresses are assigned to the devices starting at this address.

Devices settings

The devices can be selected and set like subnets. The setting dialog that opens initially shows the device properties. In addition to the freely assignable name, the device type, device version, and manufacturer of the device are also visible. Moreover, the ability for peer-to-peer communication, for routing, and for providing a time signal are displayed. The only settable value is the IP address

Setting of routing

The setting for routing is an essential feature of the System Configurator. Unlike the routing matrix in the DIGSI device manager that permits assignment of internal device objects to the IEC 61850 object/system interface, routing in the System Configurator interconnects the distributed applications. Only then is it possible for the devices to intercommunicate directly. Routing has its own setting dialog that lists all the devices it contains.

Routing itself is performed by defining an application, selection of devices, and their objects that intercommunicate.

Memory management

The storage used for ’Buffered Reports’ of the communication module is physically restricted. The same amount of storage capacity is provided to every report control block for the buffering of the reports per default . The user has, however, the ability to assign individual amounts of the storage capacity dialog controlled using the system configurator. This function is available with DIGSI 4.81 and higher in the system configurator.

6.4 Communication with the IEC 61850 Client

By means of reports data are transmitted by the server (e.g. SIPROTEC device) to the client (e.g. SICAM PAS). The client subscribes to the data from the server which provides them in a report.
There are static reports which are created by DIGSI in the system configurator and dynamic reports which the client creates in the server at runtime.
Static reports are mostly necessary for the communication with outside clients. The disadvantage is that they are created statically in the system configurator and only can be changed by re-parameterization of the device respectively. SICAM PAS uses the mechanism of the dynamic reports opposite SIPROTEC. They can be changed at any time without re-parameterization of the device from the client.

6.4.1 Overview

The report function delivers data to the client, it consists of 3 components. These are the DATA_SET(s) which defines a list of data elements. The real data (voltages, currents etc.) are monitored by an event monitor. This monitor provides a functionality which determines the data values with special criteria (e.g. limiting values, thresholds,...). These criteria are the result of the attributes of the report function. The completion of this function supplies the decision for generating of a notification which is delivered by specified channels. This notification delivers the data to the client. This notification (report) includes the data values and the reason for the activation of transmission.

NOTE

The contents of the event notification are determined by a combination of I/O scan and event monitoring. These are conceptually 2 asynchronous processes. Therefore, the number of data values included within a single notification is a local issue.

The number of data values, within a notification is determined by parameterization and is finite by the local implementation conditions. A result includes many data elements. The result is biunique indicated in the device by the Entry-ID and TimeOfEntry.

A client may initiate a general interrogation at any time to receive (once again) all data values of the past from the server. The number of events of the past is limited by the size of the device memory and the parameterization. With this function clients may refresh their database with events, which appeared by a broken line.

RCB

The Report Control Block (RCB) provides the logistic that is required for spontaneous reporting values of data from one or more Logical Nodes to one client.

The instances of report control will be configured in the server at the configuration time. A server restricts access to an instance of a report control to one client. That client exclusively “owns” that instance and receives reports from that instance of the report control only.

There are 2 classes of report control defined, each with a slightly different behavior.

BRCB

Buffered Report Control Block (BRCB) – internal events (caused by trigger options data-change, quality-change, and data-update) buffer the events (to some practical limit) and/or issue immediate sending of reports, such that values of data are not lost due to transport flow control constraints or loss of connection. BRCB provides the sequence of events (SOE) functionality.

URCB

Unbuffered Report Control Block (URCB) – internal events (caused by trigger options data-change, quality-change, and data-update) issue immediate sending of reports on a “best efforts” basis. If no association exists, or if the transport data flow is not fast enough to support it, events may be lost.

To allow multiple clients to receive the same values of data, multiple instances of the report control classes are available.

Report control block instances are named. These names must be unique within the scope of a Logical Node. The number of instances that may be visible to a specific client is a local implementation issue and must be appropriately reflected in the configuration provided (e.g. SCL). Once a report control block is reserved by a specific client, no other client has access rights to set the control block parameters.

Buffered Report Control Blocks are usually configured to be used by a specific client implementing a well-defined functionality, for example, a SCADA master. The client may know the ObjectReference of the BRCB by configuration or by the use of a naming convention.

6.4.2 IEC 61850 Buffered Report Model Static Parameterization

6.4.2.1 SCL Report Control

The static SCL report controls can be parameterized by the IEC 61850 System Configurator. They are pre-initialized. The purpose of this pre-initialization is to simplify the parameterization. With means of those values, the instances of BRCB will be initialized. Furthermore, the percentage of memory routed for the entries associated to each report control block will be assigned. This assignment can be changed with the system configurator from DIGSI 4.81 upwards.

6.4.2.2 SCD Parameterization

Standard report control block parameterization

The System configurator may change every SCL attribute except for the attributes name, buffered, and max in RptEnabled. The attribute max in RptEnabled is set to 1 by default, so an RCB can only be reserved by one client.The active configuration will be compiled into the parameter set of the EN100.

There are 2 parameterizations possible: the owner or the ownerless parameterization.

1. Ownerless parameterization: no clientLN is provided; the report control block will be available in the object directory of the EN100 but will be ownerless.
2. Owner parameterization: a clientLN is provided. The report control block will be available in the object directory but is reserved for the owner defined in the SCD file.

The current reservation of a report control block in the IED can be monitored via the extended attribute owner of the report control block.

Extended report control block parameterization

The memory of the communication module that will be used for the Entry buffering is limited. An extension of the standard parameterization is required for optimizing the memory allocation for each report control block.

If no extension is made, the only possibility for the module is to route for each report control block the same amount of memory for the buffering. The parameterization of the report control block has consequences: for instance, setting the integrity period will lead to buffer the entries periodically. With means of a dialog, the splitting of the memory can be done by the user in the System Configurator.

6.4.3 IEC 61850 Buffered Report Model Dynamic Parameterization

6.4.3.1 Dynamic Reservation of an Ownerless Report Control Block

The reservation of an ownerless report control block occurs via an MMS write access of one of the attributes ResvTms and/or RptEna (in case of a dynamic report control block, ResvTms has to be written first to reserve the Buffered Report Control Block).

The MMS write access might failed, but the reservation not; a simple example for a failed write access is enabling a report that is not fully configured.

In case of disconnection of the client, the report control block will not loose its configuration parameter, but the ownership of the client is removed after the time-out set to the value ResvTms expires. The buffering still continues, and the client can recover the ownership of the report control block after the reconnection, if ResvTms = 0, or automatically if ResvTms is greater than 0 at the reconnection time. The reason for this implementation is to guarantee the disabling or reconfiguration of a dynamic report control block from different maintenance PC for instance.

6.4.3.2 Dynamic Parameterization

The dynamic report control block has been added to the fix Edition 1 of the IEC 61850 standard, and is an extension to the report control block parameterization within the SICAM PAS Configurator (similarly to the Unbuffered Report Control Block parameterization within the SICAM PAS).

There are 2 RCBs for each LLN0. The RCBs that have not been statically parameterized (see SCD parameterization) are still instantiated in the object directory. They can be reserved to a client via the dynamic reservation of an ownerless RCB.

The enabling of a Buffered Report Control Block can only occur after at least the attributes ResvTms and DatSet (optional: RptID, BufTm, OptFlds, TrgOps, IntgPd, Entry ID, TimeofEntry) are successfully set from the client that owns the RCB. After the disconnection of a client, the attributes are not changed, only the ownership of the report control block is lost (after expiration of the ResvTms timer).

6.4.4 IEC 61850 Buffering Mechanism

6.4.4.1 The Buffered Report Control Block State Machine

If the association with a client is lost, the BRCB continues to buffer internal events. After a client has established a new association, it sets the attribute to enable the transmission of the report telegram.

NOTE

It is important to notice that the buffering of events can never be stopped; only the transmission to the client can be interrupted or disabled. The buffered events (stored while connected or disconnected) can be retrieved any time with the proper services.

6.4.4.2 Differences Between the Unbuffered and Buffer Reporting Model in the IEC 61850

The differences between both models are:

1. The report format; the buffered report format includes the Entry ID, the TimeofEntrtry, and BufferOverflow that were not part of the unbuffered report format. The attribute Entry ID is an arbitrary octet string; each buffered report telegram has a different Entry ID.
2. When the report control block is enabled and the association (connection server - client) is active, the buffered report is sent to the client with the same strategy as the unbuffered report. However, the event notification will be associated to an entry and therefore to an Entry ID (that can contain other notification), and is also stored in a buffer that can be retrieved later. At its creation, a TimeofEntrtry attribute is associated to the entry.
3. When the report control block is disabled the association (connection server - client) is unavailable (connection loss, or no ownership of a report control block), or the sending of report has been disabled by a client request. Then the event notification will be associated to an entry and therefore to an Entry ID (that can contain other notification), and is also stored in a buffer and can be retrieved later. At its creation, a TimeofEntrtry is associated to the entry. As long as the association is unavailable, the server keeps track of the telegram that would have been sent if the report was enabled, in order to set properly the Entry ID, and the TimeofEntrtry.

6.4.5 Memory Management

Each report handle has an own buffer partition pool from which it routed memory for buffering its entries.

Each report handles has a linked list of its entries and if no memory is available from its buffer partition pool, then the oldest Entries are free as long as the newest can not be stored.

6.4.6 Timing Strategy – Flow Control

The trigger to send a buffered report can be either: change/update notifications, integrity scans, general-interrogations, or responses to the client that set the Entry ID.

A sending strategy exists regarding to the timing. If no care is taken, sending the requested history of entries can lead to a disconnection with the client, depending of the amount of entries that has to be transmitted: each entry will lead to a reporting telegram.

An extended attribute is added in the report control block: maxOutReports permits a proprietary handshake with the client. The default value for this attribute is 1 (equivalent to the second one). The client may change this attribute and therefore, the number of reports sent to the client could be adjusted to its speed to process the telegrams and to request new ones.

6.4.7 Purging the Entries

The purging of the Buffered Report Control Block entries occurs either on purge request from client, or when the client change the value of one of the following configuration attributes:

RptID, TrgOps, DatSet, BufTm, and IntgPd.

Additional Information

7

This chapter describes special features of SIPROTEC 4 devices relating to implementation of IEC 61850 or Ethernet module.

7.1 Time Synchronization

SIPROTEC 4 devices have various options for synchronization of their internal clock. The details provided below apply for devices featuring Ethernet interface and IEC 61850 protocol. This device property expands the DIGSI configuration tool with an additional feature to set summer and standard time. For this purpose the user has to select *Ethernet NTP*. This requires a station network with one or 2 SNTP Server. Fig. 3-4 shows respective synchronization settings.

Redundant Time server

The software of the EN100-module supports a second, secondary time server as redundancy (as of version V3.09). The query of both servers is carried out cyclically in minute time. Normally it will be synchronized on the first (primary) time server. If the query of the primary server doesn't satisfy the criteria for a successful time synchronization, it will be changed on the secondary server. If it is not possible to synchronize on the redundant server either, after a parameterizable time delay the device carries out the indication "`time disturbance`".

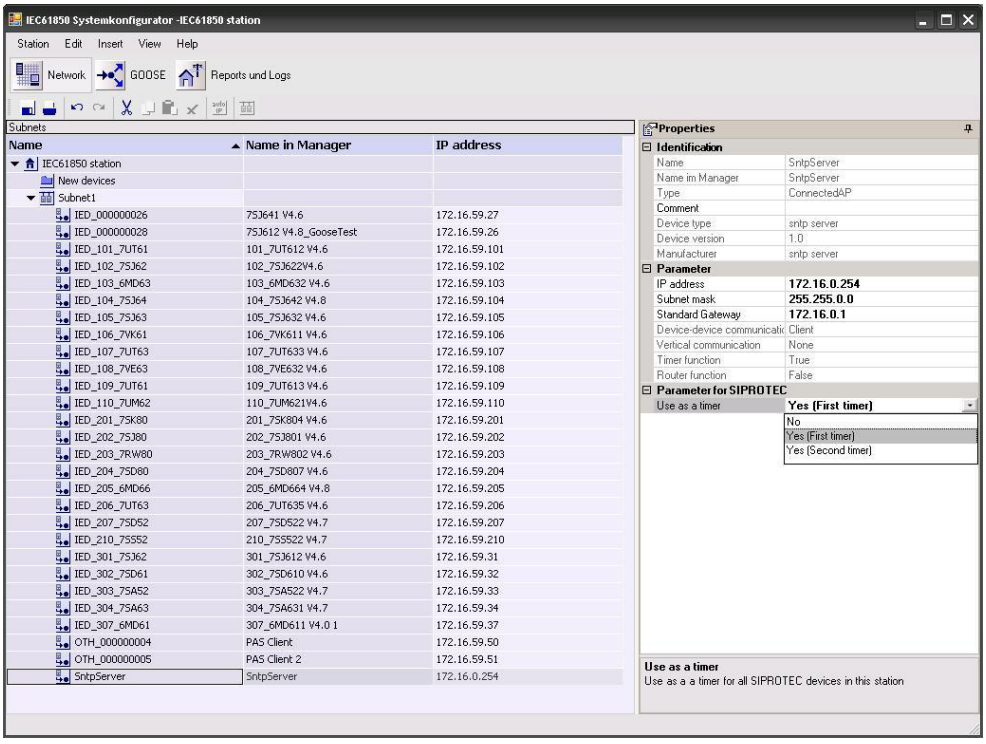


Fig. 7-1 Settings of time synchronization

IP adresse of the clock server

The IP address of the clock server itself is set in the System Configurator. An ICD file of the clock server must be imported into the Configurator for that purpose. This file is included in the DIGSI CD. An IP address is routed in the System Configurator to the clock server. After the parameter settings of the devices have been updated, the settings use the set IP address to request the time from the clock server. A prerequisite for this is that Ethernet NTP has been set as the time synchronization source.

On the module information page of the device (see Chapter 7.3) , the IP address set for the clock server can be checked.

7.1.1 Time Synchronization *Ethernet NTP*

This synchronization method is recommended for devices with a system interface according to IEC 61850; the synchronization is done without additional efforts using the Ethernet network. Besides the favored NTP servers provided by different manufacturers as devices, software solutions (NTP/SNTP Server) can also be implemented on individual or industrial PC.

Configuration

As shown in Fig. 3-4, the source of time synchronization is *Ethernet NTP*. Parameters for summer/standard time change are set with *GMT+1* (valid for Berlin, Bern, Brussels, Rome, ...).

NOTE

The daylight saving time offset refers to the GMT time (as specified) and not to the time zone.

NTP time server

The NTP servers are integrated as *'Other IEC 61850 communicators'* via an ICD File which is included in the DIGSI 4 CD. Until versions prior to V3.09 only one NTP server was supported, if 2 servers were configured, only the one with the lower IP address was addressed. From version V3.09 up the time query is extended by a second, secondary time server. The first server functions as preferred server to ensure that all equipment runs with the same master clock if possible. The second server is available as redundancy.

Status and accuracy

The internal clock of the SIPROTEC 4 device reaches the steady state of +/-1 ms after max. 15 minutes of a healthy synchronization. This internal accuracy cannot be measured here because a precise trigger option is not available. For checking purpose, a binary input is often triggered (configured: without a software filter, with recalculation of the hardware filtering time). Such measurement, however, including jitter in binary input processing, has deviations of approx. +/-3 ms.

Time fault indication

A time fault indication is output when the clock server does not respond to inquiries of the SIPROTEC 4 device (after the configured monitoring time has expired, in this example 10 minutes). From now on, the status of type time fault is set in the time stamp of all indications. The bit 'clock failure' in the IEC 61850-8.1 will be set accordingly in the time stamp of the Data Object.

The time fault indication does not appear when the SNTP server itself has no connection to the time source (e.g. no antenna signal, ...) and sends clock signals to all devices according to its internal accuracy. However, at start-up, as long as no connection has been established with the SNTP server or the time synchronization message indicates a stratum greater than 3, the bit 'ClockNotSynchronized' will be set in the time stamp of the Data Object, to indicate that the clock has not yet been synchronized.

Special features

- The precondition for this synchronization is that an SNTP Server is available in the network, is accessible and known. If the address of the server is set incorrectly, the following time appears on the home page of the module: Sa.1.01.1994. In this case, the correct address of the desired time server must be set.
- Directly after the device startup and up to the first synchronization after approx. half a minute, no valid time is available in the device.
- To enable all devices which are synchronized by the server to operate with a synchronous time among each other, the time server itself does not necessarily need to be synchronized. However, the time used in the devices is not synchronous with Greenwich Mean Time.

Online switching options at the device display

The time mode at the display may not be switched over while it is running, as conversion parameters from local time to Greenwich Mean Time are presently available only in the module. This setting change should only be made using DIGSI.

Further time modes with EN100-module

The configuration in DIGSI enables further time synchronization modes combined with the EN100-module. The correct functioning of these time synchronization modes is not presently provided by IEC 61850. Should one of these operating modes be used in special cases and is correspondingly configured in DIGSI , in such a case, the interaction between the time mode in the device and the EN100-module should be taken into account.

All real times saved in the indication buffers are local times and correspond to those displayed at the device display. The EN100-module alone can convert these local times to UTC required for the IEC 61850. The biggest problem in this case is summer/standard time change common in most countries. This results, for example, in having the time 2:10 twice a day, after the clock has been reset. In order for the module to convert both local times to the current Greenwich Mean Time, it needs to know whether it is summer or standard time at that moment. The not NTP time mode must support at least the summer/standard time bit in the local time of the device. DCF77 does support this feature, IRIG-B, internal time mode, minute pulse, but other features does not.

7.1.2 Internal Time Mode

The internal time mode is characterized by the fact that it is not externally synchronized. This time mode does not support summer/standard bit, i.e. the device does not know whether it is summer or standard time now. The daylight saving time bit displayed on the device has no relevance in this case.

In a place without summer/standard time change, the local time is set at the display and only the time zone is configured (tick "Without summer time change") for local time parameters UTC- conversion.

In a place with summer/standard time change, the following options are available:

- the device always operates with standard time,
- or to configure an appropriate time zone for the current local time (Germany e.g. in winter +1 h and in summer +2 h) which remains valid only until the next summer/ standard time change, i.e. it must be reconfigured when the next change is due (the time zone is not correctly any longer, as this change is set via the time zone setting).

In both cases, tick the *Without summer time change* parameter.

Time synchronization via DCF77

DCF77 supports the summer/standard time bit. In case of the DCF77, the time change takes place according to the local time of the transmitter in Frankfurt/M. I.e. summer/standard time change must be configured at the current location of the device. Moreover, this synchronization works only correctly at locations where the local time is synchronous with German local time (Frankfurt). This applies, for example, for Finland. The parameters are as follows:

Offset from time signal: 1 h

Time zone offset from GMT: 2 h

Daylight saving time offset from GMT: 2 h

Set the beginning and end of the daylight saving time as shown in Fig. 3-4.

Time synchronization via IRIG-B

IRIG-B does not support the summer/standard time bit. As IRIG-B does not perform any summer/standard time change, the offset from GMT is always constant. The *Offset from time signal* specified in the configuration should be reset for the *Time zone offset from GMT* module parameter. The *Without daylight saving time change* parameter should be activated.

Time synchronization via fieldbus and T103

These time modes are not available, as the respective interface cannot be simultaneously operated with the EN100-module.

Time synchronization via BI pulse

The time mode via BI[1] pulse does not support the summer/standard time bit. If the summer/standard time change is made via BI, the converted GMT time is no longer correct for IEC 61850. This application is not supported.

If no summer/standard time change is made via BI, the offset from GMT is always constant. The time zone has to be set as shown in Fig. 7-1 and the *Without daylight saving time change* parameter ticked.

1. BI: Binary input

7.1.3 Operation of the Redundant Time Server

The software of the EN100-module has been extended by interrogating a second, secondary time server. The first, primary server remains the preferred server so that all devices, if possible, operate with the same master clock. The clients on the module shall preferably synchronize with servers on the PAS.

The EN100-module interrogate both NTP servers cyclically every minute. It normally synchronizes itself on the first parameterized, the primary NTP server. If the first NTP server doesn't respond to a query twice successively within the one minute's polling interval, the time synchronization switchovers to the secondary, second server. Further switchover criteria are:

- the server shows "alarm" on the response telegram (variable leap = 3)
- the Stratum of the server is 0 (unknown) or greater than 3
- the current time is indicated with 0 (if no reception, then Hopf)
- the running time of the telegram in the net is greater than 5 ms

The switchover will be prevented if the second server delivers no considerably better time signal, i.e. if the server only was attainable last for less than 10 minutes, if it announces alarm or its Stratum is 0 or greater than 3, or it indicates the current time with 0 or the running time of the telegram in the net is greater than 5 ms. In all these cases the device then gets no longer synchronized. It runs with the internal ms time base and the last valid drift. After the parameterized time delay the device announces a time disturbance signal.

While the module is synchronizing on the second server, it also interrogates the first server. The switch back to the first server will only take place if it has performed an acceptable quality for 10 minutes as already mentioned. The switch back is delayed as long as all conditions are fulfilled.

At the startup of the module the first server will be interrogated, about 5 seconds later the second server, too. The time of the first server will also be taken if the Stratum is 0 or greater than 3 or the second server offers a better Stratum 5 seconds later.

The announcement of a time disturbance signal works purely from the view of the device. I.e. it will only be announced if the device gets no longer synchronized from the module.

For the redundant NTP client on the module this means that the announcement of the time disturbance signal will not be issued during a successful switchover on the second server. If the time delay of the indication is parameterized on the minimum value of 2 minutes in the device, which corresponds to a twice repeated failure, then the behavior isn't determined and the indication could possibly appear. So for a defined behavior the time delay for the time disturbance indication has to be parameterized up to at least 3 minutes. The time delay for the time disturbance indication is not available as a parameter on the module and therefore can neither be tested nor be used for an adapted switchover time (the above-mentioned 10 min).

While switching back to the first NTP server no time disturbance indication will appear because the transition takes place without loss of synchronization.

Additional information (EN100-module firmware version 4)

Some NTP servers are configurable to increase the stratum from 1 to e.g. 6, if the satellite reception is faulty. If the module detects that the stratum value is 4 or higher, the flag "ClockNotSynchronised" is set immediately in all reports to be send to the IEC client.

7.2 Switching Commands

Use of check bits

IEC 61850 allows to check whether switching commands are executable before they are executed. Check bits can be used to enable or disable interlocks. In the devices of the SIPROTEC 4 range, check bits are used as follows:

- If a protection device cannot perform a synchronization check (e.g. because no mandatory synchronization has been specified for a circuit-breaker) and a switching command is sent to the device via IEC 61850 where the respective check bit is set, this switching command is then rejected with a negative acknowledgment command.
- But, if a protection device cannot check the zone control[1], (circuit breaker against dead line and grounding isolator), a switching command with set interlocking check bit[2] is executed all the same.

NOTE

This specific treatment of check bits has to be taken into consideration while configuring a system.

Blocking mode

Acc. to the IEC 61850 standard, no device outputs are specified if the device is in blocking mode. SIPROTEC 4 devices allow this output in blocking mode.

1. This the case if there are no appropriate parameter settings.
2. This bit is assigned to the zone control.

7.3 GOOSE Stop

The function stops the transmission of all GOOSE messages of the device. This is useful during commissioning and during the tests of the device. Since data objects are not transmitted to other devices, this does not result in undesired reactions. Furthermore, it is then possible to check the failure monitoring for GOOSE messages in the receiving devices.

This function is available for version 4.2 and higher of the module firmware.

Parameter: GOOSE Stop

It is possible to activate the GOOSE Stop function by setting the parameter **`GOOSE-Stop`** (default setting = No) as shown in the following figure. Setting the parameter **`GOOSE-Stop`** = ***`No`*** ensures compatibility with older EN100 firmware versions, which do not support the GOOSE Stop function.

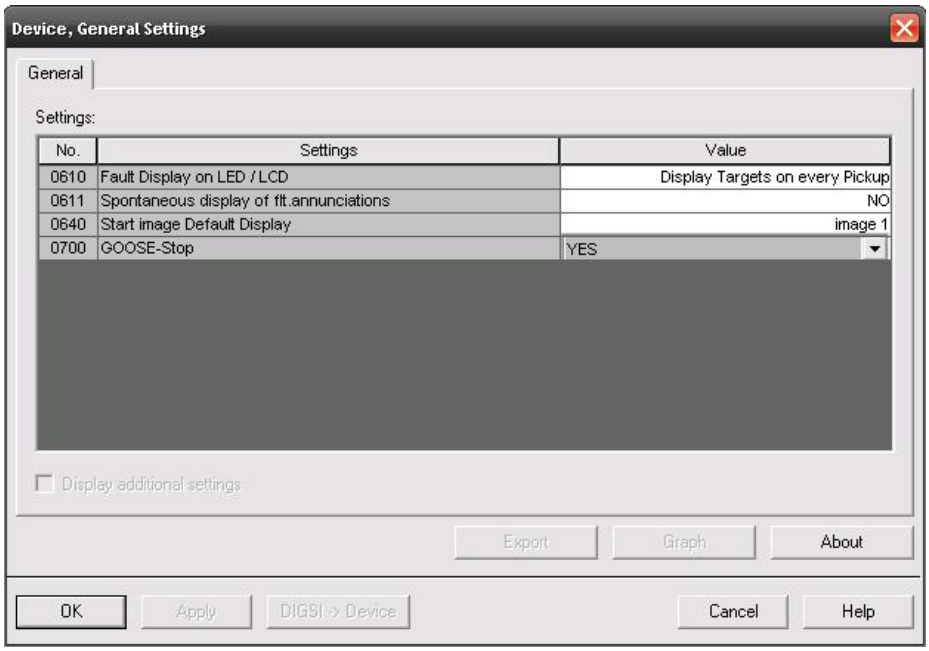


Fig. 7-2 Configuring the GOOSE Stop function

>GOOSE Stop is available for devices which support this feature with the device firmware.

>GOOSE Stop

It is possible to switch off the transmission of GOOSE messages with the message **>GO-Stop**. It is possible to link the message **>GO-Stop** to CFC or to a binary input.

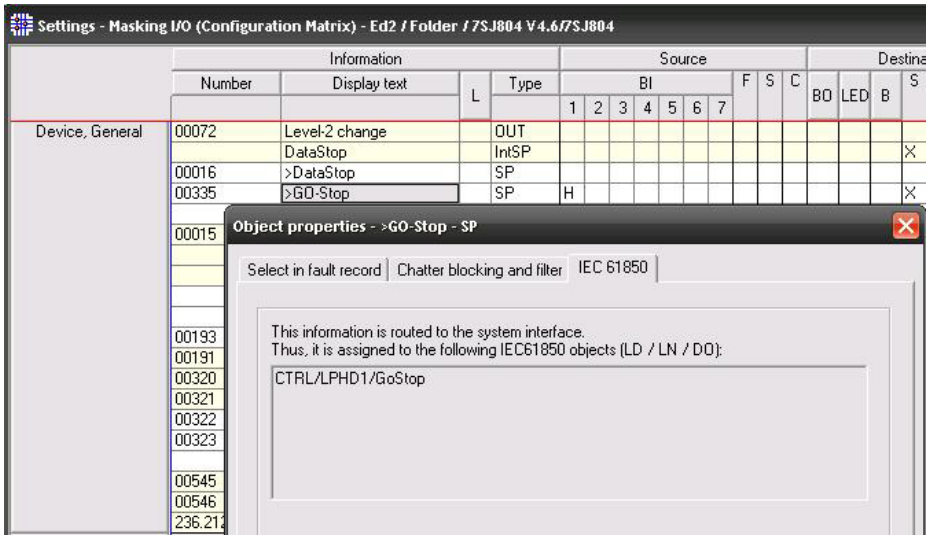


Fig. 7-3 Linking of the message **>GO-Stop**

7.4 Module Information Page

The modules have a display of their own, which can be visualized on the device display with the menu item *Menue* → *Test/Diagnose* → *Modulinfo* → *Port B* (short form: *Menue-5-5-1)*. The screen itself depends on the module type and is available only in English. The information screen of an Ethernet module with optical interface is built up as shown below. The detailed figure can be different for module firmware versions:

```
1        Network Config
2        MAC 080006865116
3        IP  172.016.052.055
4        NM  255.255.000.000
5        GW  172.016.000.001
6        NT1* 172.016.000.254
7        Chan1/2=Up/Up
8        Rx/TxCnt=23489/34403
9        Rx/TxErr=00000/00000
10       Rx/Tx10s=03221/02888
11       CPU load=68%
12       LRx1/LTx1=norm/norm
13       LRx2/LTx2=weak/----
14       Switch RSTP
15[1]    Priority=32768
16       Bridge Id=172165255
17       Hello Time=2sec
18       Max Age Tm.=20sec
19       Forward Del=15sec
20       MaxTransmCnt=100
21       R/S1=A/D R/S2=R/F
22-26    ...
27       ******* END *******
```

[1]Lines 15 to 26 are not available for Line, PRP and HSR.

Bild 7-4 Module information in the device display

Display of the connection type

The lines 1 to 11, with the exception of line 7, are the same for modules with electrical and optical interface. In modules with optical interface, line 7 shows the status of the 2 connections, whereas in modules with electrical interface it only shows the following information:

```
7        Phy1 100 MBit Full-Duplex
```

This information indicates that channel 1 of the module is currently active, and operates with 100 Mbit in Full Duplex mode.

Parameters of the optical interface

The lines from line 12 onward are only visible on the module with optical interface (operating mode: Switch), and show the settings/statues of the optical interface. The lines 15 to 20 display the RSTP parameters of the internal switches. The lines 22 to 26 contain internal displays, and are not described here.

MAC address

Line 2 contains the MAC address of the EN100-module. This address is routed only once.

Network parameters

The lines 3 to 6 show the settings of the network parameters IP address (IP), subnet mask (NM), gateway address (GW), NTP server address (NTP).

SNTP status

Line 6 has 3 functions. The contents of this line toggle in intervals of approx. 10 sec between the server address and the time elapsed since the last synchronization.

```
6          NT1* 172.016.000.254
6          NTP1/2 sync 021/026s
```

If the server address is displayed the star („*“) symbolizes an active SNTP server. The time is displayed for up to 999 sec (i.e. approx. 16 min). A display of 999 right after startup of the device signals that there is no synchronization via SNTP.

Corrupt parameters

This line also signals the existence of corrupt parameters. This is the case when the parameter settings of the module do not match the parameter settings of the device (this happens normally after modules have been exchanged between devices, without a subsequent device initialization using DIGSI). The display alternates with the values of the NTP displays:

```
6          Corrupt parameters
```

The substation controller SICAM PAS shows in that case *pending*; no IEC connection is established, but the TCP/IP functions are available.

Double IP address

The third function deals with the signalization of a double IP address. When a device starts up in the network, the existence of the IP address is checked. If the address already exists in the network, a static information to that effect is displayed in line 6:

```
6          !!MAC!!0007E908FCC8
```

In that case, the device will not be connected to the network. The double IP address can be identified from the MAC address displayed. which is part of the existing IP address.

Interface status

The lines 7 to 10 show the status of the interface. Line 7 in the view above shows that both channels are active. This information is only displayed if the internal switch is active. If one of the 2 channels is down, the ring is broken.

Line 8 shows the number of telegrams received and transmitted. This counter is not reset and signals that the interface is working properly. The telegram errors found are counted in line 9. Line 10 shows a 10 sec mean value of the telegrams received and transmitted.

Line 11 provides information on the processor load of the communication module.

The lines 12 and 13 provide information on the status of the optical interface. The first value in the line is determined from the receive output at the port; it shows *norm* for an output up to -28 dBm, weak up to -30 dBm; if the receive output is less[1], only bars will be displayed. This does not necessarily mean a broken connection; a broken connection will be shown in line 7. The status *weak* should normally not occur if the optical

budget is kept within permissible limits. If it is displayed, the connections need to be checked.

The second value is the transmit output. The display *norm* shows a transmit output of -16 dBm, which is the normal state. Lower outputs are indicated by bars. This does not indicate that the transmitter will fail straight away but that the driver, due to aging, is no longer able to deliver a transmit output of -16 dBm[1]. Whether the connection as a whole is able to function depends also on the condition of the cables and the receiver. Precise information is provided by the symbol error rate in the FEC statistics on the module home page (see Fig. 9-5).

Line 14 shows the redundancy mode *RSTP* set in the switch. The next lines show the settings relating to that operating mode. They are not shown in OSM mode. The switch positions can only be changed using DIGSI (see Fig. 3-5 to Fig. 3-7).

RSTP status

Line 21 shows the interface status in the RSTP ring. The role and the status (R/Sx=) are displayed for both channels (ports).

Roles of the ports

The following roles are defined for the ports:

- Root port role (R):
  A root port is connected with the root switch, i.e. it has a logical connection with it. With internal switches, one of the 2 ports always the role of a root port.
- Designated port role (D):
  A designated port can also establish a connection with the root switch, but in a different way. One of the 2 ports of the internal switch normally has the designated port role.
- Alternate port role (A):
  An alternate port can establish a connection in case of a failure. In stable operation, there must be exactly one alternate port in one device per ring. In the absence of a port with this role in a ring, the redundancy is not ensured; the ring is open.

Port states

In addition to the role played by them, ports have states assigned to them. The following states are defined:

- Forwarding state (F):
  This is in normal operation the state of the ports which play the root or designated role, i.e. payload telegrams are always transmitted.
- Discarding state (D)
  Discarding state means that telegrams are discarded and not forwarded. In normal operation, only the port with the alternate role has this status.
- Learning state (L):
  This state is not available in the internal switches. The switch structure is such that the port does not require a learning phase.

1. According to IEEE 802.3 the receive output window is -14 dBm to -31 dBm.
1. According to IEEE 802 the output window of the transmitter is between -14 dBm and -20 dBm.

Normal status

In our example, port 1 shows the role “alternate“ and the status “designated“, which means that this port does neither accept nor transmit telegrams from and to the device. Port 2 has role “root“ and status “forwarding“, which means that telegrams are transmitted and received through this port. We can conclude from the information displayed that this device is the logical separating point in the optical ring.

Text shown on a small display

Devices with a small alphanumeric display can only show 4 lines at one time; therefore only the first 4 lines of the view shown in Bild 7-4 can be read. More lines can be displayed by scrolling up and down with the arrow buttons.

7.5 SNMP Information

The SNMP[1] protocol is implemented in all Ethernet modules with firmware version 3.0 or later. This allows to query the status of modules. The information displayed is explained below.

A MIB[2] browser and the associated description file is required to detect the module information or module statuses using SNMP. MIB browsers allow to display SNMP information objects and their content. In Fig. 7-5 the product of iReasoning (http://www.ireasoning.com) has been used, but any browser with a comparable scope will be suitable.The file *SipEthernet.mib* describes the available information objects and allows to display them, as shown in Fig. 7-5. The MIB can be found in the internetworking under *http://www.siprotec.com*.

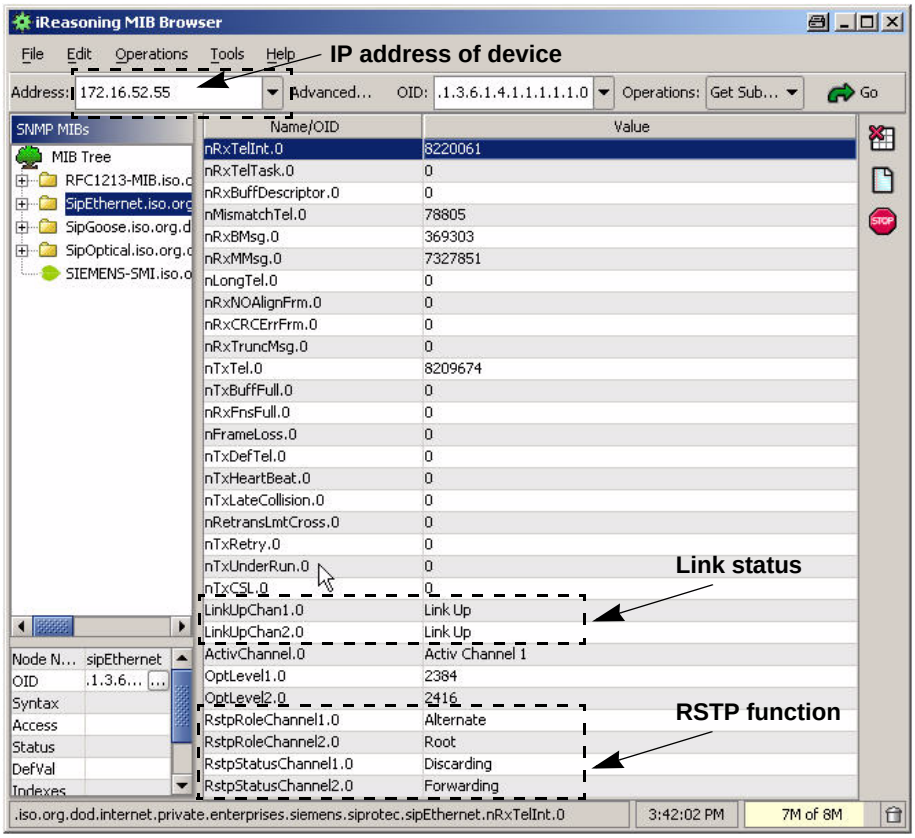


Fig. 7-5 Displays of module information

1. SNMP, **S**imple **N**etwork **M**anagement **P**rotocol
2. MIB, **M**anagement **I**nformation **B**ase

7.5.1 Display of Link And RSTP Information

To display the information, the MIB file must first be loaded into the browser. Next, the IP address of the desired device is set, and the information can be retrieved from the device. These settings and the operator action can vary from one browser to the next.[1]

Essential information on link and RSTP

Fig. 7-5 shows the 2 most essential items of information. These are the status of the 2 interfaces and the functionalities of RSTP.

If the module is operated as a switch, both channels must be active (Link Up). Data is transmitted and received on both channels.

Role of the ports

The role[2] of the ports[3] is to allow to detect interruptions in the ring. A ring structure may have a physical interruption. In that case the associated link is also set unavailable (LinkDown). The role of the port is then disabled. The physical connection via this port is interrupted, which means an error.

Logic break point in the ring

In normal operation with RSTP, however, the ring is broken at one point in the network in order to prevent telegrams from circulating endlessly, which would make network operation impossible. The roles *designated* and *root* indicate that there is no logic break point at the ports, i.e. that the logic break point is not located on the connection between this port and the other device. Only one device in the ring shows the roles *alternate* and *designated*, with the logic break point being located at the *alternate* port.

If the ports show the combination *alternate-designated* or *backup-designated*[4], the logic break point is located at the port which is identified as alternate or backup. Knowing about the logic break point is useful for commissioning (see also Bild 7-4).

Port status

The port status only changes when the network is re-configured due to an error. The logic break point is then closed. The corresponding ports then take on the status *discarding*, in which no payload data is yet transmitted; only administration information, such as changes of the role of a port, is transmitted. The status which follows, *learning*, is only transitory because of the fixed address setting of the internal switches; still no payload data is transmitted. The status *forwarding* characterizes the normal state, in which payload data telegrams are transmitted.

1. The Internet address shown in Fig. 7-6 will receive automatically an extension, such as:161, for the standard port on which the SNMP works.
2. The RSTP protocol to IEEE 802.1w defines the roles and statuses of a port.
3. Ports are here identical with the 2 interfaces that form the ring structure.
4. The *backup* role does not exist in integrated switches.

7.5.2 Display of GOOSE Information

GOOSE information can be displayed quite easily with SNMP. Only the MIB file SipGoose.mib is necessary.

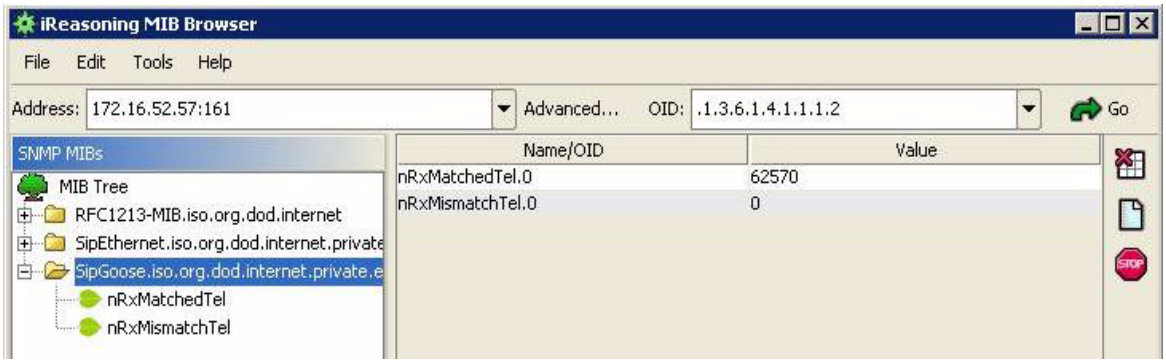


Fig. 7-6 GOOSE telegram information

The detail view in Fig. 7-6 shows the 2 counters for the GOOSE telegrams. The counter *nRxMatchedTel* shows the telegrams which have passed the multicast filter. The counter *nRxMismatchTel* shows the number of telegrams revoked by the check of the further GOOSE parameters.

Multicast filter setting

In the present case only those telegrams are received which are intended for the device. The number of blocked telegrams provides information of the network load due to other multicast telegrams. Both counter also allow to conclude the correct setting of the multicast filter, provided that the number of multicast circuits is known. Where there are several multicast circuits, some of which are not routed to the device, the counter *nRxMismatchTel* in this device must have a value that is not zero. If this is not the case, the filter setting is wrong, and overloads in the communication may be the consequence. This display is of particular importance for the commissioning of plants containing devices whose multicast addresses have not been routed using DIGSI.

This filter is automatically set in DIGSI during the configuration of GOOSE messages in DIGSI and in the System Configurator.

7.5.3 Display of RSTP Parameters

The RSTP parameters are set and changed in DIGSI. A read access to these parameters is also possible via SNMP. Using the MIB file *SipOptical.mib*, the following information is displayed:

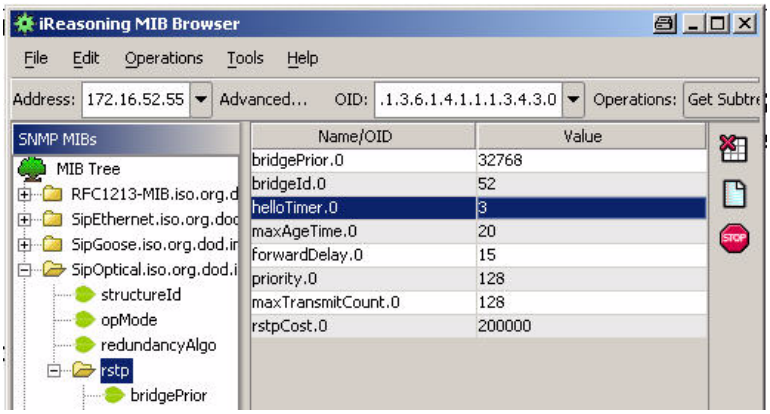


Fig. 7-7 RSTP parameter settings

The display shown in Fig. 7-7 visualizes the RSTP parameters set in DIGSI. They correspond to the values shown in the display.

Fig. 7-7 on the left shows that all existing MIB files can be loaded into the browser. This provides a tool that allows to monitor all SIPROTEC 4 devices throughout the network with regard to their accessible information.

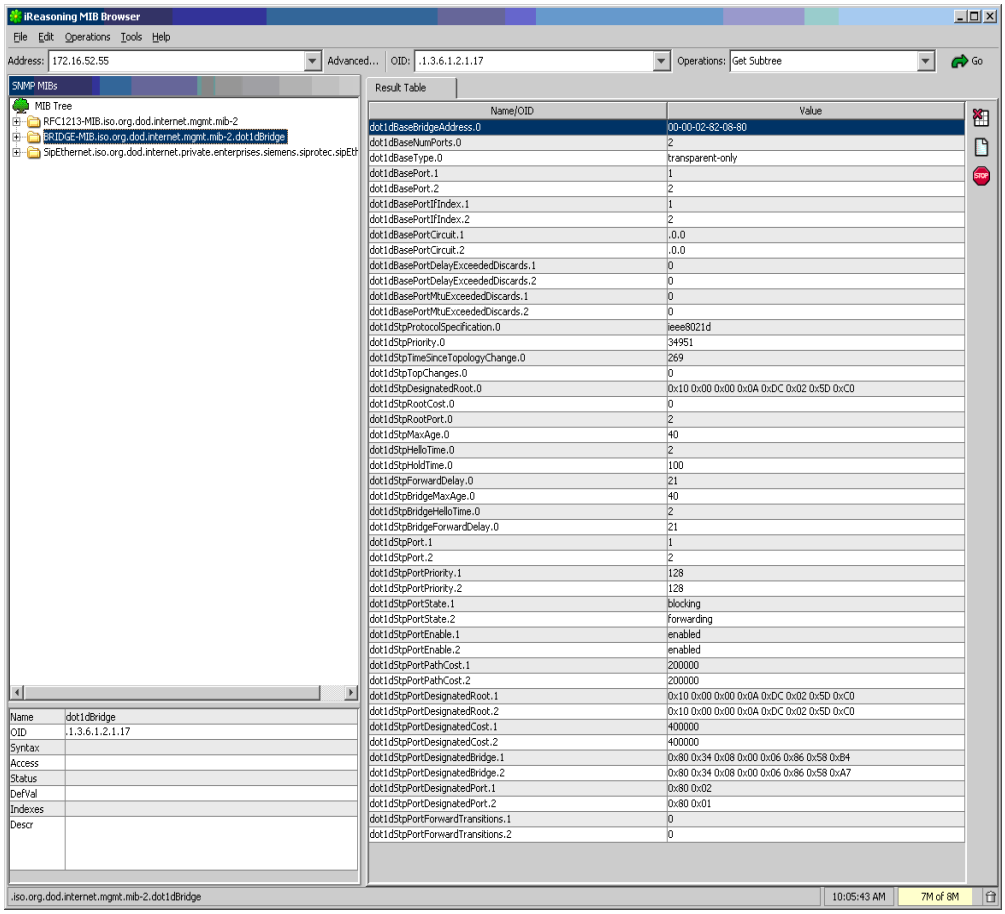
The devices can thus be integrated into the customer's power system management, and can be monitored automatically. For instance, the overall information about the optical ring allows to monitor its physical and logic state.

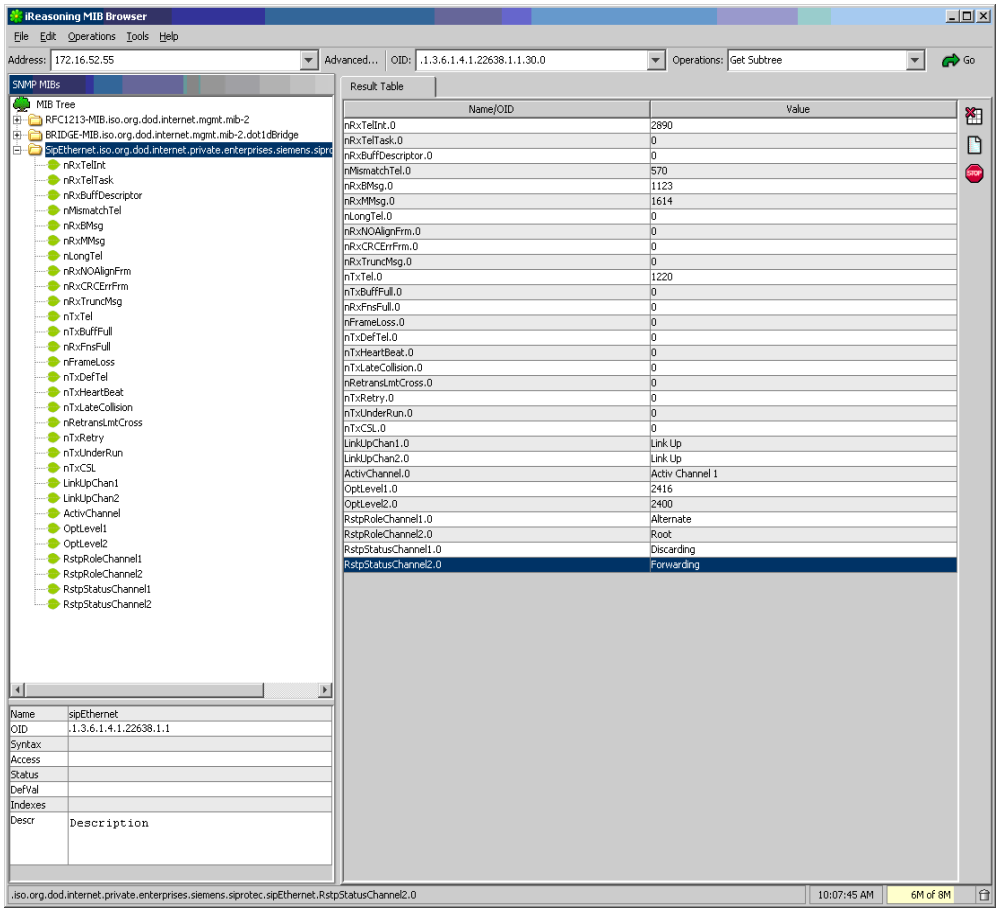
7.5.4 Display of RSTP Information to RSTP Using The Bridge MIB

Table listing For single information there are descriptions in the Bridge MIB.mib.

Name	Value
dot1dBaseBridgeAddress.0	00-00-02-82-08-80
dot1dBaseNumPorts.0	2
dot1dBaseType.0	transparent-only
dot1dBasePort.1	1
dot1dBasePort.2	2
dot1dBasePortIfIndex.1	1
dot1dBasePortIfIndex.2	2
dot1dBasePortCircuit.1	.0.0
dot1dBasePortCircuit.2	.0.0
dot1dBasePortDelayExceededDiscards.1	0
dot1dBasePortDelayExceededDiscards.2	0
dot1dBasePortMtuExceededDiscards.1	0
dot1dBasePortMtuExceededDiscards.2	0
dot1dStpProtocolSpecification.0	ieee8021d
dot1dStpPriority.0	34951
dot1dStpTimeSinceTopologyChange.0	269
dot1dStpTopChanges.0	0
dot1dStpDesignatedRoot.0	0x10 0x00 0x00 0x0A 0xDC 0x02 0x5D 0xC0
dot1dStpRootCost.0	0
dot1dStpRootPort.0	2
dot1dStpMaxAge.0	40
dot1dStpHelloTime.0	2
dot1dStpHoldTime.0	100
dot1dStpForwardDelay.0	21
dot1dStpBridgeMaxAge.0	40
dot1dStpBridgeHelloTime.0	2
dot1dStpBridgeForwardDelay.0	21
dot1dStpPort.1	1
dot1dStpPort.2	2
dot1dStpPortPriority.1	128
dot1dStpPortPriority.2	128
dot1dStpPortState.1	Blocking
dot1dStpPortState.2	Forwarding
dot1dStpPortEnable.1	Enabled
dot1dStpPortEnable.2	Enabled

Name	Value
dot1dStpPortPathCost.1	200000
dot1dStpPortPathCost.2	200000
dot1dStpPortDesignatedRoot.1	0x10 0x00 0x00 0x0A 0xDC 0x02 0x5D 0xC0
dot1dStpPortDesignatedRoot.2	0x10 0x00 0x00 0x0A 0xDC 0x02 0x5D 0xC0
dot1dStpPortDesignatedCost.1	400000
dot1dStpPortDesignatedCost.2	400000
dot1dStpPortDesignatedBridge.1	0x80 0x34 0x08 0x00 0x06 0x86 0x58 0xB4
dot1dStpPortDesignatedBridge.2	0x80 0x34 0x08 0x00 0x06 0x86 0x58 0xA7
dot1dStpPortDesignatedPort.1	0x80 0x02
dot1dStpPortDesignatedPort.2	0x80 0x01
dot1dStpPortForwardTransitions.1	0
dot1dStpPortForwardTransitions.2	0





7.6 Firmware Update in SIPROTEC Devices and Ethernet Switches

You have the alternative to update the firmware of the EN100-module. For the EN100-module, you find the actual firmware of every device in the download area of http://www.siprotec.com. Up to firmware version 4.07, update via the front interface of the protection device. With the firmware version 4.08 and higher, use the Ethernet interface to update the firmware. Both procedures are described in the documentation "Firmware / FPGA Update via the Ethernet interface of the EN100 module for PRP" and "Readme for IEC 61850 Ethernet module EN100 Firmwareversions". These documents are also available under http://www.siprotec.com.

If the device uses an optical interface and it is a participant of a ring, it is recommended by Siemens to open the ring described in the following table.

Also you have the alternative to update the firmware of the Ethernet switches. Siemens also recommends opening the rings for an update described in the following table.

Table 7-1 Overview of the update types

Type	open ring(s)	Comment
Firmware update of the SIPROTEC device	yes	The hints in the device manuals applys accordingly
Firmware update of the EN100-module	yes	–
Parameter set update (serial and Ethernet)	yes	–
EPLD update of the EN100-module	yes	–
Firmware update of the Ethernet switch	yes	Caution, a switch may be a participant of several rings simultaneous

Troubleshooting Hints

8

The subject of this chapter is troubleshooting problems with the Ethernet interface. First, here are the essential points that can prevent correct working.

No link established

If the device does not connect, first check the installation. Has the link to the switch been correctly established and have the right cables been used (no crossover cables!)? Has the correct cable been used for a direct link with the PC (crossover cables must be used in this case!)? Is the switch functioning correctly and is its supply voltage OK? Correct functioning of a link can be seen by the link status LED.

IP address

Has an IP address been set in the device? If this setting has not been made and there is also no DHCP server in the network, it will not be possible to establish a link. To validate the IP address, it is possible to execute a ping from the network to the device's IP address.

Subnet mask

Has the subnet mask been correctly set? The subnet mask results from the addressing scheme used in the network segment.

MLFB extension

Has the MLFB extension been correctly set in DIGSI? If not, the module is not parameterized and does not function.

Remote access not possible

Has the gateway address been correctly set in the device? If it is not correct, it will not be possible to access a device via 2 or more networks.

No time synchronization via Ethernet

Is there a time server in the network and what is its address? Has the address been correctly set in the device? If the device correctly parameterized for use of time synchronization via Ethernet?

If the time server is a PC, is the Windows time service deactivated and the correct NTP service started?

Visibility of module information

Module information is extremely useful in troubleshooting. See Chapter 7.3 for relevant information.

Diagnostic Functions

9

The diagnostic functions can be divided into those indicating the module status in the device, i.e. that do not require a functioning link via Ethernet, and those that are only accessible via the Ethernet network.

Diagnostic functions in the context of the device

In the context of the device, the operating message buffer is the central element where the status of the module and therefore of the link is indicated. It also contains error messages of the module. No further information on the module can be obtained in this way.

In the context of the device, the operating message buffer is the central element where the module failure message and the link status messages are logged. The messages can also be routed; in DIGSI they appear as shown in Fig. 9-1. The module failure message indicates that the module cannot operate. The 2 link failure messages indicate that there is a physical break point in the link.

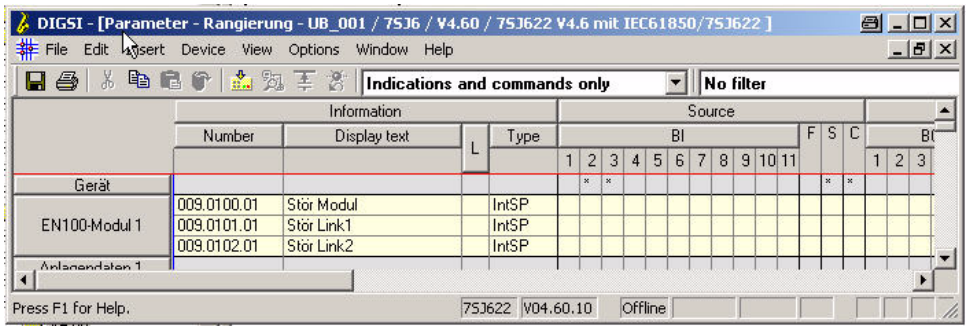


Fig. 9-1 Messages of the EN100-module in DIGSI

Module status page

The module has its own status page that can be viewed on the device display. This page can be invoked with *Menue* → *Test/Diagnose* → *Modulinfo* → *Port B*. The information is described in Chapter 7.3.

Module HOMEpage

All modules are provided with a homepage, which can be invoked on all devices using the respective IP address. Fig. 9-2 shows an example of a homepage. The homepage is invoked by entering the IP address of the device combined with *home* in the address line of the browser on the PC (e.g.: *http://172.16.52.53/home* with IP = *172.16.52.53* set with DIGSI).

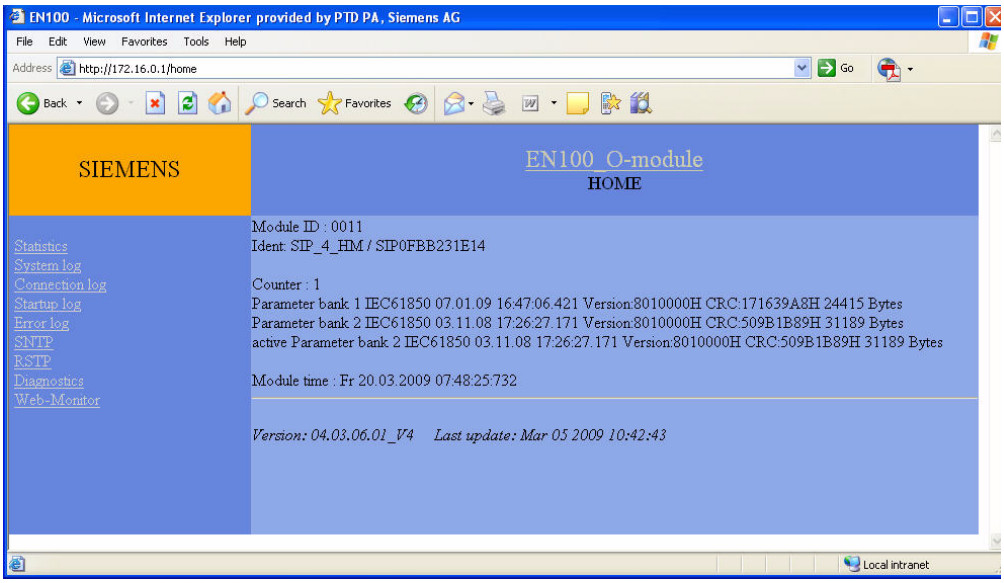


Fig. 9-2 Homepage of the EN100-modules

The module homepage always shows at its end the version and creation date of the software version loaded on the module.

The homepage is not required in normal operation, and does not contain any relevant information for it. The following pages (Table 9-1) on the left area of the homepage contains information for commissioning. They contain operational information and internal error messages.

Table 9-1 Further pages

Page	Description
Statistics-page	shows relevant information of Ethernet
System log-page	shows information of system behavior, being produced from operation time
Connection log-page	contains information about Client-Server-Connection and DIGSI-Accesses
Startup-page	contains information about run-up behavior and configuration settings respecting network- and GOOSE-Parameters
Error log-page	contains internal error messages
SNTP-page	contains information about settings and condition of time synchronization
RSTP-page	contains information about settings and condition of the network redundancy
Diagnostics-page	shows specified parameter of modules, which are accessable by Siemens on demand
Web-Monitor-page	(not available for all SIPROTEC 4 devices) shows the real-time front view of the device and some specified device parameters

In normal operation the error buffer display is empty, as shown in Fig. 9-3

Error buffer

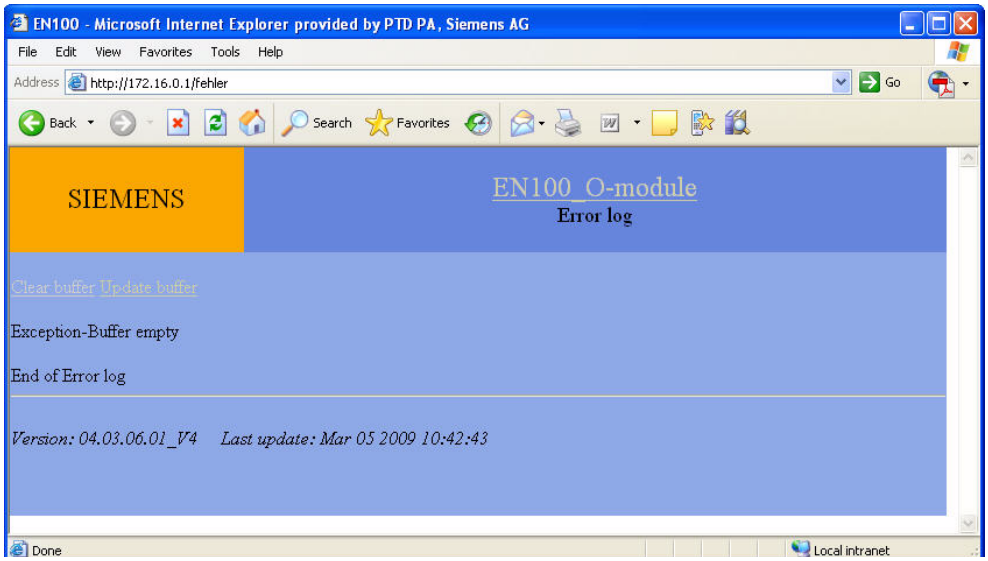


Fig. 9-3 Empty error buffer

System log

The system log serves to display internal information. A detail of the startup procedure is shown in Fig. 9-4. However, detailed insider knowledge is necessary to interpret the information displayed. In special cases it may be useful to read out the contents of the system log and send them to the hotline. Saving the log as a HTML-file is done in the Explorer.

```
+++ 00079 00136956 Do 19.03.2009 18:44:33:874 The following connection have been established:
+++ 00080 00136957 Do 19.03.2009 18:44:33:875
+++ 00081 00137335 Do 19.03.2009 18:44:34:252 MAP: GI device - module started
+++ 00082 00137534 Do 19.03.2009 18:44:34:452 MAP: GI device - module completed
+++ 00083 00138158 Do 19.03.2009 18:44:35:075 ---SFS-check start
+++ 00084 00138158 Do 19.03.2009 18:44:35:075 ---SFS-check logon
+++ 00085 00138158 Do 19.03.2009 18:44:35:075 ---SFS-check LogonAck
+++ 00086 00138162 Do 19.03.2009 18:44:35:079 ---SFS-check CdAck
+++ 00087 00138164 Do 19.03.2009 18:44:35:081 ---SFS-check MountAck
+++ 00088 48722547 Fr 20.03.2009 08:14:22:196 EES: Port 2 Link Down (extern)
+++ 00089 48722547 Fr 20.03.2009 08:14:22:196 EES: Ctrl: disable Port 2, now: P1==conn==EN100..disc..P2 (1b)
+++ 00090 48722548 Fr 20.03.2009 08:14:22:198 EES: Forw: Port 2 enable, now: 1=forw==EN100==forw=2 (12-->3c)
+++ 00091 48722548 Fr 20.03.2009 08:14:22:198 EES: Forw: Port 2 disable, now: 1-trans-EN100-block-2 (3c-->12)
+++ 00092 48725226 Fr 20.03.2009 08:14:24:876 EES: Ctrl: enable Port 2, now: P1==conn==EN100==conn==P2 (3f)
+++ 00093 48725226 Fr 20.03.2009 08:14:24:876 EES: Port 2 Link UP
+++ 00094 48735325 Fr 20.03.2009 08:14:34:976 EES: Port 1 Link Down (extern)
+++ 00095 48735325 Fr 20.03.2009 08:14:34:976 EES: Ctrl: disable Port 1, now: P1..disc..EN100==conn==P2 (2d)
+++ 00096 48735326 Fr 20.03.2009 08:14:34:977 EES: Forw: Port 1 disable, now: 1-block-EN100-block-2 (12-->3)
```

Fig. 9-4 Detail from the system log

Statistics

The statistics show a detail from the information which is available for special purposes and concerns data transmission, including switches. Fig. 9-5 shows a detail. The number of faulty symbols is of particular importance, because it indicates a poor link quality. This value is incremented when switching on/off, or on a break of the link. The number must not vary during operation.

```
nGooseHit              =     0
nGooseMiss             =     0
Relative time          = 48841041
Module CPU load        =    12%
txPacketChan1/2        = 4133241/277
rxPacketChan1/2        = 24532/4157050
FilterSrcChan1/2       = 24532/24386
FilterDstChan1/2       = 24381/4157044
FilterCrcErrCntChan1/2 = 0/0
FilterLenErrCntChan1/2 = 0/0
FilterSymErrCntChan1/2 = 343/933
overflowExtCntChan1/2  = 0/0
overflowIntCntChan1/2  = 0/0
overflowIntTraCnt      = 0
OptLevelChan1/2        = 2384(weak)/2400(norm)
EPLD-Version           = 407/2070197H
```

Fig. 9-5 Detail from the statistics

Important information to be found on the Statistic page

The figures 9-6 and 9-7 show the complete statistics. Table 9-2 contains the most important values to interpret the statistics. Set points are only given if they are static. If they are not, the entry remains empty.

Table 9-2 Information values on the statistic page

Name	Set point	Description
RxFrames		Counter for telegrams received which are forwarded to module applications and the TCP/IP stack.
BD out of sequence	0	Counter for receive buffer overflows in the communications processor. This value must always be zero.
Miss		Counter for telegrams received that do not match the MAC address of the device.
Broadcast		Counter for broadcast telegrams received
Multicast		Counter for multicast telegrams registered
More than 0x5f0 Bytes		Counter for telegrams (1520 bytes) that are too long. Such telegrams are discarded.
Non Octett	0	Counter for the number of bits which cannot be divided by 8. If this value is not equal to zero, there may be problems on the transmission link. This can also be the case if the link is physically broken.
CRC Error	0	Counter for telegrams received with a CRC-check error. Indicates possible problems on the transmission link.
Overrun	0	Counter for receive buffer overflow. Indicates possible performance problems of the Ethernet controller.
Truncated	0	MAC-internal counter. Counter for reduced telegrams received (> 2 kb)
TxFrames		Counter of telegrams transmitted.
no transmit buffer	0	Incrementing can only happen if the collision or retransmission volume is very high.
FNS queue overflow	0	Counts broadcast telegrams which were not evaluated because of a processor overload. Activation usually due to circulating telegrams.
Frames Loss	0	Counts of discarded received telegrams; if more than 1000 such telegrams have arrived per second. Can only occur with circulating telegrams.
MaxRxBDs		Max. level of the receiving buffer.
RxLoopMax	0	Counter for receiving buffer overrun.
RxOverload	0	Counter for receiving overload. Receiving telegrams are lost.
TxDef	0	Counts the 'defers' when sending frames. An incrementation of the counter indicates that half duplex mode is set.
TxHB	0	Heartbeat counter
TxLC	0	Late Collision counter
TxRL	0	Counts violations of the retransmission limit

Table 9-2 Information values on the statistic page

Name	Set point	Description
TxRC	0	Counts retransmissions. Indicates collisions
TxUN	0	Counts 'Buffer underrun'
TxCSL	0	Counts 'Carrier sense lost'
MaxTxBD		Max. level of the transmitting buffer.
nGooseHit		Counts the GOOSE telegrams received
nGooseMiss		Counts the GOOSE telegrams which passed the multicast filter, but are not addressed to the device (e.g. by incorrect GOOSE-parameterization).
Relative time		Momentary value of the relative time counter. This is a 32 bit counter which is incremented once per millisecond. Starts at 120000 (is equal to appr. 49 days, after it reboot with 0).
Module CPU load		Efficiency CPU
txPacketChan1/2		Counts of data packages, which was sent by the port.
rxPacketChan1/2		Counts of all data packages, which was received by the port.
FilterSrcChan1/2		Counter of all received data packages, which doesn't agree with all received data packages of the source address with the own address.
FilterDstChan1/2		Counter of all received data packages, which doesn't agree with all received data packages of the destination address with the own address.
FilterCRCErrCnt Chan1/2	0	Counter of data packages with CRC error
FilterLenErrCnt Chan1/2	0	Counter of data packages, which are too long or too short. The acceptable length is 64 bytes to 1518 bytes.
FilterSymErrCnt Chan1/2	0	Counter of received symbol errors on the line (4b5b value is invalid). This monitoring is completed by the Phy.
overflowExtCnt Chan1/2	0	No counter for this value.
overflowIntCnt Chan1/2	0	No counter for this value.
overflowIntTraCnt	0	No counter for this value.
OptLevelChan1/2	> 2300	Level of the optical receiver in mV. Should not be less than 2300 when the cable is connected.
EPLD Version		Current EPLD version
Malloc Size		primary storage management
Data Size, Code Size, NORMAL pool, ENTRY pool, GOOSE pool, WEAK pool		primary storage management

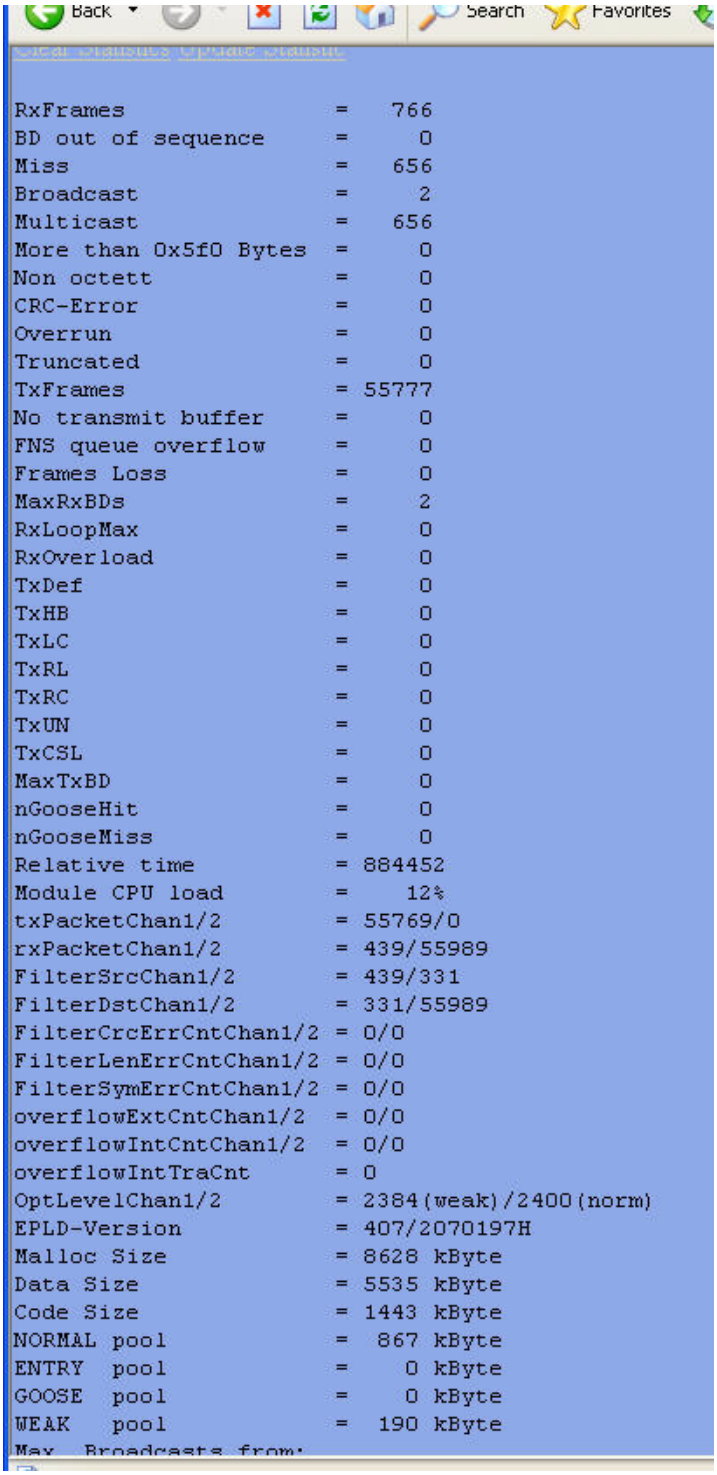


Fig. 9-6 Statistics, Part 1

The information shown in Fig. 9-7 are used for the analysis of broadcast telegram operations.

Max Broadcasts from

Lists the 4 most frequent broadcasts since the module was started. They are generated from *Broadcasts from* and contain the following information:

1. MAC address of the broadcast transmitter (MAC)
2. Quantity of this broadcast during the last 4 min (n)
3. Number of successive identical telegrams (GI)
4. Length of telegrams (Len)
5. Relative time (Rz)

Broadcasts from

Lists the current broadcasts in the running 4-minute interval. Each line contains 2 transmitters with the following:

1. MAC address of the broadcast transmitter (MAC)
2. Number of broadcasts since the interval started (n)
3. Number of successive identical telegrams (GI)
4. Length of telegrams (Len)

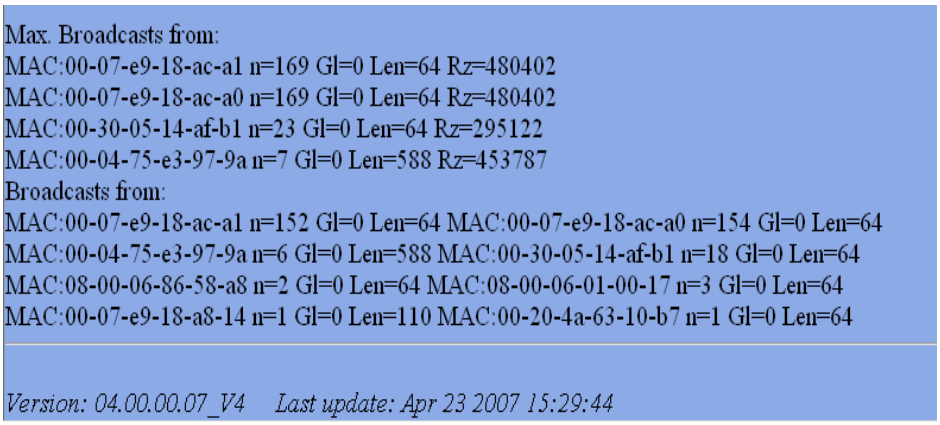


Fig. 9-7 Statistics, Part 2

The last line shows the current protocol software version and the time of generation.

PRP

The following figure shows PRP home page. The main values of the PRP home page are described in Table 9-3

.

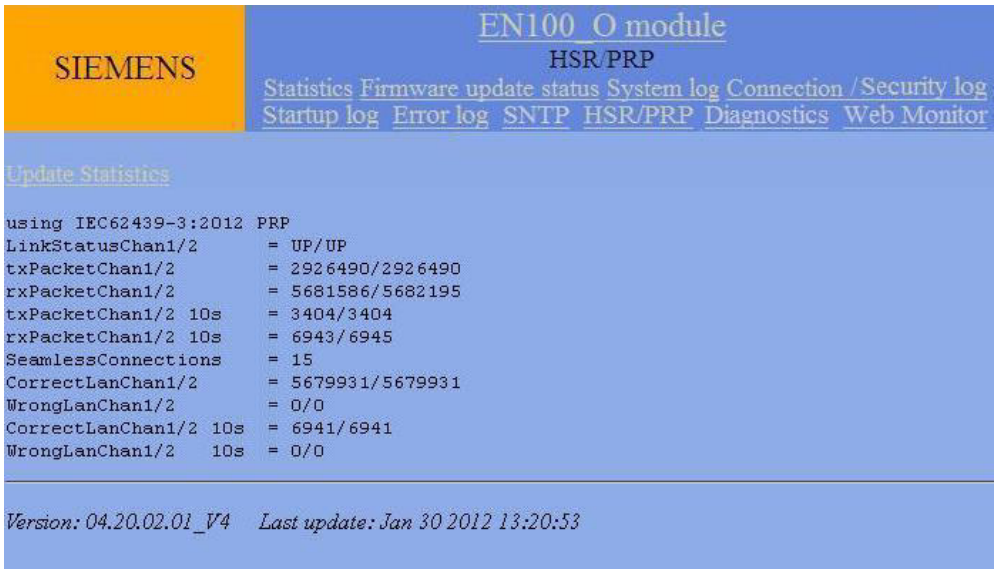


Fig. 9-8 PRP-Homepage

Table 9-3 Contents of PRP home page

Entry	Meaning
LinkStatusChan1/2	link status message
txPacketChan1/2	number of data packages sent from the port.
rxPacketChan1/2	number of data packages received by the port.
txPacketChan1/2 10s	number of data packages sent from the port within the last 10 seconds.
rxPacketChan1/2 10s	number of data packages received by the port within the last 10 seconds.
SeamlessConnections	number of modules, that have an active seamless connection. The value must be < 512.
CorrectLanChan1/2	number of PRP-packages, that have been received with a correct PRPLAN-ID.
WrongLanChan1/2	number of PRP-packages, that have been received with a wrong PRPLAN-ID. If this counter is unequal to 0 there may be a wiring error. A wiring error is present, if for example not all modules on the network have channel 1 connected to LAN A and channel 2 to LAN B.
CorrectLanChan1/2 10s	number of PRP-packages, that have been received with a correct PRPLAN-ID within the last 10 seconds.
WrongLanChan1/2 10s	number of PRP-packages, that have been received with a wrong PRPLAN-ID within the last 10 seconds.

HSR

The following figure shows the HSR homepage. The relevant values of the HSR homepage are described in Table 9-4.

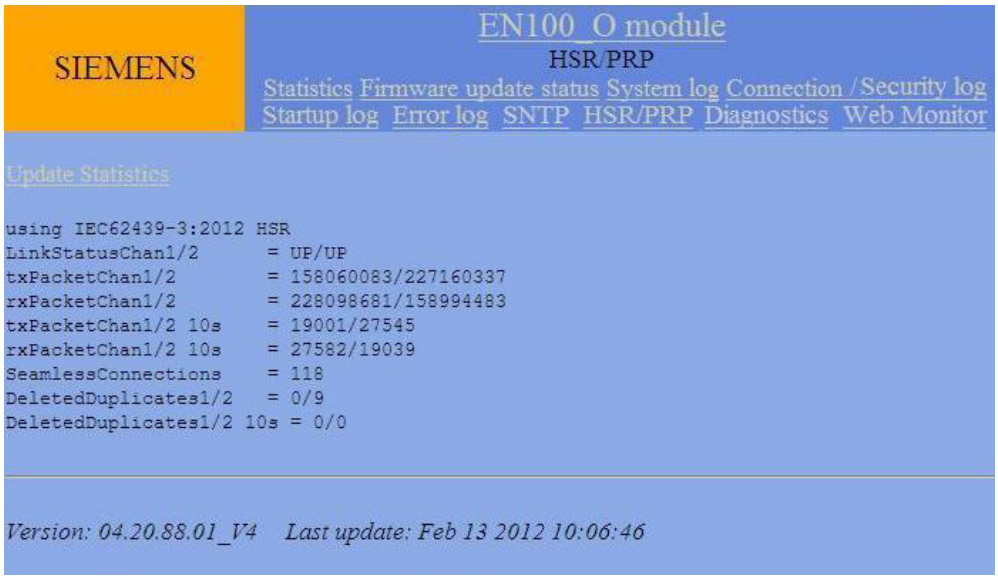


Fig. 9-9 HSR homepage

Table 9-4 Content of the HSR homepage

Entry	Meaning
LinkStatusChan1/2	Indication of link status
txPacketChan1/2	Number of data packages transmitted through the port.
rxPacketChan1/2	Number of data packages received through the port.
txPacketChan1/2 10s	Number of data packages transmitted through the port in the last 10 sec.
rxPacketChan1/2 10s	Number of data packages received through the port in the last 10 sec.
SeamlessConnections	Number of modules with an existing seamless connection. This value must be < 512.
DeletedDuplicates1/2	Number of packages that were removed from the ring via the HSR duplicate filter.
DeletedDuplicates1/2 10s	Number of packages that were removed from the ring via the HSR duplicate filter in the last 10 sec.

SNTP

The 1st lines includes:

- detail on the primary or currently active (primary or secondary) NTP server
- IP-address of the NTP server
- current time of the SIPROTEC device which receives the synchronization from the module. Within the first minutes after start-up of the device the time can differ from the time of the module for some milliseconds since the device tries to bring the current time into line jump free.

The 2nd and 3rd lines are not relevant.

The 5th and 6th line contains some variables in table form from the received NTP telegrams of the primary and secondary server as well as the time since the last received telegram and the time at the moment arising from the synchronization of the module.

The 2 tables for the max. 16 last received NTP telegrams and a short legend follow to this.

```
Clockmaster=Primary/172.16.0.249 device time: Mi 25.04.2007 09:54:01:510
leap:           0
stratum:        2
 no    peer       leap stratum poll/s prec.  delay   disp     refid       sync/s      actual time
*=1 172.016.000.249 0     1      64   -16    0,000  0,000  hPPS            0031 Mi 25.04.2007 09:54:01:510
 =2 172.016.000.250 0     1      64   -16    0,000  0,000  hPPS            0026 Mi 25.04.2007 09:54:01:510

table of last max. 16 registered sync-telegrams from server
Primary   peer=172.16.0.249 reach=0000007f/( 7) good=0000007f/( 7)
no offset delay dRx  dTx  diff (all in microseconds)
01= 00121   929 1054  424 00008 Mi 25.04.2007 09:53:30:504
02= 00126   957 1065  414 00013 Mi 25.04.2007 09:52:30:490
03= 00081   966 1091  418 -0032 Mi 25.04.2007 09:51:30:470
04= 00119   945 1082  440 00006 Mi 25.04.2007 09:50:30:408
05= 00128   946 1064  435 00015 Mi 25.04.2007 09:49:30:385
06= 00108   985 1075  432 -0005 Mi 25.04.2007 09:48:30:373
================================
avr 00113   954 1071  427

table of last max. 16 registered sync-telegrams from server
Secondary peer=172.16.0.250 reach=0000007f/( 7) good=0000007f/( 7)
no offset delay dRx  dTx  diff (all in microseconds)
01= 00113   982 1082  490 -0005 Mi 25.04.2007 09:53:35:505
02= 00116  1011 1084  493 -0002 Mi 25.04.2007 09:52:35:491
03= 00144  1009 1084  418 00026 Mi 25.04.2007 09:51:35:471
04= 00122   908 1100  446 00004 Mi 25.04.2007 09:50:35:413
05= 00124   917 1079  430 00006 Mi 25.04.2007 09:49:35:386
06= 00093   954 1104  446 -0025 Mi 25.04.2007 09:48:35:378
================================
avr 00118   963 1088  453

reach/good... 32-bit mask of last 32 reach/good quality minutes sync, oldest shift left
              and in (..) last number of continous reach/good quality minutes sync, up to 99 are displayed
offset..... difference of new time and crystal time, should less then 1000. If positiv, server is faster.
delay..... round trip delay (T4-T1)-(T3-T2), should less then 1000
dRx..... device internal receive delay, cpu load depending, should less then 2000
dTx..... device internal transmit delay, cpu load depending, should less then 2000
diff..... offset - avr(offset)
```

Fig. 9-10 SNTP

RSTP

The 1st and 2nd line show the current values of role and status of the ports 1 and 2.

The 4th line shows the detected neighbors of the module detected in the ring at port 1 and 2 over RSTP telegrams.

A listing of important RSTP information about the bridge and the 2 ports follows.

Topology Change Count

A counter is available which registers changes of the network topology. Increases are generated during the phase of commissioning typically. In a stable network the counter doesn't change. Ramp up counters are showing bad connections (e.g. loose connection). They show instability in the network and the operator has to analyze the situation and resolve the problems.

NOTE

Under "Actual" of the bridge information the RSTP parameters obtained by the root are listed. These parameters must be identical with them adjusted on the module.

The current transmit count usually is 0 durably. If it increases or already had reached a high value before (max > 20) then it indicates that the ring had changed down on the slower RSTP algorithm.

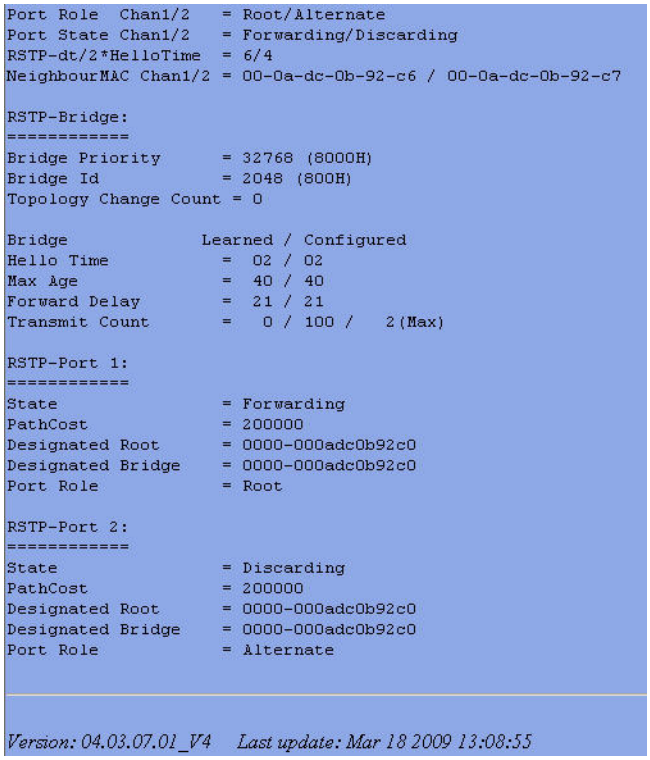


Fig. 9-11 RSTP

Technical Data

10

This chapter summarizes the technical data of the EN100-Module. Because the modules are installed in the SIPROTEC 4 devices, the data of each device as stated in the manuals apply in addition to the module's technical data given below.

Power consumption

The maximum power consumption of the module is 2.5 W.

The power supply comes directly from the CPU board of the SIPROTEC 4 device.

Connectors

The module with electrical interface is connected to the Ethernet network via RJ45 connectors.

Each module with an optical interface has 2 transceivers with a Duplex LC interface. The communication operates using light with a wavelength of 1310 nm. The module has been specified for use in the connection of multimode fiber-optic cables G50/ 125 µm or G62.5/125 µm.

Transmission rate

Both interfaces work with a transmission rate of 100 Mbps.

Switchover time

The switchover time to the second connection in the event of a link failing is no more than 10 ms. This is true for the operating mode “Line” if both ports of the module are connected to external switches.

Interface RJ45

For models with RJ45 interfaces, it is not possible to operate both interfaces at the same time if the module is being operated at the default setting “Line”. The link is automatically established on detecting the connection with a switch/partner. The second link remain unavailable until the active link is interrupted. The link on the second connection is then automatically resumed. The unavailable channel is monitored for link status. Both ports are active for electrical modules EN100-E+ where SIPROTEC 4 devices allow for the setting PRP.

LC/optical interface

The version with optical interface comprises a function that is comparable to the RJ45 interface ('Line' operating mode). The 'Switch' operating mode allows to build up redundant ring structures without using external switches[1]. In this operating mode both interfaces are active. Both interfaces are fully identical.

1. An external switch is required, however, for the connection/disconnection of information for displays etc. Pure GOOSE networks which have no connection with a control center do not require an external switch.

Optical transmitter

Wavelength: 1270 nm to 1380 nm, typically 1310 nm

Transmit output:

Fiber-optic	minimum	typical	maximum
50/125 µm, NA* = 0.2	-23.5 dBm	-20 dBm	-14 dBm
62.5/125 µm, NA = 0.275	-20 dBm	-17 dBm	-14 dBm

* Numerical aperture

Laser protection class

Laser class 1 is according to EN 60825-1 and EN 60825-2 with fiber type G50/125 µm and G62.5/125 µm.

Optical receiver

Receiver sensibility: -31 dBm_{avg} to -14 dBm_{avg}

Wavelength: 1270 nm to 1380 nm

Operating distance

max. 1.24 mil (2 km)

FO connector

Type: Duplex LC

Cable type for the optical interface

Multimode fiber-optic cables (G50/125 µm or G62,5/125 µm)

Cable type for the electrical interface

at least CAT5 S/FTP

Siemens recommends using a maximum cable length of 20 m.

Checklist for Commissioning

11

This chapter is a summary the commissioning procedure. Please note that some of the settings concern RSTP. If OSM is set as redundancy mode, no further settings are required.

11.1 Preliminary Steps

It is assumed for the following steps that all components are installed, and that the functioning of each component has been checked.

Set up address list

Siemens strongly recommends to set up first of all an address list of all components.

This list should include at least the device type, MLFB number, serial number, device firmware version, module firmware version, IP address, subnet mask, standard gateway, MAC address and IED name under IEC 61850 for each device. It is a good idea to include this information also for third-party devices such as switches etc. To this list must be added a description of the network topology. This topology description shows the interconnections between the devices.

The MAC addresses can be read out directly on the device display (menu-5-5-Enter). IP settings cannot be read until the devices have been initialized, i.e. the parameter sets loaded into the devices. For third-party devices, the information must be retrieved by the procedure described in the respective manual.

Once the list is complete, the IP addresses should be checked for duplicates. Duplicate MAC addresses are not likely to occur since they are assigned to the power system components as unique addresses.

Further hints for commissioning are available under http://www.siprotec.com.

Start up ring structure

The system is correctly set up and can now be switched on. Before power on, the ring containing the devices must be interrupted at one point. The power-on sequence is as follows:

1. Break ring structure at one point[1].
2. Energize switch. After power on, you should wait for about 20 seconds.
3. Energize devices. Siemens recommends to energize the devices in the order in which they are arranged in the ring. After power on, you should wait for each device to start up before the next device is energized[2].
4. Close the ring.[3]

Check the accessibility

After commissioning of the network, the accessibility of the components in the ring must be checked. After connecting a PC to an external switch, all IP addresses can be accessed using the PC browser. The IP address is entered directly.This connection allows to set the external switches. The settings of the modules integrated in the devices can be found on the respective device home page. The home page address always has the format

http://IP-address/home

One example of a setting is *http://172.16.52.55/home*

For commissioning and supervision supported tools, for example, Netview is available under http://www.siprotec.com.

---

1. This is strongly recommended in order to build up a stable ring structure.
2. Generally, neither the order of energizing nor the wait time are relevant. With RSTP, however, time-outs can cause a delay in building up the connection.
3. Interrupting the ring can speed up the startup; if this is not done, effects similar to those described in 3 can occur.

Please note that modules with optical interface can work both in line and in switch mode. Their home page is therefore different. The mode is set in DIGSI.

After these preliminary steps have been completed, you have an operational ring structure in which further settings can be made.

11.2 Settings of the Internal Switches

Activate RSTP	Activate the RSTP mode using DIGSI. This invokes a menu that contains all RSTP-relevant settings (see Fig. 3-7).
Set the bridge priority	The internal switches should be set to the lowest bridge priority (i.e. the highest priority number) in the system. The setting is the same for all switches. Siemens recommends a value of 32768.
Port Priority	This setting does not exist in internal switches.
Age Time	This value is set to 2 seconds.
Max Age Time	Here a value of 40 seconds is set. This ensures that even rings with up to 30 devices will work.
Transmit Count	Must be set to 100.
Set the edge ports	Setting not available.
Port Security	Setting not available.
Far Error Fault Indication	This feature is set by default, no setting by the user is required.

NOTE

Please note that the DIGSI basic settings may differ from the above. In any case, you have to make the settings recommended here.

11.3 Further Checks

Check the accessibility

After making all settings and loading the parameters, all components must be accessible through their IP address. This must be possible both with a closed and an interrupted ring.

If a device cannot be accessed, the reasons might be:

- A SIPROTEC 4 device connected by a line link to an external switch is not on,
- A SIPROTEC 4 device integrated into an optical ring is not on,
- A ring structure is broken at more than one point, so that some of the devices are not available. Break points may the devices that are not on, or broken links.

Check the home pages

The home page of the SIPROTEC 4 devices is available at address *http://IP address/home*. To be on the safe side, you should check with the statistic page there (see Fig. 9-6 and Table 9-2). The most important points to check are:

- *RSTP-Role Chan1/2 = Alternate/Root*
  If the SIPROTEC 4 devices are arranged in a ring, and the ring is closed and connected to the external switches which are also on, one device on the statistic page must always display the above text. If none of the devices in the ring does, the ring is physically broken.
- *FilterSymErrCntChan1/2 = 0/2753*
  If these 2 counters are incremented during stable operation of the device, and with neither of the 2 adjacent devices turned off, there is a poor FO connection. This can be due to an excessive attenuation by the coupling devices, or to a defective cable.
- *FNS queue overflow = 0*
  If this display is not equal zero, this suggests that there are circulating broadcast telegrams.
- *Frames Loss = 0*
  A value that is not zero indicates circulating multicast telegrams.

Appendix

12

This chapter deals with technical details which allow to better understand the function.

12.1 Function of RSTP

Tis chapter explains the behavior of the RSTP ring in the case of reconfigurations. In the figures, the port roles are shown in standard font and the states in italics.

12.1.1 Basic Concepts

RSTP

RSTP is the acronym for **R**apid **S**panning **T**ree **P**rotocol. This protocol is based on special multicast telegrams building up an information tree which prevents in structures of any kind the formation of rings, and thus of circulating telegrams which would make data transmission impossible. The roles and states of ports are of special importance: the configuration messages transmitted by each bridge contain priority vector information which allows to identify the *root* bridge, and this is the basis for calculating the path costs.

Port roles

The role of a port is variable, and based on the BPDUs (Bridge Protocol Data Unit). The system always compares the information of 2 BPDUs in order to decide which one is better. The port role is the specified accordingly.

***root* port**

The role of the *root* port is assigned to that port of a bridge[1] which provides the cheapest path to the *root* bridge. The path costs[2] are calculated on the basis of the priority vector contained in the BPDUs. In most cases, the *root* port will be that port of a bridge whose connection is located most closely to the *root* bridge. The r*oot* bridge itself is the one which transmits the best BPDUs as compared with the others. It is the only bridge which does not have a *root* port, but only *designated* ports and the highest priority.

***designated* port**

Every LAN segment needs a port who provides the best (cheapest) path to the root bridge.

All bridges in the segment listen to the BPDUs of the other bridges to find the best BPDU; in this way the *designated* port is determined. In the case of integrated switches, this port is always located opposite the *root* port (the internal port of the integrated switch is not relevant for network control). The *root* bridge is the only one that has no *root* port, since it is itself the root; it only has 2 *designated* ports. Its assignment in a stable RSTP network is shown in Fig. 12-1. This figure shows only the internal switches.

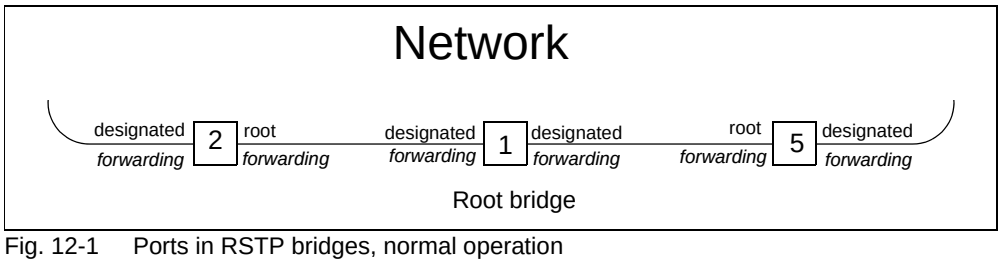


Fig. 12-1 Ports in RSTP bridges, normal operation

1. Bridges are used in the RSTP standard; they are equivalent here to the switches.
2. Path costs are the costs incurred by passing through a number of connections. They are usually correlated with the distance and the transmission rate.

***Alternate* port *backup* port**

This role is assigned to ports which in the case of an error can establish a connection via other power system components; this means that, unlike a *designated* port, they do not normally carry payload telegrams.

***Disabled* port**

This role is assigned to ports that are turned off. Such ports do not transmit payload data, and are not taken into account by RSTP.

The roles assigned to a port can change if components are removed or added, or if errors appear in the form of line interruptions.

Port states

Port states are *disabled*, *discarding*, *learning* and *forwarding*. In a stable network, the *root* ports and *designated* ports are in *forwarding* state; *alternate* ports, *disabled* ports and *backup* ports are in *discarding* state.

Status transitions

RSTP allows to reestablish connections very quickly, so that loss of telegrams is minimized. The transition of *root* and *designated* ports to the *forwarding* state is possible without a timer timeout. One *root* port can make this transition without receiving or transmitting telegrams from or to other bridges. A *designated* port can only change to the *forwarding* state after receiving a special agreement telegram sent by another bridge in the network. The delay is in this case independent of the network size; timers are only effective if RSTP telegrams are lost or transmission rates are exceeded.

Stable network

In a stable network, each bridge establishes a connection from the *root* port to the *designated* ports. These connections link all LAN with one another (it's spanning) and do not contain loops (is a tree). With integrated switches, however, there is always just one *root* and one *designated* port. LAN is in that case understood to be the part of the ring that is located downstream of that port; the structure is much simpler.

Changes of Spanning Tree information

Changes of the physical connection lead to a prompt distribution of spanning tree information in the network. Each bridge accepts this information from other bridges and LAN. Updated information is transmitted through the *designated* ports until they have reached the leaves of the spanning tree. The triggering and transmission of information ends when such information reaches designated ports which have already received the information via redundant paths.

Aging and discarding of configuration messages

In order to ensure that outdated information cannot circulate forever and prevent the distribution of new information, each configuration message is given a *message age* and a *maximum age.* The message age is incremented each time the message is received; when the maximum age is exceeded, the message is discarded and not forwarded any more. This also means that such messages have a limited range within the network.

Changes of a port state

As a result of changes on the Spanning Tree information, a *root* or *designated* port can be switched to the forwarding state. The details of port state switchover will not be discussed here; an in-depth description can be found in standard IEEE 802D-2004.

Switchover to forwarding

When 2 ports connect, as shown in Fig. 12-2, i.e. when the connection is reestablished, both ports take the state *designated* and the role *discarding*; this means that they discard payload telegrams but exchange RSTP BPDUs. When user 2 receives a BPDU from the *root* bridge through its port 1, it blocks immediately its port 2 working as root port[1] and authorizes port 1 for *forwarding*. The new state is shown in Fig. 12-3.

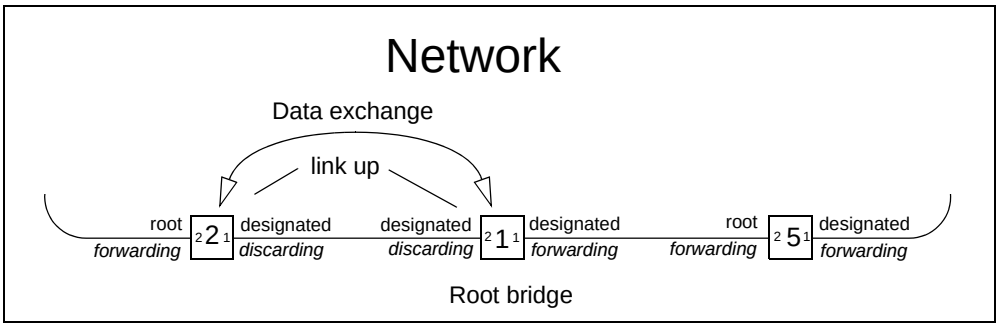


Fig. 12-2 RSTP, exchange of information

Port 1 of user 3 and port 2 of user 2 keep their roles but are now in *discarding* state. Data exchange continues, and the break point moves on rapidly in the network until a stationary state with an alternate port is reached. This procedure does not involve a timer, so that reconfiguration happens very quickly.

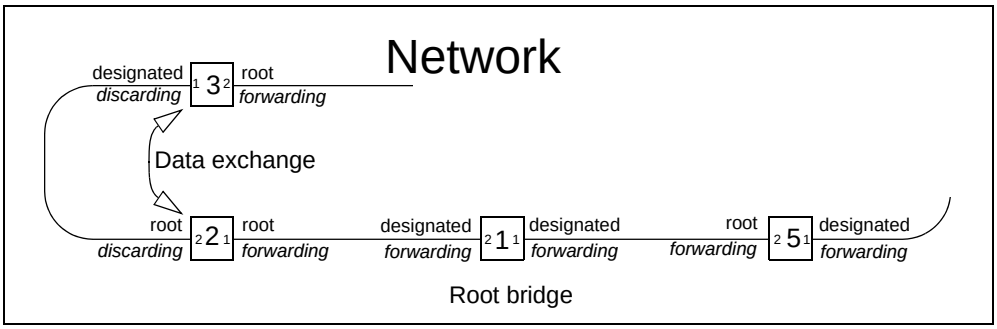


Fig. 12-3 RSTP, switchover to forwarding

Stationary state

In the stationary basic state (see Fig. 12-4), all devices are now connected to one another and to the switch; there is a physically closed ring with one logic break point.

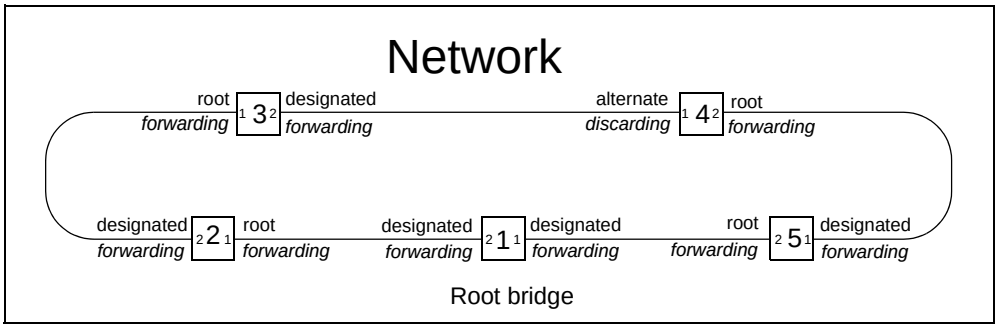


Fig. 12-4 RSTP network in stationary state

1. This is only true for non-edge ports, i.e. ports which are connected in a ring or segment and could form a ring if required. SIPROTEC 4 devices generally have only 2 non-edge ports arranged in a ring. The port of the device switch to the processor FEC is an edge port.

In terms of payload data, all ports are in *forwarding* state, i.e. they forward payload data. This is not true for the *alternate* port, which is in *discarding* state and cannot forward payload data telegrams. It constitutes the logic break point of the ring.

The root bridge is the switch with the highest priority (zero is the highest priority). The *alternate* port is usually located opposite of it.

The ring is controlled by RSTP telegrams, which can always be transmitted and received, regardless of the state. However, this does not apply to *Hello* telegrams, which can only be transmitted by *designated* ports.

Interruption at the *alternate* port

Fig. 12-5 shows the state between *alternate* and *designated* port immediately after an interruption during the stationary state shown in Fig. 12-4. The link status signals the interruption, and both ports take the *disabled* state, i.e. they do not forward any more messages.

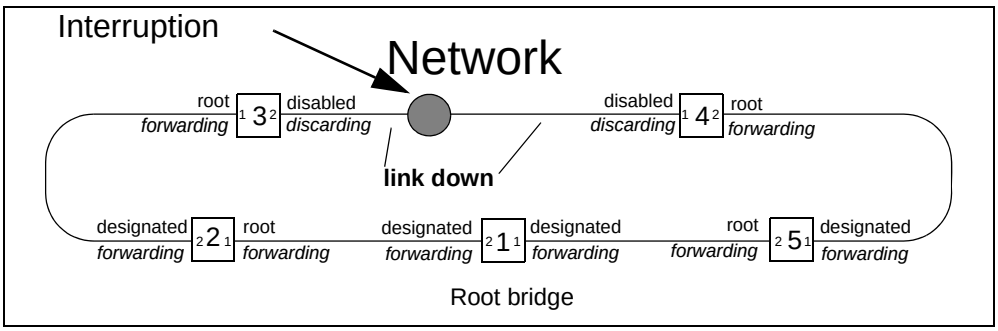


Fig. 12-5 RSTP ring, interruption at the alternate port

When the connection is reestablished, the system start again as shown in Fig. 12-2, but due to the spanning tree information the logic break point will not wander very far; the state shown in Fig. 12-6 will be reached very soon.

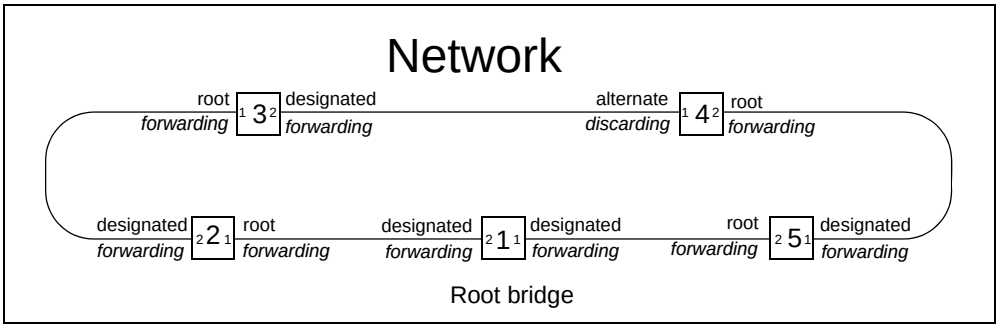


Fig. 12-6 RSTP network, stable again

12.2 System Versions vs. Functionality

Information on function extensions and error corrections with the different module firmware versions can be found in the Internet. There you can find, among other things, updated Readme files upon the release of further module firmware versions.

Glossary

BRCB	Buffered Report Control Block
CPU	Central Processing Unit
CFC	Continuous Function Chart
DC	Double Command
DHCP	Dynamic Host Configuration Protocol
DIGSI	Parameterization system for SIPROTEC 4 units
DI	Double-point Indication
SC	Single Command
SNMP	Simple Network Management Protocol
SNTP	Simple Network Time Protocol
SI	Single-point Indication
FEFI	Far End Fault Indication
GOOSE	Protocol of IEC 61850 for communication between bay devices
HSR	High-availability Seamless Redundancy
ICD	IED Configuration Description
IP	Internet Protocol
LAN	Local Area Network
MIB	Management Information Base, description file for SNMP
MMS	Manufacturing Message Specification

PICS	Protocol Implementation Conformance Statement
PRP	Parallel Redundancy Protocol
RSTP	Rapid Spanning Tree Protocol
SCD	Station Configuration Description
SI	System Interface
SNMP	Simple Network Management Protocol
SNTP	Simple Network Time Protocol
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
URCB	Unbuffered Record Control Block

Index