Modicon
MCSESR Redundancy Switch

Configuration User Guide
(Original Language)

11/2024

EIO0000005410.00

www.se.com

Legal Information

The information provided in this document contains general descriptions, technical characteristics and/or recommendations related to products/solutions.

This document is not intended as a substitute for a detailed study or operational and site-specific development or schematic plan. It is not to be used for determining suitability or reliability of the products/solutions for specific user applications. It is the duty of any such user to perform or have any professional expert of its choice (integrator, specifier or the like) perform the appropriate and comprehensive risk analysis, evaluation and testing of the products/solutions with respect to the relevant specific application or use thereof.

The Schneider Electric brand and any trademarks of Schneider Electric SE and its subsidiaries referred to in this document are the property of Schneider Electric SE or its subsidiaries. All other brands may be trademarks of their respective owner.

Schneider Electric does not grant any right or license for commercial use of the document or its content, except for a non-exclusive and personal license to consult it on an "as is" basis.

Schneider Electric reserves the right to make changes or updates with respect to or in the content of this document or the format thereof, at any time without notice.

To the extent permitted by applicable law, no responsibility or liability is assumed by Schneider Electric and its subsidiaries for any errors or omissions in the informational content of this document, as well as any non-intended use or misuse of the content thereof.

Table of Contents

Safety information

Important Information

Read these instructions carefully, and look at the equipment to become familiar with the device before trying to install, operate, service, or maintain it. The following special messages may appear throughout this documentation or on the equipment to warn of potential hazards or to call attention to information that clarifies or simplifies a procedure.

The addition of this symbol to a "Danger" or "Warning" safety label indicates that an electrical hazard exists, which will result in personal injury if the instructions are not followed.

This is the safety alert symbol. It is used to alert you to potential personal injury hazards. Obey all safety messages that follow this symbol to avoid possible injury or death.

⚠ DANGER

DANGER indicates an hazardous situation which, if not avoided, **will result in** death or serious injury.

⚠ WARNING

WARNING indicates a hazardous situation which, if not avoided, **could result in** death or serious injury.

⚠ CAUTION

CAUTION indicates a hazardous situation which, if not avoided, **could result in** minor or moderate injury.

NOTICE

NOTICE is used to address practices not related to physical injury.

Please Note

Electrical equipment should be installed, operated, serviced, and maintained only by qualified personnel. No responsibility is assumed by Schneider Electric for any consequences arising out of the use of this material.

A qualified person is one who has skills and knowledge related to the construction and operation of electrical equipment and its installation, and has received safety training to recognize and avoid the hazards involved.

Before You Begin

Do not use this product on machinery lacking effective point-of-operation guarding. Lack of effective point-of-operation guarding on a machine can result in serious injury to the operator of that machine.

⚠ WARNING

UNGUARDED EQUIPMENT

- Do not use this software and related automation equipment on equipment which does not have point-of-operation protection.
- Do not reach into machinery during operation.

Failure to follow these instructions can result in death, serious injury, or equipment damage.

This automation equipment and related software is used to control a variety of industrial processes. The type or model of automation equipment suitable for each application will vary depending on factors such as the control function required, degree of protection required, production methods, unusual conditions, government regulations, etc. In some applications, more than one processor may be required, as when backup redundancy is needed.

Only you, the user, machine builder or system integrator can be aware of all the conditions and factors present during setup, operation, and maintenance of the machine and, therefore, can determine the automation equipment and the related safeties and interlocks which can be properly used. When selecting automation and control equipment and related software for a particular application, you should refer to the applicable local and national standards and regulations. The National Safety Council's Accident Prevention Manual (nationally recognized in the United States of America) also provides much useful information.

In some applications, such as packaging machinery, additional operator protection such as point-of-operation guarding must be provided. This is necessary if the operator's hands and other parts of the body are free to enter the pinch points or other hazardous areas and serious injury can occur. Software products alone cannot protect an operator from injury. For this reason the software cannot be substituted for or take the place of point-of-operation protection.

Ensure that appropriate safeties and mechanical/electrical interlocks related to point-of-operation protection have been installed and are operational before placing the equipment into service. All interlocks and safeties related to point-of operation protection must be coordinated with the related automation equipment and software programming.

NOTE: Coordination of safeties and mechanical/electrical interlocks for point of-operation protection is outside the scope of the Function Block Library, System User Guide, or other implementation referenced in this documentation.

Start-up and Test

Before using electrical control and automation equipment for regular operation after installation, the system should be given a start-up test by qualified personnel to verify correct operation of the equipment. It is important that arrangements for such a check are made and that enough time is allowed to perform complete and satisfactory testing.

⚠ WARNING

EQUIPMENT OPERATION HAZARD

- Verify that all installation and set up procedures have been completed.
- Before operational tests are performed, remove all blocks or other temporary holding means used for shipment from all component devices.
- Remove tools, meters, and debris from equipment.

Failure to follow these instructions can result in death, serious injury, or equipment damage.

Follow all start-up tests recommended in the equipment documentation. Store all equipment documentation for future references.

Software testing must be done in both simulated and real environments.

Verify that the completed system is free from all short circuits and temporary grounds that are not installed according to local regulations (according to the National Electrical Code in the U.S.A, for instance). If high-potential voltage testing is necessary, follow recommendations in equipment documentation to prevent accidental equipment damage.

Before energizing equipment:
- Remove tools, meters, and debris from equipment.
- Close the equipment enclosure door.
- Remove all temporary grounds from incoming power lines.
- Perform all start-up tests recommended by the manufacturer.

Operation and Adjustments

The following precautions are from the NEMA Standards Publication ICS 7.1 - 1995: (In case of divergence or contradiction between any translation and the English original, the original text in the English language will prevail.)

- Regardless of the care exercised in the design and manufacture of equipment or in the selection and ratings of components, there are hazards that can be encountered if such equipment is improperly operated.
- It is sometimes possible to misadjust the equipment and thus produce unsatisfactory or unsafe operation. Always use the manufacturer’s instructions as a guide for functional adjustments. Personnel who have access to these adjustments should be familiar with the equipment manufacturer’s instructions and the machinery used with the electrical equipment.
- Only those operational adjustments required by the operator should be accessible to the operator. Access to other controls should be restricted to prevent unauthorized changes in operating characteristics.

About the Book

Document Scope

The Configuration User Guide contains the information you need to start operating the device. It takes you step by step from the first startup operation through to the basic settings for operation in your environment.

Validity Note

The characteristics of the products described in this document are intended to match the characteristics that are available on www.se.com. As part of our corporate strategy for constant improvement, we may revise the content over time to enhance clarity and accuracy. If you see a difference between the characteristics in this document and the characteristics on www.se.com, consider www.se.com to contain the latest information.

Related Documents

Document title	Reference
Modicon MCSESR Redundancy Switch Installation User Guide	EIO0000004961 (English)
	EIO0000005423 (French)
	EIO0000005424 (German)
	EIO0000005426 (Spanish)
	EIO0000005425 (Italian)
	EIO0000005427 (Chinese)
Modicon MCSESR Redundancy Switch Configuration User Guide	EIO0000005410 (English)
	EIO0000005413 (French)
	EIO0000005414 (German)
	EIO0000005416 (Spanish)
	EIO0000005415 (Italian)
	EIO0000005417 (Chinese)
Modicon MCSESR Redundancy Switch Graphic User Interface User Guide	EIO0000005411 (English)
	EIO0000005418 (French)
	EIO0000005419 (German)
	EIO0000005421 (Spanish)
	EIO0000005420 (Italian)
	EIO0000005422 (Chinese)
Modicon MCSESR Redundancy Switch Command Line Interface User Guide	EIO0000005474 (English)

You can download these technical publications and other technical information from our website at: www.se.com/ww/en/download

Product Related Information

⚠ DANGER

ELECTRIC SHOCK, EXPLOSION, OR ARC FLASH

- Disconnect all power from all equipment including connected devices prior to removing any covers or doors, or installing or removing any accessories, hardware, cables, or wires except under the specific conditions specified in the appropriate hardware guide for this equipment.
- Always use a properly rated voltage sensing device to confirm the power is off where and when indicated.
- Replace and secure all covers, accessories, hardware, cables, and wires and confirm that a proper ground connection exists before applying power to the equipment.
- Use only the specified voltage when operating this equipment and any associated products.

Failure to follow these instructions will result in death or serious injury.

This equipment has been designed to operate outside of any hazardous location. Only install this equipment in zones known to be free of a hazardous atmosphere.

⚠ DANGER

POTENTIAL FOR EXPLOSION

Install and use this equipment in non-hazardous locations only.

Failure to follow these instructions will result in death or serious injury.

⚠ WARNING

LOSS OF CONTROL

- Perform a Failure Mode and Effects Analysis (FMEA), or equivalent risk analysis, of your application, and apply preventive and detective controls before implementation.
- Provide a fall back state for undesired control events or sequences.
- Provide separate or redundant control paths wherever required.
- Supply appropriate parameters, particularly for limits.
- Review the implications of transmission delays and take actions to mitigate them.
- Review the implications of communication link interruptions and take actions to mitigate them.
- Provide independent paths for control functions (for example, emergency stop, over-limit conditions, and error conditions) according to your risk assessment, and applicable codes and regulations.
- Apply local accident prevention and safety regulations and guidelines.[1]
- Test each implementation of a system for proper operation before placing it into service.

Failure to follow these instructions can result in death, serious injury, or equipment damage.

1. For additional information, refer to NEMA ICS 1.1 (latest edition), Safety Guidelines for the Application, Installation, and Maintenance of Solid State Control and to NEMA ICS 7.1 (latest edition), Safety Standards for Construction and Guide for Selection, Installation and Operation of Adjustable-Speed Drive Systems or their equivalent governing your particular location.

⚠ WARNING

UNINTENDED EQUIPMENT OPERATION

- Only use software approved by Schneider Electric for use with this equipment.
- Update your application program every time you change the physical hardware configuration.

Failure to follow these instructions can result in death, serious injury, or equipment damage.

Terminology Derived from Standards

The technical terms, terminology, symbols and the corresponding descriptions in the information contained herein, or that appear in or on the products themselves, are generally derived from the terms or definitions of international standards.

In the area of functional safety systems, drives and general automation, this may include, but is not limited to, terms such as safety, safety function, safe state, fault, fault reset, malfunction, failure, error, error message, dangerous, etc.

Among others, these standards include:

Standard	Description
IEC 61131-2:2007	Programmable controllers, part 2: Equipment requirements and tests.
ISO 13849-1:2023	Safety of machinery: Safety related parts of control systems. General principles for design.
EN 61496-1:2013	Safety of machinery: Electro-sensitive protective equipment. Part 1: General requirements and tests.
ISO 12100:2010	Safety of machinery - General principles for design - Risk assessment and risk reduction
EN 60204-1:2006	Safety of machinery - Electrical equipment of machines - Part 1: General requirements
ISO 14119:2013	Safety of machinery - Interlocking devices associated with guards - Principles for design and selection
ISO 13850:2015	Safety of machinery - Emergency stop - Principles for design
IEC 62061:2021	Safety of machinery - Functional safety of safety-related electrical, electronic, and electronic programmable control systems
IEC 61508-1:2010	Functional safety of electrical/electronic/ programmable electronic safety related systems: General requirements.
IEC 61508-2:2010	Functional safety of electrical/electronic/ programmable electronic safety related systems: Requirements for electrical/electronic/ programmable electronic safety-related systems.
IEC 61508-3:2010	Functional safety of electrical/electronic/ programmable electronic safety related systems: Software requirements.
IEC 61784-3:2021	Industrial communication networks - Profiles - Part 3: Functional safety fieldbuses - General rules and profile definitions.
2006/42/EC	Machinery Directive
2014/30/EU	Electromagnetic Compatibility Directive
2014/35/EU	Low Voltage Directive

In addition, terms used in the present document may tangentially be used as they are derived from other standards such as:

Standard	Description
IEC 60034 series	Rotating electrical machines.
IEC 61800 series	Adjustable speed electrical power drive systems.
IEC 61158 series	Digital data communications for measurement and control – Fieldbus for use in industrial control systems.

Finally, the term zone of operation may be used in conjunction with the description of specific hazards, and is defined as it is for a hazard zone or danger zone in the Machinery Directive (2006/42/EC) and ISO 12100:2010.

NOTE: The aforementioned standards may or may not apply to the specific products cited in the present documentation. For more information concerning the individual standards applicable to the products described herein, see the characteristics tables for those product references.

Information on Non-Inclusive or Insensitive Terminology

As a responsible, inclusive company, Schneider Electric is constantly updating its communications and products that contain non-inclusive or insensitive terminology. However, despite these efforts, our content may still contain terms that are deemed inappropriate by some customers.

Trademarks

QR Code is a registered trademark of DENSO WAVE INCORPORATED in Japan and other countries.

Replacing a Device

The device provides the following plug-and-play solution for replacing a device with one of the same type.

- The new device loads the configuration profile of the replaced device from the external memory.
  See “Loading the Configuration Profile from the External Memory” on page 81.

Upon reboot, the new device gets the same IP settings that the replaced device had.

- To access the device management using HTTPS, the device uses a digital certificate. You have the option to import your own certificate to the device.
  See “HTTPS Certificate Management” on page 242.
- To access the device management using SSH, the device uses an RSA host key. You have the option to import your own host key in PEM format to the device.
  See “Loading your own Key onto the Device” on page 239.

User Interfaces

The device lets you specify the settings using the following user interfaces.

User Interface	Can be Reached through …	Prerequisite
GUI	Ethernet (In-Band)	Web browser
CLI	Ethernet (In-Band) Serial interface (Out-of-Band)	Terminal emulation software
System monitor	Serial interface (Out-of-Band)	Terminal emulation software

Graphical User Interface

System Requirements

To open the graphical user interface (GUI), you need the desktop version of a web browser with HTML5 support.

NOTE: Third-party software such as web browsers validate certificates based on criteria such as their expiration date and cryptographic parameters. Outdated certificates may cause issues due to invalid or outdated information. Example: An expired certificate or changed cryptographic parameters. To solve validation conflicts with third-party software, transfer your own up-to-date certificate onto the device or regenerate the certificate with the latest firmware.

Starting the GUI

The prerequisite for starting the GUI is that the IP parameters are configured in the device. See “Specifying the IP Parameters” on page 41.

Perform the following steps:

- ☐ Start your web browser.
- ☐ Type the IP address of the device in the address field of the web browser.
  Use the following form: `https://xxx.xxx.xxx.xxx`
  The web browser sets up the connection to the device and displays the login dialog.
- ☐ When you want to change the language of the GUI, click the appropriate link in the top right corner of the login dialog.
- ☐ Enter the user name.
- ☐ Enter the password.
- ☐ Click the *Login* button.
  The web browser displays the GUI.

Command Line Interface

The command line interface (CLI) enables you to use the functions of the device through a local or remote connection.

The CLI provides IT specialists with a familiar environment for configuring IT devices. As an experienced user or administrator, you have knowledge about the basics and about using Schneider Electric devices.

Preparing the Data Connection

Information for assembling and starting up your device can be found in the Installation User Guide.

☐ Connect the device with the network. The prerequisite for a successful data connection is the correct setting of the network parameters.

You can access the user interface of the CLI with, for example, the *PuTTY* freeware program.

☐ Install the *PuTTY* program on your computer.

Access to the CLI using Telnet

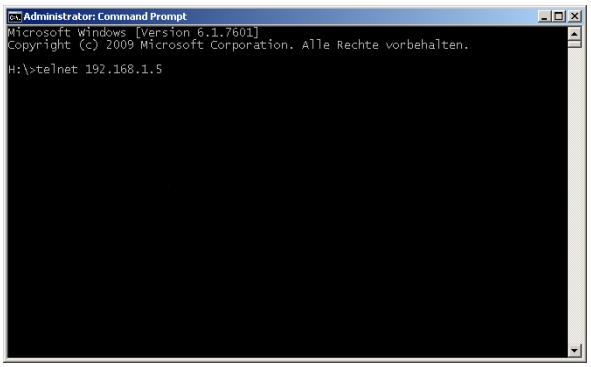
Telnet Connection using Windows

Telnet is only installed as standard in Windows versions earlier than Windows Vista.

Perform the following steps:

☐ Start the *Command Prompt* program on your computer.

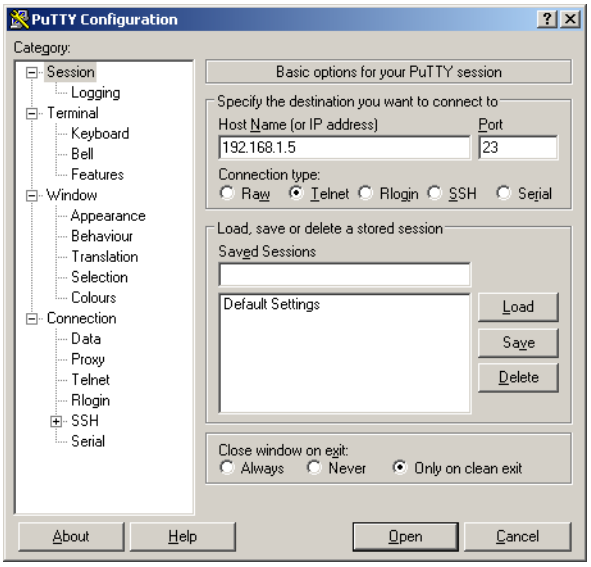
☐ Enter the `telnet <IP_address>` command.



Telnet Connection using PuTTY

Perform the following steps:

☐ Start the *PuTTY* program on your computer.



☐ In the *Host Name (or IP address)* field, enter the IP address of your device.
The IP address consists of four decimal numbers with values from `0` to `255`. The four decimal numbers are separated by points.

☐ To choose the connection type, select the *Telnet* radio button in the *Connection type* option list.

☐ Click the *Open* button to set up the data connection to your device.
The CLI appears on the screen with a window for entering the user name. The device allows up to 5 users to have access to the CLI at the same time.

NOTE: This device is a security-relevant product. Change the password during the first startup procedure.

Perform the following steps:

- ☐ Enter the user name.
  The default user name is `admin`.
- ☐ Press the **Enter** key.
- ☐ Enter the password.
  The default password is `private`.
- ☐ Press the **Enter** key.

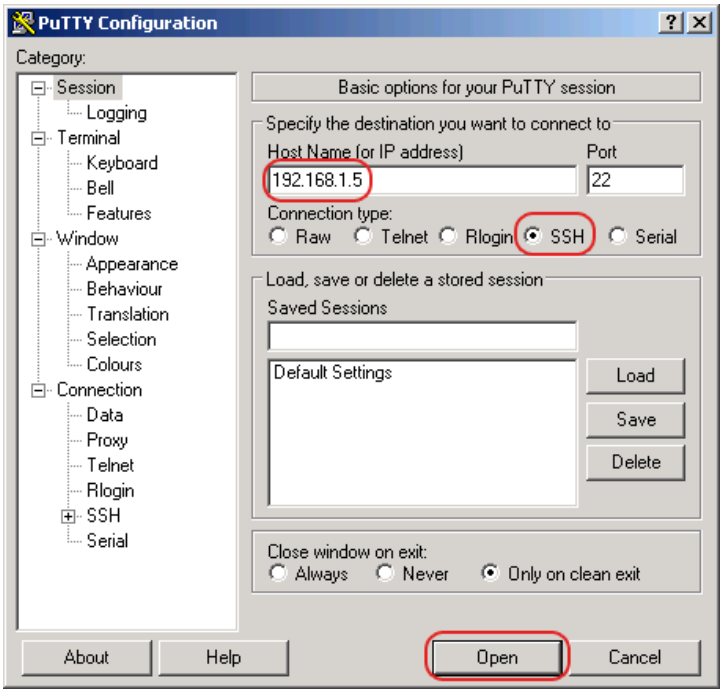
```
                Copyright (c) 2011-2024 Schneider Electric SE

                            All rights reserved

                          MCSESR Release 99.9.00

                        (Build date 2024-12-04 11:45)


                    System Name   :  MCSESR-646038d5e662
                    Management IP :  192.168.1.5
                    Subnet Mask   :  255.255.255.0
                    Base MAC      :  64:60:38:01:02:03
                    System Time   :  2024-12-06 14:56:47


NOTE: Enter '?' for Command Help.  Command help displays all options
      that are valid for the particular mode.
      For the syntax of a particular command form, please
      consult the documentation.

MCSESR>
```

Access to the CLI using SSH (Secure Shell)

In the following example, we use the *PuTTY* program. Another option to access your device using SSH is the OpenSSH Suite.

Perform the following steps:

☐ Start the *PuTTY* program on your computer.



☐ In the *Host Name (or IP address)* field you enter the IP address of your device. The IP address consists of 4 decimal numbers with values from `0` to `255`. The 4 decimal numbers are separated by points.

☐ To specify the connection type, select the *SSH* radio button in the *Connection type* option list.
After selecting and setting the required parameters, the device enables you to set up the data connection using SSH.

☐ Click the *Open* button to set up the data connection to your device.
Depending on the device and the time at which SSH was configured, setting up the connection takes up to a minute.
When you first log in, towards the end of the connection setup, the *PuTTY* program displays a message for you to verify the fingerprint of the key.

☐ Verify the fingerprint.
This helps to protect against unauthorized access.

☐ When the fingerprint matches the fingerprint of the device key, click the *Yes* button.
The device lets you display the finger prints of the device keys with the command `show ssh` or in the *Device Security > Management Access > Server* dialog, *SSH* tab.
The CLI appears on the screen with a window for entering the user name. The device allows up to 5 users to have access to the CLI at the same time.

☐ Enter the user name.
The default user name is `admin`.

☐ Press the **Enter** key.

☐ Enter the password.
The default password is `private`.

☐ Press the **Enter** key.

NOTE: This device is a security-relevant product. Change the password during the first startup procedure.

```
login as: admin
admin@192.168.1.5's password:


                Copyright (c) 2011-2024 Schneider Electric SE

                            All rights reserved

                          MCSESR Release 99.9.00

                        (Build date 2024-12-04 11:45)


                    System Name    :  MCSESR-646038d5e662
                    Management IP  :  192.168.1.5
                    Subnet Mask    :  255.255.255.0
                    Base MAC       :  64:60:38:01:02:03
                    System Time    :  2024-12-06 14:56:47


NOTE: Enter '?' for Command Help.  Command help displays all options
      that are valid for the particular mode.
      For the syntax of a particular command form, please
      consult the documentation.

MCSESR>
```

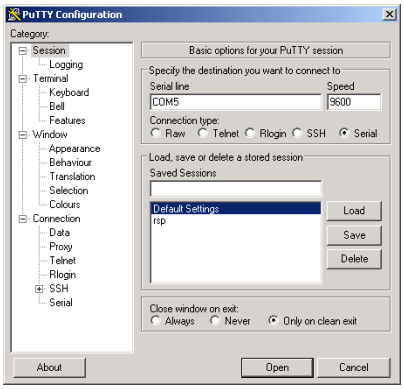
Access to the CLI using the Serial Interface

The serial interface is used to locally connect an external network management station (VT100 terminal or PC with terminal emulation). The interface lets you set up a data connection to the CLI and to the system monitor.

VT 100 Terminal Settings	
Speed	9600 bit/s
Data	8 bit
Stopbit	1 bit
Handshake	off
Parity	none

Perform the following steps:

- ☐ Connect the device to a terminal using the serial interface. Alternatively connect the device to a COM port of your PC using terminal emulation based on VT100 and press any key.
- ☐ Alternatively you set up the serial data connection to the device with the serial interface using the *PuTTY* program. Press the **Enter** key.



- ☐ Press any key on your terminal keyboard a number of times until the login screen indicates the CLI mode.
- ☐ Enter the user name.
  The default user name is `admin`.
- ☐ Press the **Enter** key.
- ☐ Enter the password.
  The default password is `private`.
- ☐ Press the **Enter** key.

NOTE: This device is a security-relevant product. Change the password during the first startup procedure.

```
                Copyright (c) 2011-2024 Schneider Electric SE

                           All rights reserved

                        MCSESR Release 99.9.00

                       (Build date 2024-12-04 11:45)


                    System Name    :  MCSESR-646038d5e662
                    Management IP  :  192.168.1.5
                    Subnet Mask    :  255.255.255.0
                    Base MAC       :  64:60:38:01:02:03
                    System Time    :  2024-12-06 14:56:47


NOTE: Enter '?' for Command Help.  Command help displays all options
      that are valid for the particular mode.
      For the syntax of a particular command form, please
      consult the documentation.

MCSESR>
```

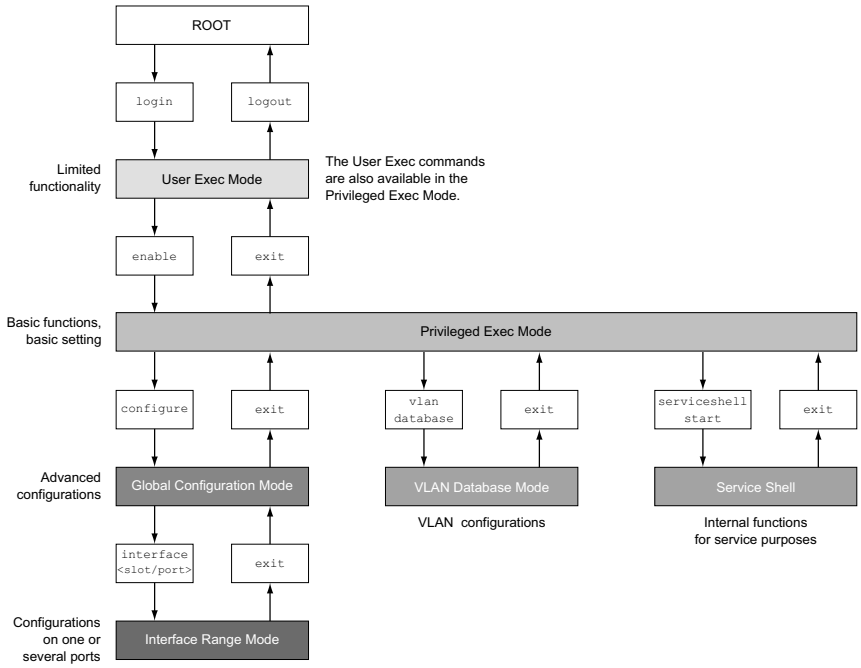
Mode-based Command Hierarchy

In the CLI, the commands are grouped in the related modes, according to the type of the command.

The commands available to you as a user depend on your privilege level (administrator, operator, guest, auditor). They also depend on the mode in which you are working. When you switch to a specific mode, the commands of the mode are available to you.

The User Exec mode commands are an exception. The CLI also enables you to execute these commands in the Privileged Exec mode.

The following figure displays the modes of the CLI.



The CLI supports, depending on the user level, the following modes:

- User Exec mode
  When you log in with the CLI, you enter the User Exec mode, which contains a limited range of commands.
  Command prompt: `(MCSESR) >`
- Privileged Exec mode
  To access the entire range of commands, enter the Privileged Exec mode. If you log in as a privileged user, you are able to enter the Privileged Exec mode in which you can also execute the User Exec mode commands.
  Command prompt: `(MCSESR) #`
- VLAN mode
  The VLAN mode contains VLAN-related commands.
  Command prompt: `(MCSESR) (VLAN)#`
- Service Shell
  The Service Shell is for service purposes only.
  Command prompt: `/mnt/fastpath #`

- Global Config mode
  The Global Config mode lets you perform modifications to the configuration. This mode groups general setup commands.
  Command prompt: `(MCSESR) (config)#`
- Interface Range mode
  The commands in the Interface Range mode affect a specific port, a selected group of multiple ports or all port of the device. The commands modify a value or switch a function on/off on one or more specific ports.
  - All physical ports in the device
    Command prompt: `(MCSESR) ((interface) all)#`
    Example: When you switch from the Global Config mode to the Interface Range mode, the command prompt changes as follows:
    ```
    (MCSESR) (config)#interface all
    (MCSESR) ((Interface)all)#
    ```
  - A single port on one interface
    Command prompt: `(MCSESR) (interface <slot/port>)#`
    Example: When you switch from the Global Config mode to the Interface Range mode, the command prompt changes as follows:
    ```
    (MCSESR) (config)#interface 2/1
    (MCSESR) (interface 2/1)#
    ```
  - A range of ports on one interface
    Command prompt: `(MCSESR) (interface <interface range> )#`
    Example: When you switch from the Global Config mode to the Interface Range mode, the command prompt changes as follows:
    ```
    (MCSESR) (config)#interface 1/2-1/4
    (MCSESR) ((Interface)1/2-1/4)#
    ```
  - A list of single ports
    Command prompt: `(MCSESR) (interface <interface list>)#`
    Example: When you switch from the Global Config mode to the Interface Range mode, the command prompt changes as follows:
    ```
    (MCSESR) (config)#interface 1/2,1/4,1/5
    (MCSESR) ((Interface)1/2,1/4,1/5)#
    ```
  - A list of port ranges and single ports
    Command prompt: `(MCSESR) (interface <complex range>)#`
    Example: When you switch from the Global Config mode to the Interface Range mode, the command prompt changes as follows:
    ```
    (MCSESR) (config)#interface 1/2-1/4,1/6-1/9
    (MCSESR) ((Interface)1/2-1/4,1/6-1/9)
    ```

The following table displays the command modes, the command prompts (input request characters) visible in the corresponding mode, and the option with which you quit this mode.

Command Mode	**Access Method**	**Quit or Start next Mode**

User Exec mode	First access level. Perform basic tasks and list system information.	To quit, enter `logout`:
		`(MCSESR) >logout`
		`Are you sure (Y/N) ?y`

Privileged Exec mode	From the User Exec mode, enter the command `enable`:
	`(MCSESR) >enable`
	`(MCSESR) #`
		To quit the Privileged Exec mode and return to the User Exec mode, enter `exit`:
		`(MCSESR) #exit`
		`(MCSESR) >`

Command Mode	Access Method	Quit or Start next Mode

VLAN mode	From the Privileged Exec mode, enter the command `vlan database`:
	`(MCSESR) #vlan database`
	`(MCSESR) (Vlan)#`
		To end the VLAN mode and return to the Privileged Exec mode, enter `exit` or press **Ctrl** + **Z**.
		`(MCSESR) (Vlan)#exit`
		`(MCSESR) #`

Global Config mode	From the Privileged Exec mode, you enter the command `configure`:
	`(MCSESR) #configure`
	`(MCSESR) (config)#`
	From the User Exec mode, you enter the command `enable`, and then in Privileged Exec mode, enter the command `Configure`:
	`(MCSESR) >enable`
	`(MCSESR) #configure`
	`(MCSESR) (config)#`
		To quit the Global Config mode and return to the Privileged Exec mode, enter `exit`:
		`(MCSESR) (config)#exit`
		`(MCSESR) #`
		To then quit the Privileged Exec mode and return to the User Exec mode, enter `exit` again:
		`(MCSESR) #exit`
		`(MCSESR) >`

Interface Range mode	From the Global Config mode you enter the command `interface {all|<slot/port>|<interface range>|<interface list>|<complex range>}`.
	`(MCSESR) (config)#interface <slot/port>`
	`(MCSESR) (interface slot/port)#`
		To quit the Interface Range mode and return to the Global Config mode, enter `exit`. To return to the Privileged Exec mode, you press **Ctrl** + **Z**.
		`(MCSESR) (interface slot/port)#exit`
		`(MCSESR) #`

When you enter a question mark (?) after the prompt, the CLI displays a list of the available commands and a short description of the commands.

```
(MCSESR)>
  cli               Set the CLI preferences.
  enable            Turn on privileged commands.
  help              Display help for various special keys.
  history           Show a list of previously run commands.
  logout            Exit this session.
  ping              Send ICMP echo packets to a specified IP address.
  show              Display device options and settings.
  telnet            Establish a telnet connection to a remote host.

(MCSESR)>
```

Executing the Commands

Syntax Analysis

When you log in with the CLI, you enter the User Exec mode. The CLI displays the prompt `(MCSESR)>` on the screen.

When you enter a command and press the **Enter** key, the CLI starts the syntax analysis. The CLI searches the command tree for the desired command.

When the command is outside the CLI command range, a message informs you of the detected error.

Example:

You want to execute the `show system info` command, but enter `info` without `f` and press the **Enter** key.

The CLI then displays a message:

```
(MCSESR)>show system ino

Error: Invalid command 'ino'
```

Command Tree

The commands in the CLI are organized in a tree structure. The commands, and where applicable the related parameters, branch down until the command is completely defined and therefore executable. The CLI verifies the input. When you entered the command and the parameters correctly and completely, execute the command with the **Enter** key.

After you entered the command and the required parameters, the other parameters entered are treated as optional parameters. When one of the parameters is undefined, the CLI displays a syntax message.

The command tree branches for the required parameters until the required parameters have reached the last branch in the structure.

With optional parameters, the command tree branches until the required parameters and the optional parameters have reached the last branch in the structure.

Structure of a Command

This section describes the syntax, conventions and terminology, and uses examples to represent them.

Format of Commands

Most of the commands include parameters.

When the command parameter is missing, the CLI informs you about the detection of an incorrect command syntax.

This manual displays the commands and parameters in the `Courier` font.

Parameters

The sequence of the parameters is relevant for the correct syntax of a command.

Parameters are required values, optional values, selections, or a combination of these things. The representation indicates the type of the parameter.

`<command>`	Commands in pointed brackets (`<>`) are obligatory.
`[command]`	Commands in square brackets (`[]`) are optional.
`<parameter>`	Parameters in pointed brackets (`<>`) are obligatory.
`[parameter]`	Parameters in square brackets (`[]`) are optional.
`...`	An ellipsis after an element indicates that you can repeat the element.
`[Choice1 | Choice2]`	A vertical line enclosed in brackets indicates a selection option. Select one value. Elements separated by a vertical line and enclosed in square brackets indicate an optional selection (Option1 or Option2 or no selection).
`{list}`	Curved brackets (`{}`) indicate that a parameter is to be selected from a list of options.
`{Choice1 | Choice2}`	Elements separated by a vertical line and enclosed in curved brackets (`{}`) indicate an obligatory selection option (option1 or option2).
`[param1 {Choice1 | Choice2}]`	Displays an optional parameter that contains an obligatory selection.
`<a.b.c.d>`	Lower case letters are wild cards. Enter parameters with the notation a.b.c.d with decimal points (for example IP addresses)
`<cr>`	Press the **Enter** key to create a line break (carriage return).

The following list displays the possible parameter values within the CLI:

Value	Description
IP address	This parameter represents a valid IPv4 address. The address consists of 4 decimal numbers with values from 0 to 255. The 4 decimal numbers are separated by a decimal point. The IP address `0.0.0.0` is a valid entry.
MAC address	This parameter represents a valid MAC address. The address consists of 6 hexadecimal numbers with values from 00 to FF. The numbers are separated by a colon, for example, `00:F6:29:B2:81:40`.
string	User-defined text with a length in the specified range, for example a maximum of 32 characters.
character string	Use double quotation marks to indicate a character string, for example `"System name with space character"`.
number	Whole integer in the specified range, for example `0..999999`.
date	Date in format `YYYY-MM-DD`.
time	Time in format `HH:MM:SS`.

Network Addresses

Network addresses are a requirement for establishing a data connection to a remote work station, a server, or another network. You distinguish between IP addresses and MAC addresses.

The IP address is an address allocated by the network administrator. The IP address is unique in one network area.

The MAC addresses are assigned by the hardware manufacturer.

The following table displays the representation and the range of the address types:

Address Type	Format	Range	Example
IP Address	nnn.nnn.nnn.nnn	nnn: 0 to 255 (decimal)	192.168.11.110
MAC Address	mm:mm:mm:mm:mm:mm	mm: 00 to ff (hexadecimal number pairs)	A7:C9:89:DD:A9:B3

Strings

A string is indicated by quotation marks. For example, `"System name with space character"`. Space characters are not valid user-defined strings. Enter a space character in a parameter between quotation marks.

Example:

```
*(MCSESR)#cli prompt Device name
Error: Invalid command 'name'

*(MCSESR)#cli prompt 'Device name'

*(Device name)#
```

Examples of Commands

Example 1: Clear Arp-table-switch

Command for clearing the ARP table of the management agent (cache).

`clear arp-table-switch` is the command name. The command is executable without any other parameters by pressing the **Enter** key.

Example 2: Radius Server Timeout

Command to configure the RADIUS server timeout value.

```
(MCSESR) (config)#radius server timeout
 <1..30>              Timeout in seconds (default: 5).
```

`radius server timeout` is the command name.

The parameter is required. The value range is `1..30`.

Example 3: Radius Server auth Modify <1..8>

Command to set the parameters for RADIUS authentication server 1.

```
(MCSESR) (config)#radius server auth modify 1
 [name]               RADIUS authentication server name.
 [port]               RADIUS authentication server port.
                      (default: 1812).
 [msgauth]            Enable or disable the message authenticator
                      attribute for this server.
 [primary]            Configure the primary RADIUS server.
 [status]             Enable or disable a RADIUS authentication
                      server entry.
 [secret]             Configure the shared secret for the RADIUS
                      authentication server.
 [encrypted]          Configure the encrypted shared secret.
  <cr>                Press Enter to execute the command.
```

`radius server auth modify` is the command name.

The parameter `<1..8>` (RADIUS server index) is required. The value range is `1..8` (integer).

The parameters `[name]`, `[port]`, `[msgauth]`, `[primary]`, `[status]`, `[secret]` and `[encrypted]` are optional.

Input Prompt

Command Mode

With the input prompt, the CLI displays which of the three modes you are in:

- `(MCSESR) >`
  User Exec mode
- `(MCSESR) #`
  Privileged Exec mode
- `(MCSESR) (config)#`
  Global Config mode
- `(MCSESR) (Vlan)#`
  VLAN Database mode
- `(MCSESR) ((Interface)all)#`
  Interface Range mode / All ports of the device
- `(MCSESR) ((Interface)2/1)#`
  Interface Range mode / A single port on one interface
- `(MCSESR) ((Interface)1/2-1/4)#`
  Interface Range mode / A range of ports on one interface
- `(MCSESR) ((Interface)1/2,1/4,1/5)#`
  Interface Range mode / A list of single ports
- `(MCSESR) ((Interface)1/1-1/2,1/4-1/6)#`
  Interface Range mode / A list of port ranges and single ports

Asterisk, Pound Sign and Exclamation Mark

- Asterisk `*`
  An asterisk `*` in the first or second position of the input prompt means that the settings in the volatile memory and the settings in the non-volatile memory are different. In your configuration, the device has detected modifications which have not been saved.
  `*(MCSESR)>`
- Pound sign `#`
  A pound sign `#` at the beginning of the input prompt means that the boot parameters and the parameters during the boot phase are different.
  `*#(MCSESR)>`
- Exclamation mark `!`
  An exclamation mark `!` at the beginning of the input prompt means that the password for the `admin` account corresponds with the default setting.
  `!(MCSESR)>`

Wildcards

The device lets you change the command line prompt.

The CLI supports the following wildcards:

Wildcard	Description
`%d`	System date
`%t`	System time

Wildcard	Description
`%i`	IP address of the device
`%m`	MAC address of the device
`%p`	Product name of the device

```
!(MCSESR)>enable

!(MCSESR)#cli prompt %i

!192.168.1.5#cli prompt (MCSESR)%d

!*(MCSESR)2024-12-06#cli prompt (MCSESR)%d%t

!*(MCSESR)2024-12-06 14:56:47#cli prompt %m

!*AA:BB:CC:DD:EE:FF#
```

Key Combinations

The following key combinations make it easier for you to work with the CLI:

Key Combination	Description
Ctrl + **H**, **Backspace**	Delete previous character
Ctrl + **A**	Go to beginning of line
Ctrl + **E**	Go to end of line
Ctrl + **F**	Go forward one character
Ctrl + **B**	Go backward one character
Ctrl + **D**	Delete current character
Ctrl + **U**, **X**	Delete to beginning of line
Ctrl + **K**	Delete to end of line
Ctrl + **W**	Delete previous word
Ctrl + **P**	Go to previous line in history buffer
Ctrl + **R**	Rewrite or paste the line
Ctrl + **N**	Go to next line in history buffer
Ctrl + **Z**	Return to root command prompt
Ctrl + **G**	Aborts running tcpdump session
Tab, **Spacebar**	Command line completion
`Exit`	Go to next lower command prompt
?	List choices

The Help command displays the possible key combinations in CLI on the screen:

```
(MCSESR) #help

HELP:
Special keys:

  Ctrl-H, BkSp delete previous character
  Ctrl-A  .... go to beginning of line
  Ctrl-E  .... go to end of line
  Ctrl-F  .... go forward one character
  Ctrl-B  .... go backward one character
  Ctrl-D  .... delete current character
  Ctrl-U, X .. delete to beginning of line
  Ctrl-K  .... delete to end of line
  Ctrl-W  .... delete previous word
  Ctrl-P  .... go to previous line in history buffer
  Ctrl-R  .... rewrites or pastes the line
  Ctrl-N  .... go to next line in history buffer
  Ctrl-Z  .... return to root command prompt
  Ctrl-G  .... aborts running tcpdump session
  Tab, <SPACE> command-line completion
  Exit    .... go to next lower command prompt
  ?       .... list choices

(MCSESR) #
```

Data Entry Elements

Command Completion

To simplify typing commands, the CLI lets you use command completion (Tab Completion). You can abbreviate key words.

- Type the beginning of a keyword. When the characters entered identify a keyword, the CLI completes the keyword after you press **Tab** or the **Spacebar**. When there is more than one option for completion, enter the letter or the letters necessary for uniquely identifying the keyword. Press the **Tab** or the **Spacebar** again. After that, the system completes the command or parameter.
- When you make a non-unique entry and press **Tab** or the **Spacebar** twice, the CLI provides you with a list of options.
- On a non-unique entry and pressing **Tab** or the **Spacebar**, the CLI completes the command up to the end of the uniqueness. When several commands exist and you press **Tab** or the **Spacebar** again, the CLI provides you with a list of options.
  Example:

```
(MCSESR) (Config)#lo
(MCSESR) (Config)#log
logging logout
```

  When you enter `lo` and **Tab** or the **Spacebar**, the CLI completes the command up to the end of the uniqueness to `log`.
  When you press **Tab** or the **Spacebar** again, the CLI provides you with a list of options (`logging logout`).

Possible Commands/Parameters

You can obtain a list of the commands or the possible parameters by entering `help` or `?`, for example by entering `(MCSESR) >show ?`

When you enter the command displayed, you get a list of the parameters available for the command `show`.

When you enter the command without space character in front of the question mark, the device displays the help text for the command itself:

```
!*#(MCSESR)(Config)#show?

   show          Display device options and settings.
```

Use Cases

Saving the Configuration

To help ensure that your password settings and other configuration changes are kept after the device is reset or after an interruption of the voltage supply, save the configuration. To do this, perform the following steps:

☐ Enter `enable` to switch to the Privileged Exec mode.

☐ Enter the following command:

`save [profile]`

☐ Execute the command by pressing the **Enter** key.

Syntax of the `radius server auth add` Command

Use this command to add a RADIUS authentication server.

- Mode: `Global Config` mode
- Privilege Level: Administrator
- Format: `radius server auth add <1..8> ip <a.b.c.d> [name <string>] [port <1..65535>]`
  - `[name]`: RADIUS authentication server name.
  - `[port]`: RADIUS authentication server port (default value: `1813`).

Parameter	Meaning	Possible Values
`<1..8>`	RADIUS server index.	`1..8`
`<a.b.c.d>`	RADIUS accounting server IP address.	IP address
`<string>`	Enter a user-defined text, max. 32 characters.	
`<1..65535>`	Enter port number between 1 and 65535.	`1..65535`

Mode and Privilege Level:

- The prerequisite for executing the command: You are in the Global Config mode. See “Mode-based Command Hierarchy” on page 25.
- The prerequisite for executing the command: You have the Administrator access role.

Syntax of commands and parameters: See “Structure of a Command” on page 28.

Examples for executable commands:

- `radius server auth add 1 ip 192.168.30.40`
- `radius server auth add 2 ip 192.168.40.50 name radiusserver2`
- `radius server auth add 3 ip 192.168.50.60 port 1813`
- `radius server auth add 4 ip 192.168.60.70 name radiusserver4 port 1814`

Service Shell

The Service Shell is for service purposes only.

The Service Shell allows access to internal functions of the device. When you need assistance with your device, the service personnel use the Service Shell to monitor internal conditions (for example, the switch or CPU registers).

NOTICE
INOPERABLE EQUIPMENT Do not execute internal functions such as deleting the non-volatile memory (*NVM*) without service technician instructions. **Failure to follow these instructions can result in equipment damage.**

Start the Service Shell

The prerequisite is that you are in User Exec mode: `(MCSESR) >`

Perform the following steps:

- ☐ Enter `enable` and press the **Enter** key.
  To reduce the effort when typing:
  - Enter `e` and press the **Tab** key.
- ☐ Enter `serviceshell start` and press the **Enter** key.
  To reduce the effort when typing:
  - Enter `ser` and press the **Tab** key.
  - Enter `s` and press the **Tab** key.

```
!MCSESR >enable

!*MCSESR #serviceshell start
 WARNING! The service shell offers advanced diagnostics and functions.
 Proceed only when instructed by a service technician.

 You can return to the previous mode using the 'exit' command.

 BusyBox v1.31.0 (2024-12-06 14:56:47 UTC) built-in shell (ash)
 Enter 'help' for a list of built-in commands.

!/mnt/fastpath #
```

Working with the Service Shell

When the Service Shell is active, the timeout of the CLI is inactive. To help prevent configuration inconsistencies, end the Service Shell before any other user starts transferring a new configuration to the device.

Display the Service Shell Commands

The prerequisite is that you already started the Service Shell.

Perform the following steps:
☐ Enter `help` and press the **Enter** key.

```
/mnt/fastpath # help
Built-in commands:
------------------
        . : [ [[ alias bg break cd chdir command continue echo eval exec
        exit export false fg getopts hash help history jobs kill let
        local pwd read readonly return set shift source test times trap
        true type ulimit umask unalias unset wait
/mnt/fastpath #
```

End the Service Shell

Perform the following steps:
☐ Enter `exit` and press the **Enter** key.

Deactivate the Service Shell Permanently in the Device

When you deactivate the Service Shell, you can continue configuring the device. However, you limit the service personnel's possibilities to perform system diagnostics. The service technician will no longer be able to access internal functions of your device.

The deactivation is irreversible. The Service Shell remains permanently deactivated. **In order to reactivate the Service Shell, the device requires disassembly by the manufacturer.**

The prerequisites are:
- The Service Shell is not started.
- You are in User Exec mode: `(MCSESR) >`

Perform the following steps:
- ☐ Enter `enable` and press the **Enter** key.
  To reduce the effort when typing:
  - Enter `e` and press the **Tab** key.
- ☐ Enter `serviceshell deactivate` and press the **Enter** key.
  To reduce the effort when typing:
  - Enter `ser` and press the **Tab** key.
  - Enter `dea` and press the **Tab** key.
- ☐ **This step is irreversible.**
  Press the **Y** key.

```
!MCSESR >enable

!*MCSESR #serviceshell deactivate
Notice: If you continue, then the Service Shell is permanently deactivated.
This step is irreversible!
For details, refer to the Configuration Manual.
Are you sure (Y/N) ?
```

System Monitor

The system monitor lets you set basic operating parameters before starting the operating system.

Functional Scope

In the system monitor, carry out the following tasks, for example:
- ▶ Manage the operating system and verify the software image.
- ▶ Update the operating system.
- ▶ Start the operating system.
- ▶ Delete configuration profiles, resetting the device to the factory defaults.
- ▶ Verify boot code information.

Starting the System Monitor

Prerequisites:
- ▶ Terminal cable for connecting the device to your PC (available as an optional accessory).
- ▶ PC with VT100 terminal emulation (such as the *PuTTY* program) or serial terminal

Perform the following steps:

- ☐ Use the terminal cable to connect the serial interface of the device with the COM port of the PC.
- ☐ Start the VT100 terminal emulation on the PC.
- ☐ Specify the following transmission parameters:

VT 100 Terminal Settings	
Speed	9600 bit/s
Data	8 bit
Stopbit	1 bit
Handshake	off
Parity	none

- ☐ Set up a connection to the device.
- ☐ Turn on the device. When the device is already on, reboot it.
  The screen displays the following message after rebooting:
  ```
  Press <1> to enter System Monitor 1.
  ```
- ☐ Press the **1** key within three seconds.
  The device starts the system monitor. The screen displays the following view:

```
System Monitor 1
(Selected OS: ...-99.9_p5-internal-999 (2024-12-04 11:45))

1  Manage operating system
2  Update operating system
3  Start selected operating system
4  Manage configurations
5  Show boot code information
q  End (reset and reboot)









sysMon1>
```

- ☐ Select a menu item by entering the number.
- ☐ To leave a submenu and return to the main menu of System Monitor 1, press the **ESC** key.

Specifying the IP Parameters

When you install the device for the first time, enter the IP parameters.

The device provides the following options for entering the IP parameters during the first installation:

- Entry using the CLI.
  When you preconfigure your device outside its operating environment, or restore the network access (In-Band) to the device, choose this Out-of-Band method.
- Entry using the Ethernet Switch Configurator protocol.
  When you have a previously installed network device or you have another Ethernet connection between your PC and the device, choose this In-Band method.
- Configuration using the external memory.
  When you are replacing a device with one device of the same type and have already saved the configuration in the external memory, choose this method.
- Using BOOTP.
  To configure the installed device using BOOTP, choose this In-Band method. You need a BOOTP server for this method. The BOOTP server assigns the configuration data to the device using its MAC address. The DHCP mode is the default mode for the configuration data reference.
- Configuration using DHCP.
  To configure the installed device using DHCP, choose this In-Band method. You need a DHCP server for this method. The DHCP server assigns the configuration data to the device using its MAC address or its system name.
- Configuration using the graphical user interface (GUI).
  When the device already has an IP address and is reachable using the network, the GUI provides you with another option for configuring the IP parameters.

IP Parameter Basics

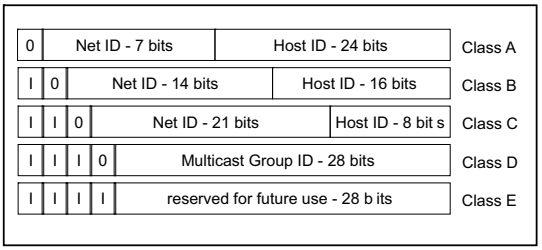
IP Address

The IP addresses consist of four bytes. Write these four bytes in decimal notation, separated by a decimal point.

RFC 1340 written in 1992, defines five IP Address classes.

Class	Network Address	Host Address	Address Range
A	1 Byte	3 Bytes	0.0.0.0 to 127.255.255.255
B	2 Bytes	2 Bytes	128.0.0.0 to 191.255.255.255
C	3 Bytes	1 Byte	192.0.0.0 to 223.255.255.255
D	–	–	224.0.0.0 to 239.255.255.255
E	–	–	240.0.0.0 to 255.255.255.255

The first byte of an IP address is the network address. The worldwide leading regulatory board for assigning network addresses is the Internet Assigned Numbers Authority (IANA). When you require an IP address block, contact your Internet Service Provider (ISP). Your ISP contacts their local higher-level organization to reserve an IP address block.



When the first bit of an IP address is zero, it belongs to class A (for example, the first octet is less than 128).

When the first bit of an IP address is one and the second bit is zero, it belongs to class B (for example, the first octet is between 128 and 191).

When the first 2 bits of an IP address are one, it belongs to class C (for example, the first octet is higher than 191).

Assigning the host address (host ID) is the responsibility of the network operator. The network operator manages the uniqueness of the assigned IP addresses.

Netmask

Routers and Gateways subdivide large networks into subnetworks. The netmask asssigns the IP addresses of the individual devices to a particular subnetwork.

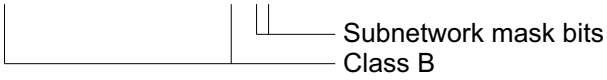
Perform subnetwork division using the netmask in much the same way as the division of the network addresses (net id) into classes A to C.

Set the bits of the host address (host id) that represent the mask to one. Set the remaining host address bits to zero (see the following examples).

Example of a subnet mask:

Decimal notation
255.255.192.0

Binary notation
11111111.11111111.11000000.00000000



Example of applying the subnet mask to IP addresses for subnetwork assignment:

Decimal notation
129.218.65.17
128 < 129 191 › Class B

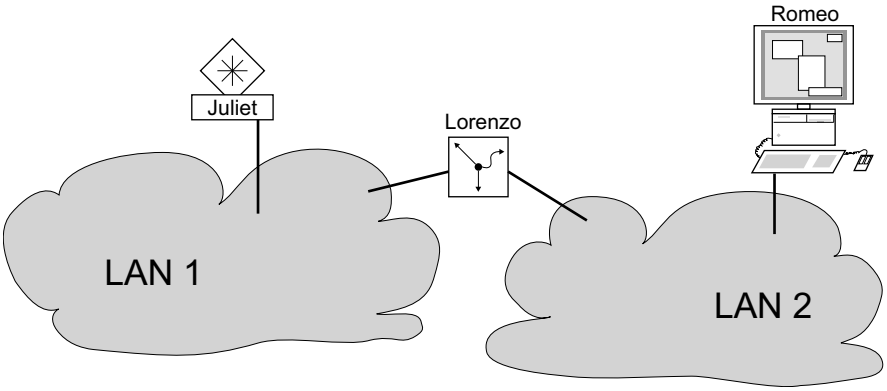
Binary notation
10000001.11011010.01000001.00010001
Subnetwork 1
Network address

Decimal notation
129.218.129.17
128 < 129 191 › Class B

Binary notation
10000001.11011010.10000001.00010001
Subnetwork 2
Network address

Example of Netmask Use

In a large network it is possible that Gateways and routers separate the management agent from its network management station. How does addressing work in such a case?



The network management station Romeo wants to send data to the management agent Juliet. Romeo knows Juliet's IP address and also knows that the router Lorenzo knows the way to Juliet.

Romeo puts his message in an envelope and writes Juliet's IP address as the destination address; for the source address he writes his own IP address on the envelope.

Romeo places this envelope in a second one with Lorenzo's MAC address as the destination and his own MAC address as the source. This process is comparable to going from layer 3 to layer 2 of the ISO/OSI base reference model.

Romeo puts the entire data packet into the mailbox, which is comparable to going from layer 2 to layer 1, that means to sending the data packet over the Ethernet.

Lorenzo receives the letter, removes the outer envelope, and recognizes from the inner envelope that the letter is meant for Juliet. He places the inner envelope in a new outer envelope and searches his address list (the ARP table) for Juliet's MAC address; he writes her MAC address on the outer envelope as the destination address and his own MAC address as the source address. He places the entire data packet in the mail box.

Juliet receives the letter and removes the outer envelope. She finds the inner envelope with Romeo's IP address. Opening the inner envelope and reading its contents corresponds to transferring the message to the higher protocol layers of the ISO/OSI layer model.

Juliet wants to send a reply to Romeo. She places her reply in an envelope with Romeo's IP address as destination and her own IP address as source. But where does she send the answer? She did not receive Romeo's MAC address. It was lost because Lorenzo replaced the outer envelope.

In the MIB, Juliet finds Lorenzo listed under the `NetGatewayIPAddr` variable as a means of communicating with Romeo. She puts the envelope with the IP addresses in another envelope with Lorenzo's MAC destination address.

The letter now travels back to Romeo via Lorenzo, the same way the first letter traveled from Romeo to Juliet.

Classless Inter-Domain Routing

Class C with a maximum of 254 addresses was too small, and class B with a maximum of 65534 addresses was too large for most users, resulting in an ineffective usage of the available class B addresses.

Class D contains reserved Multicast addresses. Class E is for experimental purposes. A non-participating Gateway ignores experimental datagrams with these destination addresses.

Since 1993, RFC 1519 has been using Classless Inter-Domain Routing (CIDR) to provide a solution. CIDR overcomes these class boundaries and supports classless address ranges.

With CIDR, you enter the number of bits that designate the IP address range. You represent the IP address range in binary form and count the mask bits that designate the netmask. The mask bits equal the number of bits used for the subnet in a given IP address range.

Example:

IP address, decimal	Network mask, decimal	IP address, binary
192.168.112.1	255.255.255.128	11000000 10101000 01110000 00000001
192.168.112.127		11000000 10101000 01110000 01111111

25 mask bits

CIDR notation: 192.168.112.0/25

Mask bits

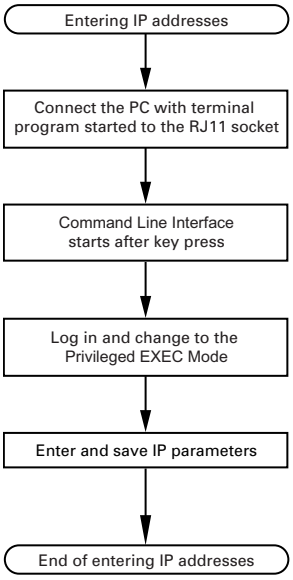
The term supernetting refers to combing a number of class C address ranges. Supernetting enables you to subdivide class B address ranges.

Specifying the IP Parameters using the CLI

There are the following methods used to enter the IP parameters:

- BOOTP/DHCP
- Ethernet Switch Configurator protocol
- External memory
- CLI using the serial connection

The device lets you specify the IP parameters using the Ethernet Switch Configurator protocol or using the CLI over the serial interface.



NOTE: If a terminal or PC with terminal emulation is unavailable in the vicinity of the installation location, you can configure the device at your own workstation, then take it to its final installation location.

Perform the following steps:

☐ Set up a connection to the device.
The start screen appears.

☐ Deactivate DHCP.

☐ Enter the IP parameters.
- ▶ Local IP address
  In the default setting, the local IP address is `0.0.0.0`.
- ▶ Netmask
  When you divide your network into subnetworks, and these are identified with a netmask, enter the netmask here. In the default setting, the local netmask is `0.0.0.0`.
- ▶ IP address of the Gateway.
  This entry is only required in cases where the device and the network management station or TFTP server are located in different subnetworks (see on page 43 “Example of Netmask Use”).
  Specify the IP address of the Gateway between the subnetwork with the device and the path to the network management station.
  In the default setting, the IP address is `0.0.0.0`.

☐ Save the configuration specified using `copy config running-config nvm`.

`enable`	Change to the Privileged EXEC mode.
`network protocol none`	Deactivating DHCP.
`network parms 10.0.1.23 255.255.255.0`	Assign the device the IP address `10.0.1.23` and the netmask `255.255.255.0`. You have the option of also assigning a Gateway address.
`copy config running-config nvm`	Save the settings in the non-volatile memory (`nvm`) in the selected configuration profile.

After entering the IP parameters, configure the device using the GUI.

Specifying the IP Parameters using Ethernet Switch Configurator

The Ethernet Switch Configurator protocol allows you to assign IP parameters to the device using Ethernet.

Configure other parameters using the GUI.

Install the Ethernet Switch Configurator software on your PC.

Perform the following steps:
☐ Start the Ethernet Switch Configurator program.

When Ethernet Switch Configurator is started, the program automatically searches the network for those devices that support the Ethernet Switch Configurator protocol.

Ethernet Switch Configurator uses the first network interface found for the PC. When your computer has several network cards, select the one you want in the Ethernet Switch Configurator toolbar.

Ethernet Switch Configurator displays a line for every device that responds to a Ethernet Switch Configurator protocol inquiry.

Ethernet Switch Configurator allows you to identify the devices displayed.
- ☐ Select a device line.
- ☐ To set the LEDs to flashing for the selected device, click the *Signal* button on the tool bar. To stop the flashing, click the *Signal* button again.
- ☐ By double-clicking a line, you open a window, in which you specify the device name and the IP parameter.

NOTE: Disable the Ethernet Switch Configurator function in the device after you assigned the IP parameters to the device.

NOTE: Save the settings to retain the entries after a restart.

Specifying the IP Parameters using the GUI

Perform the following steps:

- ☐ Open the *Basic Settings > Network* dialog.
- ☐ In the *VLAN ID* field, specify the VLAN in which the device management can be accessed over the network.

You can only access the device management using ports that are members of the relevant VLAN.

The *MAC address* field displays the MAC address of the device with which you access the device over the network.

- ☐ In the *Ethernet Switch Configurator protocol v1/v2* frame, specify the settings to access the device using the Ethernet Switch Configurator software.
- ☐ The Ethernet Switch Configurator protocol lets you allocate an IP address to the device on the basis of its MAC address. Activate the Ethernet Switch Configurator protocol if you want to allocate an IP address to the device from your PC with the Ethernet Switch Configurator software.
- ☐ In the *Management interface* frame, first specify where the device gets its IP parameters from:

▶ In the `BOOTP` mode, the configuration uses a BOOTP or DHCP server on the basis of the MAC address of the device.
▶ In the `DHCP` mode, the configuration uses a DHCP server on the basis of the MAC address or the name of the device.
▶ In the `Local` mode, the device uses the network parameters from the internal device memory.

NOTE: When you change the allocation mode of the IP address, the device activates the new mode immediately after you click the ✓ button.

- ☐ If required, enter the IP address, the netmask and the Gateway in the *IP parameter* frame.
- ☐ Save the changes temporarily. To do this, click the ✓ button.

Specifying the IP Parameters using BOOTP

With the *BOOTP* function activated, the device sends a boot request message to the BOOTP server. The boot request message contains the client ID configured in the *Basic Settings > Network* dialog. The BOOTP server enters the client ID into a database and assigns an IP address. The server answers with a boot reply message. The boot reply message contains the assigned IP address.

Specifying the IP Parameters using DHCP

The Dynamic Host Configuration Protocol (DHCP) is a further development of BOOTP, which it has replaced. The DHCP additionally lets the configuration of a DHCP client use a name instead of using the MAC address.

For the DHCP, this name is known as the Client Identifier in accordance with RFC 2131.

The device uses the name entered under sysName in the system group of the MIB II as the Client Identifier. You can change the system name using the GUI (see dialog *Basic Settings > System*), the CLI, or SNMP.

The device sends its system name to the DHCP server. The DHCP server then uses the system name to allocate an IP address as an alternative to the MAC address.

In addition to the IP address, the DHCP server sends
- the netmask
- the default Gateway (if available)
- the TFTP URL of the configuration file (if available).

The device applies the configuration data to the appropriate parameters. When the DHCP server assigns the IP address, the device permanently saves the configuration data in non-volatile memory.

Options	Meaning
1	Subnet Mask
2	Time Offset
3	Router
4	Time server
12	Host Name
42	NTP server
61	Client Identifier
66	TFTP Server Name
67	Bootfile Name

The advantage of using DHCP instead of BOOTP is that the DHCP server can restrict the validity of the configuration parameters (Lease) to a specific time period (known as dynamic address allocation). Before this period (Lease Duration) elapses, the DHCP client can attempt to renew the lease. Alternatively, the client can negotiate a new lease. The DHCP server then allocates a random, free address.

To help avoid this, DHCP servers provide the explicit configuration option of assigning a specific client the same IP address based on a unique hardware ID (known as static address allocation).

In the default setting, DHCP is activated. As long as DHCP is activated, the device attempts to obtain an IP address. When the device cannot find a DHCP server after restarting, it will not have an IP address. The *Basic Settings > Network* dialog lets you activate or deactivate DHCP.

NOTE: When using ConneXium Network Manager, verify that DHCP allocates the original IP address to every device.

The appendix contains a configuration example of the BOOTP/DHCP-server.

Example of a DHCP-configuration file:

```
# /etc/dhcpd.conf for DHCP Daemon
#
subnet 10.1.112.0 netmask 255.255.240.0 {
option subnet-mask 255.255.240.0;
option routers 10.1.112.96;
}
#
# Host berta requests IP configuration
# with her MAC address
#
host berta {
hardware ethernet 00:80:63:08:65:42;
fixed-address 10.1.112.82;
}
#
# Host hugo requests IP configuration
# with his client identifier.
#
host hugo {
#
option dhcp-client-identifier "hugo";
option dhcp-client-identifier 00:68:75:67:6f;
fixed-address 10.1.112.83;
server-name "10.1.112.11";
filename "/agent/config.dat";
}
```

Lines beginning with the # character contain comments.

The lines preceding the individually listed devices refer to settings that apply to the following device.

The fixed-address line assigns a permanent IP address to the device.

For more information, refer to the DHCP server manual.

Management Address Conflict Detection

You assign an IP address to the device using several different methods. This function helps the device detect IP address conflicts on a network after boot up and the device also verifies periodically during operation. This function is described in RFC 5227.

When enabled, the device sends an SNMP trap informing you that it detected an IP address conflict.

The following list contains the default settings for this function:
- *Operation*: `On`
- *Detection mode*: `active and passive`
- *Send periodic ARP probes*: `selected`
- *Detection delay [ms]*: `200`
- *Release delay [s]*: `15`
- *Address protections*: `3`
- *Protection interval [ms]*: `200`
- *Send trap*: `selected`

Active and Passive Detection

Actively verifying the network helps prevent the device from connecting to the network with a duplicate IP address. After connecting the device to a network or after configuring the IP address, the device immediately verifies if its IP address exists within the network. To verify the network for address conflicts, the device sends four ARP probes with the detection delay of 200 ms into the network. When the IP address exists, the device attempts to return to the previous configuration, and make another verification after the configured release delay time.

When you disable active detection, the device sends two gratuitous APR announcements in 2 s intervals. Using the ARP announcements with passive detection enabled, the device polls the network to determine if there is an address conflict. After resolving an address conflict or after expired release delay time, the device reconnects to the network. Following 10 detected conflicts, when the configured release delay interval is less than 60 s, the device sets the release delay interval to 60 s.

After the device performs active detection or you disable the active detection function, with passive detection enabled the device listens on the network for other devices using the same IP address. When the device detects a duplicate IP address, it initially defends its address by employing the ACD mechanism in the passive detection mode and sends out gratuitous ARPs. The number of protections that the device sends and the protection interval are configurable. To resolve conflicts, as long as the remote device remains connected to the network, the network interface of the local device disconnects from the network.

When a DHCP server assigns an IP address to the device and an address conflict occurs, the device returns a DHCP decline message.

The device uses the ARP probe method, which has the following advantages:
- ARP caches on other devices remain unchanged.
- The method is robust through multiple ARP probe transmissions.

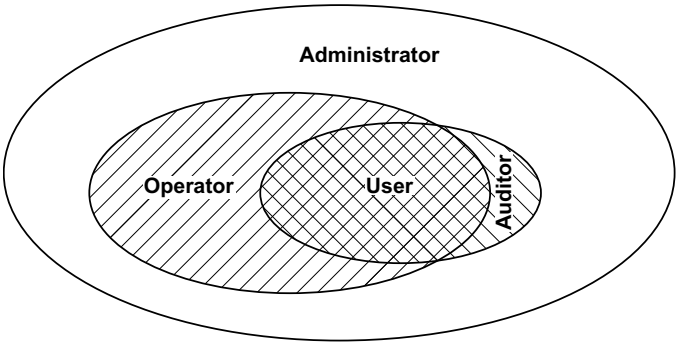
Access to the Device

Access Roles

The device functions available depend on your access role. When you are logged in with a specific access role, the functions of the access role are available to you.

The commands available to you as a user also depend on the CLI mode in which you are working. See “Mode-based Command Hierarchy” on page 25.

The device offers the following access roles:



Access Role	User Authorizations
`User`	Users logged in with the access role `User` are authorized to monitor the device.
`Auditor`	Users logged in with the access role `Auditor` are authorized to monitor the device and to save the log file in the *Diagnostics > Report > Audit Trail* dialog.
`Operator`	Users logged in with the access role `Operator` are authorized to monitor the device and to change the settings – except for security settings for device access.
`Administrator`	Users logged in with the access role `Administrator` are authorized to monitor the device and to change the settings.
`Unauthorized`	Unauthorized users are blocked, and the device rejects the user login. Assign this value to temporarily lock the user account. If a detected error occurs during an access role change, the device assigns this access role to the user account.

First Login (Password Change)

To help prevent undesired access to the device, you must change the default password during initial setup.

Perform the following steps:
- ☐ Open the GUI, the Schneider Electric Viewer application, or the CLI the first time you log in.
- ☐ Log in with the default password. See Modicon MCSESR Redundancy Switch Installation User Guide.
  The device prompts you to type in a new password.
- ☐ Type in your new password.
  Choose a password that contains at least eight characters, which includes upper-case characters, lower-case characters, numerical digits, and special characters.
- ☐ When you log in with the CLI, the device prompts you to confirm your new password.
- ☐ Log in again with your new password.

NOTE: If you lose your password, contact your local support team.

Authentication Lists

When you access the device using a specific connection, the device verifies the login credentials in an authentication list that contains the policies the device uses for authentication.

The prerequisite for access to the device management is that at least one policy is assigned to the authentication list of the application through which access is performed.

Applications

The device provides an application for each type of connection through which you access the device:
- ▶ Access to the CLI using a serial connection: `Console(V.24)`
- ▶ Access to the CLI using SSH: `SSH`
- ▶ Access to the CLI using Telnet: `Telnet`
- ▶ Access to the GUI: `WebInterface`

The device provides an application to control the access to the network from connected end devices using port-based access control: `8021x`

Policies

When you log in with valid login data, the device gives you access to its device management. The device authenticates your user account using the following policies:

- User management of the device
- RADIUS

When the end device logs in with valid login data, the device lets the connected end devices have access to the network with the port-based access control according to IEEE 802.1X. The device authenticates the end devices using the following policies:

- RADIUS
- Integrated Authentication Server (IAS)

The device provides a fall-back solution. To use this option, specify more than one policy in the authentication list. When authentication is unsuccessful using the present policy, the device applies the next specified policy.

Managing Authentication Lists

Manage the authentication lists in the GUI or in the CLI. To do this, perform the following steps:

☐ Open the *Device Security > Authentication List* dialog.

The dialog displays the authentication lists that are set up.

`show authlists`	Displays the authentication lists that are set up.

☐ Deactivate the authentication list for applications that have no access to the device, for example `8021x`.

☐ In the *Active* column of the authentication list `defaultDot1x8021AuthList`, clear the checkbox.

☐ Save the changes temporarily. To do this, click the button.

`authlists disable defaultDot1x8021AuthList`	Deactivates the authentication list `defaultDot1x8021AuthList`.

Adjust the Settings

Example: Set up a separate authentication list for the `WebInterface` application, which is, by default, included in the `defaultLoginAuthList` authentication list.

The device forwards authentication requests to a RADIUS server in the network. As a fall-back solution, the device authenticates user accounts using the local user management. To do this, perform the following steps:

☐ Create a `loginGUI` authentication list.

☐ Open the *Device Security > Authentication List* dialog.

☐ Click the button.
The dialog displays the *Create* window.

☐ Enter a name in the *Name* field.
In this example, enter `loginGUI`.

☐ Click the *Ok* button.
The device adds a new table entry.

`enable`	Change to the Privileged EXEC mode.
`configure`	Change to the Configuration mode.
`authlists add loginGUI`	Creates the `loginGUI` authentication list.

☐ Select the policies for the `loginGUI` authentication list.

☐ In the *Policy 1* column, select the *`radius`* value.

☐ In the *Policy 2* column, select the *`local`* value.

☐ In the *Policy 3* to *Policy 5* columns, select the *`reject`* value to help prevent further fall-back.

☐ Save the changes temporarily. To do this, click the button.

`authlists set-policy loginGUI radius local reject reject reject`	Assigns the `radius`, `local` and `reject` policies to the `loginGUI` authentication list.
`show authlists`	Displays the authentication lists that are set up.

☐ Assign an application to the `loginGUI` authentication list.

☐ In the *Device Security > Authentication List* dialog, select the `loginGUI` authentication list.

☐ Click the button and *Allocate applications*.
The dialog displays the *Allocate applications* window.

☐ In the left column, select the `WebInterface` application.

☐ Click the button.
The right column now displays the `WebInterface` application.

☐ Click the *Ok* button.
The dialog displays the updated settings:
– The *Dedicated applications* column of `loginGUI` authentication list displays the `WebInterface` application.
– The *Dedicated applications* column of `defaultLoginAuthList` authentication list does not display the `WebInterface` application.

☐ Save the changes temporarily. To do this, click the button.

`show applists`	Displays the applications and the allocated lists.
`applists set-authlist WebInterface loginGUI`	Assigns the `loginGUI` application to the `WebInterface` authentication list.

User Management

When you log in with valid login data, the device gives you access to its device management. The device authenticates your user account either using the local user management or a RADIUS server in the network. To get the device to use the user management, assign the `local` policy to an authentication list, see the *Device Security > Authentication List* dialog.

In the local user management, manage the user accounts. One user account is typically allocated to each user.

Access Roles

The device lets you use a role-based authorization model to control access to the device management. Users to whom a specific authorization profile is allocated are allowed to use commands and functions at the same authorization profile or a lower one.

The device uses the authorization profiles on every application with which the device management can be accessed.

Every user account is linked to an access role that regulates the access to the individual functions of the device. Depending on the planned activity for the respective user, assign a pre-defined access role to the user. The device defines the following access roles:

Role	Description	Authorized for the following Activities
Administrator	The user is authorized to monitor and administer the device.	All activities with read/write access, including the following activities reserved for an administrator: ▶ Add, modify or delete user accounts. ▶ Activate, deactivate or unlock user accounts. ▶ Change all passwords. ▶ Configure password management. ▶ Set or change the system time ▶ Load files to the device, for example device configurations, certificates or software images. ▶ Reset settings and security-related settings to the delivery state. ▶ Configure the RADIUS server and authentication lists. ▶ Apply scripts using the CLI ▶ Enable/disable CLI logging and SNMP logging. ▶ Activate and deactivate external memory. ▶ Activate and deactivate the system monitor. ▶ Enable/disable the services for access to the device management (for example SNMP). ▶ Configure access restrictions to the GUI or the CLI based on the IP addresses.
Operator	The user is authorized to monitor and configure the device - except for security-related settings.	Access activities with read/write access, except for the above-named activities, which are reserved for an administrator.

Role	Description	Authorized for the following Activities
Auditor	The user is authorized to monitor the device and to save the log file in the *Diagnostics > Report > Audit Trail* dialog.	Monitor activities with read access.
Guest	The user is authorized to monitor the device - except for security-related settings.	Monitor activities with read access.
Unauthorized	No access to the device possible. ▶ As an administrator, you assign this access role to temporarily lock a user account. ▶ If an administrator assigns a different access role to the user account and an error is detected, the device assigns this access role to the user account.	No activities allowed.

Managing User Accounts

Manage the user accounts in the GUI or in the CLI. To do this, perform the following steps:

☐ Open the *Device Security > User Management* dialog.

The dialog displays the active user accounts.

`show users` Displays the active user accounts.

Default Setting

In delivery state, the `admin` account is set up in the device.

Parameter	Default Setting
User name	`admin`
Password	`private`
Role	`administrator`
User locked	`cleared`
Policy check	`cleared`
SNMP auth type	`hmacmd5`
SNMP encryption type	`des`

Change the password for the `admin` account before making the device available in the network.

Changing Default Passwords

To help prevent unauthorized access, change the password of the default user account. To do this, perform the following steps:

☐ Change the password for the `admin` account.

☐ Open the *Device Security > User Management* dialog.

The dialog displays the active user accounts.

☐ To obtain a higher level of complexity for the password, select the checkbox in the *Policy check* column.
Before saving it, the device verifies the password according to the policy specified in the *Password policy* frame.

NOTE: The password verification can lead to a message in the *Security status* frame in the *Basic Settings > System* dialog. Specify the settings in the *Basic Settings > System* dialog for the activity that requires your attention.

☐ Click the row of the relevant user account in the *Password* field. Enter a password of at least six characters.
Up to 64 alphanumeric characters are allowed.
- ▶ The device differentiates between upper and lower case.
- ▶ The minimum length of the password is specified in the *Configuration* frame. The device constantly verifies the minimum length of the password.

☐ Save the changes temporarily. To do this, click the ✓ button.

`enable`	Change to the Privileged EXEC mode.
`configure`	Change to the Configuration mode.
`users password-policy-check <user> enable`	Verifies passwords for the `<user>` account based on the specified policy, so you can obtain a higher level of complexity for the password.

NOTE: When you display the security status, the password verification can lead to a message (`show security-status all`). You can change the settings that create this message with the command `security-status monitor pwd-policy-inactive`.

`users password <user> SECRET`	Specifies the `SECRET` password for the `<user>` account. Enter at least six characters.
`save`	Save the settings in non-volatile memory (`nvm`) in the selected configuration profile.

Setting up a new User Account

Allocate a separate user account for each user that accesses the device management.

In the following example, we create a user account for an `operator` role. Users with the `operator` role are authorized to monitor and configure the device - except for security-related settings. To do this, perform the following steps:

☐ Create a new user account.

- ☐ Open the *Device Security > User Management* dialog.
- ☐ Click the button.
  The dialog displays the *Create* window.
- ☐ Enter the name in the *User name* field.
  In this example, we use the name `USER`.
- ☐ Click the *Ok* button.
- ☐ To obtain a higher level of complexity for the password, select the checkbox in the *Policy check* column.
  Before saving it, the device verifies the password according to the policy specified in the *Password policy* frame.
- ☐ In the *Password* field, enter a password of at least six characters.
  Up to 64 alphanumeric characters are allowed.
  - ▶ The device differentiates between upper and lower case.
  - ▶ The minimum length of the password is specified in the *Configuration* frame. The device constantly verifies the minimum length of the password.
- ☐ In the *Role* column, select the user role.
  In this example, use the `operator` role.
- ☐ To activate the user account, select the checkbox in the *Active* column.
- ☐ Save the changes temporarily. To do this, click the button.
  The dialog displays the active user accounts.

`enable`	Change to the Privileged EXEC mode.
`configure`	Change to the Configuration mode.
`users add USER`	Creates the `USER` account.
`users password-policy-check USER enable`	Activates the verification of the password of the `USER` account based on the specified policy, which allows you to obtain a higher level of complexity.

`users password USER SECRET`	Specifies the `SECRET` password for the `USER` account. Enter at least six characters.
`users access-role USER operator`	Assign the `operator` role to the `USER` account.
`users enable USER`	Activates the `USER` account.
`show users`	Displays the active user accounts.
`save`	Save the settings in non-volatile memory (`nvm`) in the selected configuration profile.

NOTE: When you create a new user account in the CLI, remember to allocate the password.

Deactivating the User Account

After a user account is deactivated, the device denies its access to the device management. In contrast to completely deleting it, deactivating a user account lets you keep the settings and reuse them later. To do this, perform the following steps:

☐ To keep user account settings and reuse them later, temporarily deactivate the user account.

☐ Open the *Device Security > User Management* dialog.
The dialog displays the active user accounts.

☐ In the row for the relevant user account, clear the checkbox in the *Active* column.

☐ Save the changes temporarily. To do this, click the  button.

`enable`	Change to the Privileged EXEC mode.
`configure`	Change to the Configuration mode.
`users disable <user>`	Disables the user account.
`show users`	Displays the active user accounts.
`save`	Save the settings in non-volatile memory (`nvm`) in the selected configuration profile.

☐ To permanently deactivate the user account settings, delete the user account.

☐ Select the row for the relevant user account.

☐ Click the  button.

`users delete <user>`	Deletes the `<user>` account.
`show users`	Displays the active user accounts.
`save`	Save the settings in non-volatile memory (`nvm`) in the selected configuration profile.

Adjusting Policies for Passwords

The device verifies passwords to ensure they adhere to the specified policy so that you can obtain a higher level of complexity.

The device lets you activate or deactivate the verification separately in each user account. When you select the checkbox and the new password fulfills the policy requirements, the device accepts the password change.

In the default settings, the policy uses practical values. You can adjust the policy to meet your requirements. To do this, perform the following steps:
☐ Adjust the policy for passwords to meet your requirements.

☐ Open the *Device Security > User Management* dialog.

In the *Configuration* frame, you specify the number of login attempts to allow before the device locks out the user. Also specify the minimum number of characters required in a password.

NOTE: Only users with `administrator` authorization can remove the lock.

The number of login attempts as well as the possible lockout of the user apply only through the following methods:
- the GUI
- the SSH protocol
- the Telnet protocol

NOTE: When accessing device management through the CLI serial connection, the number of login attempts is unlimited.

☐ Specify the values to meet your requirements.
- In the *Login attempts* field, you specify the number of times that a user can attempt to log in in the range `0..5`.
  The value `0` deactivates the function.
- The *Min. password length* field lets you enter values in the range `1..64`.

The dialog displays the policy in the *Password policy* frame.

☐ Adjust the values to meet your requirements.
- Values in the range `1` through `16` are allowed.
  The value `0` deactivates the relevant policy.

To apply the entries specified in the *Configuration* and *Password policy* frames, select the checkbox in the *Policy check* column for a particular user.

☐ Save the changes temporarily. To do this, click the button.

`enable`	Change to the Privileged EXEC mode.
`configure`	Change to the Configuration mode.
`passwords min-length 6`	Specifies the policy for the minimum length of the password.
`passwords min-lowercase-chars 1`	Specifies the policy for the minimum number of lower case letters in the password.
`passwords min-numeric-chars 1`	Specifies the policy for the minimum number of digits in the password.
`passwords min-special-chars 1`	Specifies the policy for the minimum number of special characters in the password.

`passwords min-uppercase-chars 1`	Specifies the policy for the minimum number of upper case letters in the password.
`show passwords`	Displays the active policies.
`save`	Save the settings in non-volatile memory (`nvm`) in the selected configuration profile.

SNMP Access

The SNMP protocol lets you work with a network management system to monitor the device over the network and change its settings.

SNMPv1/v2 Access

Using SNMPv1 or SNMPv2 the network management system and the device communicate unencrypted. Every SNMP packet contains the community name in plain text and the IP address of the sender.

The community names `user` for read accesses and `admin` for write accesses are preset in the device. If SNMPv1/v2 is enabled, then the device lets anyone who knows the community name have access to the device.

To help prevent unwanted access, perform the following steps:

- ☐ Change the default community names in the device.
  Treat the community names with discretion.
  Anyone who knows the community name for write access, has the ability to change the settings of the device.
- ☐ Specify a different community name for read/write access than for read access.
- ☐ Use SNMPv1 or SNMPv2 only in environments protected from eavesdropping. The protocols do not use encryption.
- ☐ Use, if possible, SNMPv3 and disable the access using SNMPv1 and SNMPv2 in the device.

SNMPv3 Access

Using SNMPv3 the network management system and the device communicate encrypted. The network management system authenticates itself with the device using the login credentials of a user. The prerequisite for the SNMPv3 access is that in the network management system uses the same settings that are defined in the device.

The device lets you specify the *SNMP auth type* and *SNMP encryption type* parameters individually in each user account.

When you set up a new user account in the device, the parameters are preset so that the network management system ConneXium Network Manager reaches the device immediately.

The user accounts set up in the device use the same passwords in the GUI, in the CLI, and for SNMPv3.

To adapt the SNMPv3 parameters of the user account settings to the settings in your network management system, perform the following steps:

- ☐ Open the *Device Security > User Management* dialog.

The dialog displays the active user accounts.

- ☐ Click the row of the relevant user account in the *SNMP auth type* field. Select the desired setting.
- ☐ Click the row of the relevant user account in the *SNMP encryption type* field. Select the desired setting.
- ☐ Save the changes temporarily. To do this, click the  button.

`enable`	Change to the Privileged EXEC mode.
`configure`	Change to the Configuration mode.
`users snmpv3 authentication <user> md5 | sha1`	Assigning the HMAC-MD5 or HMACSHA protocol for authentication requests to the user account `<user>`.
`users snmpv3 encryption <user> des | aescfb128 | none`	Assigns the DES or AES-128 algorithm to the user account `<user>`. With this algorithm, the device encrypts authentication requests. The value `none` removes the encryption.
`show users`	Display the user accounts that have been configured.
`save`	Save the settings in the non-volatile memory (`nvm`) in the selected configuration profile.

Synchronizing the System Time in the Network

Many applications rely on a time that is as correct as possible. The necessary accuracy, and thus the allowable deviation from the actual time, depends on the application area.

Examples of application areas include:
- Log entries
- Time stamping of production data
- Process control

The device lets you synchronize the time on the network using the following options:
- The Simple Network Time Protocol (SNTP) is a solution for low accuracy requirements. Under ideal conditions, SNTP achieves an accuracy in the millisecond range. The accuracy depends on the signal delay.
- IEEE 1588 with the Precision Time Protocol (PTP) achieves accuracies on the order of fractions of microseconds. This method is suitable even for demanding applications up to and including process control.

When the involved devices support the PTP protocol, it is the better choice. PTP is more accurate, has advanced methods of error correction, and causes a low network load. The implementation of PTP is comparatively easy.

NOTE: According to the PTP and SNTP standards, both protocols function in parallel in the same network. However, since both protocols influence the system time of the device, situations can occur in which the two protocols conflict with each other.

Basic Settings

In the *Time > Basic Settings* dialog, you specify general settings for the time.

Setting the Time

When no reference time source is available to you, you have the option to set the time in the device.

After a cold start or reboot, if no real-time clock is available or the real-time clock contains an invalid time, then the device initializes its clock with January 1, 00:00h. After the power supply is switched off, the device buffers the settings of the real-time clock up to 24 hours.

Alternatively, you configure the settings in the device so that it automatically obtains the time from a PTP clock or from an SNTP server.

Alternatively, you configure the settings in the device so that it automatically obtains the time from an SNTP server.

Perform the following steps:

☐ Open the *Time > Basic Settings* dialog.

▶ The *System time (UTC)* field displays the UTC (Universal Time Coordinated) of the device. UTC is the time relating to the coordinated world time measurement. UTC is the same worldwide and does not take local time shifts into account.

▶ The time in the *System time* field comes from the *System time (UTC)* plus the *Local offset [min]* value and a possible shift due to daylight saving time.

NOTE: PTP sends the International Atomic Time (TAI). As of July 1, 2020, the TAI time is 37 s ahead of the UTC time. When the PTP reference time source of the UTC offset is set correctly, the device automatically corrects this difference on the display in the *System time (UTC)* field.

☐ In order to cause the device to apply the time of your PC to the *System time* field, click the *Set time from PC* button.
Based on the value in the *Local offset [min]* field, the device calculates the time in the *System time (UTC)* field: The *System time (UTC)* comes from the *System time* minus the *Local offset [min]* value and a possible shift due to daylight saving time.

▶ The *Time source* field displays the origin of the time data. The device automatically selects the source with the greatest accuracy.
The source is initially `local`.
When SNTP is active and the device receives a valid SNTP packet, the device sets its time source to `sntp`.
When PTP is active and the device receives a valid PTP message, the device sets its time source to `ptp`. The device prioritizes PTP ahead of SNTP.

▶ The *Local offset [min]* value specifies the time difference between the local time and the *System time (UTC)*.

☐ In order to cause the device to determine the time zone on your PC, click the *Set time from PC* button. The device calculates the local time difference from UTC and enters the difference into the *Local offset [min]* field.

NOTE: The device provides the option to obtain the local offset from a DHCP server.

☐ Save the changes temporarily. To do this, click the ✓ button.

`enable`	Change to the Privileged EXEC mode.
`configure`	Change to the Configuration mode.
`clock set <YYYY-MM-DD> <HH:MM:SS>`	Set the system time of the device.
`clock timezone offset <-780..840>`	Enter the time difference between the local time and the received UTC time in minutes.
`save`	Save the settings in the non-volatile memory (`nvm`) in the selected configuration profile.

Automatic Daylight Saving Time Changeover

When you operate the device in a time zone in which there is a summer time change, you set up the automatic daylight saving time changeover on the *Daylight saving time* tab.

When daylight saving time is enabled, the device sets the local system time forward by 1 hour at the beginning of daylight saving time. At the end of daylight saving time, the device sets the local system time back again by 1 hour. To do this, perform the following steps:

- ☐ Open the *Time > Basic Settings* dialog, *Daylight saving time* tab.
- ☐ To select a preset profile for the start and end of daylight saving time, click the *Profile...* button in the *Operation* frame.
- ☐ When no matching daylight saving time profile is available, you specify the changeover times in the *Summertime begin* and *Summertime end* fields. For both time points, you specify the month, the week within this month, the weekday, and the time of day.
- ☐ To enable the function, select the `On` radio button in the *Operation* frame.
- ☐ Save the changes temporarily. To do this, click the button.

`enable`	Change to the Privileged EXEC mode.
`configure`	Change to the Configuration mode.
`clock summer-time mode <disable|recurring|eu|usa>`	Configure the automatic daylight saving time changeover: enable/disable or activate with a profile.
`clock summer-time recurring start`	Enter the start time for the changeover.
`clock summer-time recurring end`	Enter the end time for the changeover.
`save`	Save the settings in the non-volatile memory (`nvm`) in the selected configuration profile.

SNTP

The Simple Network Time Protocol (SNTP) lets you synchronize the system time in your network. The device supports the SNTP client and the SNTP server function.

The SNTP server makes the UTC (Universal Time Coordinated) available. UTC is the time relating to the coordinated world time measurement. The UTC is the same worldwide and ignores local time shifts.

SNTP is a simplified version of NTP (Network Time Protocol). The data packets are identical with SNTP and NTP. Accordingly, both NTP and SNTP servers serve as a time source for SNTP clients.

NOTE: Statements in this chapter relating to external SNTP servers also apply to NTP servers.

SNTP knows the following operation modes for the transmission of time:

- *Unicast*
  In *Unicast* operation mode, an SNTP client sends requests to an SNTP server and expects a response from this server.
- *Broadcast*
  In *Broadcast* operation mode, an SNTP server sends SNTP messages to the network in specified intervals. SNTP clients receive these SNTP messages and evaluate them.

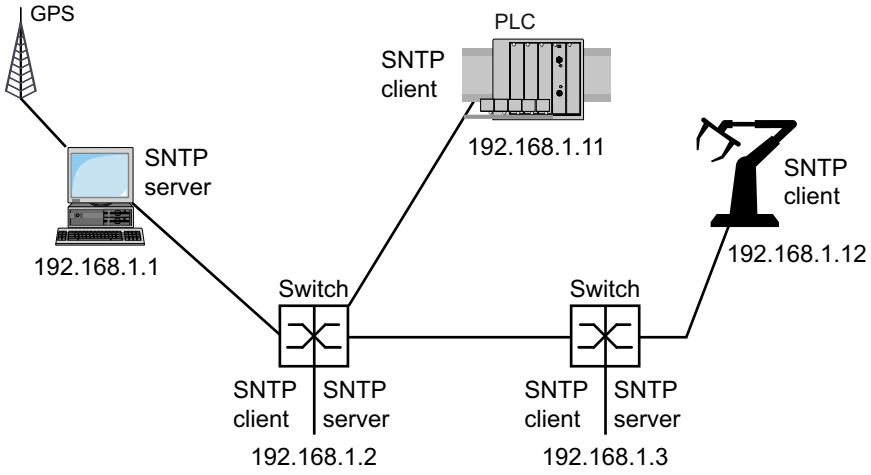
IPv4 Destination Address	Send SNTP Packets to
0.0.0.0	Nobody
224.0.1.1	*Multicast* address for SNTP messages
255.255.255.255	*Broadcast* address

NOTE: An SNTP server in *Broadcast* operation mode also responds to direct requests using *Unicast* from SNTP clients. In contrast, SNTP clients work in either *Unicast* or *Broadcast* operation mode.

Preparation

Perform the following steps:

- ☐ To get an overview of how the time is passed on, draw a network plan with the devices participating in SNTP.
  When planning, bear in mind that the accuracy of the time depends on the delays of the SNTP messages. To minimize delays and their variance, place an SNTP server in each network segment. Each of these SNTP servers synchronizes its own system time as an SNTP client with its parent SNTP server (SNTP cascade). The highest SNTP server in the SNTP cascade has the most direct access to a reference time source.



NOTE: For precise time distribution, between SNTP servers and SNTP clients you preferably use network components (routers and switches) that forward the SNTP packets with a low and uniform transmission time (latency).

▶ An SNTP client sends its requests to up to 4 configured SNTP servers. When there is no response from the 1st SNTP server, the SNTP client sends its requests to the 2nd SNTP server. When this request is also unsuccessful, it sends the request to the 3rd and finally the 4th SNTP server. If none of these SNTP servers respond, the SNTP client loses its synchronization. The SNTP client periodically sends requests to each SNTP server until a server delivers a valid time.

NOTE: The device provides the option of obtaining a list of SNTP server IP addresses from a DHCP server.

☐ If no reference time source is available to you, then determine a device with an SNTP server as a reference time source. Adjust its system time at regular intervals.

Defining Settings of the SNTP Client

As an SNTP client, the device obtains the time information from SNTP or NTP servers and synchronizes its system clock accordingly. To do this, perform the following steps:

☐ Open the *Time > SNTP > Client* dialog.

☐ Set the SNTP operation mode.
In the *Configuration* frame, select one of the following values in the *Mode* field:

▶ `unicast`
The device sends requests to an SNTP server and expects a response from this server.

▶ `broadcast`
The device waits for *Broadcast* or *Multicast* messages from SNTP servers on the network.

☐ To synchronize the time only once, select the *Disable client after successful sync* checkbox.
After synchronization, the device disables the *SNTP Client* function.

▶ The table displays the SNTP server to which the SNTP client sends a request in *Unicast* operation mode. The table contains up to 4 SNTP server definitions.

☐ To add a table entry, click the button.

☐ Specify the connection data of the SNTP server.

☐ To enable the function, select the `On` radio button in the *Operation* frame.

☐ Save the changes temporarily. To do this, click the button.

▶ The *State* field displays the status of the *SNTP Client* function.

Device	192.168.1.1	192.168.1.2	192.168.1.3	192.168.1.11	192.168.1.12
SNTP Client function	*Off*	*On*	*On*	*On*	*On*
Configuration: Mode	unicast	unicast	unicast	unicast	unicast
Request interval [s]	30	30	30	30	30
SNTP Server address(es)	–	192.168.1.1	192.168.1.2192.168.1.1	192.168.1.2192.168.1.1	192.168.1.3192.168.1.2192.168.1.1

Specifying SNTP Server Settings

When the device operates as an SNTP server, it provides its system time in coordinated world time (UTC) in the network. To do this, perform the following steps:

- ☐ Open the *Time > SNTP > Server* dialog.
- ☐ To enable the function, select the *On* radio button in the *Operation* frame.
- ☐ To enable the *Broadcast* operation mode, select the *Broadcast admin mode* radio button in the *Configuration* frame.
  In *Broadcast* operation mode, the SNTP server sends SNTP messages to the network in specified intervals. The SNTP server also responds to the requests from SNTP clients in *Unicast* operation mode.
  - ☐ In the *Broadcast destination address* field, you set the IPv4 address to which the SNTP server sends the SNTP packets. Set a *Broadcast* address or a *Multicast* address.
  - ☐ In the *Broadcast UDP port* field, you specify the number of the UDP port to which the SNTP server sends the SNTP packets in *Broadcast* operation mode.
  - ☐ In the *Broadcast VLAN ID* field, you specify the ID of the VLAN to which the SNTP server sends the SNTP packets in *Broadcast* operation mode.
  - ☐ In the *Broadcast send interval [s]* field, you enter the time interval at which the SNTP server of the device sends SNTP *Broadcast* packets.
- ☐ Save the changes temporarily. To do this, click the button.
- ▶ The *State* field displays the status of the *SNTP Server* function.

Device	192.168.1.1	192.168.1.2	192.168.1.3	192.168.1.11	192.168.1.12
SNTP Server function	*On*	*On*	*On*	*Off*	*Off*
UDP port	123	123	123	123	123
Broadcast admin mode	cleared	cleared	cleared	cleared	cleared
Broadcast destination address	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0
Broadcast UDP port	123	123	123	123	123

Device	192.168.1.1	192.168.1.2	192.168.1.3	192.168.1.11	192.168.1.12
Broadcast VLAN ID	1	1	1	1	1
Broadcast send interval [s]	128	128	128	128	128
Disable server at local time source	cleared	cleared	cleared	cleared	cleared

PTP

In order for LAN-controlled applications to work without latency, precise time management is required. With PTP (Precision Time Protocol), IEEE 1588 describes a method that enables precise synchronization of clocks in the network.

PTP enables synchronization with an accuracy of a few 100 ns. PTP uses Multicasts for the synchronization messages, which keeps the network load low.

Types of Clocks

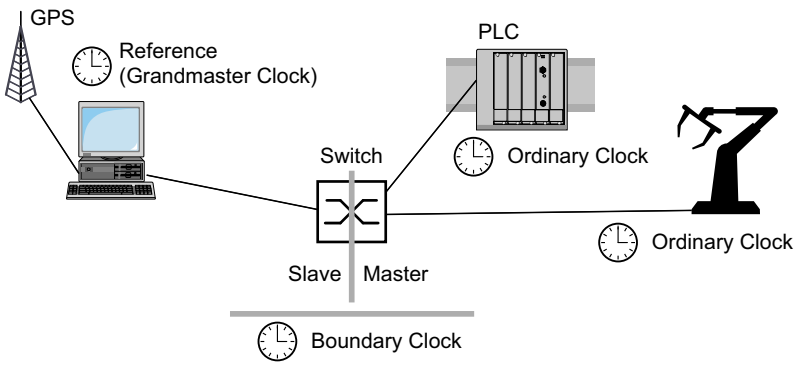
PTP defines the roles of “master” and “slave” for the clocks in the network:
- A master clock (reference time source) distributes its time.
- A slave clock synchronizes itself with the timing signal received from the master clock.

Boundary Clock

The transmission time (latency) in routers and switches has a measurable effect on the precision of the time transmission. To correct such inaccuracies, PTP defines what are known as boundary clocks.

In a network segment, a boundary clock is the reference time source (master clock) to which the subordinate slave clocks synchronize. Typically routers and switches take on the role of boundary clock.

The boundary clock in turn obtains the time from a higher-level reference time source (Grandmaster).



Transparent Clock

Switches typically take on the Transparent Clock role to enable high accuracy across the cascades. The Transparent Clock is a Slave clock that corrects its own transmission time when it forwards received synchronization messages.

Ordinary Clock

PTP designates the clock in a end device as an “Ordinary Clock”. An Ordinary Clock functions either as a master clock or slave clock.

Best Master Clock Algorithm

The devices participating in PTP designate a device in the network as a reference time source (Grandmaster). Here the “Best Master Clock” algorithm is used, which determines the accuracy of the clocks available in the network.

The “Best Master Clock” algorithm evaluates the following criteria:
- *Priority 1*
- *Clock class*
- *Clock accuracy*
- *Clock variance*
- *Priority 2*

The algorithm first evaluates the value in the *Priority 1* field of the participating devices. The device with the smallest value in the *Priority 1* field becomes the reference time source (Grandmaster). When the value is the same for multiple devices, the algorithm takes the next criterion. When this is also the same, it takes the next criterion after this one. If these values are the same for multiple devices, then the smallest value in the *Clock identity* field determines which device becomes the reference time source (Grandmaster).

In the settings of the boundary clock, the device lets you individually specify the values for *Priority 1* and *Priority 2*. This lets you influence which device will be the reference time source (Grandmaster) in the network.

Delay Measurement

The delay of the synchronization messages between the devices affects the accuracy. The delay measurement lets the devices take into account the average delay.

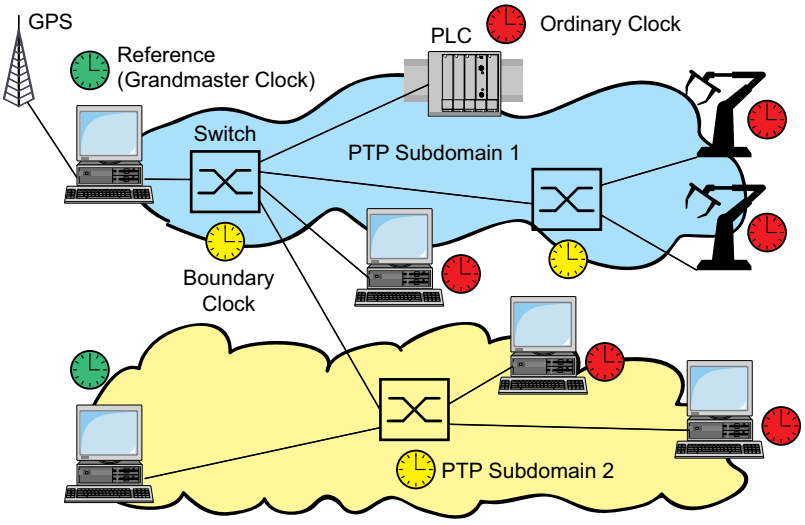
PTP version 2 offers the following methods for delay measurement:
- `e2e` (End to End)
  The slave clock measures the delay of synchronization messages to the master clock.

- *e2e-optimized*
  The slave clock measures the delay of synchronization messages to the master clock.
  This method is available only for transparent clocks. The device forwards the synchronization messages sent using Multicast only to the master clock, keeping the network load low. When the device receives a synchronization message from another master clock, it forwards the synchronization messages only to this new port.
  When the device does not have a master clock defined, it forwards synchronization messages to every port.
- *p2p* (Peer to Peer)
  The slave clock measures the delay of synchronization messages to the master clock.
  In addition, the master clock measures the delay to each slave clock, even across blocked ports. This requires that the master and slave clock support Peer-to-Peer (*p2p*).
  In case of interruption of a redundant ring, for example, the slave clock becomes the master clock and the master clock becomes the slave clock. This switch occurs without loss of precision, because the clocks already take into account the delay in the other direction.

NOTE: When you specify the value *p2p*, in column *Network protocol*, you can specify the value IEEE 802.3 only.

PTP Domains

The device transmits synchronization messages only from and to devices in the same PTP domain. The device lets you set the domain for the boundary clock and for the transparent clock individually.



Using PTP

In order to synchronize the clocks precisely with PTP, only use switches with a boundary clock or transparent clock as nodes.

Perform the following steps:

- ☐ To gain an overview of the distribution of clocks, draw a network plan with the devices involved in PTP.
- ☐ Specify the role for each participating switch (boundary clock or transparent clock). In the device, this setting is called *PTP mode*.

PTP Mode	Application
`v2-boundary-clock`	As a boundary clock, the device distributes synchronization messages to the slave clocks in the subordinate network segment. The boundary clock in turn obtains the time from a higher-level reference time source (Grandmaster).
`v2-transparent-clock`	As a transparent clock, the device forwards received synchronization messages after they have been corrected by the delay of the transparent clock.

- ☐ Enable PTP on each participating switch.
  PTP is then configured on a largely automatic basis.
- ☐ Enable PTP on the end devices.
- ☐ The device lets you influence which device in the network becomes the reference clock (Grandmaster). Therefore, change the default value in the *Priority 1* and *Priority 2* fields for the *Boundary Clock*.

Managing Configuration Profiles

If you change the settings of the device during operation, then the device stores the changes in its memory (*RAM*). After a reboot the settings are lost.

In order to keep the changes after a reboot, the device lets you save the settings in a configuration profile in the non-volatile memory (*NVM*). In order to make it possible to switch to other settings, the non-volatile memory offers storage space for multiple configuration profiles.

If an external memory is connected, then the device automatically saves a copy of the configuration profile in the external memory (*ENVM*). You can disable this function.

Detecting Changed Settings

The device stores changes made to settings during operation in its volatile memory (*RAM*). The configuration profile in the non-volatile memory (*NVM*) remains unchanged until you save the changed settings explicitly. Until then, the configuration profiles in memory and non-volatile memory are different. The device helps you recognize changed settings.

Volatile Memory (RAM) and Non-volatile Memory (NVM)

You can recognize when the configuration profile in the volatile memory (*RAM*) is different from the selected configuration profile in the non-volatile memory (*NVM*). To do this, perform the following steps:

- ☐ Verify the status bar at the top of the menu:
  - When a flashing  icon is visible, the configuration profiles differ.
  - When no  icon is visible, the configuration profiles match.

Or:

- ☐ Open the *Basic Settings > Load/Save* dialog.
- ☐ Verify the status of the checkbox in the *Information* frame:
  - When the checkbox is cleared, the configuration profiles differ.
  - When the checkbox is selected, the configuration profiles match.

```
show config status

Configuration Storage sync State
--------------------------------
running-config to NV.....................out of sync
...
```

External Memory (EAM) and Non-volatile Memory (NVM)

You can also recognize when the copy in the external memory (EAM) is different from the configuration profile in the non-volatile memory (*NVM*). To do this, perform the following steps:

- ☐ Open the *Basic Settings > Load/Save* dialog.
- ☐ Verify the status of the checkbox in the *Information* frame:
  - When the checkbox is cleared, the configuration profiles differ.
  - When the checkbox is selected, the configuration profiles match.

```
show config status

Configuration Storage sync State
--------------------------------
...
NV to EAM.................................out of sync
...
```

Saving the Settings

Saving the Configuration Profile in the Device

If you change the settings of the device during operation, then the device stores the changes in its memory (RAM). In order to keep the changes after a reboot, save the configuration profile in the non-volatile memory (*NVM*).

Saving a Configuration Profile

The device stores the settings in the selected configuration profile in the non-volatile memory (*NVM*).

Perform the following steps:

- ☐ Open the *Basic Settings > Load/Save* dialog.
- ☐ Verify that the required configuration profile is selected.
  You can recognize the selected configuration profile because the checkbox in the *Selected* column is selected.
- ☐ Click the  button.

`show config profiles nvm`	Displays the configuration profiles contained in the non-volatile memory (`nvm`).
`enable`	Change to the Privileged EXEC mode.
`save`	Save the settings in the non-volatile memory (`nvm`) in the selected configuration profile.

Copying Settings to a Configuration Profile

The device lets you store the settings saved in the memory (`RAM`) in a configuration profile other than the selected configuration profile. In this way you create a new configuration profile in the non-volatile memory (*`NVM`*) or overwrite an existing one.

Perform the following steps:

- ☐ Open the *Basic Settings > Load/Save* dialog.
- ☐ Click the  button and then the *Save As..* item.
  The dialog displays the *Save As..* window.
- ☐ In the *Name* field, change the name of the configuration profile. If you keep the proposed name, the device will overwrite an existing configuration profile of the same name.
- ☐ Click the *Ok* button.

The new configuration profile is selected.

`show config profiles nvm`	Displays the configuration profiles contained in the non-volatile memory (`nvm`).
`enable`	Change to the Privileged EXEC mode.
`copy config running-config nvm profile <string>`	Save the settings in the configuration profile named `<string>` in the non-volatile memory (`nvm`). If present, the device overwrites a configuration profile of the same name. The new configuration profile is selected.

Selecting a Configuration Profile

When the non-volatile memory (*NVM*) contains multiple configuration profiles, you have the option to select any configuration profile there. The device stores the settings in the selected configuration profile. Upon reboot, the device loads the settings of the selected configuration profile into the memory (RAM).

Perform the following steps:

- ☐ Open the *Basic Settings > Load/Save* dialog.

The table displays the configuration profiles present in the device. You can recognize the selected configuration profile because the checkbox in the *Selected* column is selected.

- ☐ In the table select the entry of the required configuration profile stored in the non-volatile memory (*NVM*).
- ☐ Click the ☰ button and then the *Select* item.

In the *Selected* column, the checkbox of the configuration profile is now selected.

`enable`	Change to the Privileged EXEC mode.
`show config profiles nvm`	Displays the configuration profiles contained in the non-volatile memory (`nvm`).
`configure`	Change to the Configuration mode.
`config profile select nvm 1`	Identifier of the configuration profile. Take note of the adjacent name of the configuration profile.
`save`	Save the settings in the non-volatile memory (`nvm`) in the selected configuration profile.

Saving the Configuration Profile in the External Memory

When an external memory is connected and you save a configuration profile, the device automatically saves a copy in the *Selected external memory*. In the default setting, the function is enabled. You can disable this function.

Perform the following steps:

- ☐ Open the *Basic Settings > External Memory* dialog.
- ☐ Select the checkbox in the *Backup config when saving* column in order to enable the device to automatically save a copy in the external memory during the saving process.
- ☐ To deactivate the function, clear the checkbox in the *Backup config when saving* column.
- ☐ Save the changes temporarily. To do this, click the ✓ button.

`enable`	Change to the Privileged EXEC mode.
`configure`	Change to the Configuration mode.
`config envm config-save usb`	Enable the function. When you save a configuration profile, the device saves a copy in the external memory. `usb` = External USB memory
`save`	Save the settings in the non-volatile memory (`nvm`) in the selected configuration profile.

Backup the Configuration Profile on a Remote Server

The device lets you automatically backup the configuration profile to a remote server. The prerequisite is that you activate the function before you save the configuration profile.

After you save the configuration profile in the non-volatile memory (*NVM*), the device sends a copy to the specified URL.

Perform the following steps:

- ☐ Open the *Basic Settings > Load/Save* dialog.
  In the *Backup config on a remote server when saving* frame, perform the following steps:
- ☐ In the *URL* field, specify the server as well as the path and file name of the backed up configuration profile.
- ☐ Click the *Set credentials* button.
  The dialog displays the *Credentials* window.
- ☐ Enter the login credentials needed to authenticate on the remote server.
- ☐ In the *Operation* option list, enable the function.
- ☐ Save the changes temporarily. To do this, click the ✓ button.

`enable`	Change to the Privileged EXEC mode.
`show config remote-backup`	Check status of the function.
`configure`	Change to the Configuration mode.
`config remote-backup destination`	Enter the destination URL for the configuration profile backup.
`config remote-backup username`	Enter the user name to authenticate on the remote server.
`config remote-backup password`	Enter the password to authenticate on the remote server.
`config remote-backup operation`	Enable the function.

If the transfer to the remote server is unsuccessful, then the device logs this event in the log file (System Log).

Exporting a Configuration Profile

The device lets you save a configuration profile to a server as an XML file. If you use the GUI, then you have the option to save the XML file directly to your PC.

Prerequisites:
- To save the file on a server, you need a configured server on the network.
- To save the file to an SCP or SFTP server, you also need the user name and password to access this server.

Perform the following steps:

- ☐ Open the *Basic Settings > Load/Save* dialog.
- ☐ In the table select the entry of the required configuration profile.

Export the configuration profile to your PC. To do this, perform the following steps:

- ☐ Click the link in the *Profile name* column.
- ☐ Select the storage location and specify the file name.
- ☐ Click the *Ok* button.

The configuration profile is now saved as an XML file in the specified location.

Export the configuration profile to a remote server. To do this, perform the following steps:

- ☐ Click the ☰ button and then the *Export...* item.
  The dialog displays the *Export...* window.
- ☐ In the *URL* field, specify the file URL on the remote server:
  - ☐ To save the file on an FTP server, specify the URL for the file in the following form:
    `ftp://<user>:<password>@<IP address>:<port>/<file name>`
  - ☐ To save the file on a TFTP server, specify the URL for the file in the following form:
    `tftp://<IP address>/<path>/<file name>`
  - ☐ To save the file on an SCP or SFTP server, specify the URL for the file in one of the following forms:
    `scp://` or `sftp://<user>:<password>@<IP address>/<path>/<file name>`
    `scp://` or `sftp://<IP address>/<path>/<file name>`
    When you click the *Ok* button, the device displays the *Credentials* window. There you enter *User name* and *Password* to log in to the server.
- ☐ Click the *Ok* button.
  The configuration profile is now saved as an XML file in the specified location.

`show config profiles nvm`	Displays the configuration profiles contained in the non-volatile memory (`nvm`).
`enable`	Change to the Privileged EXEC mode.
`copy config running-config remote tftp://<IP_address>/<path>/<file_name>`	Save the settings on a TFTP server.

`copy config nvm remote sftp://<user_name>:<password>@<IP_address>/<path>/<file_name>`	Save the selected configuration profile in the non-volatile memory (`nvm`) on a SFTP server.
`copy config nvm profile config3 remote tftp://<IP_address>/<path>/<file_name>`	Save the configuration profile `config3` in the non-volatile memory (`nvm`) on a TFTP server.
`copy config nvm profile config3 remote ftp://<IP_address>:<port>/<path>/<file_name>`	Save the configuration profile `config3` in the non-volatile memory (`nvm`) on an FTP server.

Loading Settings

If you save multiple configuration profiles in the memory, then you have the option to load a different configuration profile.

Activating a Configuration Profile

The non-volatile memory of the device can contain multiple configuration profiles. If you activate a configuration profile stored in the non-volatile memory (*NVM*), then you immediately change the settings in the device. The device does not require a reboot.

Perform the following steps:

- ☐ Open the *Basic Settings > Load/Save* dialog.
- ☐ In the table select the entry of the required configuration profile.
- ☐ Click the ☰ button and then the *Activate* item.

The device copies the settings to the memory (`RAM`) and disconnects from the GUI. The device immediately uses the settings of the configuration profile.

- ☐ Reload the GUI.
- ☐ Log in again.

In the *Selected* column, the checkbox of the configuration profile that was activated before is selected.

`show config profiles nvm`	Displays the configuration profiles contained in the non-volatile memory (`nvm`).
`enable`	Change to the Privileged EXEC mode.
`copy config nvm profile config3 running-config`	Activate the settings of the configuration profile `config3` in the non-volatile memory (`nvm`). The device copies the settings into the volatile memory and disconnects the connection to the CLI. The device immediately uses the settings of the configuration profile `config3`.

Loading the Configuration Profile from the External Memory

If an external memory is connected, then the device loads a configuration profile from the external memory upon restart automatically. The device lets you save these settings in a configuration profile in non-volatile memory.

When the external memory contains the configuration profile of an identical device, you have the possibility to transfer the settings from one device to another.

Perform the following steps:

☐ Verify that the device loads a configuration profile from the external memory upon restart.
In the default setting, the function is enabled. If the function is disabled, enable it again as follows:

☐ Open the *Basic Settings > External Memory* dialog.

☐ In the *Config priority* column, select the value `first`.

☐ Save the changes temporarily. To do this, click the ✓ button.

`enable`	Change to the Privileged EXEC mode.
`configure`	Change to the Configuration mode.
`config envm load-priority usb first`	Enable the function. Upon reboot, the device loads a configuration profile from the external memory. `usb` = External USB memory
`show config envm settings`	Displays the settings of the external memory (`envm`).

```
Type   Status      Auto Update Save Config Config Load Prio
------ ----------- ----------- ----------- ----------------
usb    ok          [x]         [x]         first
```

`save`	Save the settings in a configuration profile in the non-volatile memory (*`NVM`*) of the device.

Using the CLI, the device lets you copy the settings from the external memory directly into the non-volatile memory (*NVM*).

`show config profiles nvm`	Displays the configuration profiles contained in the non-volatile memory (`nvm`).
`enable`	Change to the Privileged EXEC mode.
`copy config envm profile config3 nvm`	Copy the configuration profile `config3` from the external memory (`envm`) to the non-volatile memory (`nvm`).

The device can also automatically load a configuration profile from a script file during the boot process.

Prerequisites:
- Verify that the external memory is connected before you start the device.
- The root directory of the external memory contains a text file `startup.txt` with the content `script=<file_name>`. The placeholder `<file_name>` represents the script file that the device executes during the boot process.
- The root directory of the external memory contains the script file. You have the option to save the script with a user-specified name. Save the file with the file extension `.cli`.

NOTE: Verify that the script saved in the external memory is not empty. If the script is empty, then the device loads the next configuration profile as per the configuration priority settings.

After applying the script, the device automatically saves the configuration profile from the script file as an XML file in the external memory. When you type the appropriate command into the script file, you have the option to disable this function:

☐ `no config envm config-save usb`
The device does not create a copy in the external USB memory.

When the script file contains an incorrect command, the device does not apply this command during the boot process. The device logs the event in the log file (System Log).

Importing a Configuration Profile

The device lets you import from a server a configuration profile saved as an XML file. If you use the GUI, then you can import the XML file directly from your PC.

Prerequisites:
- To save the file on a server, you need a configured server on the network.
- To save the file to an SCP or SFTP server, you also need the user name and password to access this server.

Perform the following steps:

- ☐ Open the *Basic Settings > Load/Save* dialog.
- ☐ Click the ☰ button and then the *Import...* item.
  The dialog displays the *Import...* window.
- ☐ In the *Select source* drop-down list, select the location from where the device imports the configuration profile.
  - *PC/URL*
    The device imports the configuration profile from the local PC or from a remote server.
  - *External memory*
    The device imports the configuration profile from the external memory.

Import the configuration profile from the local PC or from a remote server. To do this, perform the following steps:

- ☐ Import the configuration profile:
  - ☐ When the file is located on an FTP server, specify the URL for the file in the following form:
    `ftp://<user>:<password>@<IP address>:<port>/<file name>`
  - ☐ When the file is located on a TFTP server, specify the URL for the file in the following form:
    `tftp://<IP address>/<path>/<file name>`
  - ☐ When the file is located on an SCP or SFTP server, specify the URL for the file in one of the following forms:
    `scp://` or `sftp://<IP address>/<path>/<file name>`
    When you click the *Start* button, the device displays the *Credentials* window. There you enter *User name* and *Password* to log in to the server.
    `scp://` or `sftp://<user>:<password>@<IP address>/<path>/<file name>`
- ☐ In the *Destination* frame, specify where the device saves the imported configuration profile:
  - ☐ In the *Profile name* field, specify the name under which the device saves the configuration profile.
  - ☐ In the *Storage type* field, specify the storage location for the configuration profile.
- ☐ Click the *Ok* button.

The device copies the configuration profile into the specified memory.

If you specified the value `ram` in the *Destination* frame, then the device disconnects the GUI and uses the settings immediately.

Import the configuration profile from the external memory. To do this, perform the following steps:

- ☐ In the *Import profile from external memory* frame, *Profile name* drop-down list, select the name of the configuration profile to be imported.
  The prerequisite is that the external memory contains an exported configuration profile.

- ☐ In the *Destination* frame, specify where the device saves the imported configuration profile:
  - ☐ In the *Profile name* field, specify the name under which the device saves the configuration profile.
- ☐ Click the *Ok* button.

The device copies the configuration profile into the non-volatile memory (*NVM*) of the device.

If you specified the value `ram` in the *Destination* frame, then the device disconnects the GUI and uses the settings immediately.

`enable`	Change to the Privileged EXEC mode.
`copy config remote ftp://<IP_address>:<port>/<path>/<file_name> running-config`	Import and activate the settings of a configuration profile saved on an FTP server. The device copies the settings into the volatile memory and disconnects the connection to the CLI. The device immediately uses the settings of the imported configuration profile.
`copy config remote tftp://<IP_address>/ <path>/<file_name> running-config`	Import and activate the settings of a configuration profile saved on a TFTP server. The device copies the settings into the volatile memory and disconnects the connection to the CLI. The device immediately uses the settings of the imported configuration profile.
`copy config remote sftp://<user name>:<password>@<IP_address>/<path>/<file_name> running-config`	Import and activate the settings of a configuration profile saved on a SFTP server. The device copies the settings into the volatile memory and disconnects the connection to the CLI. The device immediately uses the settings of the imported configuration profile.
`copy config remote ftp://<IP_address>:<port>/<path>/<file_name> nvm profile config3`	Import the settings of a configuration profile saved on an FTP server and save the settings in the configuration profile `config3` in the non-volatile memory (`nvm`).
`copy config remote tftp://<IP_address>/<path>/<file_name> nvm profile config3`	Import the settings of a configuration profile saved on a TFTP server and save the settings in the configuration profile `config3` in the non-volatile memory (`nvm`).

Reset the Device to the Factory Defaults

If you reset the settings in the device to the delivery state, then the device deletes the configuration profiles in the volatile memory and in the non-volatile memory.

If an external memory is connected, then the device also deletes the configuration profiles saved in the external memory.

The device then reboots and loads the factory settings.

Using the GUI or CLI

Perform the following steps:

- ☐ Open the *Basic Settings > Load/Save* dialog.
- ☐ Click the button, then *Back to factory...*.
  The dialog displays a message.
- ☐ Click the *Ok* button.

The device deletes the configuration profiles in the memory (`RAM`) and in the non-volatile memory (*`NVM`*).

If an external memory is connected, then the device also deletes the configuration profiles saved in the external memory.

After a brief period, the device restarts and loads the delivery settings.

`enable`	Change to the Privileged EXEC mode.
`clear factory`	Deletes the configuration profiles from the non-volatile memory and from the external memory. If an external memory is connected, then the device also deletes the configuration profiles saved in the external memory. After a brief period, the device restarts and loads the delivery settings.

Using the System Monitor

Prerequisite:

- Your PC is connected with the serial connection of the device using a terminal cable.

Perform the following steps:

- ☐ Restart the device.
- ☐ To change to the System Monitor, press the **1** key within 3 seconds when prompted during reboot.
  The device loads the System Monitor.

- ☐ To change from the main menu to the `Manage configurations` menu, press the **4** key.
- ☐ To execute the `Clear configs and boot params` command, press the **1** key.
- ☐ To load the factory settings, press the **Enter** key.
  The device deletes the configuration profiles in the memory (`RAM`) and in the non-volatile memory (*`NVM`*).
  If an external memory is connected, then the device also deletes the configuration profiles saved in the external memory.
- ☐ To change to the main menu, press the **q** key.
- ☐ To reboot the device with factory settings, press the **q** key.

Loading Software Updates

Schneider Electric is continually working on improving and developing their software. Verify regularly if there is an updated version of the software. You can find information and software downloads on the Schneider Electric product pages on the Internet at www.se.com.

The device gives you the following options for updating the device software:
- Software Update from the PC
- Software Update from a Server
- Software Update from the External Memory
- Loading a Previous Software Version

NOTE: The device settings are kept after updating the device software.

You can see the version of the installed device software in the login dialog of the GUI.

To display the version of the installed software when you are already logged in, perform the following steps:

☐ Open the *Basic Settings > Software* dialog.
The *Running version* field displays the version number and creation date of the device software that the device loaded during the last restart and is running.

`enable`	Change to the Privileged EXEC mode.
`show system info`	Displays the system information such as the version number and creation date of the device software that the device loaded during the last restart and is running.

Software Update from the PC

The prerequisite is that the image file of the device software is saved on a data carrier which is accessible from your PC.

Perform the following steps:

☐ Navigate to the folder where the image file of the device software is saved.
☐ Open the *Basic Settings > Software* dialog.
☐ Drag and drop the image file in the  area. Alternatively click in the area to select the file.
☐ To start the update procedure, click the *Start* button.
As soon as the update procedure is completed successfully, the device displays an information that the software is successfully updated.
Upon restart, the device loads the installed device software.

Software Update from a Server

To update the software using SFTP or SCP you need a server on which the image file of the device software is saved.

To update the software using TFTP, SFTP or SCP you need a server on which the image file of the device software is saved.

Perform the following steps:

- ☐ Open the *Basic Settings > Software* dialog.
- ☐ In the *Software update* frame, *URL* field, enter the URL for the image file in the following form:
  - ▶ When the image file is saved on an FTP server:
    `ftp://<IP_address>:<port>/<path>/<image_file_name>.bin`
  - ▶ When the image file is saved on a TFTP server:
    `tftp://<IP_address>/<path>/<image_file_name>.bin`
  - ▶ When the image file is saved on a SCP or SFTP server:
    `scp://` or `sftp://<IP_address>/<path>/<image_file_name>.bin`
    `scp://` or `sftp://<username>:<password>@<IP_address>/<path>/<image_file_name>.bin`
    When you enter the URL without the user name and password, the device displays the *Credentials* window. There you enter the login credentials needed to log in to the server.
- ☐ To start the update procedure, click the *Start* button.
  The device copies the running device software into the backup memory. As soon as the update procedure is completed successfully, the device displays an information that the software is successfully updated. Upon restart, the device loads the installed device software.

`enable`	Change to the Privileged EXEC mode.
`copy firmware remote tftp://10.0.1.159/product.bin system`	Transfer the `product.bin` file from the TFTP server with the IP address `10.0.1.159` to the device.

Software Update from the External Memory

Manually—initiated by the Administrator

The device lets you update the device software. The prerequisite is that the image file of the device software is located in the external memory.

Perform the following steps:

- ☐ Open the *Basic Settings > Software* dialog.
- ☐ In the table mark the row which displays the name of the desired image file in the external memory.
- ☐ Right-click to display the context menu.
- ☐ To start the update procedure, click in the context menu the *Update* item. The device copies the running device software into the backup memory. As soon as the update procedure is completed successfully, the device displays an information that the software is successfully updated. Upon restart, the device loads the installed device software.

Automatically—initiated by the Device

When the following files are located in the external memory during a restart, the device updates the device software automatically:

- ▶ the image file of the device software
- ▶ a text file `startup.txt` with the content

```
autoUpdate=<Image_file_name>.bin
```

The prerequisite is that in the *Basic Settings > External Memory* dialog, you select the checkbox in the *Software auto update* column. This is the default setting in the device.

Perform the following steps:

- ☐ Copy the image file of the new device software into the main directory of the external memory. Use only an image file suitable for the device.
- ☐ Create a text file `startup.txt` in the main directory of the external memory.
- ☐ Open the `startup.txt` file in the text editor and add the following line:

```
autoUpdate=<Image_file_name>.bin
```

- ☐ Install the external memory in the device.

☐ Restart the device.
During the booting process, the device verifies automatically the following criteria:
- Is an external memory connected?
- Is a `startup.txt` file in the main directory of the external memory?
- Does the image file exist which is specified in the `startup.txt` file?
- Is the software version of the image file more recent than the software running in the device?

When the criteria are fulfilled, the device starts the update procedure.
The device copies the running device software into the backup memory.
As soon as the update procedure is completed successfully, the device reboots automatically and loads the new software version.

☐ Verify the result of the update procedure. The log file in the *Diagnostics > Report >* System Log dialog contains one of the following messages:
- `S_watson_AUTOMATIC_SWUPDATE_SUCCESS`
  Software update completed successfully
- `S_watson_AUTOMATIC_SWUPDATE_ABORTED`
  Software update aborted
- `S_watson_AUTOMATIC_SWUPDATE_ABORTED_WRONG_FILE`
  Software update aborted due to incorrect image file
- `S_watson_AUTOMATIC_SWUPDATE_ABORTED_SAVING_FILE`
  Software update aborted because the device did not save the image file.

Loading a Previous Software Version

The device lets you replace the device software with a previous version. The basic settings in the device are kept after replacing the device software.

NOTE: Only the settings for functions which are available in the newer device software version are lost.

Configuring the Ports

The following port configuration functions are available.

- Enabling/disabling the port
- Selecting the operating mode

Enabling/Disabling the Port

In the default setting, every port is enabled. For a higher level of access security, disable unconnected ports. To do this, perform the following steps:

- ☐ Open the *Basic Settings > Port* dialog, *Configuration* tab.
- ☐ To enable a port, select the checkbox in the *Port on* column.
- ☐ To disable a port, clear the checkbox in the *Port on* column.
- ☐ Save the changes temporarily. To do this, click the ✓ button.

`enable`	Change to the Privileged EXEC mode.
`configure`	Change to the Configuration mode.
`interface 1/1`	Change to the interface configuration mode of interface `1/1`.
`no shutdown`	Enable the interface.

Selecting the Operating Mode

In the default setting, the ports are set to *Automatic configuration* operating mode.

NOTE: The active automatic configuration has priority over the manual configuration.

Perform the following steps:

- ☐ Open the *Basic Settings > Port* dialog, *Configuration* tab.
- ☐ If the device connected to this port requires a fixed setting, then perform the following steps:
  - ☐ Deactivate the function. Clear the checkbox in the *Automatic configuration* column.
  - ☐ In the *Manual configuration* column, enter the desired operating mode (transmission rate, duplex mode).
- ☐ Save the changes temporarily. To do this, click the ✓ button.

`enable`	Change to the Privileged EXEC mode.
`configure`	Change to the Configuration mode.
`interface 1/1`	Change to the interface configuration mode of interface `1/1`.
`no auto-negotiate`	Disable the automatic configuration mode.
`speed 100 full`	Port speed 100 Mbit/s, full duplex

Assistance in the Protection from Unauthorized Access

The device offers functions that help you protect the device against unauthorized access.

After you set up the device, carry out the following steps in order to reduce possible unauthorized access to the device.

- Changing the SNMPv1/v2 community
- Disabling SNMPv1/v2
- Disabling HTTP
- Using your own HTTPS certificate
- Using your own SSH key
- Disabling Telnet
- Disabling Ethernet Switch Configurator
- Enable IP access restriction
- Adjusting the session timeouts

Changing the SNMPv1/v2 Community

SNMPv1/v2 works unencrypted. Every SNMP packet contains the IP address of the sender and the plaintext community name with which the sender accesses the device. If SNMPv1/v2 is enabled, then the device lets anyone who knows the community name access the device.

The community names `user` for read accesses and `admin` for write accesses are preset. If you are using SNMPv1 or SNMPv2, then change the default community name. Treat the community names with discretion. To do this, perform the following steps:

- ☐ Open the *Device Security > Management Access > SNMPv1/v2 Community* dialog.

  The dialog displays the communities that are set up.
- ☐ For the `Write` community, specify in the *Name* column the community name.
  - Up to 32 alphanumeric characters are allowed.
  - The device differentiates between upper and lower case.
  - Specify a different community name than for read access.
- ☐ Save the changes temporarily. To do this, click the ✓ button.

`enable`	Change to the Privileged EXEC mode.
`configure`	Change to the Configuration mode.

`snmp community rw <community name>`	Specify the community for read/write access.
`show snmp community`	Display the communities that have been configured.
`save`	Save the settings in the non-volatile memory (`nvm`) in the selected configuration profile.

Disabling SNMPv1/v2

If you need SNMPv1 or SNMPv2, then use these protocols only in environments protected from eavesdropping. SNMPv1 and SNMPv2 do not use encryption. The SNMP packets contain the community in clear text. Use, if possible, SNMPv3 in the device and disable the access using SNMPv1 and SNMPv2. To do this, perform the following steps:

- ☐ Open the *Device Security > Management Access > Server* dialog, *SNMP* tab.

The dialog displays the settings of the SNMP server.

- ☐ To deactivate the SNMPv1 protocol, you clear the *SNMPv1* checkbox.
- ☐ To deactivate the SNMPv2 protocol, you clear the *SNMPv2* checkbox.
- ☐ Save the changes temporarily. To do this, click the ✓ button.

`enable`	Change to the Privileged EXEC mode.
`configure`	Change to the Configuration mode.
`no snmp access version v1`	Deactivate the SNMPv1 protocol.
`no snmp access version v2`	Deactivate the SNMPv2 protocol.
`show snmp access`	Display the SNMP server settings.
`save`	Save the settings in the non-volatile memory (`nvm`) in the selected configuration profile.

Disabling HTTP

The web server provides the GUI with the protocol HTTP or HTTPS. HTTPS connections are encrypted, while HTTP connections are unencrypted.

The HTTP protocol is enabled by default. If you disable HTTP, then no unencrypted access to the GUI is possible. To do this, perform the following steps:

- ☐ Open the *Device Security > Management Access > Server* dialog, *HTTP* tab.
- ☐ To disable the HTTP protocol, select the *Off* radio button in the *Operation* frame.
- ☐ Save the changes temporarily. To do this, click the ✓ button.

`enable`	Change to the Privileged EXEC mode.
`configure`	Change to the Configuration mode.
`no http server`	Disable the HTTP protocol.

If the HTTP protocol is disabled, then you can reach the GUI of the device only by HTTPS. In the address bar of the web browser, enter the string `https://` before the IP address of the device.

If the HTTPS protocol is disabled and you also disable HTTP, then the GUI is unaccessible. To work with the GUI, enable the HTTPS server using the CLI. To do this, perform the following steps:

`enable`	Change to the Privileged EXEC mode.
`configure`	Change to the Configuration mode.
`https server`	Enable the HTTPS protocol.

Disabling Telnet

The device lets you remotely access the device management using Telnet or SSH. Telnet connections are unencrypted, while SSH connections are encrypted.

The Telnet server is enabled in the device by default. If you disable Telnet, then unencrypted remote access to the CLI is no longer possible. To do this, perform the following steps:

- ☐ Open the *Device Security > Management Access > Server* dialog, *Telnet* tab.
- ☐ To disable the Telnet server, select the *Off* radio button in the *Operation* frame.
- ☐ Save the changes temporarily. To do this, click the ✓ button.

`enable`	Change to the Privileged EXEC mode.
`configure`	Change to the Configuration mode.
`no telnet server`	Disable the Telnet server.

If the SSH server is disabled and you also disable Telnet, then access to the CLI is only possible through the serial interface of the device. To work remotely with the CLI, enable SSH. To do this, perform the following steps:

- ☐ Open the *Device Security > Management Access > Server* dialog, *SSH* tab.
- ☐ To enable the *SSH* server, select the *On* radio button in the *Operation* frame.
- ☐ Save the changes temporarily. To do this, click the ✓ button.

`enable`	Change to the Privileged EXEC mode.
`configure`	Change to the Configuration mode.
`ssh server`	Enable the SSH server.

Disabling the Ethernet Switch Configurator Access

Ethernet Switch Configurator lets you assign IP parameters to the device over the network during commissioning. Ethernet Switch Configurator communicates in the device management VLAN without encryption and authentication.

After the device is commissioned, set Ethernet Switch Configurator to read-only or disable Ethernet Switch Configurator access completely. To do this, perform the following steps:

- ☐ Open the *Basic Settings > Network* dialog.
- ☐ To take away write permission from the Ethernet Switch Configurator software, in the *Ethernet Switch Configurator protocol v1/v2* frame, specify the value `readOnly` in the *Access* field.
- ☐ To disable Ethernet Switch Configurator access completely, select the *Off* radio button in the *Ethernet Switch Configurator protocol v1/v2* frame.
- ☐ Save the changes temporarily. To do this, click the ✓ button.

`enable`	Change to the Privileged EXEC mode.
`network ethernet-switch-conf mode read-only`	Disable write permission of the Ethernet Switch Configurator software.
`no network ethernet-switch-conf operation`	Disable Ethernet Switch Configurator access.

Activating the IP Access Restriction

In the default setting, you access the device management from any IP address and with the supported protocols.

The IP access restriction lets you restrict access to the device management to selected IP address ranges and selected IP-based protocols.

Example:

The device is to be accessible only from the company network using the GUI. The administrator has additional remote access using SSH. The company network has the address range `192.168.1.0/24` and remote access from a mobile network with the IP address range `109.237.176.0/24`. The SSH application program has the fingerprint of the RSA key.

Parameter	Company Network	Mobile Phone Network
Network address	`192.168.1.0`	`109.237.176.0`
Netmask	`24`	`24`
Desired protocols	https, snmp	ssh

Perform the following steps:

- ☐ Open the *Device Security > Management Access > IP Access Restriction* dialog.
- ☐ Clear the checkbox in the *Active* column for the entry.
  This entry lets users have access to the device from any IP address and the supported protocols.

Address range of the company network:

- ☐ To add a table entry, click the button.
- ☐ Specify the address range of the company network in the *IP address range* column: `192.168.1.0/24`
- ☐ For the address range of the corporate network, deactivate the undesired protocols. The *HTTPS*, *SNMP*, and *Active* checkboxes remain selected.

Address range of the mobile phone network:

- ☐ To add a table entry, click the button.
- ☐ Specify the address range of the mobile network in the *IP address range* column: `109.237.176.0/24`
- ☐ For the address range of the mobile network, deactivate the undesired protocols. The *SSH* and *Active* checkboxes remain selected.

Before you enable the function, verify that at least one active entry in the table lets you have access. Otherwise, if you change the settings, then the connection to the device terminates. Access to the device management is only possible using the CLI through the serial interface of the device.

- ☐ To enable IP access restriction, select the `On` radio button in the *Operation* frame.
- ☐ Save the changes temporarily. To do this, click the button.

`enable`	Change to the Privileged EXEC mode.
`show network management access global`	Displays if IP access restriction is enabled or disabled.
`show network management access rules`	Display the entries that have been configured.
`no network management access operation`	Disable the IP access restriction.
`network management access add 2`	Create the entry for the address range of the company network. Number of the next available index in this example: `2`.
`network management access modify 2 ip 192.168.1.0`	Specify the IP address of the company network.
`network management access modify 2 mask 24`	Specify the netmask of the company network.
`network management access modify 2 ssh disable`	Deactivate SSH for the address range of the company network. Repeat the operation for every unwanted protocol.
`network management access add 3`	Create an entry for the address range of the mobile phone network. Number of the next available index in this example: `3`.
`network management access modify 3 ip 109.237.176.0`	Specify the IP address of the mobile phone network.
`network management access modify 3 mask 24`	Specify the netmask of the mobile phone network.
`network management access modify 3 snmp disable`	Deactivate SNMP for the address range of the mobile phone network. Repeat the operation for every unwanted protocol.
`no network management access status 1`	Deactivate the default entry. This entry lets users have access to the device from any IP address and the supported protocols.
`network management access status 2`	Activate an entry for the address range of the company network.
`network management access status 3`	Activate an entry for the address range of the mobile phone network.
`show network management access rules`	Display the entries that have been configured.
`network management access operation`	Enable the IP access restriction.

Adjusting the Session Timeouts

The device lets you automatically terminate the session upon inactivity of the logged-on user. The session timeout is the period of inactivity after the last user action.

You can specify a session timeout for the following applications:
- CLI sessions using an SSH connection
- CLI sessions using a Telnet connection
- CLI sessions using a serial connection
- GUI

Timeout for CLI Sessions using a SSH Connection

Perform the following steps:

- ☐ Open the *Device Security > Management Access > Server* dialog, *SSH* tab.
- ☐ Specify the timeout period in minutes in the *Configuration* frame, *Session timeout [min]* field.
- ☐ Save the changes temporarily. To do this, click the ✓ button.

`enable`	Change to the Privileged EXEC mode.
`configure`	Change to the Configuration mode.
`ssh timeout <0..160>`	Specify the timeout period in minutes for CLI sessions using an SSH connection.

Timeout for CLI Sessions using a Telnet Connection

Perform the following steps:

- ☐ Open the *Device Security > Management Access > Server* dialog, *Telnet* tab.
- ☐ Specify the timeout period in minutes in the *Configuration* frame, *Session timeout [min]* field.
- ☐ Save the changes temporarily. To do this, click the ✓ button.

`enable`	Change to the Privileged EXEC mode.
`configure`	Change to the Configuration mode.
`telnet timeout <0..160>`	Specify the timeout period in minutes for CLI sessions using a Telnet connection.

Timeout for CLI Sessions using a Serial Connection

Perform the following steps:

- ☐ Open the *Device Security > Management Access > CLI* dialog, *Global* tab.
- ☐ Specify the timeout period in minutes in the *Configuration* frame, *V.24 timeout [min]* field.
- ☐ Save the changes temporarily. To do this, click the ✓ button.

`enable`	Change to the Privileged EXEC mode.
`cli serial-timeout <0..160>`	Specify the timeout period in minutes for CLI sessions using a serial connection.

Session Timeout for the GUI

Perform the following steps:

- ☐ Open the *Device Security > Management Access > Web* dialog.
- ☐ Specify the timeout period in minutes in the *Configuration* frame, *Web interface session timeout [min]* field.
- ☐ Save the changes temporarily. To do this, click the ✓ button.

`enable`	Change to the Privileged EXEC mode.
`network management access web timeout <0..160>`	Specify the timeout period in minutes for GUI sessions

Controlling the Data Traffic

The device verifies the data packets to be forwarded in accordance with defined rules. Data packets to which the rules apply are either forwarded by the device or blocked. If data packets do not correspond to any of the rules, then the device blocks the packets.

Routing ports to which no rules are assigned allow packets to pass through. As soon as a rule is assigned, the assigned rules are processed first. After that, the specified standard action of the device takes effect.

The device provides the following functions for controlling the data stream:
- Service request control (Denial of Service, DoS)

The device observes and monitors the data stream. The device takes the results of the observation and the monitoring and combines them with the rules for the network security to create a status table. Based on this status table, the device determines whether to accept, drop or reject data.

Helping Protect against Unauthorized Access

With this function, the device supports you in helping protect against invalid or falsified data packets targeted at certain services or devices. You have the option of specifying filters in order to help restrict data stream for protection against denial-of-service attacks. The activated filters verify incoming data packets and discard them as soon as a match with the filter criteria is found.

The *Network Security > DoS > Global* dialog contains 2 frames in which you activate different filters. To activate them, select the corresponding checkboxes.

In the *TCP/UDP* frame, you activate up to 4 filters that only influence TCP and UDP packets. Using this filter, you deactivate port scans, which attackers use to try to recognize devices and services offered. The filters operate as follows:

Filter	Action
Activate Null Scan Filter	The device detects and discards incoming TCP packets with the following properties: - No TCP flags are set. - The TCP sequence number is 0.
Activate Xmas Filter	The device detects and discards incoming TCP packets with the following properties: - The TCP flags *FIN*, *URG* and *PSH* are simultaneously set. - The TCP sequence number is 0.
Activate SYN/FIN Filter	The device detects and discards incoming TCP packets in which the TCP flags *SYN* and *FIN* are simultaneously set.
Activate Minimal Header Filter	The device detects and discards incoming TCP packets in which the TCP header is too short.

The *ICMP* frame offers you 2 filter options for ICMP packets. Fragmentation of incoming ICMP packets is a sign of an attack. If you activate this filter, then the device detects fragmented ICMP packets and discards them. Using the *Allowed payload size [byte]* parameter, you can also specify the maximum permissible size of the payload of the ICMP packets. The device discards data packets that exceed this byte specification.

NOTE: You can combine the filters in any way in the *Network Security > DoS > Global* dialog. When several filters are selected, a logical Or applies: If the first or second (or the third, etc.) filter applies to a data packet, then the device discards it.

Network Load Control

The device features a number of functions that can help you reduce the network load:

- Direct packet distribution
- Multicasts
- Rate limiter
- Prioritization - QoS
- Flow control

Direct Packet Distribution

The device reduces the network load with direct packet distribution.

On each of its ports, the device learns the sender MAC address of received data packets. The device stores the combination of port and MAC address in its MAC address table (FDB).

By applying the “Store and Forward” method, the device buffers data received and verifies it for validity before forwarding it. The device rejects invalid and erroneous data packets.

Learning MAC Addresses

When the device receives a data packet, it verifies if the MAC address of the sender is already stored in the MAC address table (FDB). When the MAC address of the sender is unknown, the device generates a new entry. The device then compares the destination MAC address of the data packet with the entries stored in the MAC address table (FDB):

- The device forwards packets with a known destination MAC address directly to ports that have already received data packets from this MAC address.
- The device floods data packets with unknown destination addresses, that is, the device forwards these data packets to every port.

Aging of Learned MAC Addresses

Addresses that have not been detected by the device for an adjustable period of time (aging time) are deleted from the MAC address table (FDB) by the device. A reboot or resetting of the MAC address table deletes the entries in the MAC address table (FDB).

Static Address Entries

In addition to learning the sender MAC address, the device also provides the option to set MAC addresses manually. These MAC addresses remain configured and persist through resetting of the MAC address table (FDB) as well as rebooting of the device.

Static address entries allow the device to forward data packets directly to selected ports. If you do not specify a destination port, then the device discards the corresponding data packets.

You manage the static address entries in the GUI or in the CLI.

Perform the following steps:

☐ Create a static address entry.

☐ Open the *Switching > Filter for MAC Addresses* dialog.

☐ Add a user-configurable MAC address:

- ▶ Click the button.
  The dialog displays the *Create* window.
- ▶ In the *Address* field, specify the destination MAC address.
- ▶ In the *VLAN ID* field, specify the ID of the VLAN.
- ▶ In the *Port* list, select the ports to which the device forwards data packets with the specified destination MAC address in the specified VLAN.
  When you have defined a Unicast MAC address in the *Address* field, select only one port.
  When you have defined a Multicast MAC address in the *Address* field, select one or more ports.
  If you want the device to discard data packets with the destination MAC address, then do not select any port.
- ▶ Click the *Ok* button.

☐ Save the changes temporarily. To do this, click the button.

`enable`	Change to the Privileged EXEC mode.
`configure`	Change to the Configuration mode.
`mac-filter <MAC address> <VLAN ID>`	Create the MAC address filter, consisting of a MAC address and VLAN ID.
`interface 1/1`	Change to the interface configuration mode of interface `1/1`.
`mac-filter <MAC address> <VLAN ID>`	Assign the port to a previously created MAC address filter.
`save`	Save the settings in the non-volatile memory (`nvm`) in the selected configuration profile.

☐ Convert a learned MAC address into a static address entry.

☐ Open the *Switching > Filter for MAC Addresses* dialog.

☐ To convert a learned MAC address into a static address entry, select the value `permanent` in the *Status* column.

☐ Save the changes temporarily. To do this, click the ✔ button.

☐ Disable a static address entry.

☐ Open the *Switching > Filter for MAC Addresses* dialog.

☐ To disable a static address entry, select the value `invalid` in the *Status* column.

☐ Save the changes temporarily. To do this, click the ✔ button.

`enable`	Change to the Privileged EXEC mode.
`configure`	Change to the Configuration mode.
`interface 1/1`	Change to the interface configuration mode of interface `1/1`.
`no mac-filter <MAC address> <VLAN ID>`	Cancel the assignment of the MAC address filter on the port.
`exit`	Change to the Configuration mode.
`no mac-filter <MAC address> <VLAN ID>`	Deleting the MAC address filter, consisting of a MAC address and VLAN ID.
`exit`	Change to the Privileged EXEC mode.
`save`	Save the settings in the non-volatile memory (`nvm`) in the selected configuration profile.

☐ Delete learned MAC addresses.

☐ To delete the learned addresses from the MAC address table (FDB), open the *Basic Settings > Restart* dialog and click the *Reset MAC address table* button.

`clear mac-addr-table` Delete the learned MAC addresses from the MAC address table (FDB).

Multicasts

By default, the device floods data packets with a Multicast address, that is, the device forwards the data packets to every port. This leads to an increased network load.

The use of IGMP snooping can reduce the network load caused by Multicast data traffic. IGMP snooping lets the device send Multicast data packets only on those ports to which devices that are a member in the Multicast group are connected.

Example of a Multicast Application

Surveillance cameras transmit images to monitors in the machine room and in the monitoring room. With an IP Multicast transmission, the cameras transmit their graphic data over the network in Multicast packets.

The Internet Group Management Protocol (IGMP) organizes the Multicast data traffic between the Multicast routers and the monitors. The switches in the network between the Multicast routers and the monitors monitor the IGMP data traffic continuously (“IGMP Snooping”).

Switches register logins for receiving a Multicast stream (IGMP report). The device then creates an entry in the MAC address table (FDB) and forwards Multicast packets only to the ports on which it has previously received IGMP reports.

IGMP Snooping

The Internet Group Management Protocol (IGMP) describes the distribution of Multicast information between routers and connected receivers on Layer 3. IGMP Snooping describes the function of a switch of continuously monitoring IGMP traffic and optimizing its own transmission settings for this data traffic.

The *IGMP Snooping* function in the device operates according to RFC 4541 (Considerations for Internet Group Management Protocol (IGMP) and Multicast Listener Discovery (MLD) Snooping Switches).

Multicast routers with an active *IGMP* function periodically request (query) registration of Multicast streams in order to determine the associated IP Multicast group members. IP Multicast group members reply with a Report message. This Report message contains the parameters required by the *IGMP* function. The Multicast router enters the IP Multicast group address from the Report message in its routing table. This causes it to forward data packets with this IP Multicast group in the destination address field according to its routing table.

When leaving a Multicast group (IGMP version 2 and greater), receivers log out with a “Leave” message and do not send any more Report messages. If it does not receive any more Report messages from this receiver within a certain time (aging time), then the Multicast router removes the routing table entry of a receiver.

When several IGMP Multicast routers are in the same network, the device with the smaller IP address takes over the query function. When there are no Multicast routers on the network, you have the option to enable the query function in an appropriately equipped switch.

A switch that connects one Multicast receiver with a Multicast router analyzes the IGMP information with the IGMP snooping method.

The IGMP snooping method also makes it possible for switches to use the *IGMP* function. A switch stores the MAC addresses derived from IP addresses of the Multicast receivers as recognized Multicast addresses in its MAC address table (FDB). In addition, the switch identifies the ports on which it has received reports for a specific Multicast address. In this way, the switch forwards Multicast packets only to ports to which Multicast receivers are connected. The other ports do not receive these packets.

A special feature of the device is the possibility of determining the processing of data packets with unknown Multicast addresses. Depending on the setting, the device discards these data packets or forwards them to every port. By default, the device transmits the data packets only to ports with connected devices, which in turn receive query packets. You also have the option of additionally sending known Multicast packets to query ports.

Setting IGMP Snooping

Perform the following steps:

- ☐ Open the *Switching > IGMP Snooping > Global* dialog.
- ☐ To enable the function, select the `On` radio button in the *Operation* frame.

When the *IGMP Snooping* function is disabled, the device behaves as follows:
- ▶ The device ignores the received query and report messages.
- ▶ The device forwards (floods) received data packets with a Multicast address as the destination address to every port.

- ☐ Save the changes temporarily. To do this, click the ✔ button.

☐ Specifying the settings for a port:

- ☐ Open the *Switching > IGMP Snooping > Configuration* dialog, *Port* tab.
- ☐ To activate the *IGMP Snooping* function on a port, select the checkbox in the *Active* column for the relevant port.
- ☐ Save the changes temporarily. To do this, click the ✔ button.

☐ Specifying the settings for a VLAN:

- ☐ Open the *Switching > IGMP Snooping > Configuration* dialog, *VLAN ID* tab.
- ☐ To activate the *IGMP Snooping* function for a specific VLAN, select the checkbox in the *Active* column for the relevant VLAN.
- ☐ Save the changes temporarily. To do this, click the ✔ button.

Setting the IGMP Querier Function

The device optionally sends active query messages; alternatively, it responds to query messages or detects other Multicast queriers in the network (*IGMP Snooping Querier* function).

Prerequisite:

The *IGMP Snooping* function is enabled globally.

Perform the following steps:

- ☐ Open the *Switching > IGMP Snooping > Querier* dialog.
- ☐ In the *Operation* frame, enable/disable the *IGMP Snooping Querier* function of the device globally.
- ☐ To activate the *IGMP Snooping Querier* function for a specific VLAN, select the checkbox in the *Active* column for the relevant VLAN.

- The device carries out a selection process: When the IP source address of the other Multicast querier is lower than its own, the device switches to the passive state, in which it does not send out any more query requests.
- In the *Address* column, you specify the IP Multicast address that the device inserts as the sender address in generated query requests. You use the address of the Multicast router.

☐ Save the changes temporarily. To do this, click the button.

IGMP Snooping Enhancements (table)

The *Switching > IGMP Snooping > Snooping Enhancements* dialog provides you access to enhanced settings for the *IGMP Snooping* function. You activate or deactivate the settings on a per port basis in a VLAN.

The following settings are possible:

- `Static`
  Use this setting to set the port as a static query port. The device forwards every IGMP message on a static query port, even if it has previously received no IGMP query messages on this port. When the static option is disabled and the device has previously received IGMP query messages, it forwards IGMP messages on this port. When this is the case, the entry displays `L` (“learned”).
- `Learn by LLDP`
  A port with this setting automatically discovers other Schneider Electric devices using LLDP (Link Layer Discovery Protocol). The device then learns the IGMP query status of this port from these Schneider Electric devices and configures the *IGMP Snooping Querier* function accordingly. The `ALA` entry indicates that the `Learn by LLDP` function is activated. When the device has found another Schneider Electric device on this port in this VLAN, the entry also displays an `A` (“automatic”).
- `Forward All`
  With this setting, the device forwards the data packets addressed to a Multicast address to this port. The setting is suitable in the following situations, for example:
  – For diagnostic purposes.
  – For devices in an MRP ring: After the ring is switched, the `Forward All` function makes it possible to reconfigure the network rapidly for data packets with registered Multicast destination addresses. Activate the `Forward All` function on every ring port.

Prerequisite:

The *IGMP Snooping* function is enabled globally.

Perform the following steps:

☐ Open the *Switching > IGMP Snooping > Snooping Enhancements* dialog.
☐ Double-click the desired port in the desired VLAN.
☐ To activate one or more functions, select the corresponding options.
☐ Click the *Ok* button.
☐ Save the changes temporarily. To do this, click the button.

`enable`	Change to the Privileged EXEC mode.
`vlan database`	Change to the VLAN configuration mode.
`igmp-snooping vlan-id 1 forward-all 1/1`	Activate the `Forward All` function for port `1/1` in VLAN `1`.

Configure Multicasts

The device lets you configure the exchange of Multicast data packets. The device provides different options depending on whether the data packets are to be sent to unknown or known Multicast receivers.

The settings for unknown Multicast addresses are global for the entire device. The following options can be selected:
- The device discards unknown Multicasts.
- The device forwards unknown Multicasts to every port.
- The device forwards unknown Multicasts only to ports that have previously received query messages (query ports).

NOTE: The exchange settings for unknown Multicast addresses also apply to the reserved IP addresses from the “Local Network Control Block” (`224.0.0.0..224.0.0.255`). This behavior can affect higher-level routing protocols.

For each VLAN, you specify the sending of Multicast packets to known Multicast addresses individually. The following options can be selected:
- The device forwards known Multicasts to the ports that have previously received query messages (query ports) and to the registered ports. Registered ports are ports with Multicast receivers registered with the corresponding Multicast group. This option helps ensure that the transfer works with basic applications without further configuration.
- The device forwards known Multicasts only to the registered ports. The advantage of this setting is that it uses the available bandwidth optimally through direct distribution.

Prerequisite:

The *IGMP Snooping* function is enabled globally.

Perform the following steps:

- ☐ Open the *Switching > IGMP Snooping > Multicasts* dialog.
- ☐ In the *Configuration* frame, you specify how the device sends data packets to unknown Multicast addresses.
  - *send to registered ports*
    The device forwards packets with unknown Multicast address to every query port.
  - *send to query and registered ports*
    The device forwards packets with unknown Multicast address to every port.
- ☐ In the *Known multicasts* column, you specify how the device sends data packets to known Multicast addresses in the corresponding VLAN. Click the relevant field and select the desired value.
- ☐ Save the changes temporarily. To do this, click the button.

Rate Limiter

The rate limiter function helps ensure stable operation even with high traffic volumes by limiting traffic on the ports. The rate limitation is performed individually for each port, as well as separately for inbound and outbound traffic.

If the data rate on a port exceeds the defined limit, then the device discards the overload on this port.

Rate limitation occurs entirely on Layer 2. In the process, the rate limiter function ignores protocol information on higher levels such as IP or TCP. This can affect the TCP traffic.

To minimize these effects, use the following options:

- Limit the rate limitation to certain packet types, for example, Broadcasts, Multicasts, and Unicasts with an unknown destination address.
- Limit the outbound data traffic instead of the inbound traffic. The outbound rate limitation works better with TCP flow control due to device-internal buffering of the data packets.
- Increase the aging time for learned Unicast addresses.

Perform the following steps:

- ☐ Open the *Switching > Rate Limiter* dialog.
- Activate the rate limiter and set limits for the data rate. The settings apply on a per port basis and are broken down by type of traffic:
  - Received Broadcast data packets
  - Received Multicast data packets
  - Received Unicast data packets with an unknown destination address

  To activate the rate limiter on a port, select the checkbox for at least one category. In the *Threshold unit* column, you specify if the device interpretes the threshold values as percent of the port bandwidth or as packets per second. The threshold value `0` deactivates the rate limiter.
- ☐ Save the changes temporarily. To do this, click the button.

QoS/Priority

QoS (Quality of Service) is a procedure defined in IEEE 802.1D which is used to distribute resources in the network. QoS lets you prioritize the data of necessary applications.

When there is a heavy network load, prioritizing helps prevent data traffic with lower priority from interfering with delay-sensitive data traffic. Delay-sensitive data traffic includes, for example, voice, video, and real-time data.

Description of Prioritization

For data traffic prioritization, traffic classes are defined in the device. The device prioritizes higher traffic classes over lower traffic classes. The number of traffic classes depends on the device type.

To provide for optimal data flow for delay-sensitive data, you assign higher traffic classes to this data. You assign lower traffic classes to data that is less sensitive to delay.

Assigning Traffic Classes to the Data

The device automatically assigns traffic classes to inbound data (traffic classification). The device takes the following classification criteria into account:

- Methods according to which the device carries out assignment of received data packets to traffic classes:
  - `trustDot1p`
    The device uses the priority of the data packet contained in the VLAN tag.
  - `trustIpDscp`
    The device uses the QoS information contained in the IP header (ToS/DiffServ).
  - `untrusted`
    The device ignores possible priority information within the data packets and uses the priority of the receiving port directly.
- The priority assigned to the receiving port.

Both classification criteria are configurable.

During traffic classification, the device uses the following rules:

- When the receiving port is set to `trustDot1p` (default setting), the device uses the data packet priority contained in the VLAN tag. When the data packets do not contain a VLAN tag, the device is guided by the priority of the receiving port.
- When the receiving port is set to `trustIpDscp`, the device uses the QoS information (ToS/DiffServ) in the IP header. When the data packets do not contain IP packets, the device is guided by the priority of the receiving port.
- When the receiving port is set to `untrusted`, the device is guided by the priority of the receiving port.

Prioritizing Traffic Classes

For prioritization of traffic classes, the device uses the following methods:

- `Strict`
  When transmission of data of a higher traffic class is no longer taking place or the relevant data is still in the queue, the device sends data of the corresponding traffic class. If every traffic class is prioritized according to the `Strict` method, then under high network load the device can permanently block the data of lower traffic classes.
- `Weighted Fair Queuing`
  The traffic class is assigned a specific bandwidth. This helps ensure that the device sends the data traffic of this traffic class, although there is a lot of data traffic in higher traffic classes.

Handling of Received Priority information

Applications label data packets with the following prioritization information:

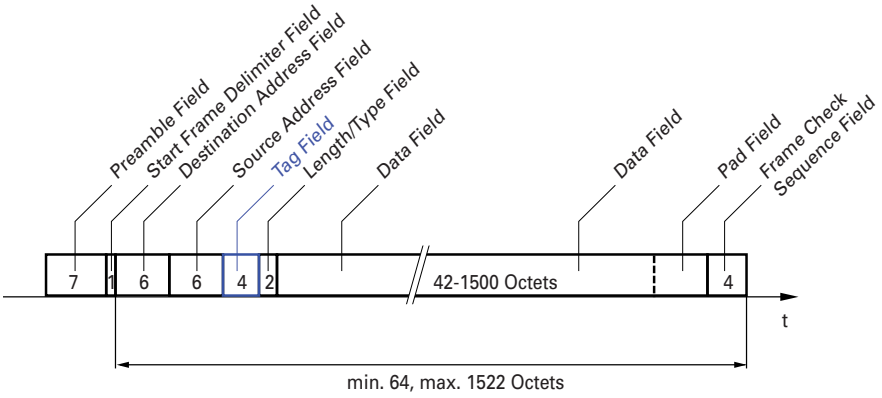
- VLAN priority based on IEEE 802.1Q/ 802.1D (Layer 2)
- Type-of-Service (ToS) or DiffServ (DSCP) for VLAN Management IP packets (Layer 3)

The device lets you evaluate this priority information using the following options:

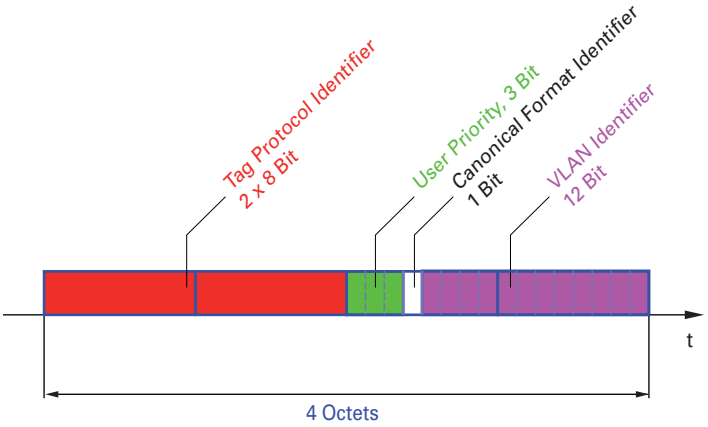
- `trustDot1p`
  The device assigns VLAN-tagged data packets to the different traffic classes according to their VLAN priorities. The corresponding allocation is configurable. The device assigns the priority of the receiving port to data packets it receives without a VLAN tag.
- `trustIpDscp`
  The device assigns the IP packets to the different traffic classes according to the DSCP value in the IP header, although the packet was also VLAN-tagged. The corresponding allocation is configurable. The device prioritizes non-IP packets according to the priority of the receiving port.
- `untrusted`
  The device ignores the priority information in the data packets and assigns the priority of the receiving port to them.

VLAN Tagging

For the VLAN and prioritizing functions, the IEEE 802.1Q standard provides for integrating a MAC frame in the VLAN tag. The VLAN tag consists of 4 bytes and is between the source address field (“Source Address Field”) and type field (“Length / Type Field”).



For data packets with VLAN tags, the device evaluates the following information:
- Priority information
- When VLANs are configured, VLAN tagging



Data packets with VLAN tags containing priority information but no VLAN information (VLAN ID = 0), are called Priority Tagged Frames.

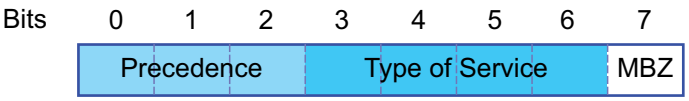
NOTE: Network protocols and redundancy mechanisms use the highest traffic class 7. Therefore, select other traffic classes for application data.

When using VLAN prioritizing, consider the following special features:
- End-to-end prioritizing requires the VLAN tags to be transmitted to the entire network. The prerequisite is that every network component is VLAN-capable.
- Routers are not able to send and receive packets with VLAN tags through port-based router interfaces.

IP ToS (Type of Service)

The Type-of-Service field (ToS) in the IP header was already part of the IP protocol from the start, and is used to differentiate different services in IP networks. Even back then, there were ideas about differentiated treatment of IP packets, due to the limited bandwidth available and the unreliable connection paths. Because of the continuous increase in the available bandwidth, there was no need to use the ToS field.

Only with the real-time requirements of today's networks has the ToS field become significant again. Selecting the ToS byte of the IP header enables you to differentiate between different services. However, this field is not widely used in practice.



Bits (0-2): IP Precedence Defined	Bits (3-6): Type of Service Defined	Bit (7)
111 - Network Control	0000 - [all normal]	0 - Zero
110 - Internetwork Control	1000 - [minimize delay]	–
101 - CRITIC / ECP	0100 - [maximize throughput	–
100 - Flash Override	0010 - [maximize reliability]	–

Bits (0-2): IP Precedence Defined	Bits (3-6): Type of Service Defined	Bit (7)
011 - Flash	0001 - [minimize monetary cost]	–
010 - Immediate	–	–
001 - Priority	–	–
000 - Routine	–	–

Handling of Traffic Classes

The device provides the following options for handling traffic classes:
- Strict Priority
- Weighted Fair Queuing
- Strict Priority combined with Weighted Fair Queuing
- Queue management

Strict Priority Description

With the Strict Priority setting, the device first transmits data packets that have a higher traffic class (higher priority) before transmitting a data packet with the next highest traffic class. When there are no other data packets remaining in the queue, the device transmits a data packet with the lowest traffic class (lowest priority). In some cases, if there is a high volume of high-priority traffic waiting to be sent on this port, then the device does not send packets with a low priority.

In delay-sensitive applications, such as VoIP or video, Strict Priority lets data to be sent immediately.

Weighted Fair Queuing Description

With Weighted Fair Queuing, also called Weighted Round Robin (WRR), you assign a minimum or reserved bandwidth to each traffic class. This helps ensure that data packets with a lower priority are also sent although the network is very busy.

The reserved values range from 0% through 100% of the available bandwidth, in steps of 1%.
- A reservation of 0 is equivalent to a "no bandwidth" setting.
- The sum of the individual bandwidths can be up to 100%.

When you assign Weighted Fair Queuing to every traffic class, the entire bandwidth of the corresponding port is available to you.

Combining Strict Priority and Weighted Fair Queuing

When combining Weighted Fair Queuing with Strict Priority, verify that the highest traffic class of Weighted Fair Queuing is lower than the lowest traffic class of Strict Priority.

If you combine Weighted Fair Queuing with Strict Priority, then a high Strict Priority network load can significantly reduce the bandwidth available for Weighted Fair Queuing.

Queue Management

Defining Settings for Queue Management

Perform the following steps:

- ☐ Open the *Switching > QoS/Priority > Queue Management* dialog.

The total assigned bandwidth in the *Min. bandwidth [%]* column is 100%.

- ☐ To activate Weighted Fair Queuing for *Traffic class* = `0`, proceed as follows:
  - ▶ Clear the checkbox in the *Strict priority* column.
  - ▶ In the *Min. bandwidth [%]* column, specify the value `5`.
- ☐ To activate Weighted Fair Queuing for *Traffic class* = `1`, proceed as follows:
  - ▶ Clear the checkbox in the *Strict priority* column.
  - ▶ In the *Min. bandwidth [%]* column, specify the value `20`.
- ☐ To activate Weighted Fair Queuing for *Traffic class* = `2`, proceed as follows:
  - ▶ Clear the checkbox in the *Strict priority* column.
  - ▶ In the *Min. bandwidth [%]* column, specify the value `30`.
- ☐ To activate Strict Priority for *Traffic class* = `3`, proceed as follows:
  - ▶ Select the checkbox in the *Strict priority* column.
- ☐ To activate Weighted Fair Queuing for *Traffic class* = `4`, proceed as follows:
  - ▶ Clear the checkbox in the *Strict priority* column.
  - ▶ In the *Min. bandwidth [%]* column, specify the value `10`.
- ☐ Save the changes temporarily. To do this, click the ✔ button.

`enable`	Change to the Privileged EXEC mode.
`configure`	Change to the Configuration mode.
`cos-queue weighted 0`	Enabling Weighted Fair Queuing for traffic class `0`.
`cos-queue min-bandwidth: 0 5`	Assigning a weight of `5` % to traffic class `0`.
`cos-queue weighted 1`	Enabling Weighted Fair Queuing for traffic class `1`.
`cos-queue min-bandwidth: 1 20`	Assigning a weight of `20` % to traffic class `1`.

```
cos-queue weighted 2
```
Enabling Weighted Fair Queuing for traffic class 2.

```
cos-queue min-bandwidth: 2 30
```
Assigning a weight of 30 % to traffic class 2.

```
show cos-queue
Queue Id  Min. bandwidth  Scheduler type
--------  --------------  --------------
0         5               weighted
1         20              weighted
2         30              weighted
3         0               strict
4         0               strict
5         0               strict
6         0               strict
7         0               strict
```

Management Prioritization

In order for you to constantly have access to the device management, although there is a high network load, the device lets you prioritize management packets.

When prioritizing management packets, the device sends the management packets with priority information.

- On Layer 2, the device modifies the VLAN priority in the VLAN tag.
  The prerequisite for this function is that the corresponding ports are set to allow sending packets with a VLAN tag.
- On Layer 3, the device modifies the IP-DSCP value.

Setting Prioritization

Assigning the Port Priority

Perform the following steps:

- ☐ Open the *Switching* > *QoS/Priority* > *Port Configuration* dialog.
- ☐ In the *Port priority* column, you specify the priority with which the device forwards the data packets received on this port without a VLAN tag.
- ☐ In the *Trust mode* column, you specify the criteria the device uses to assign a traffic class to data packets received.
- ☐ Save the changes temporarily. To do this, click the button.

`enable`	Change to the Privileged EXEC mode.
`configure`	Change to the Configuration mode.
`interface 1/1`	Change to the interface configuration mode of interface `1/1`.
`vlan priority 3`	Assign interface `1/1` the port priority `3`.
`exit`	Change to the Configuration mode.

Assigning VLAN Priority to a Traffic Class

Perform the following steps:

- ☐ Open the *Switching > QoS/Priority > 802.1D/p Mapping* dialog.
- ☐ To assign a traffic class to a VLAN priority, insert the associated value in the *Traffic class* column.
- ☐ Save the changes temporarily. To do this, click the ✔ button.

`enable`	Change to the Privileged EXEC mode.
`configure`	Change to the Configuration mode.
`classofservice dot1p-mapping 0 2`	Assigning a VLAN priority of `0` to traffic class `2`.
`classofservice dot1p-mapping 1 2`	Assigning a VLAN priority of `1` to traffic class `2`.
`exit`	Change to the Privileged EXEC mode.
`show classofservice dot1p-mapping`	Display the assignment.

Assign Port Priority to Received Data Packets

Perform the following steps:

`enable`	Change to the Privileged EXEC mode.
`configure`	Change to the Configuration mode.
`interface 1/1`	Change to the interface configuration mode of interface `1/1`.
`classofservice trust untrusted`	Assigning the `untrusted` mode to the interface.
`classofservice dot1p-mapping 0 2`	Assigning a VLAN priority of `0` to traffic class `2`.
`classofservice dot1p-mapping 1 2`	Assigning a VLAN priority of `1` to traffic class `2`.
`vlan priority 1`	Specifying the value `1` for the port priority.
`exit`	Change to the Configuration mode.

```
exit
```
Change to the Privileged EXEC mode.

```
show classofservice trust
```
Displaying the Trust mode of the ports/ interfaces.

```
 Interface Trust Mode
 --------- -------------
 1/1       untrusted
 1/2       dot1p
 1/3       dot1p
 1/4       dot1p
 1/5       dot1p
 1/6       dot1p
 1/7       dot1p
```

Assigning DSCP to a Traffic Class

Perform the following steps:

- ☐ Open the *Switching > QoS/Priority > IP DSCP Mapping* dialog.
- ☐ Specify the desired value in the *Traffic class* column.
- ☐ Save the changes temporarily. To do this, click the ✔ button.

```
enable
```
Change to the Privileged EXEC mode.

```
configure
```
Change to the Configuration mode.

```
classofservice  ip-dscp-mapping
cs1 1
```
Assigning the DSCP value `CS1` to traffic class `1`.

```
show classofservice  ip-dscp-
mapping
    IP DSCP       Traffic Class
 -------------    -------------
   be                  2
   1                   2
   .                   .
   .                   .
   (cs1)               1
   .                   .
```
Displaying the IP DSCP assignments

Assign the DSCP Priority to Received IP Data Packets

Perform the following steps:

```
enable
```
Change to the Privileged EXEC mode.

```
configure
```
Change to the Configuration mode.

```
interface 1/1
```
Change to the interface configuration mode of interface `1/1`.

```
classofservice trust ip-dscp
```
Assigning the `trust ip-dscp` mode globally.

```
exit
```
Change to the Configuration mode.

```
show classofservice trust
```
Displaying the Trust mode of the ports/ interfaces.

```
 Interface     Trust Mode
 ----------    -------------
 1/1           ip-dscp
 1/2           dot1p
 1/3           dot1p
 .             .
 .             .
 1/5           dot1p
 .             .
```

Configuring Layer 2 Management Priority

Perform the following steps:

- ☐ Open the *Switching > QoS/Priority > Global* dialog.
- ☐ In the *VLAN priority for management packets* field, specify the VLAN priority with which the device sends management data packets.
- ☐ Save the changes temporarily. To do this, click the ✓ button.

```
enable
```
Change to the Privileged EXEC mode.

```
network management priority
dot1p 7
```
Assigning the VLAN priority of 7 to management packets. The device sends management packets with the highest priority.

```
show network parms
```
Displaying the priority of the VLAN in which the device management is located.

```
IPv4 Network
------------
...
Management VLAN priority.....................7
...
```

Configuring Layer 3 Management Priority

Perform the following steps:

- ☐ Open the *Switching > QoS/Priority > Global* dialog.
- ☐ In the *IP DSCP value for management packets* field, specify the DSCP value with which the device sends management data packets.
- ☐ Save the changes temporarily. To do this, click the ✓ button.

`enable`	Change to the Privileged EXEC mode.
`network management priority ip-dscp 56`	Assigning the DSCP value of `56` to management packets. The device sends management packets with the highest priority.
`show network parms`	Displaying the priority of the VLAN in which the device management is located.

```
IPv4 Network
------------
...
Management IP-DSCP value.....................56
```

Flow Control

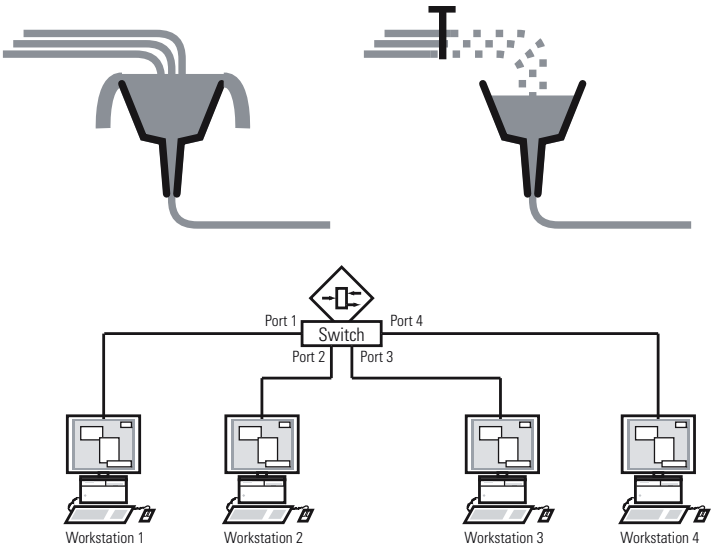
If a large number of data packets are received in the priority queue of a port at the same time, then this can cause the port memory to overflow. This happens, for example, when the device receives data on a Gigabit port and forwards it to a port with a lower bandwidth. The device discards surplus data packets.

The flow control mechanism described in standard IEEE 802.3 helps ensure that no data packets are lost due to a port memory overflowing. Shortly before a port memory is completely full, the device signals to the connected devices that it is not accepting any more data packets from them.

- In full-duplex mode, the device sends a pause data packet.
- In half-duplex mode, the device simulates a collision.

The following figure displays how flow control works. Workstations 1, 2, and 3 want to simultaneously transmit a large amount of data to Workstation 4. The combined bandwidth of Workstations 1, 2, and 3 is greater than the bandwidth of Workstation 4. This causes an overflow on the receive queue of port 4. The left funnel symbolizes this status.

When the flow control function on ports 1, 2 and 3 of the device is enabled, the device reacts before the funnel overflows. The funnel on the right illustrates ports 1, 2 and 3 sending a message to the transmitting devices to control the transmition speed. This results in the receiving port no longer being overwhelmed and is able to process the incoming traffic.



Halfduplex or Fullduplex Link

Flow Control with a half Duplex Link

In the example, there is a halfduplex link between Workstation 2 and the device.

Before the send queue of port 2 overflows, the device sends data back to Workstation 2. Workstation 2 detects a collision and stops transmitting.

Flow Control with a full Duplex Link

In the example, there is a fullduplex link between Workstation 2 and the device.

Before the send queue of port 2 overflows, the device sends a request to Workstation 2 to include a short delay in the sending transmission.

Setting up the Flow Control

Perform the following steps:

- ☐ Open the *Switching > Global* dialog.
- ☐ Select the *Flow control* checkbox.
  With this setting you enable flow control in the device.
- ☐ Open the *Basic Settings > Port* dialog, *Configuration* tab.
- ☐ To enable the Flow Control on a port, select the checkbox in the *Flow control* column.
- ☐ Save the changes temporarily. To do this, click the button.

NOTE: When you are using a redundancy function, you deactivate the flow control on the participating ports. If the flow control and the redundancy function are active at the same time, it is possible that the redundancy function operates differently than intended.

VLANs

In the simplest case, a virtual LAN (VLAN) consists of a group of network participants in one network segment who can communicate with each other as though they belonged to a separate LAN.

More complex VLANs span out over multiple network segments and are also based on logical (instead of only physical) connections between network participants. VLANs are an element of flexible network design. It is easier to reconfiguring logical connections centrally than cable connections.

The device supports independent VLAN learning in accordance with the IEEE 802.1Q standard which defines the *VLAN* function.

Using VLANs has many benefits. The following list displays the top benefits:

- Network load limiting
  VLANs reduce the network load considerably as the devices transmit Broadcast, Multicast, and Unicast packets with unknown (unlearned) destination addresses only inside the virtual LAN. The rest of the data network forwards traffic as normal.
- Flexibility
  You have the option of forming user groups based on the function of the participants apart from their physical location or medium.
- Clarity
  VLANs give networks a clear structure and make maintenance easier.

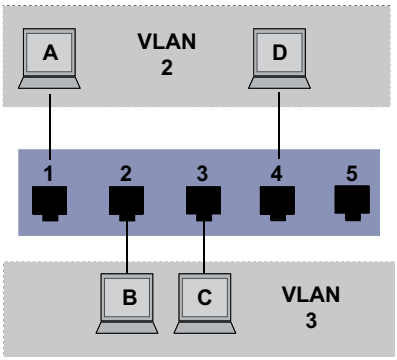
Examples of VLANs

The following practical examples provide an introduction to the structure of a VLAN.

NOTE: When configuring VLANs you use an interface to access the device management that will remain unchanged. For this example, you use either interface 1/6 or the serial connection to configure the VLANs.

Example 1

The example displays a minimal VLAN configuration (port-based VLAN). An administrator has connected multiple end devices to a transmission device and assigned them to 2 VLANs. This effectively prohibits any data transmission between the VLANs, whose members communicate only within their own VLANs.



When setting up the VLANs, you create communication rules for every port, which you enter in ingress (incoming) and egress (outgoing) tables.

The ingress table specifies which VLAN ID a port assigns to the incoming data packets. Hereby, you use the port address of the end device to assign it to a VLAN.

The egress table specifies on which ports the device sends the packets from this VLAN.
- `T` = Tagged (with a tag field, marked)
- `U` = Untagged (without a tag field, unmarked)

For this example, the status of the TAG field of the data packets has no relevance, so you use the setting `U`.

Terminal	Port	Port VLAN Identifier (PVID)
A	1	2
B	2	3
C	3	3
D	4	2
–	5	1

VLAN ID	Port				
–	1	2	3	4	5
1	–	–	–	–	U
2	U	–	–	U	–
3	–	U	U	–	–

Perform the following steps:
☐ Setting up the VLAN

☐ Open the *Switching > VLAN > Configuration* dialog.

☐ Click the button.
The dialog displays the *Create* window.

☐ In the *VLAN ID* field, specify the value `2`.

- ☐ Click the *Ok* button.
- ☐ For the VLAN, specify the name `VLAN2`:
  Double-click in the *Name* column and specify the name.
  For VLAN `1`, in the *Name* column, change the value `Default` to `VLAN1`.
- ☐ Repeat the previous steps to create a VLAN `3` with the name `VLAN3`.

`enable`	Change to the Privileged EXEC mode.
`vlan database`	Change to the VLAN configuration mode.
`vlan add 2`	Creates a new VLAN with the VLAN ID `2`.
`name 2 VLAN2`	Assign the name `2` to the VLAN `VLAN2`.
`vlan add 3`	Creates a new VLAN with the VLAN ID `3`.
`name 3 VLAN3`	Assign the name `3` to the VLAN `VLAN3`.
`name 1 VLAN1`	Assign the name `1` to the VLAN `VLAN1`.
`exit`	Change to the Privileged EXEC mode.
`show vlan brief`	Display the VLAN configuration.

```
Max. VLAN ID..................................... 4042
Max. supported VLANs............................. 16
Number of currently configured VLANs............ 3
vlan unaware mode................................ disabled
VLAN ID VLAN Name                       VLAN Type VLAN Creation Time
---- -------------------------------- --------- -------------------
1       VLAN1                           default    0 days, 00:00:05
2       VLAN2                           static     0 days, 02:44:29
3       VLAN3                           static     0 days, 02:52:26
```

☐ Setting up the ports

- ☐ Open the *Switching > VLAN > Port* dialog.
- ☐ To assign the port to a VLAN, specify the desired value in the corresponding column.
  Possible values:
  - `T` = The port is a member of the VLAN. The port transmits tagged data packets.
  - `U` = The port is a member of the VLAN. The port transmits untagged data packets.
  - `F` = The port is not a member of the VLAN.
  - `-` = The port is not a member of this VLAN.

  Because end devices usually interpret untagged data packets, you specify the value `U`.
- ☐ Save the changes temporarily. To do this, click the ✔ button.
- ☐ Open the *Switching > VLAN > Port* dialog.
- ☐ In the *Port-VLAN ID* column, specify the VLAN ID of the related VLAN: `2` or `3`
- ☐ Because end devices usually interpret untagged data packets, in the *Acceptable packet types* column, you specify the value `admitAll` for end device ports.
- ☐ Save the changes temporarily. To do this, click the ✔ button.

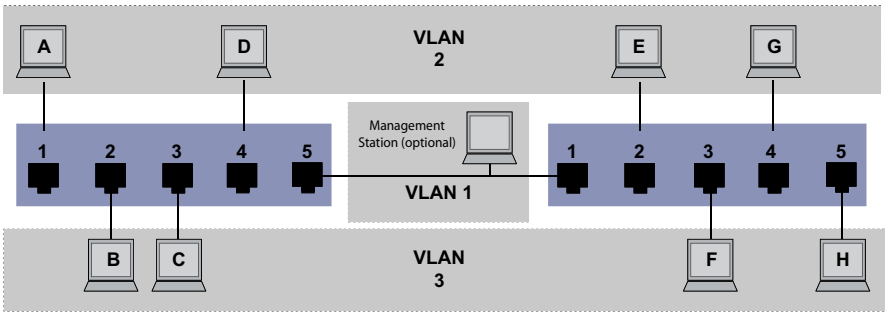
The value in the *Ingress filtering* column has no affect on how this example functions.

`enable`	Change to the Privileged EXEC mode.
`configure`	Change to the Configuration mode.
`interface 1/1`	Change to the interface configuration mode of interface `1/1`.
`vlan participation include 2`	The port `1/1` becomes a member of the VLAN `2` and transmits the data packets without a VLAN tag.
`vlan pvid 2`	Assign the port VLAN ID `1/1` to port `2`.
`exit`	Change to the Configuration mode.
`interface 1/2`	Change to the interface configuration mode of interface `1/2`.
`vlan participation include 3`	The port `1/2` becomes a member of the VLAN `3` and transmits the data packets without a VLAN tag.
`vlan pvid 3`	Assign the port VLAN ID `1/2` to port `3`.
`exit`	Change to the Configuration mode.
`interface 1/3`	Change to the interface configuration mode of interface `1/3`.
`vlan participation include 3`	The port `1/3` becomes a member of the VLAN `3` and transmits the data packets without a VLAN tag.
`vlan pvid 3`	Assign the port VLAN ID `1/3` to port `3`.
`exit`	Change to the Configuration mode.
`interface 1/4`	Change to the interface configuration mode of interface `1/4`.
`vlan participation include 2`	The port `1/4` becomes a member of the VLAN `2` and transmits the data packets without a VLAN tag.
`vlan pvid 2`	Assign the port VLAN ID `1/4` to port `2`.
`exit`	Change to the Configuration mode.
`exit`	Change to the Privileged EXEC mode.
`show vlan id 3`	Displays details for VLAN `3`.

```
VLAN ID           : 3
VLAN Name         : VLAN3
VLAN Type         : Static
Interface   Current   Configured   Tagging
----------  --------  -----------  --------
1/1            -      Autodetect   Tagged
1/2         Include   Include      Untagged
1/3         Include   Include      Untagged
1/4            -      Autodetect   Tagged
1/5            -      Autodetect   Tagged
```

Example 2

The second example displays a more complex configuration with 3 VLANs (1 to 3). Along with the Switch from example 1, you use a second Switch (on the right in the example).



The terminal devices of the individual VLANs (A to H) are spread over 2 transmission devices (Switches). Such VLANs are therefore known as distributed VLANs. If the VLAN is configured correctly, then an optional network management station is also shown, which enables access to every network component.

NOTE: In this case, VLAN 1 has no significance for the end device communication, but it is required for the administration of the transmission devices via what is known as the Management VLAN.

As in the previous example, uniquely assign the ports with their connected terminal devices to a VLAN. With the direct connection between the 2 transmission devices (uplink), the ports transport packets for both VLANs. To differentiate these uplinks you use “VLAN tagging”, which handles the data packets accordingly. Thus, you maintain the assignment to the respective VLANs.

Perform the following steps:

- ☐ Add Uplink Port 5 to the ingress and egress tables from example 1.
- ☐ Create new ingress and egress tables for the right switch, as described in the first example.

The egress table specifies on which ports the device sends the packets from this VLAN.

- ▶ `T` = Tagged (with a tag field, marked)
- ▶ `U` = Untagged (without a tag field, unmarked)

In this example, tagged packets are used in the communication between the transmission devices (Uplink), as packets for different VLANs are differentiated at these ports.

Terminal	Port	Port VLAN Identifier (PVID)
A	1	2
B	2	3
C	3	3
D	4	2
Uplink	5	1

Terminal	Port	Port VLAN Identifier (PVID)
Uplink	1	1
E	2	2
F	3	3
G	4	2
H	5	3

VLAN ID	Port				
–	1	2	3	4	5
1	–	–	–	–	U
2	U	–	–	U	T
3	–	U	U	–	T

VLAN ID	Port				
–	1	2	3	4	5
1	U	–	–	–	–
2	T	U	–	U	–
3	T	–	U	–	U

The communication relationships here are as follows: end devices on ports 1 and 4 of the left device and end devices on ports 2 and 4 of the right device are members of VLAN 2 and can thus communicate with each other. The behavior is the same for the end devices on ports 2 and 3 of the left device and the end devices on ports 3 and 5 of the right device. These belong to VLAN 3.

The end devices recognize their respective part of the network. Participants outside this VLAN cannot be reached. The device also sends Broadcast, Multicast, and Unicast packets with unknown (unlearned) destination addresses only inside a VLAN.

Here, the devices use VLAN tagging (IEEE 801.1Q) within the VLAN with the ID 1 (Uplink). The letter `T` in the egress table of the ports indicates VLAN tagging.

The configuration of the example is the same for the device on the right. Proceed in the same way, using the ingress and egress tables created above to adapt the previously configured left device to the new environment.

Perform the following steps:

☐ Setting up the VLAN

- ☐ Open the *Switching > VLAN > Configuration* dialog.
- ☐ Click the  button.
  The dialog displays the *Create* window.
- ☐ In the *VLAN ID* field, specify the VLAN ID, for example `2`.
- ☐ Click the *Ok* button.
- ☐ For the VLAN, specify the name `VLAN2`:
  Double-click in the *Name* column and specify the name.
  For VLAN `1`, in the *Name* column, change the value `Default` to `VLAN1`.
- ☐ Repeat the previous steps to create a VLAN `3` with the name `VLAN3`.

`enable`	Change to the Privileged EXEC mode.
`vlan database`	Change to the VLAN configuration mode.
`vlan add 2`	Creates a new VLAN with the VLAN ID `2`.
`name 2 VLAN2`	Assign the name `2` to the VLAN `VLAN2`.
`vlan add 3`	Creates a new VLAN with the VLAN ID `3`.
`name 3 VLAN3`	Assign the name `3` to the VLAN `VLAN3`.
`name 1 VLAN1`	Assign the name `1` to the VLAN `VLAN1`.
`exit`	Change to the Privileged EXEC mode.
`show vlan brief`	Display the VLAN configuration.

```
Max. VLAN ID..................................... 4042
Max. supported VLANs............................. 16
Number of currently configured VLANs............ 3
vlan unaware mode................................ disabled
VLAN ID VLAN Name                       VLAN Type VLAN Creation Time
---- -------------------------------- --------- -------------------
1       VLAN1                           default    0 days, 00:00:05
2       VLAN2                           static     0 days, 02:44:29
3       VLAN3                           static     0 days, 02:52:26
```

☐ Setting up the ports

☐ Open the *Switching > VLAN > Port* dialog.

☐ To assign the port to a VLAN, specify the desired value in the corresponding column.
Possible values:
- `T` = The port is a member of the VLAN. The port transmits tagged data packets.
- `U` = The port is a member of the VLAN. The port transmits untagged data packets.
- `F` = The port is not a member of the VLAN.
- `-` = The port is not a member of this VLAN.

Because end devicees usually interpret untagged data packets, you specify the value `U`.
You specify the `T` setting on the uplink port on which the VLANs communicate with each other.

☐ Save the changes temporarily. To do this, click the ✓ button.

☐ Open the *Switching > VLAN > Port* dialog.

☐ In the *Port-VLAN ID* column, specify the VLAN ID of the related VLAN: `1`, `2` or `3`

☐ Because end devices usually interpret untagged data packets, in the *Acceptable packet types* column, you specify the value `admitAll` for end device ports.

☐ For the uplink port, in the *Acceptable packet types* column, specify the value `admitOnlyVlanTagged`.

☐ Select the checkbox in the *Ingress filtering* column for the uplink ports to evaluate VLAN tags on this port.

☐ Save the changes temporarily. To do this, click the ✓ button.

`enable`	Change to the Privileged EXEC mode.
`configure`	Change to the Configuration mode.
`interface 1/1`	Change to the interface configuration mode of interface `1/1`.
`vlan participation include 1`	The port `1/1` becomes a member of the VLAN `1` and transmits the data packets without a VLAN tag.
`vlan participation include 2`	The port `1/1` becomes a member of the VLAN `2` and transmits the data packets without a VLAN tag.
`vlan tagging 2 enable`	The port `1/1` becomes a member of the VLAN `2` and transmits the data packets with a VLAN tag.
`vlan participation include 3`	The port `1/1` becomes a member of the VLAN `3` and transmits the data packets without a VLAN tag.
`vlan tagging 3 enable`	The port `1/1` becomes a member of the VLAN `3` and transmits the data packets with a VLAN tag.
`vlan pvid 1`	Assigning the Port VLAN ID `1` to port `1/1`.
`vlan ingressfilter`	Activate ingress filtering on port `1/1`.
`vlan acceptframe vlanonly`	Port `1/1` only forwards packets with a VLAN tag.
`exit`	Change to the Configuration mode.
`interface 1/2`	Change to the interface configuration mode of interface `1/2`.
`vlan participation include 2`	The port `1/2` becomes a member of the VLAN `2` and transmits the data packets without a VLAN tag.
`vlan pvid 2`	Assigning the Port VLAN ID `2` to port `1/2`.
`exit`	Change to the Configuration mode.
`interface 1/3`	Change to the interface configuration mode of interface `1/3`.
`vlan participation include 3`	The port `1/3` becomes a member of the VLAN `3` and transmits the data packets without a VLAN tag.
`vlan pvid 3`	Assigning the Port VLAN ID `3` to port `1/3`.
`exit`	Change to the Configuration mode.
`interface 1/4`	Change to the interface configuration mode of interface `1/4`.
`vlan participation include 2`	The port `1/4` becomes a member of the VLAN `2` and transmits the data packets without a VLAN tag.
`vlan pvid 2`	Assigning the Port VLAN ID `2` to port `1/4`.
`exit`	Change to the Configuration mode.
`interface 1/5`	Change to the interface configuration mode of interface `1/5`.
`vlan participation include 3`	The port `1/5` becomes a member of the VLAN `3` and transmits the data packets without a VLAN tag.
`vlan pvid 3`	Assigning the Port VLAN ID `3` to port `1/5`.

```
exit                                    Change to the Configuration mode.
exit                                    Change to the Privileged EXEC mode.
show vlan id 3                          Displays details for VLAN 3.
VLAN ID.....................3
VLAN Name...................VLAN3
VLAN Type...................Static
VLAN Creation Time..........0 days, 00:07:47 (System Uptime)
VLAN Routing................disabled

Interface   Current   Configured   Tagging
----------  --------  -----------  --------
1/1         Include   Include      Tagged
1/2         -         Autodetect   Untagged
1/3         Include   Include      Untagged
1/4         -         Autodetect   Untagged
1/5         Include   Include      Untagged
```

Guest VLAN / Unauthenticated VLAN

A Guest VLAN lets a device provide port-based Network Access Control (IEEE 802.1x) to non-802.1x capable supplicants. This feature provides a mechanism to allow guests to access external networks only. If you connect non-802.1x capable supplicants to an active unauthorized 802.1x port, then the supplicants send no responds to 802.1x requests. Since the supplicants send no responses, the port remains in the unauthorized state. The supplicants have no access to external networks.

The Guest VLAN supplicant is a per-port basis configuration. When you configure a port as a Guest VLAN and connect non-802.1x capable supplicants to this port, the device assigns the supplicants to the Guest VLAN. Adding supplicants to a Guest VLAN causes the port to change to the authorized state allowing the supplicants to access to external networks.

An Unauthenticated VLAN lets the device provide service to 802.1x capable supplicants which authenticate incorrectly. This function lets the unauthorized supplicants have access to limited services. If you configure an Unauthenticated VLAN on a port with 802.1x port authentication and the global operation enabled, then the device places the port in an Unauthenticated VLAN. When a 802.1x capable supplicant incorrectly authenticates on the port, the device adds the supplicant to the Unauthenticated VLAN. If you also configure a Guest VLAN on the port, then non-802.1x capable supplicants use the Guest VLAN.

If the port has an Unauthenticated VLAN assigned, then the reauthentication timer counts down. When the time specified in the *Reauthentication period [s]* column expires and supplicants are present on the port, the Unauthenticated VLAN reauthenticates. When no supplicants are present, the device places the port in the configured Guest VLAN.

The following example explains how to create a Guest VLAN. Create an Unauthorized VLAN in the same manner.

Perform the following steps:

- ☐ Open the *Switching > VLAN > Configuration* dialog.
- ☐ Click the button.
  The dialog displays the *Create* window.
- ☐ In the *VLAN ID* field, specify the value `10`.
- ☐ Click the *Ok* button.
- ☐ For the VLAN, specify the name `Guest`:
  Double-click in the *Name* column and specify the name.
- ☐ Click the button.
  The dialog displays the *Create* window.
- ☐ In the *VLAN ID* field, specify the value `20`.
- ☐ Click the *Ok* button.
- ☐ For the VLAN, specify the name `Not authorized`:
  Double-click in the *Name* column and specify the name.
- ☐ Open the *Network Security > 802.1X Port Authentication > Global* dialog.
- ☐ To enable the function, select the `On` radio button in the *Operation* frame.
- ☐ Save the changes temporarily. To do this, click the button.
- ☐ Open the *Network Security > 802.1X Port Authentication > Port Configuration* dialog.
- ☐ Specify the following settings for port `1/4`:
  - The value `auto` in the *Port control* column
  - The value `10` in the *Guest VLAN ID* column
  - The value `20` in the *Unauthenticated VLAN ID* column
- ☐ Save the changes temporarily. To do this, click the button.

`enable`	Change to the Privileged EXEC mode.
`vlan database`	Change to the VLAN configuration mode.
`vlan add 10`	Creates VLAN `10`.
`vlan add 20`	Creates VLAN `20`.
`name 10 Guest`	Renames VLAN `10` to `Guest`.
`name 20 Unauth`	Renames VLAN `20` to `Unauth`.
`exit`	Change to the Privileged EXEC mode.
`configure`	Change to the Configuration mode.
`dot1x system-auth-control enable`	Enable the *802.1X Port Authentication* function globally.
`dot1x port-control auto`	Enables port control on port `1/4`.
`interface 1/4`	Change to the interface configuration mode of interface `1/4`.
`dot1x guest-vlan 10`	Assign the guest vlan to port `1/4`.
`dot1x unauthenticated-vlan 20`	Assign the unauthorized vlan to port `1/4`.
`exit`	Change to the Configuration mode.

RADIUS VLAN Assignment

The RADIUS VLAN assignment feature makes it possible for a RADIUS VLAN ID attribute to be associated with an authenticated client. When a client authenticates successfully, and the RADIUS server sends a VLAN attribute, the device associates the client with the RADIUS assigned VLAN. As a result, the device adds the physical port as an member to the appropriate VLAN and sets the port VLAN ID (PVID) with the given value. The port transmits the data packets without a VLAN tag.

Creating a Voice VLAN

Use the Voice VLAN feature to separate voice and data traffic on a port, by VLAN and/or priority. A primary benefit of using Voice VLAN is to help ensure the sound quality of an IP phone in cases where there is high data traffic on the port.

The device uses the source MAC address to identify and prioritize the voice data flow. Using a MAC address to identify devices helps prevent a rogue client from connecting to the same port causing the voice traffic to deteriorate.

Another benefit of the Voice VLAN feature is that a VoIP phone obtains a VLAN ID or priority information using LLDP-MED. As a result, the VoIP phone sends voice data as tagged, priority tagged or untagged. This depends on the Voice VLAN Interface configuration.

The following Voice VLAN interface modes are possible. The first 3 methods segregate and prioritize voice and data traffic. Traffic segregation results in an increased voice traffic quality during high traffic periods.

- Configuring the port to using the `vlan` mode lets the device tag the voice data coming from a VoIP phone with the user-defined voice VLAN ID. The device assigns regular data to the default port VLAN ID.
- Configuring the port to use the `dot1p-priority` mode lets the device tag the data coming from a VoIP phone with VLAN 0 and the user-defined priority. The device assigns the default priority of the port to regular data.
- Configure both the voice VLAN ID and the priority using the `vlan/dot1p-priority` mode. In this mode the VoIP phone sends voice data with the user-defined voice VLAN ID and priority information. The device assigns the default PVID and priority of the port to regular data.
- When configured as `untagged`, the phone sends untagged packets.
- When configured as `none`, the phone uses its own configuration to send voice traffic.

VLAN Unaware Mode

The *VLAN unaware mode* defines the operation of the device in a LAN segmented by VLANs. The device accepts packets and processes them according to its inbound rules. Based on the IEEE 802.1Q specifications, the function governs how the device processes VLAN tagged packets.

Use the VLAN aware mode to apply the user-defined VLAN topology configured by the network administrator. When the device forwards packets, it uses VLAN tagging and the IP or Ethernet address. The device processes inbound and outbound packets according to the defined rules. VLAN configuration is a manual process.

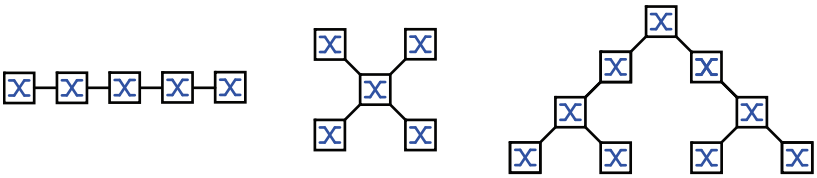
Use the VLAN unaware mode to forward traffic as received, without any modification. When the device receives packets as tagged, it transmits tagged packets. When the device receives packets as untagged, it transmits untagged packets. Regardless of VLAN assignment mechanisms, the device assigns packets to VLAN ID 1 and to a Multicast group, indicating that the packet flood domain is according to the VLAN.

Redundancy

Network Topology vs. Redundancy Protocols

When using Ethernet, a significant prerequisite is that data packets follow a single (unique) path from the sender to the receiver. The following network topologies support this prerequisite:

- Line topology
- Star topology
- Tree topology



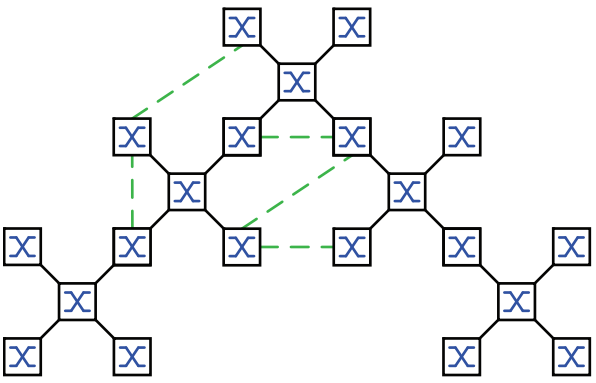
To maintain communication in case a connection interruption is detected, install additional physical connections between the network nodes. Redundancy protocols help ensure that the additional connections remain switched off while the original connection is still operational. When a connection interruption is detected, the redundancy protocol generates a new path from the sender to the receiver via the alternative connection.

To introduce redundancy onto Layer 2 of a network, you first define which network topology you require. Depending on the network topology selected, you then choose from the redundancy protocols that can be used with this network topology.

Network Topologies

Meshed Topology

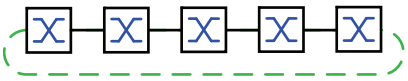
For networks with star or tree topologies, redundancy procedures are only possible in connection with physical loop creation. The result is a meshed topology.



For operating in this network topology, the device provides you with the following redundancy protocols:
- Rapid Spanning Tree (RSTP)

Ring Topology

In networks with a line topology, you can use redundancy procedures by connecting the ends of the line. This creates a ring topology.



For operating in this network topology, the device provides you with the following redundancy protocols:
- Media Redundancy Protocol (MRP)
- Rapid Spanning Tree (RSTP)

Redundancy Protocols

For operating in different network topologies, the device provides you with the following redundancy protocols:

Redundancy Protocol	Network Topology	Comments
MRP	Ring	The switching time can be selected and is practically independent of the number of devices. An MRP-Ring consists of up to 50 devices that support the MRP protocol according to IEC 62439. When you only use Schneider Electric devices, up to 100 devices are possible in the MRP-Ring.
PRP	Random structure of the PRP LANs	Uninterrupted availability. On the path from the sender to the receiver, PRP transports a data packet in parallel via 2 mutually independent LANs.
RSTP	Random structure	The switching time depends on the network topology and the number of devices. - typically < 1 s with RSTP - typically < 30 s with STP
Link Aggregation	Random structure	A Link Aggregation Group is the combining of 2 or more, full-duplex point-to-point links operating at the same rate, on a single switch to increase bandwidth.
Link Backup	Random structure	When the device detects an error on the primary link, the device transfers traffic to the backup link. You typically use Link Backup in service-provider or enterprise networks.

If the flow control and the redundancy function are active at the same time, it is possible that the redundancy function operates differently than intended.

⚠ WARNING

UNINTENDED EQUIPMENT OPERATION

If you are using a redundancy function, then you deactivate the flow control on the participating device ports.

Failure to follow these instructions can result in death, serious injury, or equipment damage.

Combinations of Redundancies

	MRP	RSTP	Link Aggregation	Link Backup	PRP
MRP	▲	– – –	– – –	– – –	– – –
RSTP	▲ 1)	▲	– – –	– – –	– – –
Link Aggregation	▲ 2)	▲ 2)	▲	– – –	– – –
Link Backup	▲	▲	▲	▲	– – –
PRP 3)	▲	▲ 1)	▲	▲	▲ 3)

▲ Combination applicable

1) A redundant coupling between these network topologies will possibly lead to loops.

2) Combination applicable on the same port

3) Available only on port 1 and port 2.

Media Redundancy Protocol (MRP)

Since May 2008, the Media Redundancy Protocol (MRP) has been a standardized solution for ring redundancy in the industrial environment.

MRP is compatible with redundant ring coupling, supports VLANs, and is distinguished by very short reconfiguration times.

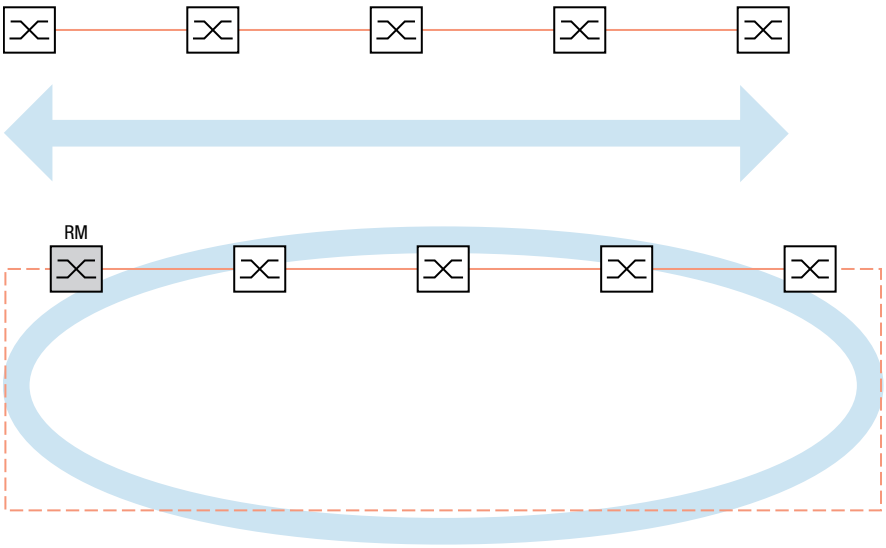
An MRP-Ring consists of up to 50 devices that support the MRP protocol according to IEC 62439. When you only use Schneider Electric devices, up to 100 devices are possible in the MRP-Ring.

When you use the fixed MRP redundant port (Fixed Backup) and a primary ring link error is detected, the Ring Manager forwards data to the secondary ring link. When the primary link is restored, the secondary link continues to be in use.

Network Structure

The concept of ring redundancy lets you construct high-availability ring-shaped network structures.

With the help of the RM (**R**ing**M**anager) function, the two ends of a backbone in a line structure can be closed to a redundant ring. The Ring Manager keeps the redundant line open as long as the line structure is intact. When a segment becomes inoperable, the Ring Manager immediately closes the redundant line, and line structure is intact again.



Reconfiguration Time

When a line section error is detected, the Ring Manager changes the MRP-Ring back into a line structure. You define the maximum time for the reconfiguration of the line in the Ring Manager.

Possible values for the maximum delay time:

- `500ms`
- `30ms`

NOTE: If every device in the ring supports the shorter delay time, then you can configure the reconfiguration time with a value less than `500ms`.

Otherwise the devices that only support longer delay times might not be reachable due to overloading. Loops can occur as a result.

Advanced Mode

For times even shorter than the specified reconfiguration times, the device provides the advanced mode. When the ring participants inform the Ring Manager of interruptions in the ring via link-down notifications, the advanced mode speeds up the link error detection.

Schneider Electric devices support link-down notifications. Therefore, you generally activate the advanced mode in the Ring Manager.

When you are using devices that do not support link-down notifications, the Ring Manager reconfigures the line in the selected maximum reconfiguration time.

Prerequisites for MRP

Before setting up an MRP-Ring, verify that the following conditions are fulfilled:

- All ring participants support MRP.
- The ring participants are connected to each other via the ring ports. Apart from the device's neighbors, no other ring participants are connected to the respective device.
- All ring participants support the configuration time specified in the Ring Manager.
- There is only one Ring Manager in the ring.

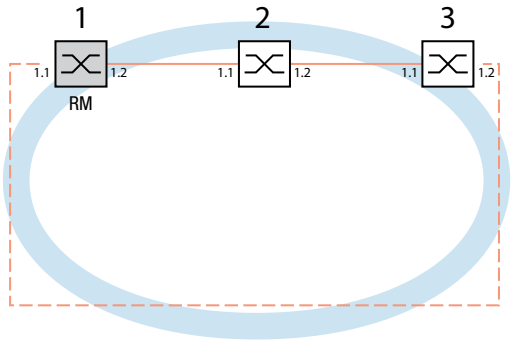
If you are using VLANs, then configure every ring port with the following settings:

- ☐ Deactivate ingress filtering - see the *Switching > VLAN > Port* dialog.
- ☐ Define the port VLAN ID (PVID) - see the *Switching > VLAN > Port* dialog.
  - PVID = `1` in cases where the device transmits the MRP data packets untagged (VLAN ID = `0` in *Switching > L2-Redundancy > MRP* dialog)
    By setting the PVID = `1`, the device automatically assigns the received untagged packets to VLAN 1.
  - PVID = `any` in cases where the device transmits the MRP data packets in a VLAN (VLAN ID ≥ `1` in the *Switching > L2-Redundancy > MRP* dialog)
- ☐ Define egress rules - see *Switching > VLAN > Configuration* dialog.
  - `U` (untagged) for the ring ports of VLAN 1 in cases where the device transmits the MRP data packets untagged (VLAN ID = `0` in the *Switching > L2-Redundancy > MRP* dialog, the MRP ring is not assigned to a VLAN).
  - `T` (tagged) for the ring ports of the VLAN which you assign to the MRP ring. Select `T`, in cases where the device transmits the MRP data packets in a VLAN (VLAN ID ≥ `1` in the *Switching > L2-Redundancy > MRP* dialog).

Example Configuration

A backbone network contains 3 devices in a line structure. To increase the availability of the network, you convert the line structure to a redundant ring structure. Devices from different manufacturers are used. All devices support MRP. On every device you define ports 1.1 and 1.2 as ring ports.

When a primary ring link error is detected, the Ring Manager sends data on the secondary ring link. When the primary link is restored, the secondary link reverts back to the backup mode.



The following example configuration describes the configuration of the Ring Manager device (1). You configure the 2 other devices (2 to 3) in the same way, but without activating the *Ring manager* function. This example does not use a VLAN. You specify the value `30ms` as the ring recovery time. Every device supports the advanced mode of the Ring Manager.

- ☐ Set up the network to meet your demands.
- ☐ Configure every port so that the transmission speed and the duplex settings of the lines correspond to the following table:

Port Type	Bit Rate	Port on	Automatic configuration	Manual configuration
TX	100 Mbit/s	`selected`	`cleared`	*`100 Mbit/s FDX`*
TX	1 Gbit/s	`selected`	`selected`	–
Optical	100 Mbit/s	`selected`	`cleared`	*`100 Mbit/s FDX`*
Optical	1 Gbit/s	`selected`	`selected`	–

NOTE: You configure optical ports without support for autonegotiation (automatic configuration) with 100 Mbit/s full duplex (FDX) or 1000 Mbit/s full duplex (FDX).

NOTE: You configure optical ports without support for autonegotiation (automatic configuration) with 100 Mbit/s full duplex (FDX).

NOTE: Configure every device of the MRP-Ring individually. Before you connect the redundant line, verify that you have completed the configuration of every device of the MRP-Ring. You thus help avoid loops during the configuration phase.

⚠ WARNING

UNINTENDED EQUIPMENT OPERATION

- To help avoid loops during the configuration phase, configure each device of the *MRP* configuration individually.
- Before you connect the redundant lines, complete the configuration of the other devices of the ring configuration.

Failure to follow these instructions can result in death, serious injury, or equipment damage.

You deactivate the flow control on the participating ports.

If the flow control and the redundancy function are active at the same time, it is possible that the redundancy function operates differently than intended. (Default setting: flow control deactivated globally and activated on every port.)

Disable the *Spanning Tree* function in every device in the network. To do this, perform the following steps:

- ☐ Open the *Switching* > *L2-Redundancy* > *Spanning Tree* > *Global* dialog.
- ☐ Disable the function.
  In the state on delivery, Spanning Tree is enabled in the device.

`enable`	Change to the Privileged EXEC mode.
`configure`	Change to the Configuration mode.
`no spanning-tree operation`	Switches Spanning Tree off.
`show spanning-tree global`	Displays the parameters for checking.

Enable MRP on every device in the network. To do this, perform the following steps:

- ☐ Open the *Switching* > *L2-Redundancy* > *MRP* dialog.
- ☐ Specify the desired ring ports.

In the CLI you first define an additional parameter, the MRP domain ID. Configure every ring participant with the same MRP domain ID. The MRP domain ID is a sequence of 16 number blocks (8-bit values).

When configuring with the GUI, the device uses the default value `255 255 255 255 255 255 255 255 255 255 255 255 255 255 255 255`.

`mrp domain add default-domain`	Creates a new MRP domain with the ID `default-domain`.
`mrp domain modify port primary 1/1`	Specifies port *1/1* as ring port `1`.
`mrp domain modify port secondary 1/2`	Specifies port *1/2* as ring port `2`.

Enable the *Fixed backup* port. To do this, perform the following steps:

☐ Enable the Ring Manager.
For the other devices in the ring, leave the setting as *Off*.

☐ To allow the device to continue sending data on the secondary port after the ring is restored, select the *Fixed backup* checkbox.

NOTE: When the device reverts back to the primary port, the maximum ring recovery time can be exceeded.

When you clear the *Fixed backup* checkbox, and the ring is restored, the Ring Manager blocks the secondary port and unblocks the primary port.

```
mrp domain modify port secondary
1/2 fixed-backup enable
```

Activates the *Fixed backup* function on the secondary port. The secondary port continues forwarding data after the ring is restored.

☐ Enable the Ring Manager.
For the other devices in the ring, leave the setting as *Off*.

```
mrp domain modify mode   manager
```

Specifies that the device operates as the *Ring manager*. For the other devices in the ring, use the default setting.

☐ Select the checkbox in the *Advanced mode* field.

```
mrp domain modify
advanced-mode enabled
```

Activates the advanced mode.

☐ In the *Ring recovery* field, select the value *30ms*.

```
mrp domain modify
recovery-delay 200ms
```

Specifies the value *30ms* as the max. delay time for the reconfiguration of the ring.

NOTE: If selecting the value *30ms* for the ring recovery does not provide the ring stability necessary to meet the requirements of your network, then select the value *500ms*.

☐ Switch the operation of the MRP-Ring on.

☐ Save the changes temporarily. To do this, click the ✓ button.

`mrp domain modify operation enable`	Activates the MRP-Ring.

When every ring participant is configured, close the line to the ring. To do this, you connect the devices at the ends of the line via their ring ports.

Verify the messages from the device. To do this, perform the following steps:

`show mrp`	Displays the parameters for checking.

The *Operation* field displays the operating state of the ring port.

Possible values:

- `forwarding`
  The port is enabled, connection exists.
- `blocked`
  The port is blocked, connection exists.
- `disabled`
  The port is disabled.
- `not-connected`
  No connection exists.

The *Information* field displays messages for the redundancy configuration and the possible causes of detected errors.

When the device is operating as a ring client or a Ring Manager, the following messages are possible:

- *Redundancy available*
  The redundancy is set up. When a component of the ring is down, the redundant line takes over its function.
- *Configuration error: Error on ringport link.*
  An error is detected in the cabling of the ring ports.

When the device is operating as a Ring Manager, the following messages are possible:

- *Configuration error: Packets from another ring manager received.*
  Another device exists in the ring that is operating as the Ring Manager. Activate the *Ring manager* function on exactly one device in the ring.
- *Configuration error: Ring link is connected to wrong port.*
  A line in the ring is connected with a different port instead of with a ring port. The device only receives test data packets on one ring port.

When applicable, integrate the MRP ring into a VLAN. To do this, perform the following steps:

☐ In the *VLAN ID* field, define the MRP VLAN ID. The MRP VLAN ID determines in which of the configured VLANs the device transmits the MRP packets.
To set the MRP VLAN ID, first configure the VLANs and the corresponding egress rules in the *Switching > VLAN > Configuration* dialog.
– If the MRP-Ring is not assigned to a VLAN (like in this example), then leave the VLAN ID as `0`.
In the *Switching > VLAN > Configuration* dialog, specify the VLAN membership as `U` (untagged) for the ring ports in VLAN `1`.
– If the MRP-Ring is assigned to a VLAN, then enter a VLAN ID >`0`.
In the *Switching > VLAN > Configuration* dialog, specify the VLAN membership as `T` (tagged) for the ring ports in the selected VLAN.

`mrp domain modify vlan <0..4042>`	Assigns the VLAN ID.

Parallel Redundancy Protocol (PRP)

Unlike ring redundancy protocols, PRP uses 2 separate LANs for uninterrupted availability. On the path from the sender to the receiver, PRP sends 2 data packets in parallel via the 2 mutually independent LANs. The receiver processes the first data packet received and discards the second data packet of the pair. The international standard IEC 62439-3 defines the Parallel Redundancy Protocol (PRP).

NOTE: When PRP is active, it uses the interfaces 1/1 and 1/2. As seen in the *Switching > VLAN*, *Switching > Rate Limiter* and *Switching > Filter for MAC Addresses* dialogs, the *PRP* function replaces the interfaces 1/1 and 1/2 with the interface prp/1. Configure the VLAN membership, the rate limiting, and the MAC filtering for the interface prp/1.

Implementation

When the upper protocol layers send a data packet, the PRP interface creates a “twin packet” from the original packet. The PRP interface then transmits one data packet of the pair to each participating LAN simultaneously. The packets traverse different LANs and therefore have different run times.

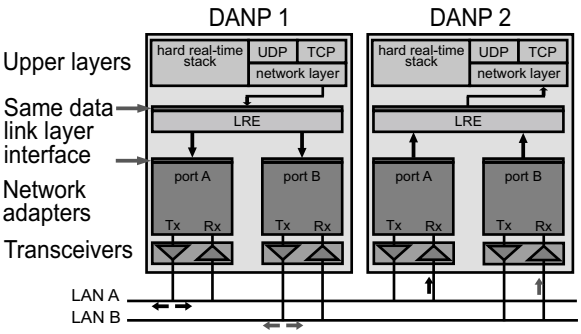
The receiving PRP interface forwards the first packet of a pair towards the upper protocol layers and discards the second packet. When viewed from the application, a PRP interface functions like a standard Ethernet interface.

The PRP interface or a Redundancy Box (RedBox) injects a Redundancy Control Trailer (RCT) into each packet. The RCT is a 48-bit identification field that identifies the duplicates. This field contains LAN identification (LAN A or B), information about the length of the payload, and a 16-bit sequence number. The twin packets therefore differ only in the LAN identification and, as a result, in the FCS checksum. The PRP interface increments the sequence number for each packet sent. Using the unique attributes included in each packet, such as physical MAC source address and sequence number, the receiving RedBox or Double Attached Node (DAN) interface identifies and discards duplicates.

Depending on the packet size, with PRP it attains a reduced throughput of the available bandwidth, due to the addition of the RCT trailer.

LRE Functionality

Each Double Attached Node implementing PRP (DANP) has 2 LAN ports that operate in parallel. The Link Redundancy Entity (LRE) connects the upper protocol layers with every individual port.



The LRE has the following tasks:

- Handling of duplicates
- Management of redundancy

When transmitting packets from the upper protocol layers, the LRE sends them from both ports at nearly the same time. The 2 data packets pass through the LANs with different delays. When the device receives the first data packet, the LRE forwards it to the upper protocol layers and discards the second data packet received.

For the upper protocol layers, the LRE behaves like a normal port.

To identify the twin packets, the LRE attaches an RCT with a sequential number to the packets. The LRE also periodically sends multicast PRP supervision packets and evaluates the multicast PRP supervision packets of the other RedBoxes and DANPs.

The device lets you view the received supervision packet entries. The entries in the *Switching > L2-Redundancy > PRP > DAN/VDAN Table* are helpful for detecting redundancy and connection issues. For example, in an index the *Last seen B* timestamp resets and the *Last seen A* timestamp remains the same. The *Last seen A* and *Last seen B* timestamps steadily resetting indicate a normal condition.

NOTE: According to IEC 62439, the Entry Forget Time is 400 ms. The Entry Forget Time is the time after which the device removes an entry from the duplicate table. When the device receives the 2nd packet of a pair after 400 ms or later, the device processes the 2nd packet instead of discarding it. To help prevent this, use a maximum bandwidth of 90%.

NOTE: If the inter-frame gap is shorter than the latency between the 2 LANs, then a frame-ordering mismatch can occur. Frame-ordering mismatch is a phenomenon of the PRP protocol. The only solution to help avoid a frame-ordering mismatch is to verify that the inter-frame gap is greater than the latency between the LANs.

PRP Network Structure

PRP uses 2 independent LANs. The topology of each of these LANs is arbitrary, and ring, star, bus and meshed topologies are possible.

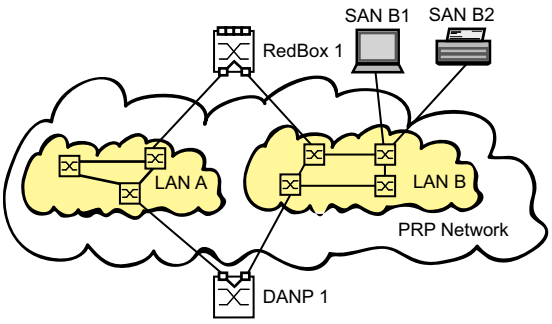
The main advantage of PRP is zero recovery time with an active (transit) LAN. When the end device receives no packets from one of the LANs, the second (transit) LAN maintains the connection. As long as one (transit) LAN is available, repairs and maintenance on the other (transit) LAN have no impact on the data packet transmission.

The elementary devices of a PRP network are the RedBox (Redundancy Box) and the DANP (Double Attached Node implementing PRP). Both devices have one connection each to the (transit) LANs.

The devices in the (transit) LAN are conventional switches. The devices transmit PRP data packets transparently, without evaluating the RCT information.

NOTE: The RCT trailer increases the packet size by 6 bytes. Configure the MTU size ≥ 1524 bytes for LAN A and B devices.

Terminal devices that connect directly to a device in the (transit) LAN are SANs (Single Attached Nodes). SANs connected to a LAN have no redundancy. To use the PRP redundant network, connect the SAN to the PRP network via a RedBox.

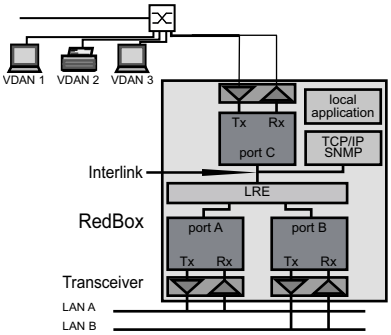


Connecting RedBoxes and DANPs to a PRP network

DANPs have 2 interfaces for the connection to the PRP network. A RedBox is a DANP that contains additional switch ports. Use the switch ports to integrate one or more SANs into the PRP network redundantly.

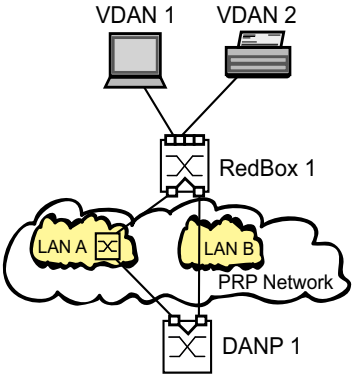
When sending a data packet to the PRP network, the Link Redundancy Entity (LRE) in the RedBox creates a twin packet. When the LRE receives the first data packet of the twin pair, the LRE forwards the data packet, and discards the second data packet of the twin pair.

NOTE: The RedBox supports up to 128 hosts. If you attempt to support more than 128 hosts with the RedBox, then the device drops packets.



Example Configuration

The following example uses a PRP network with 4 devices. Verify that the LAN A and LAN B ports contain 100 Mbit/s optical SFP interfaces. Connect Port A to LAN A and Port B to LAN B.



NOTE: *PRP* is available for devices with an FPGA (hardware for extended functions). The product code indicates if your device supports *PRP*. To use the functions, load the device software supporting *PRP*.

The *PRP* function reserves ports *1/1* and *1/2*. This removes the possibility of using other redundancy protocols such as Spanning Tree or MRP in parallel on ports *1/1* and *1/2*.

- ☐ If you use Spanning Tree in parallel to PRP, then deactivate Spanning Tree on ports *1/1* and *1/2*. Also deactivate the *Root guard*, *TCN guard*, and *Loop guard* functions on ports *1/1* and *1/2*.
- ☐ If you use MRP in parallel to PRP, then specify the other free device ports as MRP-Ring ports.

Configure both the RedBox 1 and DANP 1 devices. To do this, perform the following steps:

- ☐ Open the *Switching > L2-Redundancy > PRP > Configuration* dialog.

In the *Supervision packet receiver* frame, perform the following step:

- ☐ To analyze received PRP supervision packets, activate the *Evaluate supervision packets* checkbox.

In the *Supervision packet sender* frame, perform the following steps:

- ☐ To transmit PRP supervision packets from this device, activate *Active*.
- ☐ The device sends either only its own PRP supervision packets, or sends both its own supervision packets and packets of connected devices. To transmit packets for VDANs listed in the *Switching > L2-Redundancy > PRP > DAN/VDAN Table*, select the *Send VDAN packets* checkbox. When deactivated, the device forwards only its own supervision packets. After installing new PRP devices, deactivate this function to maintain a clear overview of the PRP supervision packets on remote devices.
- ☐ To enable the ports, in the *Port A* and *Port B* frames, select the value *On*.
- ☐ To enable the function, select in the *Operation* frame the *On* radio button.
- ☐ Save the changes temporarily. To do this, click the button.
- ☐ To load the configuration saved in the volatile memory, click the button.
- ☐ Open the *Switching > L2-Redundancy > PRP > Proxy Node Table* dialog to view the terminating VDAN devices for which this device provides PRP conversion.
- ☐ To remove this list, click *Reset*.
- ☐ To load the list of connected devices, click the button.
- ☐ Open the *Switching > L2-Redundancy > PRP > Statistics* dialog to view the quality of the traffic that traverses the device. The device detects errors and displays them according to MIB Managed Objects and the respective link.
- ☐ To remove the entry in the statistics table, click *Reset*.
- ☐ To load the updated statistics, click the button.

The device lets you view the received supervision packet entries. The entries in the *Switching > L2-Redundancy > PRP > DAN/VDAN Table* are helpful for detecting redundancy and connection issues. For example, in an index the *Last seen B* timestamp resets and the *Last seen A* timestamp remains the same. The *Last seen A* and *Last seen A* timestamps steadily resetting indicate a normal condition.

⚠ WARNING

UNINTENDED EQUIPMENT OPERATION

If you deactivate the *PRP* function, then deactivate either Port A or B to help prevent network loops.

Failure to follow these instructions can result in death, serious injury, or equipment damage.

`enable`	Change to the Privileged EXEC mode.
`configure`	Change to the Configuration mode.
`no mrp operation`	Disable the option.
`no spanning-tree operation`	Disable the option.
`interface 1/1`	Change to the interface configuration mode of interface *1/1*.

`no shutdown`	Enable the interface.
`exit`	Change to the Configuration mode.
`interface 1/2`	Change to the interface configuration mode of interface *1/2*.
`no shutdown`	Enable the interface.
`exit`	Change to the Configuration mode.
`prp instance 1 supervision evaluate`	Enable evaluation of received supervision packets.
`prp instance 1 supervision send`	Enable supervision packet transmission.
`prp instance 1 supervision redbox-exclusively`	Sends supervision packets only for this RedBox. Use the `no` form of the command to send supervision packets for each connected VDAN and this RedBox. The prerequisite is that you enable the supervision packet send function.
`prp operation`	Enable the *PRP* function.
`show prp counters`	Display the PRP counters.
`show prp node-table`	Display the node table.
`show prp proxy-node-table`	Display the proxy node table.

Spanning Tree

NOTE: The Spanning Tree Protocol is a protocol for MAC bridges. For this reason, the following description uses the term bridge for the device.

Local networks are getting bigger and bigger. This applies to both the geographical expansion and the number of network participants. Therefore, it is advantageous to use multiple bridges, for example:

- to reduce the network load in sub-areas,
- to set up redundant connections and
- to overcome distance limitations.

However, using multiple bridges with multiple redundant connections between the subnetworks can lead to loops and thus interruption of communication across the network. To help avoid this, you can use Spanning Tree. Spanning Tree enables loop-free switching through the systematic deactivation of redundant connections. Redundancy enables the systematic reactivation of individual connections as needed.

RSTP is a further development of the Spanning Tree Protocol (STP) and is compatible with it. When a connection or a bridge becomes inoperable, the STP requires a maximum of 30 seconds to reconfigure. This is no longer acceptable in time-sensitive applications. RSTP achieves average reconfiguration times of less than a second. When you use RSTP in a ring topology with 10 to 20 devices, you can even achieve reconfiguration times in the order of milliseconds.

NOTE: RSTP reduces a layer 2 network topology with redundant paths into a tree structure (Spanning Tree) that does not contain any more redundant paths. One of the devices takes over the role of the root bridge here. The maximum number of devices permitted in an active branch (from the root bridge to the tip of the branch) is specified by the variable *Max age*. The preset value for *Max age* is `20`, which can be increased up to `40`.

If the device working as the root is inoperable and another device takes over its function, then the *Max age* setting of the new root bridge determines the maximum number of devices allowed in a branch.

NOTE: The RSTP standard requires that every device within a network operates with the (Rapid) Spanning Tree Algorithm. When STP and RSTP are used at the same time, the advantages of faster reconfiguration with RSTP are lost in the network segments that are operated in combination.

A device that only supports RSTP works together with MSTP devices by not assigning an MST region to itself, but rather the CST (Common Spanning Tree).

Basics

Because RSTP is a further development of the STP, every of the following descriptions of the STP also apply to RSTP.

The Tasks of the STP

The Spanning Tree Algorithm reduces network topologies built with bridges and containing ring structures due to redundant links to a tree structure. In doing so, STP opens ring structures according to preset rules by deactivating redundant paths. When a path is interrupted because a network component becomes inoperable, STP reactivates the previously deactivated path again. This lets redundant links increase the availability of communication.

STP determines a bridge that represents the STP tree structure‘s base. This bridge is called root bridge.

Features of the STP algorithm:
- automatic reconfiguration of the tree structure in the case of a bridge becoming inoperable or the interruption of a data path
- the tree structure is stabilized up to the maximum network size,
- stabilization of the topology within a short time period
- topology can be specified and reproduced by the administrator
- transparency for the end devices
- low network load relative to the available transmission capacity due to the tree structure created

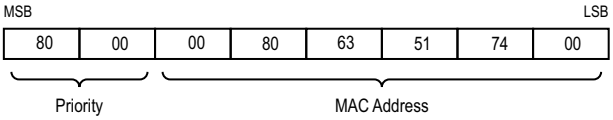
Bridge Parameters

In the context of Spanning Tree, each bridge and its connections are uniquely described by the following parameters:
- Bridge Identifier
- Root Path Cost for the bridge ports,
- Port Identifier

Bridge Identifier

The Bridge Identifier consists of 8 bytes. The 2 highest-value bytes are the priority. When configuring the network, the Management Administrator can change the default setting for the priority number which is 32768 (8000H). The 6 lowest-value bytes of the bridge identifier are the bridge's MAC address. The MAC address lets each bridge have unique bridge identifiers.

The bridge with the smallest number for the bridge identifier has the highest priority.

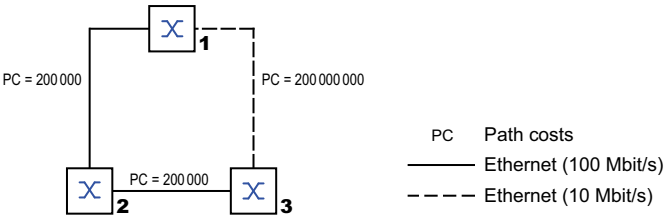


Root Path Cost

Each path that connects 2 bridges is assigned a cost for the transmission (path cost). The device determines this value based on the transmission speed. The device assigns a higher path cost to paths with lower transmission speeds.

Alternatively, the Administrator can set the path cost. Like the device, the Administrator assigns a higher path cost to paths with lower transmission speeds. However, since the Administrator can choose this value freely, he/she has a tool with which he/she can give a certain path an advantage among redundant paths.

The root path cost is the sum of the individual costs of those paths that a data packet has to traverse from a connected bridge's port to the root bridge.

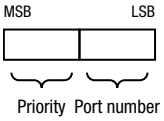


Data Rate	Typical Value	Typical Range	Possible Range
≤100 kbit/s	200 000 000[1]	20 000 000-200 000 000	1-200 000 000
1 Mbit/s	20 000 000[1]	2 000 000-200 000 000	1-200 000 000
10 Mbit/s	2 000 000[1]	200 000-20 000 000	1-200 000 000
100 Mbit/s	200 000[1]	20 000-2 000 000	1-200 000 000
1 Gbit/s	20 000	2 000-200 000	1-200 000 000
10 Gbit/s	2 000	200-20 000	1-200 000 000
100 Gbit/s	200	20-2 000	1-200 000 000
1 Tbit/s	20	2-200	1-200 000 000
10 Tbit/s	2	1-20	1-200 000 000

1. Verify that bridges, which conform to IEEE 802.1D-1998 and only support 16-bit values for the past costs, use the value 65535 (FFFFH) for path costs in cases where they are used in conjunction with bridges that support 32-bit values for the path costs.

Port Identifier

The port identifier consists of 2 bytes. One part, the lower-value byte, contains the physical port number. This provides a unique identifier for the port of this bridge. The second, higher-value part is the port priority, which is specified by the Administrator (default value: 128). It also applies here that the port with the smallest number for the port identifier has the highest priority.

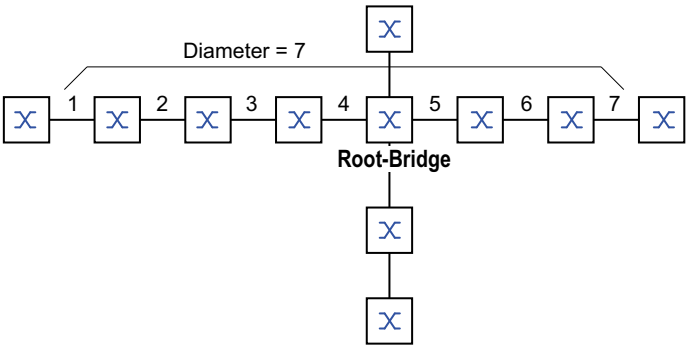


Max Age and Diameter

The “Max Age” and “Diameter” values largely determine the maximum expansion of a Spanning Tree network.

Diameter

The number of connections between the devices in the network that are furthest removed from each other is known as the network diameter.



The network diameter that can be achieved in the network is MaxAge-1.

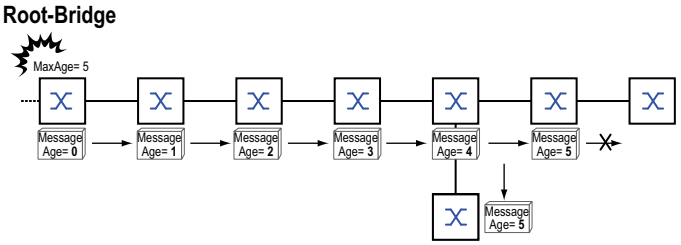
In the state on delivery, MaxAge = 20 and the maximum diameter that can be achieved = 19. When you set the maximum value of 40 for MaxAge, the maximum diameter that can be achieved = 39.

MaxAge

Every STP-BPDU contains a “MessageAge” counter. When a bridge is passed through, the counter increases by 1.

Before forwarding a STP-BPDU, the bridge compares the “MessageAge” counter with the “MaxAge” value specified in the device:

- When MessageAge < MaxAge, the bridge forwards the STP-BPDU to the next bridge.
- When MessageAge = MaxAge, the bridge discards the STP-BPDU.



Rules for Creating the Tree Structure

Bridge information

To determine the tree structure, the bridges need more detailed information about the other bridges located in the network.

To obtain this information, each bridge sends a BPDU (Bridge Protocol Data Unit) to the other bridges.

The contents of a BPDU include:

- Bridge identifier
- Root path costs
- Port identifier

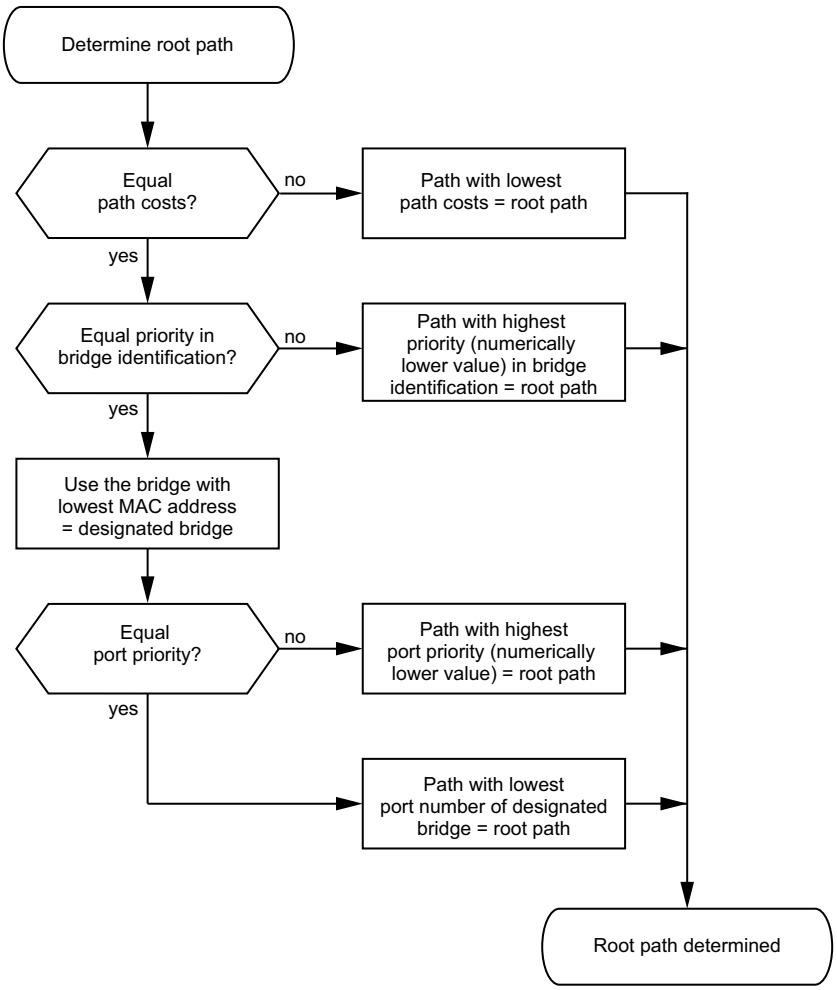
(see IEEE 802.1D)

Setting up the Tree Structure

The bridge with the smallest number for the bridge identifier is called the root bridge. It is (or will become) the root of the tree structure.

The structure of the tree depends on the root path costs. Spanning Tree selects the structure so that the path costs between each individual bridge and the root bridge become as small as possible.

- When there are multiple paths with the same root path costs, the bridge further away from the root determines which port it blocks. For this purpose, it uses the bridge identifiers of the bridge closer to the root. The bridge blocks the port that leads to the bridge with the numerically higher ID (a numerically higher ID is the logically worse one). When 2 bridges have the same priority, the bridge with the numerically larger MAC address has the numerically higher ID, which is logically the worse one.
- When multiple paths with the same root path costs lead from one bridge to the same bridge, the bridge further away from the root uses the port identifier of the other bridge as the last criterion. See section “Port Identifier” on page 153. In the process, the bridge blocks the port that leads to the port with the numerically higher ID (a numerically higher ID is the logically worse one). When 2 ports have the same priority, the port with the higher port number has the numerically higher ID, which is logically the worse one.



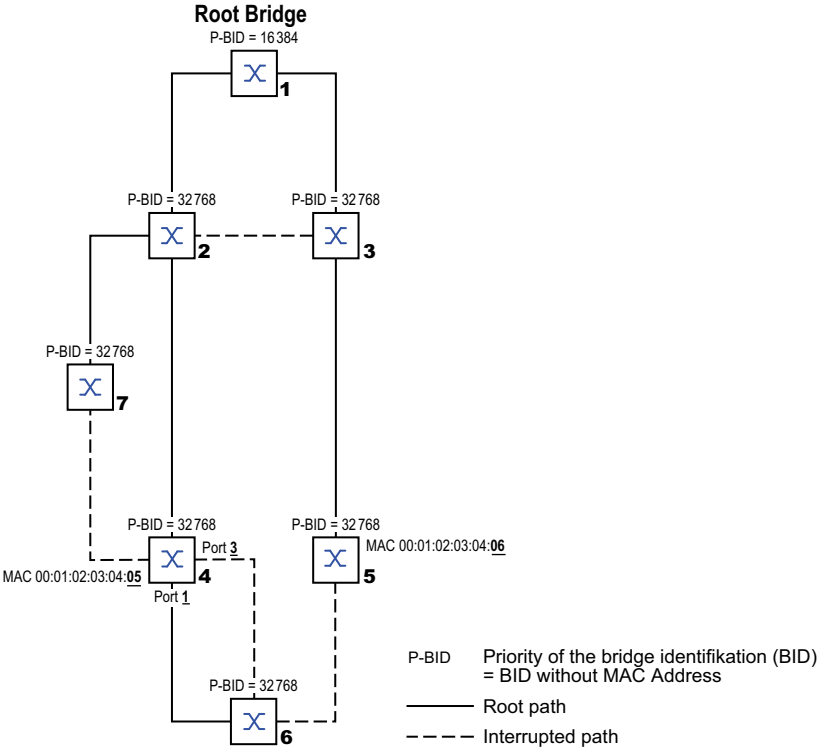
Examples

Example of Determining the Root Path

You can use the network plan illustrated hereafter to follow the flow chart given in section “Setting up the Tree Structure” on page 155 for determining the root path. The administrator has specified a priority in the bridge identification for each bridge. The bridge with the smallest numerical value for the bridge identification takes on the role of the root bridge, in this case, bridge 1. In the example every sub-path has the same path costs. The protocol blocks the path between bridge 2 and bridge 3 as a connection from bridge 3 via bridge 2 to the root bridge would result in higher path costs.

The path from bridge 6 to the root bridge is interesting:

- The path via bridge 5 and bridge 3 creates the same root path costs as the path via bridge 4 and bridge 2.
- STP selects the path using the bridge that has the lowest MAC address in the bridge identification (bridge 4 in the illustration).
- There are also 2 paths between bridge 6 and bridge 4.
  The port identifier is decisive here (Port 1 < Port 3).



NOTE: When the present root bridge goes down, the MAC address in the bridge identifier alone determines which bridge becomes the new root bridge, because the Administrator does not change the default values for the priorities of the bridges in the bridge identifier, apart from the value for the root bridge.

Example of Manipulating the Root Path

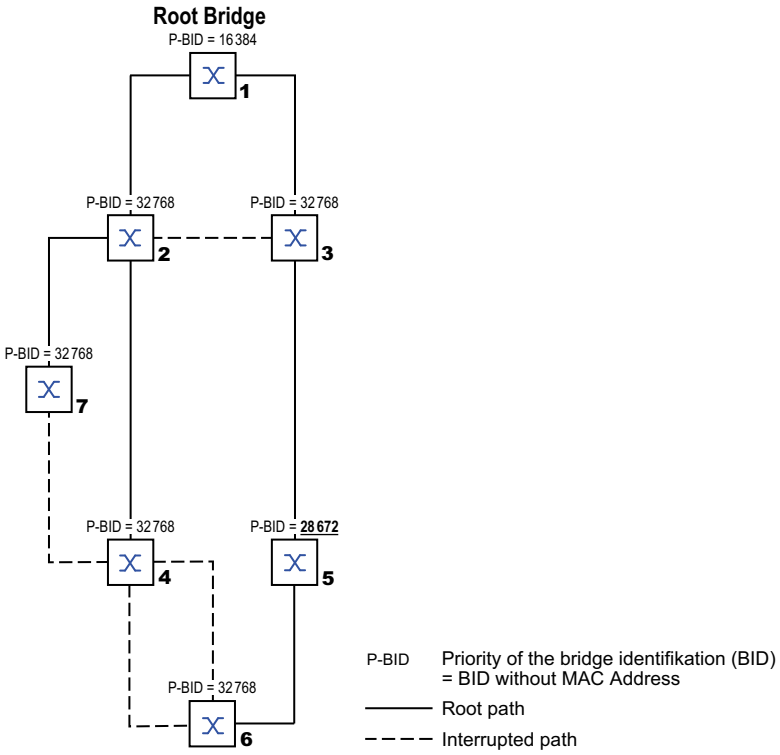
You can use the network plan illustrated hereafter to follow the flow chart given in section “Setting up the Tree Structure” on page 155 for determining the root path. The Administrator has performed the following:

- Left the default value of 32768 (8000H) for every bridge apart from bridge 1 and bridge 5, and
- assigned to bridge 1 the value 16384 (4000H), thus making it the root bridge.
- To bridge 5, he/she assigned the value 28672 (7000H).

The protocol blocks the path between bridge 2 and bridge 3 as a connection from bridge 3 via bridge 2 to the root bridge would mean higher path costs.

The path from bridge 6 to the root bridge is interesting:

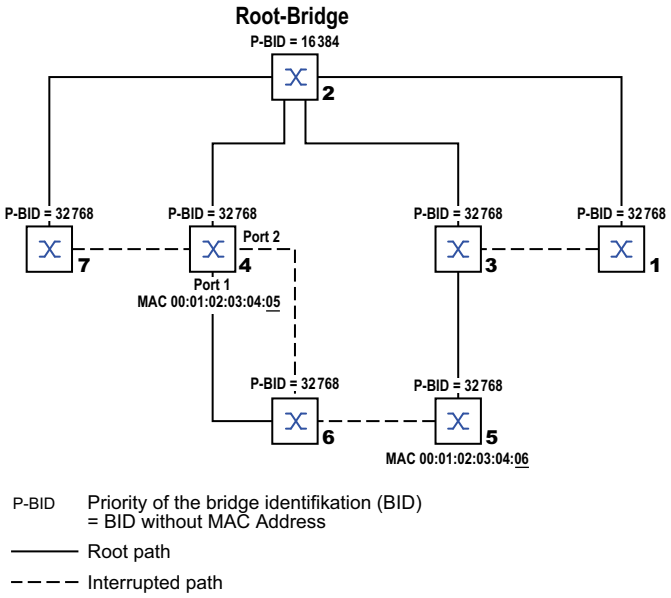
▶ The bridges select the path via bridge 5 because the value 28672 for the priority in the bridge identifier is smaller than value 32768.



Example of Manipulating the Tree Structure

The Management Administrator soon discovers that this configuration with bridge 1 as the root bridge is invalid. On the paths from bridge 1 to bridge 2 and bridge 1 to bridge 3, the control packets which the root bridge sends to every other bridge add up.

When the Management Administrator configures bridge 2 as the root bridge, the burden of the control packets on the subnetworks is distributed much more evenly. The result is the configuration illustrated hereafter. The path costs for most of the bridges to the root bridge have decreased.



The Rapid Spanning Tree Protocol

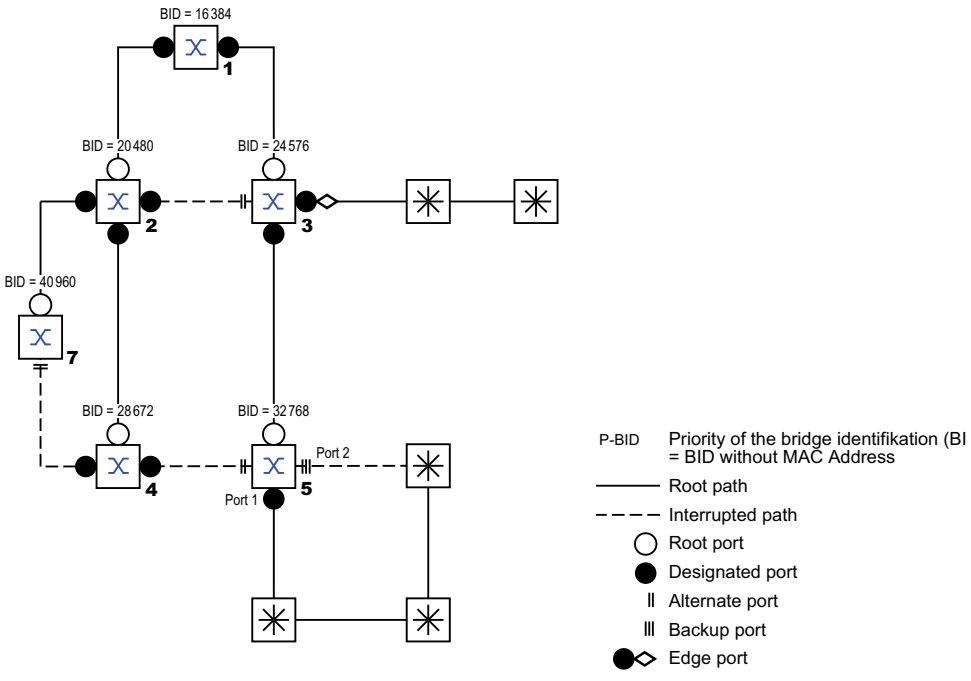
The RSTP uses the same algorithm for determining the tree structure as STP. When a link or bridge becomes inoperable, RSTP merely changes parameters, and adds new parameters and mechanisms that speed up the reconfiguration.

The ports play a significant role in this context.

Port Roles

RSTP assigns each bridge port one of the following roles:

- Root Port:
  This is the port at which a bridge receives data packets with the lowest path costs from the root bridge.
  When there are multiple ports with equally low path costs, the bridge ID of the bridge that leads to the root (designated bridge) determines which of its ports is given the role of the root port by the bridge further away from the root.
  When a bridge has multiple ports with equally low path costs to the same bridge, the bridge uses the port ID of the bridge leading to the root (designated bridge) to determine which port it selects locally as the root port. See the flow chart given in section “Setting up the Tree Structure” on page 155.
  The root bridge does not have a root port.
- Designated port:
  The bridge in a network segment that has the lowest root path costs is the designated bridge.
  When more than one bridge has the same root path costs, the bridge with the smallest value bridge identifier becomes the designated bridge. The designated port on this bridge is the port that connects a network segment leading away from the root bridge. When a bridge is connected to a network segment with more than one port (via a hub, for example), the bridge gives the role of the designated port to the port with the better port ID.
- Edge port
  Every network segment with no additional RSTP bridges is connected with exactly one designated port. In this case, this designated port is also an edge port. The distinction of an edge port is the fact that it does not receive any RST BPDUs (Rapid Spanning Tree Bridge Protocol Data Units).
- Alternate port
  When the connection to the root bridge is lost, this blocked port takes over the task of the root port. The alternate port provides a backup for the connection to the root bridge.
- Backup port
  This is a blocked port that serves as a backup in case the connection to the designated port of this network segment (without any RSTP bridges) is lost
- Disabled port
  This is a port that does not participate in the Spanning Tree Operation, that means, the port is switched off or does not have any connection.



Port states

Depending on the tree structure and the state of the selected connection paths, the RSTP assigns the ports their states.

STP Port state	Administrative Bridge Port state	MAC Operational	RSTP Port state	Active Topology (port Role)
DISABLED	Disabled	FALSE	Discarding[1]	Excluded (disabled)
DISABLED	Enabled	FALSE	Discarding[a]	Excluded (disabled)
BLOCKING	Enabled	TRUE	Discarding[2]	Excluded (alternate, backup)
LISTENING	Enabled	TRUE	Discarding[b]	Included (root, designated)
LEARNING	Enabled	TRUE	Learning	Included (root, designated)
FORWARDING	Enabled	TRUE	Forwarding	Included (root, designated)

1. The dot1d-MIB displays “Disabled”.
2. The dot1d-MIB displays “Blocked”.

Meaning of the RSTP port states:
- Disabled: Port does not belong to the active topology
- Discarding: No address learning in FDB, no data traffic except for STP-BPDUs
- Learning: Address learning active (FDB), no data traffic apart from STP-BPDUs
- Forwarding: Address learning active (FDB), sending and receiving of every packet type (not only STP-BPDUs)

Spanning Tree Priority Vector

To assign roles to the ports, the RSTP bridges exchange configuration information with each other. This information is known as the Spanning Tree Priority Vector. It is part of the RSTP BPDUs and contains the following information:
- Bridge identification of the root bridge
- Root path costs of the sending bridge
- Bridge identification of the sending bridge
- Port identifiers of the ports through which the message was sent
- Port identifiers of the ports through which the message was received

Based on this information, the bridges participating in RSTP are able to determine port roles themselves and define the port states of their own ports.

Fast Reconfiguration

Why can RSTP react faster than STP to an interruption of the root path?

- Introduction of edge-ports:
  During a reconfiguration, RSTP sets an edge port into the transmission mode after 3 seconds (default setting). To ascertain that no bridge sending BPDUs is connected, RSTP waits for the “Hello Time” to elapse.
  When you verify that an end device is and remains connected to this port, there are no waiting times at this port in the case of a reconfiguration.
- Introduction of alternate ports:
  As the port roles are already distributed in normal operation, a bridge can immediately switch from the root port to the alternate port after the connection to the root bridge is lost.
- Communication with neighboring bridges (point-to-point connections):
  Decentralized, direct communication between neighboring bridges enables reaction without wait periods to status changes in the spanning tree topology.
- Address table:
  With STP, the age of the entries in the FDB determines the updating of communication. RSTP immediately deletes the entries in those ports affected by a reconfiguration.
- Reaction to events:
  Without having to adhere to any time specifications, RSTP immediately reacts to events such as connection interruptions, connection reinstatements, etc.

NOTE: Data packages could be duplicated and/or arrive in an incorrect order at the recipient during the reconfiguration phase of the RSTP topology. You may also use the Spanning Tree Protocol or select another redundancy procedure described in this manual.

Configuring the Device

⚠ WARNING

UNINTENDED EQUIPMENT OPERATION

- To help avoid loops during the configuration phase, configure each device of the *Spanning Tree* configuration individually.
- Before you connect the redundant lines, complete the configuration of the other devices of the *Spanning Tree* configuration.

Failure to follow these instructions can result in death, serious injury, or equipment damage.

RSTP configures the network topology completely autonomously. The device with the lowest bridge priority automatically becomes the root bridge. However, to define a specific network structure regardless, you specify a device as the root bridge. In general, a device in the backbone takes on this role.

Perform the following steps:

- ☐ Set up the network to meet your requirements, initially without redundant lines.
- ☐ You deactivate the flow control on the participating ports.
  If the flow control and the redundancy function are active at the same time, it is possible that the redundancy function operates differently than intended.
  (Default setting: flow control deactivated globally and activated on every port.)

☐ Disable MRP on every device.
☐ Enable Spanning Tree on every device in the network.
In the state on delivery, Spanning Tree is switched on in the device.

Perform the following steps:

☐ Open the *Switching > L2-Redundancy > Spanning Tree > Global* dialog.
☐ Enable the function.
☐ Save the changes temporarily. To do this, click the ✓ button.

`enable`	Change to the Privileged EXEC mode.
`configure`	Change to the Configuration mode.
`spanning-tree operation`	Enables Spanning Tree.
`show spanning-tree global`	Displays the parameters for checking.

Now connect the redundant lines.

Define the settings for the device that takes over the role of the root bridge.

Perform the following steps:

☐ In the *Priority*field you enter a numerically lower value.
The bridge with the numerically lowest bridge ID has the highest priority and becomes the root bridge of the network.
☐ Save the changes temporarily. To do this, click the ✓ button.

`spanning-tree mst priority 0 <0..61440>`	Specifies the bridge priority of the device. **NOTE:** Specify the bridge priority in the range `0..61440` in steps of 4096.

After saving, the dialog shows the following information:
- The *Bridge is root* checkbox is selected.
- The *Root port* field shows the value `0.0`.
- The *Root path cost* field shows the value `0`.

`show spanning-tree global`	Displays the parameters for checking.

☐ If applicable, then change the values in the *Forward delay [s]* and *Max age* fields.
– The root bridge transmits the changed values to the other devices.
☐ Save the changes temporarily. To do this, click the ✓ button.

`spanning-tree forward-time <4..30>`	Specifies the delay time for the status change in seconds.
`spanning-tree max-age <6..40>`	Specifies the maximum permissible branch length, for example the number of devices to the root bridge.
`show spanning-tree global`	Displays the parameters for checking.

NOTE: The parameters *Forward delay [s]* and *Max age* have the following relationship:

Forward delay [s] ≥ (*Max age*/2) + 1

If you enter values in the fields that contradict this relationship, then the device replaces these values with the last valid values or with the default value.

NOTE: When possible, do not change the value in the “Hello Time” field.

Verify the following values in the other devices:
- Bridge ID (bridge priority and MAC address) of the corresponding device and the root bridge.
- Number of the device port that leads to the root bridge.
- Path cost from the root port of the device to the root bridge.

Perform the following steps:

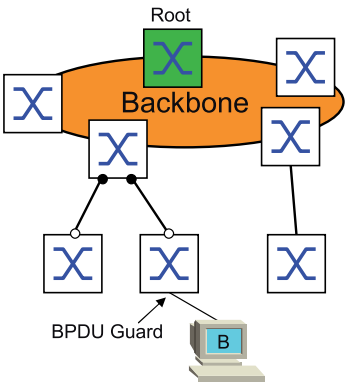
`show spanning-tree global`	Displays the parameters for checking.

Guards

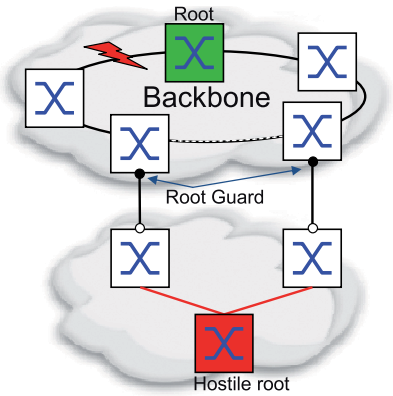
The device lets you activate various protection functions (guards) in the device ports.

The following protection functions help protect your network from incorrect configurations, loops and attacks with STP-BPDUs:

- BPDU Guard – for manually specified edge ports (end device ports)
  You activate this protection function globally in the device.

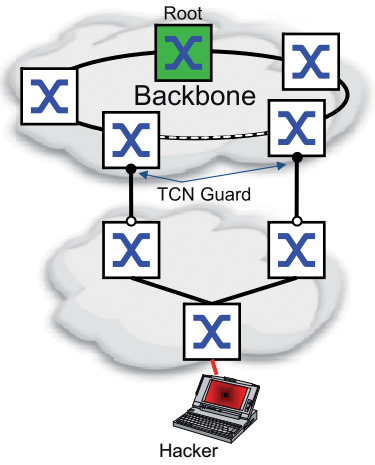


  Terminal device ports do not normally receive any STP-BPDUs. If an attacker still attempts to feed in STP-BPDUs on this port, then the device deactivates the device port.
- Root Guard – for designated ports
  You activate this protection function separately for every device port.

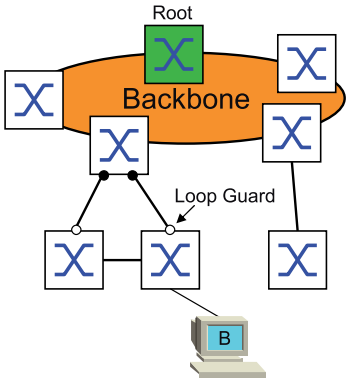


  When a designated port receives an STP-BPDU with better path information to the root bridge, the device discards the STP-BPDU and sets the transmission state of the port to `discarding` instead of `root`.
  When there are no STP-BPDUs with better path information to the root bridge, after 2 × *Hello time [s]* the device resets the state of the port to a value according to the port role.

- TCN Guard – for ports that receive STP-BPDUs with a Topology Change flag
  You activate this protection function separately for every device port.



  If the protection function is activated, then the device ignores Topology Change flags in received STP-BPDUs. This does not change the content of the address table (FDB) of the device port. However, additional information in the BPDU that changes the topology is processed by the device.
- Loop Guard – for root, alternate and backup ports
  You activate this protection function separately for every device port.



  If the port does not receive any more STP-BPDUs, then this protection function helps prevent the transmission status of a port from unintentionally being changed to `forwarding`. If this situation occurs, then the device designates the loop status of the port as inconsistent, but does not forward any data packets.

Activating the BPDU Guard

Perform the following steps:

- ☐ Open the *Switching > L2-Redundancy > Spanning Tree > Global* dialog.
- ☐ Select the *BPDU guard* checkbox.
- ☐ Save the changes temporarily. To do this, click the ✓ button.

`enable`	Change to the Privileged EXEC mode.
`configure`	Change to the Configuration mode.
`spanning-tree bpdu-guard`	Activates the BPDU Guard.
`show spanning-tree global`	Displays the parameters for checking.

- ☐ Open the *Switching* > *L2-Redundancy* > *Spanning Tree* > *Port* dialog.
- ☐ Switch to the *CIST* tab.
- ☐ For end device ports, select the checkbox in the *Admin edge port*column.
- ☐ Save the changes temporarily. To do this, click the ✔ button.

`interface <x/y>`	Change to the interface configuration mode of interface `<x/y>`.
`spanning-tree edge-port`	Designates the port as a terminal device port (edge port).
`show spanning-tree port x/y`	Displays the parameters for checking.
`exit`	Leaves the interface mode.

When an edge port receives an STP-BPDU, the device behaves as follows:

- ▶ The device deactivates this port.
  In the *Basic Settings* > *Port* dialog, *Configuration* tab, the checkbox for this port in the *Port on* column is cleared.
- ▶ The device designates the port.

You can determine if a port has disabled itself because of a received a BPDU. To do this, perform the following steps:

In the *Switching* > *L2-Redundancy* > *Spanning Tree* > *Port* dialog, *Guards* tab, the checkbox in the *BPDU guard effect* column is `selected`.

`show spanning-tree port x/y`	Displays the parameters of the port for checking. The value of the *BPDU guard effect* parameter is `enabled`.

Reset the status of the device port to the value `forwarding`. To do this, perform the following steps:

- ☐ When the port still receives BPDUs:
  - – Remove the manual definition as an edge port (end device port).
    or
  - – Deactivate the BPDU Guard.
- ☐ Activate the device port again.

Activating Root Guard / TCN Guard / Loop Guard

Perform the following steps:

- ☐ Open the *Switching > L2-Redundancy > Spanning Tree > Port* dialog.
- ☐ Switch to the *Guards* tab.
- ☐ For designated ports, select the checkbox in the *Root guard* column.
- ☐ For ports that receive STP-BPDUs with a Topology Change flag, select the checkbox in the *TCN guard* column.
- ☐ For root, alternate or backup ports, select the checkbox in the *Loop guard* column.

NOTE: The *Root guard* and *Loop guard* functions are mutually exclusive. If you try to activate the *Root guard* function while the *Loop guard* function is active, then the device deactivates the *Loop guard* function.

- ☐ Save the changes temporarily. To do this, click the ✔ button.

`enable`	Change to the Privileged EXEC mode.
`configure`	Change to the Configuration mode.
`interface <x/y>`	Change to the interface configuration mode of interface `<x/y>`.
`spanning-tree guard-root`	Switches the Root Guard on at the designated port.
`spanning-tree guard-tcn`	Switches the TCN Guard on at the port that receives STP-BPDUs with a Topology Change flag.
`spanning-tree guard-loop`	Switches the Loop Guard on at a root, alternate or backup port.
`exit`	Leaves the interface mode.
`show spanning-tree port x/y`	Displays the parameters of the port for checking.

Link Aggregation

The *Link Aggregation* function using the single switch method helps you overcome 2 limitations with Ethernet links, namely bandwidth, and redundancy.

The *Link Aggregation* function helps you overcome bandwidth limitations of individual ports. The *Link Aggregation* function lets you combine 2 or more links in parallel, creating 1 logical link between 2 devices. The parallel links increase the bandwidth for traffic between the 2 devices.

You typically use the *Link Aggregation* function on the network backbone. The function provides you an inexpensive way to incrementally increase bandwidth.

Furthermore, the *Link Aggregation* function provides for redundancy. When a link goes down, with 2 or more links configured in parallel, the other links in the group continue to forward traffic.

The default settings for a new *Link Aggregation* instance are as follows:
- In the *Active* column, the checkbox is selected.
- In the *Send trap (Link up/down)* column, the checkbox is selected.
- In the *Static link aggregation* column, the checkbox is cleared.
- In the *Active ports (min.)* column, the value is `1`.

Methods of Operation

The device operates on the Single Switch method. The Single Switch method provides you an inexpensive way to grow your network. The single switch method states that you need one device on each side of a link to provide the physical ports. The device balances the traffic load across the group member ports.

The device also uses the Same Link Speed method in which the group member ports are full-duplex, point-to-point links having the same transmission rate. The first port that you add to the group is the master port and determines the bandwidth for the other member ports of the Link Aggregation Group.

The device lets you set up up to 1 Link Aggregation groups. The number of useable ports per Link Aggregation group depends on the device.

Link Aggregation Example

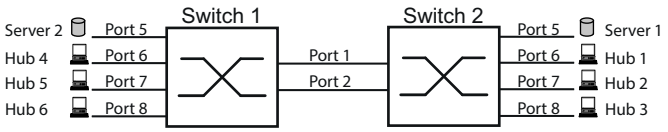
⚠ WARNING

UNINTENDED EQUIPMENT OPERATION

- To help avoid loops during the configuration phase, configure each device of the *Link Aggregation* configuration individually.
- Before you connect the redundant lines, complete the configuration of the other devices of the *Link Aggregation* configuration.

Failure to follow these instructions can result in death, serious injury, or equipment damage.

Connect multiple workstations using one aggregated link group between Switch 1 and 2. By aggregating multiple links, higher speeds are achievable without a hardware upgrade.



Configure Switch 1 and 2 in the GUI. To do this, perform the following steps:

- ☐ Open the *Switching > L2-Redundancy > Link Aggregation* dialog.
- ☐ Click the button.
  The dialog displays the *Create* window.
- ☐ In the *Trunk port* drop-down list, select the instance number of the link aggregation group.
- ☐ In the *Port* drop-down list, select port *1/1*.
- ☐ Click the *Ok* button.
- ☐ Repeat the preceding steps and select the port *1/2*.
- ☐ Click the *Ok* button.
- ☐ Save the changes temporarily. To do this, click the button.

`enable`	Change to the Privileged EXEC mode.
`configure`	Change to the Configuration mode.
`link-aggregation add lag/1`	Creates a Link Aggregation Group `lag/1`.
`link-aggregation modify lag/1 addport 1/1`	Adds port *1/1* to the Link Aggregation Group.
`link-aggregation modify lag/1 addport 1/2`	Adds port *1/2* to the Link Aggregation Group.

Link Backup

Link Backup provides a redundant link for traffic on Layer 2 devices. When the device detects an error on the primary link, the device transfers traffic to the backup link. You typically use Link Backup in service-provider or enterprise networks.

You set up the backup links in pairs, one as a primary and one as a backup. When providing redundancy for enterprise networks for example, the device lets you set up more than one pair. The maximum number of link backup pairs is: total number of physical ports / 2. Furthermore, when the state of a port participating in a link backup pair changes, the device sends an SNMP trap.

When configuring link backup pairs, remember the following rules:

- A link pair consists of any combination of physical ports. For example, one port is a 100 Mbit port and the other is a 1000 Mbit SFP port.
- A specific port is a member of one link backup pair at any given time.
- Verify that the ports of a link backup pair are members of the same VLAN with the same VLAN ID. When the primary port or backup port is a member of a VLAN, assign the second port of the pair to the same VLAN.

The default setting for this function is inactive without any link backup pairs.

NOTE: Verify that the Spanning Tree Protocol is disabled on the Link Backup ports.

Fail back Description

Link Backup also lets you set up a *Fail back* option. When you activate the *Fail back* function and the primary link returns to normal operation, the device first blocks traffic on the backup port and then forwards traffic on the primary port. This process helps protect the device from causing loops in the network.

When the primary port returns to the link up and active state, the device supports 2 modes of operation:

- When you inactivate *Fail back*, the primary port remains in the blocking state until the backup link fails.
- When you activate *Fail back*, and after the *Fail back delay [s]* timer expires, the primary port returns to the forwarding state and the backup port changes to down.

In the cases listed above, the port forcing its link to forward traffic, first sends a "flush FDB" packet to the remote device. The flush packet helps the remote device quickly rediscover the MAC addresses.

Example Configuration

⚠ WARNING

UNINTENDED EQUIPMENT OPERATION

- To help avoid loops during the configuration phase, configure each device of the *Link Backup* configuration individually.
- Before you connect the redundant lines, complete the configuration of the other devices of the *Link Backup* configuration.

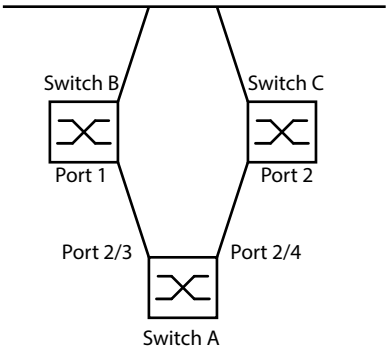
Failure to follow these instructions can result in death, serious injury, or equipment damage.

In the example network below, you connect ports *2/3* and *2/4* on Switch A to the uplink Switches B and C. When you set up the ports as a Link Backup pair, one of the ports forwards traffic and the other port is in the blocking mode.

The primary, port *2/3* on Switch A, is the active port and is forwarding traffic to port 1 on Switch B. Port *2/4* on Switch A is the backup port and blocks traffic.

When Switch A disables port *2/3* because of a detected error, port *2/4* on Switch A starts forwarding traffic to port 2 on Switch C.

When port *2/3* returns to the active state, “no shutdown“, with *Fail back* activated, and *Fail back delay [s]* set to 30 seconds. After the timer expires, port *2/4* first blocks the traffic and then port *2/3* starts forwarding the traffic.



The following tables contain examples of parameters to configure Switch A.

Perform the following steps:

- ☐ Open the *Switching > L2-Redundancy > Link Backup* dialog.
- ☐ Enter a new Link Backup pair in the table:
  - ☐ Click the button.
    The dialog displays the *Create* window.
  - ☐ In the *Primary port* drop-down list, select port *2/3*.
    In the *Backup port* drop-down list, select port *2/4*.
  - ☐ Click the *Ok* button.
- ☐ In the *Description* textbox, enter `Link_Backup_1` as the name for the backup pair.
- ☐ To activate the *Fail back* function for the link backup pair, select the *Fail back* checkbox.
- ☐ Set the timer for the link backup pair, enter `30` s in *Fail back delay [s]*.
- ☐ To activate the link backup pair, select the *Active* checkbox.
- ☐ To enable the function, select the *On* radio button in the *Operation* frame.

`enable`	Change to the Privileged EXEC mode.
`configure`	Change to the Configuration mode.
`interface 2/3`	Change to the interface configuration mode of interface *2/3*.
`link-backup add 2/4`	Creates a Link Backup instance where port *2/3* is the primary port and port *2/4* is the backup port.
`link-backup modify 2/4 description Link_Backup_1`	Specifies the string `Link_Backup_1` as the name of the backup pair.
`link-backup modify 2/4 failback-status enable`	Enable the *Fail back delay [s]*.
`link-backup modify 2/4 failback-time 30`	Specify the time for the *Fail back delay [s]* as `30` s.
`link-backup modify 2/4 status enable`	Enable the Link Backup instance.
`exit`	Change to the Configuration mode.
`link-backup operation`	Enable the *Link Backup* function globally in the device.

Operation Diagnosis

The device provides you with the following diagnostic tools:
- Sending SNMP traps
- Monitoring the Device Status
- Out-of-Band signaling using the signal contact
- Port status indication
- Event counter at port level
- Detecting non-matching duplex modes
- Auto-Disable
- Displaying the SFP status
- Topology discovery
- Detecting IP address conflicts
- Detecting loops
- Reports
- Monitoring data traffic on a port (port mirroring)
- Syslog
- Event log
- Cause and action management during selftest

Sending SNMP Traps

The device immediately reports unusual events which occur during normal operation to the network management station. This is done by messages called SNMP traps that bypass the polling procedure (“polling” means querying the data stations at regular intervals). SNMP traps allow you to react quickly to unusual events.

Examples of such events are:
- Hardware reset
- Changes to the configuration
- Segmentation of a port

The device sends SNMP traps to various hosts to increase the transmission reliability for the messages. The unacknowledged SNMP trap message consists of a packet containing information about an unusual event.

The device sends SNMP traps to those hosts entered in the trap destination table. The device lets you configure the trap destination table with the network management station using SNMP.

List of SNMP Traps

The following table displays possible SNMP traps sent by the device.

Name of the SNMP Trap	Meaning
authenticationFailure	When a station attempts to access an agent without authorisation, this trap is sent.
coldStart	Sent after a restart.
sa2DevMonSenseExtNvmRemoval	When the external memory has been removed, this trap is sent.
linkDown	When the connection to a port is interrupted, this trap is sent.
linkUp	When connection is established to a port, this trap is sent.
sa2DevMonSensePSState	When the status of a power supply unit changes, this trap is sent.
sa2SigConStateChange	When the status of the signal contact changes in the operation monitoring, this trap is sent.
newRoot	When the sending agent becomes the new root of the spanning tree, this trap is sent.
topologyChange	When the port changes from blocking to forwarding or from forwarding to blocking, this trap is sent.
alarmRisingThreshold	When the RMON input exceeds its upper threshold, this trap is sent.
alarmFallingThreshold	When the RMON input goes below its lower threshold, this trap is sent.
sa2AgentPortSecurityViolation	When a MAC address detected on this port does not match the settings of the parameter sa2AgentPortSecurityEntry, this trap is sent.
sa2DiagSelftestActionTrap	When a self test for the four categories “task”, “resource”, “software”, and “hardware” is performed according to the configured settings, this trap is sent.
sa2MrpReconfig	When the configuration of the MRP ring changes, this trap is sent.
sa2DiagIfaceUtilizationTrap	When the threshold of the interface exceeds or undercuts the upper or lower threshold specified, this trap is sent.
sa2LogAuditStartNextSector	When the audit trail after completing one sector starts a new one, this trap is sent.
sa2PtpSynchronizationChance	When the status of the PTP synchronization has been changed, this trap is sent.
sa2ConfigurationSavedTrap	After the device has successfully saved its configuration locally, this trap is sent.
sa2ConfigurationChangedTrap	When you change the configuration of the device for the first time after it has been saved locally, this trap is sent.
sa2PlatformStpInstanceLoopInconsistentStartTrap	When the port in this STP instance changes to the “loop inconsistent” status, this trap is sent.
sa2PlatformStpInstanceLoopInconsistentEndTrap	When the port in this STP instance leaves the “loop inconsistent” status receiving a BPDU packet, this trap is sent.

SNMP Traps for Configuration Activity

After you save a configuration in the memory, the device sends a `sa2ConfigurationSavedTrap`. This SNMP trap contains both the state variables of non-volatile memory (*NVM*) and external memory (*ENVM*) indicating if the running configuration is in sync with the non-volatile memory, and with the external memory. You can also trigger this SNMP trap by copying a configuration file to the device, replacing the active saved configuration.

Furthermore, the device sends a `sa2ConfigurationChangedTrap`, whenever you change the local configuration, indicating a mismatch between the running and saved configuration.

SNMP Trap Setting

The device lets you send an SNMP trap as a reaction to specific events. Create at least one trap destination that receives SNMP traps.

Perform the following steps:

- ☐ Open the *Diagnostics > Status Configuration > Alarms (Traps)* dialog.
- ☐ Click the button.
  The dialog displays the *Create* window.
- ☐ In the *Name* frame, specify the name that the device uses to identify itself as the source of the SNMP trap.
- ☐ In the *Address* frame, specify the IP address of the trap destination to which the device sends the SNMP traps.
- ☐ In the *Active* column, select the entries that the device takes into account when it sends SNMP traps.
- ☐ Save the changes temporarily. To do this, click the button.

For example, in the following dialogs you specify when the device triggers an SNMP trap:

- *Basic Settings > Port* dialog
- *Network Security > Port Security* dialog
- *Switching > L2-Redundancy > Link Aggregation* dialog
- *Diagnostics > Status Configuration > Device Status* dialog
- *Diagnostics > Status Configuration > Security Status* dialog
- *Diagnostics > Status Configuration > Signal Contact* dialog
- *Diagnostics > Status Configuration > MAC Notification* dialog
- *Diagnostics > System > IP Address Conflict Detection* dialog
- *Diagnostics > System > Selftest* dialog
- *Diagnostics > Ports > Port Monitor* dialog

ICMP Messaging

The device lets you use the Internet Control Message Protocol (ICMP) for diagnostic applications, for example ping and trace route. The device also uses ICMP for time-to-live and discarding messages in which the device forwards an ICMP message back to the packet source device.

Use the ping network tool to test the path to a particular host across an IP network. The traceroute diagnostic tool displays paths and transit delays of packets across a network.

Monitoring the Device Status

The device status provides an overview of the overall condition of the device. Many process visualization systems record the device status for a device in order to present its condition in graphic form.

The device displays its status as `error` or `ok` in the *Device status* frame. The device determines this status from the individual monitoring results.

The device enables you to:
- Out-of-Band signalling using a signal contact
- signal the changed device status by sending an SNMP trap
- detect the device status in the *Basic Settings* > *System* dialog of the GUI
- query the device status in the CLI

The *Global* tab of the *Diagnostics* > *Status Configuration* > *Device Status* dialog lets you configure the device to send a trap to the management station for the following events:
- Incorrect supply voltage
  - at least one of the 2 supply voltages is not operating
  - the internal supply voltage is not operating
- When the device is operating outside of the user-defined temperature threshold
- Loss of the redundancy (in ring manager mode)
- The interruption of link connection(s)
  Configure at least one port for this feature. When the link is down, you specify which ports the device signals in the *Port* tab of the *Diagnostics* > *Status Configuration* > *Device Status* dialog in the *Propagate connection error* row.
- The removal of the external memory.
  The configuration in the external memory is out-of-sync with the configuration in the device.

Select the corresponding entries to decide which events the device status includes.

NOTE: With a non-redundant voltage supply, the device reports the absence of a supply voltage. To disable this message, feed the supply voltage over both inputs or ignore the monitoring.

Monitored Events

Name	Meaning
Temperature	Monitors in case the temperature exceeds or falls below the value specified.
Ring redundancy	When ring redundancy is present, enable this function.
Connection errors	Enable this function to monitor every port link event in which the *Propagate connection error* checkbox is active.
External memory removal	Enable this function to monitor the presence of an external storage device.
External memory not in sync	The device monitors synchronization between the device configuration and the configuration stored in the external memory (*ENVM*).
Power supply	Enable this function to monitor the power supply.

Configuring the Device Status

Perform the following steps:

- ☐ Open the *Diagnostics > Status Configuration > Device Status* dialog, *Global* tab.
- ☐ For the parameters to be monitored, select the checkbox in the *Monitor* column.
- ☐ To send an SNMP trap to the management station, activate the *Send trap* function in the *Traps* frame.
- ☐ In the *Diagnostics > Status Configuration > Alarms (Traps)* dialog, create at least one trap destination that receives SNMP traps.
- ☐ Save the changes temporarily. To do this, click the ✓ button.
- ☐ Open the *Basic Settings > System* dialog.
- ☐ To monitor the temperature, at the bottom of the *System data* frame, you specify the temperature thresholds.
- ☐ Save the changes temporarily. To do this, click the ✓ button.

`enable`	Change to the Privileged EXEC mode.
`configure`	Change to the Configuration mode.
`device-status trap`	When the device status changes, send an SNMP trap.
`device-status monitor envm-not-in-sync`	Monitors the configuration profiles in the device and in the external memory. The *Device status* changes to `error` in the following situations: • The configuration profile only exists in the device. • The configuration profile in the device differs from the configuration profile in the external memory.

`device-status monitor envm-removal`	Monitors the active external memory. When you remove the active external memory from the device, the value in the *Device status* frame changes to `error`.
`device-status monitor power-supply 1`	Monitors the power supply unit `1`. When the device has a detected power supply error, the value in the *Device status* frame changes to `error`.
`device-status monitor ring-redundancy`	Monitors the ring redundancy. The *Device status* changes to `error` in the following situations: • The redundancy function becomes active (loss of redundancy reserve). • The device is a normal ring participant and detects an error in its settings.
`device-status monitor temperature`	Monitors the temperature in the device. When the temperature exceeds or falls below the specified limit, the value in the *Device status* frame changes to `error`.

In order to enable the device to monitor an active link without a connection, first enable the global function, then enable the individual ports.

Perform the following steps:

- ☐ Open the *Diagnostics > Status Configuration > Device Status* dialog, *Global* tab.
- ☐ For the *Connection errors* parameter, select the checkbox in the *Monitor* column.
- ☐ Open the *Diagnostics > Status Configuration > Device Status* dialog, *Port* tab.
- ☐ For the *Propagate connection error* parameter, select the checkbox in the column of the ports to be monitored.
- ☐ Save the changes temporarily. To do this, click the ✔ button.

`enable`	Change to the Privileged EXEC mode.
`configure`	Change to the Configuration mode.
`device-status monitor link-failure`	Monitors the ports/interfaces link. When the link interrupts on a monitored port/interface, the value in the *Device status* frame changes to `error`.
`interface 1/1`	Change to the interface configuration mode of interface `1/1`.
`device-status link-alarm`	Monitors the port/interface link. When the link interrupts on the port/interface, the value in the *Device status* frame changes to `error`.

NOTE: The above commands activate monitoring and trapping for the supported components. When you want to activate or deactivate monitoring for individual components, you will find the corresponding syntax in the “Command Line Interface” reference manual or in the help of the CLI console. To display the help in CLI, insert a question mark `?` and press the **Enter** key.

Displaying the Device Status

Perform the following steps:

☐ Open the *Basic Settings > System* dialog.

`show device-status all`	In the EXEC Privilege mode: Displays the device status and the setting for the device status determination.

Security Status

The Security Status provides an overview of the overall security of the device. Many processes aid in system visualization by recording the security status of the device and then presenting its condition in graphic form. The device displays the overall security status in the *Basic Settings > System* dialog, *Security status* frame.

In the *Global* tab of the *Diagnostics > Status Configuration > Security Status* dialog the device displays its status as `error` or `ok` in the *Security status* frame. The device determines this status from the individual monitoring results.

The device enables you to:
- Out-of-Band signalling using a signal contact
- signal the changed security status by sending an SNMP trap
- detect the security status in the *Basic Settings > System* dialog of the GUI
- query the security status in the CLI

Monitored Events

Perform the following steps:
☐ Specify the events that the device monitors.
☐ For the corresponding parameter, select the checkbox in the *Monitor* column.

Name	Meaning
Password default settings unchanged	After installation change the passwords. When active and the default passwords remain unchanged, the device displays an alarm.
Min. password length < 8	Create passwords more than 8 characters long. When active, the device monitors the *Min. password length* setting.
Password policy settings deactivated	The device monitors the settings located in the *Device Security > User Management* dialog for password policy requirements.
User account password policy check deactivated	The device monitors the settings of the *Policy check* checkbox. When *Policy check* is inactive, the device sends an SNMP trap.

Name	Meaning
Telnet server active	The device monitors when you enable the *Telnet* function.
HTTP server active	The device monitors when you enable the *HTTP* function.
SNMP unencrypted	The device monitors when you enable the *SNMPv1* or *SNMPv2* function.
Access to system monitor with V.24 possible	The device monitors the System Monitor status.
Saving the configuration profile on the external memory possible	The device monitors the possibility to save configurations to the external non-volatile memory.
Link interrupted on enabled device ports	The device monitors the link status of active ports.
Access with Ethernet Switch Configurator possible	The device monitors when you enable the Ethernet Switch Configurator read/write access function.
Load unencrypted config from external memory	The device monitors the security settings for loading the configuration from the external NVM.
IEC61850-MMS active	The device monitors the IEC 61850-MMS protocol activation setting.
Modbus TCP active	The device monitors the Modbus TCP/IP protocol activation setting.
Self-signed HTTPS certificate present	The device monitors the HTTPS server for self-created digital certificates.

Configuring the Security Status

Perform the following steps:

- ☐ Open the *Diagnostics > Status Configuration > Security Status* dialog, *Global* tab.
- ☐ For the parameters to be monitored, select the checkbox in the *Monitor* column.
- ☐ To send an SNMP trap to the management station, activate the *Send trap* function in the *Traps* frame.
- ☐ Save the changes temporarily. To do this, click the button.
- ☐ In the *Diagnostics > Status Configuration > Alarms (Traps)* dialog, create at least one trap destination that receives SNMP traps.

`enable`	Change to the Privileged EXEC mode.
`configure`	Change to the Configuration mode.
`security-status monitor pwd-change`	To monitor the password for the locally set up user account `admin`. When the password for the `admin` account is the default setting, the value in the *Security status* frame changes to `error`.

`security-status monitor pwd-min-length`	Monitors the value specified in the *Min. password length* policy. When the value for the *Min. password length* policy is less than `8`, the value in the *Security status* frame changes to `error`.
`security-status monitor pwd-policy-config`	Monitors the password policy settings. When the value for at least one of the following policies is specified as `0`, the value in the *Security status* frame changes to `error`. • *Upper-case characters (min.)* • *Lower-case characters (min.)* • *Digits (min.)* • *Special characters (min.)*
`security-status monitor pwd-policy-inactive`	Monitors the password policy settings. When the value for at least one of the following policies is specified as `0`, the value in the *Security status* frame changes to `error`.
`security-status monitor telnet-enabled`	Monitors the Telnet server. When you enable the Telnet server, the value in the *Security status* frame changes to `error`.
`security-status monitor http-enabled`	Monitors the HTTP server. When you enable the HTTP server, the value in the *Security status* frame changes to `error`.
`security-status monitor snmp-unsecure`	Monitors the SNMP server. When at least one of the following conditions applies, the value in the *Security status* frame changes to `error`: • The *SNMPv1* function is enabled. • The *SNMPv2* function is enabled. • The encryption for SNMPv3 is disabled. You enable the encryption in the *Device Security > User Management* dialog, in the *SNMP encryption type* field.
`security-status monitor sysmon-enabled`	To monitor the activation of the System Monitor function in the device.
`security-status monitor extnvm-upd-enabled`	To monitor the activation of the external non volatile memory update.
`security-status monitor iec61850-mms-enabled`	Monitors the *IEC61850-MMS* function. When you enable the *IEC61850-MMS* function, the value in the *Security status* frame changes to `error`.
`security-status trap`	When the device status changes, it sends an SNMP trap.

In order to enable the device to monitor an active link without a connection, first enable the global function, then enable the individual ports.

Perform the following steps:

- ☐ Open the *Diagnostics > Status Configuration > Security Status* dialog, *Global* tab.
- ☐ For the *Link interrupted on enabled device ports* parameter, select the checkbox in the *Monitor* column.
- ☐ Save the changes temporarily. To do this, click the ✔ button.
- ☐ Open the *Diagnostics > Status Configuration > Device Status* dialog, *Port* tab.
- ☐ For the *Link interrupted on enabled device ports* parameter, select the checkbox in the column of the ports to be monitored.
- ☐ Save the changes temporarily. To do this, click the ✔ button.

`enable`	Change to the Privileged EXEC mode.
`configure`	Change to the Configuration mode.
`security-status monitor no-link-enabled`	Monitors the link on active ports. When the link interrupts on an active port, the value in the *Security status* frame changes to *`error`*.
`interface 1/1`	Change to the interface configuration mode of interface `1/1`.
`security-status monitor no-link`	Monitors the link on interface/port `1`.

Displaying the Security Status

Perform the following steps:

- ☐ Open the *Basic Settings > System* dialog.

`show security-status all`	In the EXEC Privilege mode, display the security status and the setting for the security status determination.

Out-of-Band Signaling

The device uses the signal contact to control external devices and monitor device functions. Function monitoring enables you to perform remote diagnostics.

The device reports the operating status using a break in the potential-free signal contact (relay contact, closed circuit) for the selected mode. The device monitors the following functions:

- Incorrect supply voltage
  - at least one of the 2 supply voltages is not operating
  - the internal supply voltage is not operating
- When the device is operating outside of the user-defined temperature threshold
- Events for ring redundancy
  Loss of the redundancy (in ring manager mode)
  In the default setting, ring redundancy monitoring is inactive. The device is a normal ring participant and detects an error in the local configuration.
- The interruption of link connection(s)
  Configure at least one port for this feature. In the *Propagate connection error* frame, you specify which ports the device signals for a link interruption. In the default setting, link monitoring is inactive.
- The removal of the external memory.
  The configuration in the external memory does not match the configuration in the device.

Select the corresponding entries to decide which events the device status includes.

NOTE: With a non-redundant voltage supply, the device reports the absence of a supply voltage. To disable this message, feed the supply voltage over both inputs or ignore the monitoring.

Controlling the Signal Contact

With the `Manual setting` mode you control this signal contact remotely.

Application options:

- Simulation of an error detected during SPS error monitoring
- Remote control of a device using SNMP, such as switching on a camera

Perform the following steps:

- ☐ Open the *Diagnostics > Status Configuration > Signal Contact* dialog, *Global* tab.
- ☐ To control the signal contact manually, in the *Configuration* frame, select the `Manual setting` item in the *Mode* drop-down list.
- ☐ To open the signal contact, you select the `open` radio button in the *Configuration* frame.
- ☐ To close the signal contact, you select the `close` radio button in the *Configuration* frame.
- ☐ Save the changes temporarily. To do this, click the button.

`enable`	Change to the Privileged EXEC mode.
`configure`	Change to the Configuration mode.
`signal-contact 1 mode manual`	Select the manual setting mode for signal contact `1`.
`signal-contact 1 state open`	Open signal contact `1`.
`signal-contact 1 state closed`	Close signal contact `1`.

Monitoring the Device and Security Statuses

In the *Configuration* field, you specify which events the signal contact indicates.

- *Device status*
  Using this setting the signal contact indicates the status of the parameters monitored in the *Diagnostics > Status Configuration > Device Status* dialog.
- *Security status*
  Using this setting the signal contact indicates the status of the parameters monitored in the *Diagnostics > Status Configuration > Security Status* dialog.
- *Device/Security status*
  Using this setting the signal contact indicates the status of the parameters monitored in the *Diagnostics > Status Configuration > Device Status* and the *Diagnostics > Status Configuration > Security Status* dialog.

Configuring the Operation Monitoring

Perform the following steps:

- ☐ Open the *Diagnostics > Status Configuration > Signal Contact* dialog, *Global* tab.
- ☐ To monitor the device functions using the signal contact, in the *Configuration* frame, specify the value *Monitoring correct operation* in the *Mode* field.
- ☐ For the parameters to be monitored, select the checkbox in the *Monitor* column.
- ☐ To send an SNMP trap to the management station, activate the *Send trap* function in the *Traps* frame.
- ☐ Save the changes temporarily. To do this, click the ✓ button.
- ☐ In the *Diagnostics > Status Configuration > Alarms (Traps)* dialog, create at least one trap destination that receives SNMP traps.
- ☐ Save the changes temporarily. To do this, click the ✓ button.
- ☐ You specify the temperature thresholds for the temperature monitoring in the *Basic Settings > System* dialog.

`enable`	Change to the Privileged EXEC mode.
`configure`	Change to the Configuration mode.
`signal-contact 1 monitor temperature`	Monitors the temperature in the device. When the temperature exceeds / falls below the threshold values, the signal contact opens.
`signal-contact 1 monitor ring-redundancy`	Monitors the ring redundancy. The signal contact opens in the following situations: • The redundancy function becomes active (loss of redundancy reserve). • The device is a normal ring participant and detects an error in its settings.
`signal-contact 1 monitor link-failure`	Monitors the ports/interfaces link. When the link interrupts on a monitored port/ interface, the signal contact opens.
`signal-contact 1 monitor envm-removal`	Monitors the active external memory. When you remove the active external memory from the device, the signal contact opens.
`signal-contact 1 monitor envm-not-in-sync`	Monitors the configuration profiles in the device and in the external memory. The signal contact opens in the following situations: • The configuration profile only exists in the device. • The configuration profile in the device differs from the configuration profile in the external memory.
`signal-contact 1 monitor power-supply 1`	Monitors the power supply unit `1`. When the device has a detected power supply error, the signal contact opens.
`signal-contact 1 monitor module-removal 1`	Monitors module `1`. When you remove module `1` from the device, the signal contact opens.
`signal-contact 1 trap`	Enables the device to send an SNMP trap when the status of the operation monitoring changes.
`no signal-contact 1 trap`	Disabling the SNMP trap

In order to enable the device to monitor an active link without a connection, first enable the global function, then enable the individual ports.

Perform the following steps:

- ☐ In the *Monitor* column, activate the *Link interrupted on enabled device ports* function.
- ☐ Open the *Diagnostics > Status Configuration > Device Status* dialog, *Port* tab.

`enable`	Change to the Privileged EXEC mode.
`configure`	Change to the Configuration mode.
`signal-contact 1 monitor link-failure`	Monitors the ports/interfaces link. When the link interrupts on a monitored port/ interface, the signal contact opens.
`interface 1/1`	Change to the interface configuration mode of interface `1/1`.
`signal-contact 1 link-alarm`	Monitors the port/interface link. When the link interrupts on the port/interface, the signal contact opens.

Monitored Events

Name	Meaning
Temperature	When the temperature exceeds or falls below the value specified.
Ring redundancy	When ring redundancy is present, enable this function to monitor.
Connection errors	Enable this function to monitor every port link event in which the *Propagate connection error* checkbox is active.
External memory not in sync with NVM	The device monitors synchronization between the device configuration and the configuration stored in the external memory (*ENVM*).
External memory removed	Enable this function to monitor the presence of an external storage device.
Power supply	Enable this function to monitor the power supply.

Displaying the Signal Contact's Status

The device gives you additional options for displaying the status of the signal contact:

- Display in the GUI
- Query in the CLI

Perform the following steps:

☐ Open the *Basic Settings > System* dialog.
The *Signal contact status* frame displays the signal contact status and informs you about alarms that have occurred. When an alarm exists, the frame is highlighted.

`show signal-contact 1 all`	Displays signal contact settings for the specified signal contact.

Port Status Indication

To view the status of the ports, perform the following steps:

☐ Open the *Basic Settings > System* dialog.

The dialog displays the device with the configuration. Furthermore, the dialog indicates the status of the individual ports with a symbol.

The following symbols represent the status of the individual ports. In some situations, these symbols interfere with one another. When you position the mouse pointer over the port icon, a bubble help displays a detailed description of the port state.

Criterion	Symbol
Bandwidth of the port	10 Mbit/s Port activated, connection okay, full-duplex mode 100 Mbit/s Port activated, connection okay, full-duplex mode 1000 Mbit/s Port activated, connection okay, full-duplex mode
Operating state	Half-duplex mode enabled See the *Basic Settings > Port* dialog, *Configuration* tab, *Automatic configuration* checkbox, *Manual configuration* field and *Manual cable crossing (Auto. conf. off)* field. Autonegotiation enabled See the *Basic Settings > Port* dialog, *Configuration* tab, *Automatic configuration* checkbox. The port is blocked by a redundancy function.
AdminLink	The port is deactivated, connection okay The port is deactivated, no connection set up See the *Basic Settings > Port* dialog, *Configuration* tab, *Port on* checkbox and *Link/Current settings* field.

Port Event Counter

The port statistics table lets experienced network administrators identify possible detected issues in the network.

This table displays the contents of various event counters. The packet counters add up the events sent and the events received. In the *Basic Settings > Restart* dialog, you can reset the event counters.

Counter	Indication of possible Weakness
Received fragments	• Non-functioning controller of the connected device • Electromagnetic interference in the transmission medium
CRC Error	• Non-functioning controller of the connected device • Electromagnetic interference in the transmission medium • Inoperable component in the network
Collisions	• Non-functioning controller of the connected device • Network over extended/lines too long • Collision or a detected error with a data packet

Perform the following steps:

- ☐ To display the event counter, open the *Basic Settings > Port* dialog, *Statistics* tab.
- ☐ To reset the counters, in the *Basic Settings > Restart* dialog, click the *Clear port statistics* button.

Detecting Non-matching Duplex Modes

Issues occur when 2 ports directly connected to each other have mismatching duplex modes. These issues are difficult to track down. The automatic detection and reporting of this situation has the benefit of recognizing mismatching duplex modes before issues occur.

This situation arises from an incorrect configuration, for example, deactivation of the automatic configuration on the remote port.

A typical effect of this non-matching is that at a low data rate, the connection seems to be functioning, but at a higher bi-directional traffic level the local device records a lot of detected CRC errors, and the connection falls significantly below its nominal capacity.

The device lets you detect this situation and report it to the network management station. In the process, the device evaluates the detected error counters of the port in the context of the port settings.

Possible Causes of Port Error Events

The following table lists the duplex operating modes for TX ports, with the possible error events. The meanings of terms used in the table are as follows:

- Collisions
  In half-duplex mode, collisions mean normal operation.
- Duplex issue
  Mismatching duplex modes.
- EMI
  Electromagnetic interference.
- Network extension
  The network extension is too great, or too many cascading hubs.
- Collisions, Late Collisions
  In full-duplex mode, no incrementation of the port counters for collisions or Late Collisions.
- CRC Error
  The device evaluates these detected errors as non-matching duplex modes in the manual full duplex mode.

Nb	Automatic Configuration	Present Duplex Mode	Detected Error Events (≥ 10 after Link Up)	Duplex Modes	Possible causes
1	selected	Half duplex	None	OK	
2	selected	Half duplex	Collisions	OK	
3	selected	Half duplex	Late Collisions	Duplex issue detected	Duplex issue, EMI, network extension
4	selected	Half duplex	CRC Error	OK	EMI
5	selected	Full duplex	None	OK	
6	selected	Full duplex	Collisions	OK	EMI
7	selected	Full duplex	Late Collisions	OK	EMI
8	selected	Full duplex	CRC Error	OK	EMI
9	cleared	Half duplex	None	OK	
10	cleared	Half duplex	Collisions	OK	
11	cleared	Half duplex	Late Collisions	Duplex issue detected	Duplex issue, EMI, network extension
12	cleared	Half duplex	CRC Error	OK	EMI
13	cleared	Full duplex	None	OK	
14	cleared	Full duplex	Collisions	OK	EMI
15	cleared	Full duplex	Late Collisions	OK	EMI
16	cleared	Full duplex	CRC Error	Duplex issue detected	Duplex issue, EMI

Auto-Disable

The device can disable a port due to several configurable reasons. Each reason causes the port to “shut down”. In order to recover the port from the shut down state, you can manually clear the condition which caused the port to shut down or specify a timer to automatically re-enable the port.

If the configuration displays a port as enabled, but the device detects an error or change in the condition, then the software shuts down that port. In other words, the device software disables the port because of a detected error or change in the condition.

If a port is auto-disabled, then the device effectively shuts down the port and the port blocks traffic. The port LED flashes green 3 times per period and identifies the reason for the shutdown. In addition, the device creates a log file entry which lists the causes of the deactivation. When you re-enable the port after a timeout using the *Auto-Disable* function, the device generates a log entry.

The *Auto-Disable* function provides a recovery function which automatically enables an auto-disabled port after a user-defined time. When this function enables a port, the device sends an SNMP trap with the port number, but without a value for the *Reason* parameter.

The *Auto-Disable* function serves the following purposes:
- It assists the network administrator in port analysis.
- It reduces the possibility that this port causes the network to be instable.

The *Auto-Disable* function is available for the following functions:
- *Link flap* (*Port Monitor* function)
- *CRC/Fragments* (*Port Monitor* function)
- Duplex Mismatch detection (*Port Monitor* function)
- *Spanning Tree*
- *Port Security*
- *Overload detection* (*Port Monitor* function)
- *Link speed/Duplex mode detection* (*Port Monitor* function)

In the following example, you configure the device to disable a port due to detected violations to the thresholds specified the *Diagnostics > Ports > Port Monitor* dialog, *CRC/Fragments* tab, and then automatically re-enable the disabled port.

Perform the following steps:

- ☐ Open the *Diagnostics > Ports > Port Monitor* dialog, *CRC/Fragments* tab.
- ☐ Verify that the thresholds specified in the table concur to your preferences for port `1/1`.
- ☐ Open the *Diagnostics > Ports > Port Monitor* dialog, *Global* tab.
- ☐ To enable the function, select the `On` radio button in the *Operation* frame.
- ☐ To allow the device to disable the port due to detected errors, select the checkbox in the *CRC/Fragments on* column for port `1/1`.

☐ In the *Action* column you can choose how the device reacts to detected errors. In this example, the device disables port `1/1` for threshold violations and then automatically re-enables the port.
▶ To allow the device to disable and automatically re-enable the port, select the value `auto-disable` and configure the *Auto-Disable* function. The value `auto-disable` only works in conjunction with the *Auto-Disable* function.
The device can also disable a port without auto re-enabling.
▶ To allow the device to disable the port only, select the value `disable port`.
To manually re-enable a disabled port, select the port.
Click the ☰ button and then the *Reset* item.
▶ When you configure the *Auto-Disable* function, the value `disable port` also automatically re-enables the port.

☐ Open the *Diagnostics > Ports > Port Monitor* dialog, *Auto-disable* tab.

☐ To allow the device to auto re-enable the port after it was disabled due to detected threshold violations, select the checkbox in the *CRC error* column.

☐ Open the *Diagnostics > Ports > Port Monitor* dialog, *Port* tab.

☐ Specify the delay time as 120 s in the *Reset timer [s]* column for the ports you want to enable.

NOTE: The *Reset* item lets you enable the port before the time specified in the *Reset timer [s]* column counts down.

`enable`	Change to the Privileged EXEC mode.
`configure`	Change to the Configuration mode.
`interface 1/1`	Change to the interface configuration mode of interface `1/1`.
`port-monitor condition crc-fragments count 2000`	Specifying the CRC-Fragment counter to 2000 parts per million.
`port-monitor condition crc-fragments interval 15`	Sets the measure interval to 15 seconds for CRC-Fragment detection.
`auto-disable timer 120`	Specifies the waiting period of `120` seconds, after which the *Auto-disable* function re-enables the port.
`exit`	Change to the Configuration mode.
`auto-disable reason crc-error`	Activate the auto-disable CRC function.
`port-monitor condition crc-fragments mode`	Activate the CRC-Fragments condition to trigger an action.
`port-monitor operation`	Activate the *Port Monitor* function.

When the device disables a port due to threshold violations, the device lets you use the following commands to manually reset the disabled port.

Perform the following steps:

`enable`	Change to the Privileged EXEC mode.
`configure`	Change to the Configuration mode.
`interface 1/1`	Change to the interface configuration mode of interface `1/1`.
`auto-disable reset`	Lets you enable the port before the Timer counts down.

Displaying the SFP Status

The SFP status display lets you look at the SFP module connections and their properties. The properties include:

- module type
- serial number of media module
- temperature in ° C
- transmission power in mW
- receive power in mW

Perform the following step:

☐ Open the *Diagnostics > Ports > SFP* dialog.

Topology Discovery

IEEE 802.1AB defines the Link Layer Discovery Protocol (LLDP). LLDP lets you automatically detect the LAN network topology.

Devices with LLDP active:

- broadcast their connection and management information to neighboring devices on the shared LAN. When the receiving device has its *LLDP* function active, evaluation of the devices occur.
- receive connection and management information from neighbor devices on the shared LAN, provided these adjacent devices also have LLDP active.
- build a management information database and object definitions for storing information about adjacent devices with LLDP active.

As the main element, the connection information contains an exact, unique identifier for the connection end point: MAC (Service Access Point). This is made up of a device identifier which is unique on the entire network and a unique port identifier for this device.

- Chassis identifier (its MAC address)
- Port identifier (its port-MAC address)
- Description of port
- System name
- System description
- Supported system capabilities
- Active system capabilities
- Interface ID of the management address
- VLAN-ID of the port
- Auto-negotiation status on the port
- Medium, half/full duplex setting and port speed setting
- Information about the VLANs installed in the device (VLAN-ID and VLAN name, irrespective of whether the port is a VLAN participant).

A network management station can call up this information from devices with activated LLDP. This information enables the network management station to map the topology of the network.

Non-LLDP devices normally block the special Multicast LLDP IEEE MAC address used for information exchange. Non-LLDP devices therefore discard LLDP packets. If you position a non-LLDP capable device between 2 LLDP capable devices, then the non-LLDP capable device prohibits information exchanges between the 2 LLDP capable devices.

The Management Information Base (MIB) for a device with LLDP capability holds the LLDP information in the lldp MIB and in the private SA2-LLDP-EXT-HM-MIB and SA2-LLDP-MIB.

Displaying the Topology Discovery Results

Display the topology of the network. To do this, perform the following step:

- ☐ Open the *Diagnostics > LLDP > Topology Discovery* dialog, *LLDP* tab.

When you use a port to connect several devices, for example via a hub, the table contains a line for each connected device.

Activating Display FDB Entries at the bottom of the table lets you display devices without active LLDP support in the table. In this case, the device also includes information from its FDB (forwarding database).

If you connect the port to devices with the topology discovery function active, then the devices exchange LLDP Data Units (LLDPDU) and the topology table displays these neighboring devices.

When a port connects only devices without an active topology discovery, the table contains a line for this port to represent the connected devices. This line contains the number of connected devices.

The FDB address table contains MAC addresses of devices that the topology table hides for the sake of clarity.

LLDP-Med

LLDP for Media Endpoint Devices (LLDP-MED) is an extension to LLDP that operates between endpoint devices. Endpoints include devices such as IP phones, or other Voice over IP (VoIP) devices or servers and network devices such as switches. It specifically provides support for VoIP applications. LLDP-MED provides this support using an additional set of common type-length-value (TLV) advertisement messages, for capabilities discovery, network policy, Power over Ethernet, inventory management and location information.

The device supports the following TLV messages:

- capabilities TLV
  Lets the LLDP-MED endpoints determine the capabilities that the connected device supports and what capabilities the device has enabled.
- Network policy TLV
  Lets both network connectivity devices and endpoints advertise VLAN configurations and associated attributes for the specific application on that port. For example, the device notifies a phone of the VLAN number. The phone connects to a switch, obtain its VLAN number, and then starts communicating with the call control.

LLDP-MED provides the following functions:

- Network policy discovery, including VLAN ID, 802.1p priority and Diffserv code point (DSCP)
- Device location and topology discovery based on LAN-level MAC/port information
- Endpoint move detection notification, from network connectivity device to the associated VoIP management application
- Extended device identification for inventory management
- Identification of endpoint network connectivity capabilities, for example, multi-port IP Phone with embedded switch or bridge capability
- Application level interactions with the LLDP protocol elements to provide timely startup of LLDP to support rapid availability of an Emergency Call Service
- Applicability of LLDP-MED to Wireless LAN environments, support for Voice over Wireless LAN

Detecting Loops

Loops in the network cause connection interruptions or data loss. This also applies to temporary loops. The automatic detection and reporting of this situation lets you detect it faster and diagnose it more easily.

⚠ WARNING

UNINTENDED EQUIPMENT OPERATION

- To help avoid loops during the configuration phase, configure each device of the ring individually.
- Before you connect the redundant lines, complete the configuration of the other devices of the ring configuration.

Failure to follow these instructions can result in death, serious injury, or equipment damage.

An incorrect configuration causes loops, for example, deactivating Spanning Tree.

The device lets you detect the effects typically caused by loops and report this situation automatically to the network management station. You have the option here to specify the magnitude of the loop effects that trigger the device to send a report.

BPDU frames sent from the designated port and received on either a different port of the same device or the same port within a short time, is a typical effect of a loop.

To verify if the device has detected a loop, perform the following steps:

- ☐ Open the *Switching* > *L2-Redundancy* > *Spanning Tree* > *Port* dialog, *CIST* tab.
- ☐ Verify the value in the *Port state* and *Port role* fields. If the *Port state* field displays the value `discarding` and the *Port role* field displays the value `backup`, then the port is in a loop status.
  or
- ☐ Open the *Switching* > *L2-Redundancy* > *Spanning Tree* > *Port* dialog, *Guards* tab.
- ☐ Verify the value in the *Loop state* column. If the field displays the value `true`, then the port is in a loop status.

Reports

The following lists reports and buttons available for diagnostics:

- System Log file
  The log file is an HTML file in which the device writes device-internal events.
- Audit Trail
  Logs successful commands and user comments. The file also includes SNMP logging.
- Persistent Logging
  When the external memory is present, the device saves log entries in a file in the external memory. These files are available after power down. The maximum size, maximum number of retainable files and the severity of logged events are configurable. After obtaining the user-defined maximum size or maximum number of retainable files, the device archives the entries and starts a new file. The device deletes the oldest file and renames the other files to maintain the configured number of files. To review these files use the CLI or copy them to an external server for future reference.
- *Download support information*
  This button lets you download system information as a ZIP archive.

In service situations, these reports provide the technician with the necessary information.

Global Settings

Using this dialog you enable or disable where the device sends reports, for example, to a Console, a Syslog Server, or a connection to the CLI. You also set at which severity level the device writes events into the reports.

Perform the following steps:

- ☐ Open the *Diagnostics > Report > Global* dialog.
- ☐ To send a report to the console, specify the desired level in the *Console logging* frame, *Severity* field.
- ☐ To enable the function, select the `On` radio button in the *Console logging* frame.
- ☐ Save the changes temporarily. To do this, click the ✓ button.

The device buffers logged events in 2 separate storage areas so that the device keeps log entries for urgent events. Specify the minimum severity for events that the device logs to the buffered storage area with a higher priority.

Perform the following steps:

- ☐ To send events to the buffer, specify the desired level in the *Buffered logging* frame, *Severity* field.
- ☐ Save the changes temporarily. To do this, click the ✓ button.

When you activate the logging of SNMP requests, the device logs the requests as events in the Syslog. The *Log SNMP get request* function logs user requests for device configuration information. The *Log SNMP set request* function logs device configuration events. Specify the minimum level for events that the device logs in the Syslog.

Perform the following steps:

- ☐ Enable the *Log SNMP get request* function for the device in order to send SNMP Read requests as events to the Syslog server.
  To enable the function, select the `On` radio button in the *SNMP logging* frame.
- ☐ Enable the *Log SNMP set request* function for the device in order to send SNMP Write requests as events to the Syslog server.
  To enable the function, select the `On` radio button in the *SNMP logging* frame.
- ☐ Choose the desired severity level for the get and set requests.
- ☐ Save the changes temporarily. To do this, click the ✓ button.

When active, the device logs configuration changes made using the CLI, to the audit trail. This feature is based on the IEEE 1686 standard for Substation Intelligent Electronic Devices.

Perform the following steps:

- ☐ Open the *Diagnostics > Report > Global* dialog.
- ☐ To enable the function, select the `On` radio button in the *CLI logging* frame.
- ☐ Save the changes temporarily. To do this, click the button.

The device lets you save the following system information data in one ZIP file on your PC:

- `audittrail.html`
- `defaultconfig.xml`
- `script`
- `runningconfig.xml`
- `supportinfo.html`
- `systeminfo.html`
- `systemlog.html`

The device creates the file name of the ZIP archive automatically in the format `<IP_address>_<system_name>.zip`.

Perform the following steps:

- ☐ Click the button and then the *Download support information* item.
- ☐ Select the directory in which you want to save the support information.
- ☐ Save the changes temporarily. To do this, click the button.

Syslog

The device enables you to send messages about device internal events to one or more Syslog servers (up to 8). Additionally, you also include SNMP requests to the device as events in the Syslog.

NOTE: To display the logged events, open the *Diagnostics > Report > Audit Trail* dialog or the *Diagnostics > Report > System Log* dialog.

Perform the following steps:

- ☐ Open the *Diagnostics > Syslog* dialog.
- ☐ To add a table entry, click the button.
- ☐ In the *IP address* column, enter the IP address of the Syslog server.
- ☐ In the *Destination UDP port* column, specify the UDP port on which the Syslog server expects the log entries.
- ☐ In the *Min. severity* column, specify the minimum severity level that an event requires for the device to send a log entry to this Syslog server.
- ☐ Select the checkbox in the *Active* column.
- ☐ To enable the function, select the `On` radio button in the *Operation* frame.
- ☐ Save the changes temporarily. To do this, click the button.

In the *SNMP logging* frame, configure the following settings for read and write SNMP requests:

Perform the following steps:

- ☐ Open the *Diagnostics > Report > Global* dialog.
- ☐ Enable the *Log SNMP get request* function for the device in order to send SNMP Read requests as events to the Syslog server.
  To enable the function, select the `On` radio button in the *SNMP logging* frame.
- ☐ Enable the *Log SNMP set request* function for the device in order to send SNMP Write requests as events to the Syslog server.
  To enable the function, select the `On` radio button in the *SNMP logging* frame.
- ☐ Choose the desired severity level for the get and set requests.
- ☐ Save the changes temporarily. To do this, click the ✔ button.

`enable`	Change to the Privileged EXEC mode.
`configure`	Change to the Configuration mode.
`logging host add 1 addr 10.0.1.159 severity 3`	Adds a new recipient in the Syslog servers list. The value `3` specifies the severity level of the event that the device logs. The value `3` means `error`.
`logging syslog operation`	Enable the *Syslog* function.
`exit`	Change to the Privileged EXEC mode.
`show logging host`	Display the Syslog host settings.

```
No.    Server IP      Port   Max. Severity   Type        Status
-----  -------------- -----  --------------  ----------  -------
1      10.0.1.159     514    error           systemlog   active
```

`configure`	Change to the Configuration mode.
`logging snmp-requests get operation`	Logs SNMP GET requests.
`logging snmp-requests get severity 5`	The value `5` specifies the severity level of the event that the device logs in case of SNMP GET requests. The value `5` means `notice`.
`logging snmp-requests set operation`	Logs SNMP SET requests.
`logging snmp-requests set severity 5`	The value `5` specifies the severity level of the event that the device logs in case of SNMP SET requests. The value `5` means `notice`.
`exit`	Change to the Privileged EXEC mode.
`show logging snmp`	Display the SNMP logging settings.

```
Log SNMP GET requests              : enabled
Log SNMP GET severity              : notice
Log SNMP SET requests              : enabled
Log SNMP SET severity              : notice
```

System Log

The device lets you call up a log file of the system events. The table in the *Diagnostics > Report > System Log* dialog lists the logged events.

Perform the following steps:

- ☐ To update the content of the log, click the button.
- ☐ To save the content of the log as an html file, click the button and then the *Reset* item.
- ☐ To delete the content of the log, click the button and then the *Reset* item.
- ☐ To search the content of the log for a key word, use the search function of your web browser.

NOTE: You have the option to also send the logged events to one or more Syslog servers.

Audit Trail

The *Diagnostics > Report > Audit Trail* dialog contains system information and changes to the device configuration performed through the CLI and SNMP. In the case of device configuration changes, the dialog displays Who changed What and When.

The *Diagnostics > Syslog* dialog lets you specify up to 8 Syslog servers to which the device sends Audit Trails.

The following list contains log events:

- changes to configuration parameters
- Commands (except `show` commands) using the CLI
- Command `logging audit-trail <string>` using the CLI which logs the comment
- Automatic changes to the System Time
- watchdog events
- locking a user after several unsuccessful login attempts
- User login, either locally or remote, using the CLI
- Manual, user-initiated, logout
- Timed logout after a user-defined period of inactivity in the CLI
- file transfer operation including a Firmware Update
- Configuration changes using Ethernet Switch Configurator
- Automatic configuration or firmware updates using the external memory
- Blocked access to the device management due to invalid login
- rebooting
- opening and closing SNMP over HTTPS tunnels
- Detected power interruptions

Network Analysis with TCPdump

Tcpdump is a packet-sniffing UNIX utility used by network administrators to monitor and analyze traffic on a network. A couple of reasons for sniffing traffic on a network is to verify connectivity between hosts, or to analyze the traffic traversing the network.

TCPDump provides the possibility to decode or capture packets received and transmitted by the device. This function is available using the `debug` command. Refer to the “Command Line Interface” reference manual for further information about the TCPDump function.

Monitoring the Data Traffic

The device lets you forward data packets that pass through the device to a destination port. There you can monitor and evaluate the data packets.

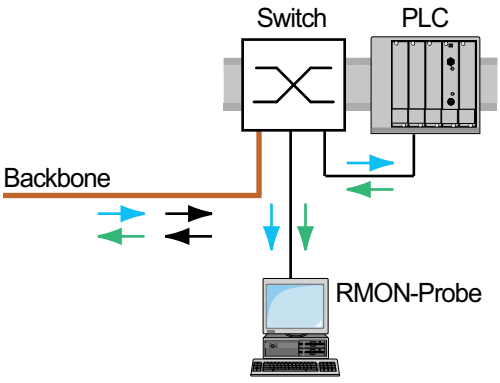
The device provides you with the following options:

- Port Mirroring

Port Mirroring

The *Port Mirroring* function lets you copy data packets from physical source ports to a physical destination port.

You monitor the data traffic on the source ports in the sending and receiving directions with a management tool connected on the destination port, for example an RMON probe. The function has no affect on the data traffic running on the source ports.



On the destination port, the device only forwards the data packets copied from the source ports.

Before you switch on the *Port Mirroring* function, select the checkbox *Allow management* to access the device management via the destination port. The device lets users access the device management via the destination port without interrupting the active *Port Mirroring* session.

NOTE: The device duplicates multicasts, broadcasts and unknown unicasts on the destination port.

The VLAN settings on the destination port remain unchanged. Prerequisite for access to the device management on the destination port is that the destination port is a member of the device management VLAN.

Restrictions apply to ports on which the following redundancy protocols are active:

- PRP
  To monitor the data stream on PRP ports, specify the source port `1/1`. On the source port `1/1`, the *Port Mirroring* function records:
  - Data packets coming into the PRP network from the outside through the device
  - Data packets after duplicate recognition that leave the PRP network through the device
  - No Link Local packets that protocols like LLDP work with

Enabling the Port Mirroring Function

Perform the following steps:

- ☐ Open the *Diagnostics > Ports > Port Mirroring* dialog.
- ☐ Specify the source ports.
  Select the checkbox in the *Enabled* column for the relevant ports.
- ☐ Specify the destination port.
  In the *Destination port* frame, select the desired port in the *Primary port* drop-down list.
  The drop-down list only displays available ports. Ports that are already specified as source ports are unavailable.
- ☐ In order to access the device management via the destination port:
  In the *Destination port* frame, select the *Allow management* checkbox.
- ☐ Save the changes temporarily. To do this, click the button.

To deactivate the *Port Mirroring* function and restore the default settings, click the button and then the *Reset config* item.

Self-test

The device verifies its assets during the boot process and occasionally thereafter. The device verifies system task availability or termination and the available amount of memory. Furthermore, the device verifies for application functionality and any hardware degradation in the chip set.

If the device detects a loss in integrity, then the device responds to the degradation with a user-defined action. The following categories are available for configuration.

- `task`
  Action to be taken in case a task is unsuccessful.
- `resource`
  Action to be taken due to the lack of resources.

- `software`
  Action taken for loss of software integrity; for example, code segment checksum or access violations.
- `hardware`
  Action taken due to hardware degradation

Configure each category to produce an action in case the device detects a loss in integrity. The following actions are available for configuration.

- `log only`
  This action writes a message to the logging file.
- `send trap`
  Sends an SNMP trap to the trap destination.
- `reboot`
  If activated, then a detected error in the category will cause the device to reboot.

Perform the following steps:

- ☐ Open the *Diagnostics > System > Selftest* dialog.
- ☐ In the *Action* column, specify the action to perform for a cause.
- ☐ Save the changes temporarily. To do this, click the ✓ button.

`enable`	Change to the Privileged EXEC mode.
`configure`	Change to the Configuration mode.
`selftest action task log-only`	To send a message to the event log when a task is unsuccessful.
`selftest action resource send-trap`	When there are insufficient resources, send an SNMP trap.
`selftest action software send-trap`	When the software integrity has been lost, send an SNMP trap.
`selftest action hardware reboot`	To reboot the device when hardware degradation occurs.

Disabling these functions lets you decrease the time required to restart the device after a cold start. You find these options in the *Diagnostics > System > Selftest* dialog, *Configuration* frame.

- *RAM test*
  Activates/deactivates the *RAM test* function during a cold start.
- *SysMon1 is available*
  Activates/deactivates the System Monitor function during a cold start.
- *Load default config on error*
  Activates/deactivates the loading of the default device configuration in case no readable configuration is available during a restart.

The following settings block your access to the device permanently in case the device does not detect any readable configuration profile at restart.

- The *SysMon1 is available* checkbox is cleared.
- The *Load default config on error* checkbox is cleared.

This is the case, for example, when the password of the configuration profile that you are loading differs from the password set in the device. To have the device unlocked again, contact your sales partner.

Perform the following steps:

`selftest ramtest`	Enable RAM selftest on cold start.
`no selftest ramtest`	Disable the "ramtest“ function.
`selftest system-monitor`	Enable the "SysMon1“ function.
`no selftest system-monitor`	Disable the "SysMon1“ function.
`show selftest action`	Show status of the actions to be taken in the event of device degradation.
`show selftest settings`	Display the settings for "ramtest" and "SysMon" settings in event of a cold start.

Advanced Functions of the Device

Using the Device as a DHCP Server

A DHCP server ("Dynamic Host Configuration Protocol") assigns IP addresses, Gateways, and other networking definitions such as DNS and NTP parameters to clients.

The DHCP operations fall into 4 basic phases: IP discovery, IP lease offer, IP request, and IP lease acknowledgment. Use the acronym DORA which stands for Discovery, Offer, Request, and Acknowledgement to help remember the phases. The server receives client data on UDP port 67 and forwards data to the client on UDP port 68.

The DHCP server provides an IP address pool or "pool", from which it allocates IP addresses to clients. The pool consists of a list of entries. An entry defines either a specific IP address or an IP address range.

The device lets you activate the DHCP server globally and per interface.

IP Addresses Assigned per Port or per VLAN

The DHCP server assigns a static IP address or dynamic range of IP addresses to a client connected to a port or a VLAN. The device lets you create entries for either a port or a VLAN. When creating an entry to assign an IP address to a VLAN, the port entry grays out. When creating an entry to assign an IP address to a port, the VLAN entry grays out.

Static allocation means that the DHCP server assigns the same IP address to a specific client. The DHCP server identifies the client using a unique hardware ID. A static address entry contains one IP address, and applies it to a port or VLAN on which the server receives a request from a specific client. For static allocation, create a pool entry for the ports or one specific port, enter the IP address, and leave the *Last IP address* column empty. Specify a hardware ID with which the DHCP server uniquely identifies the client. This ID is either a MAC address, a client ID, a remote ID, or a circuit ID. When a client contacts the server with the configured hardware ID, the DHCP server allocates the static IP address.

The device also lets you assign a dynamic IP address range to ports or VLANs from which the DHCP server allocates a free IP address from a pool. To add a dynamic pool entry for the ports or VLANs, specify the first and last IP addresses for the IP address range, leaving the *MAC address*, *Client ID*, *Remote ID*, and *Circuit ID* columns empty. Creating multiple pool entries lets you have IP address ranges that contain gaps.

DHCP Server Static IP Address Example

In this example, configure the device to allocate a static IP address to a port. The device recognizes clients with unique hardware identification. The Hardware ID in this case is the client MAC address `00:24:E8:D6:50:51`. To do this, perform the following steps:

- ☐ Open the *Advanced > DHCP Server > Pool* dialog.
- ☐ To add a table entry, click the  button.
- ☐ In the *IP address* column, specify the value `192.168.23.42`.
- ☐ In the *Port* column, specify the value `1/1`.
- ☐ In the *MAC address* column, specify the value `00:24:E8:D6:50:51`.
- ☐ To assign the IP address to the client infinitely, in the *Lease time [s]* column, specify the value `4294967295`.
- ☐ Select the checkbox in the *Active* column.
- ☐ Open the *Advanced > DHCP Server > Global* dialog.
- ☐ For port `1/1`, select the checkbox in the *DHCP server active* column.
- ☐ To enable the function, select the `On` radio button in the *Operation* frame.
- ☐ Save the changes temporarily. To do this, click the  button.

`enable`	Change to the Privileged EXEC mode.
`configure`	Change to the Configuration mode.
`dhcp-server pool add 1 static 192.168.23.42`	Creating an entry with index `1` and adding the IP address `192.168.23.42` to the static pool.
`dhcp-server pool modify 1 mode interface 1/1`	Assign the static address in index `1` to interface `1/1`.
`dhcp-server pool modify 1 mode mac 00:24:E8:D6:50:51`	Assign the IP address in index `1` to the device with the MAC address `00:24:E8:D6:50:51`.
`dhcp-server pool mode 1`	Enable the index `1` pool entry.
`dhcp-server pool modify 1 leasetime infinite`	To allocate the IP address to the client infinitely, modify the entry with index `1`.
`dhcp-server operation`	Enable the DHCP server globally.
`interface 1/1`	Change to the interface configuration mode of interface `1/1`.
`dhcp-server operation`	Activate the *DHCP Server* server function on this port.

DHCP Server Dynamic IP Address Range Example

The device lets you create dynamic IP address ranges. Leave the *MAC address*, *Client ID*, *Remote ID* and *Circuit ID* fields empty. To create dynamic IP address ranges with gaps between the ranges add several entries to the table. To do this, perform the following steps:

- ☐ Open the *Advanced > DHCP Server > Pool* dialog.
- ☐ To add a table entry, click the  button.
- ☐ In the *IP address* column, specify the value `192.168.23.92`. This is the first IP address of the range.
- ☐ In the *Last IP address* column, specify the value `192.168.23.142`. This is the last IP address of the range.

In the *Lease time [s]* column, the default setting is 60 days.

- ☐ In the *Port* column, specify the value `1/2`.
- ☐ Select the checkbox in the *Active* column.
- ☐ Open the *Advanced > DHCP Server > Global* dialog.
- ☐ For port `1/2`, select the checkbox in the *DHCP server active* column.
- ☐ To enable the function, select the `On` radio button in the *Operation* frame.
- ☐ Save the changes temporarily. To do this, click the  button.

`enable`	Change to the Privileged EXEC mode.
`configure`	Change to the Configuration mode.
`dhcp-server pool add 2 dynamic 192.198.23.92 192.168.23.142`	Add a dynamic pool with an IP range from `192.168.23.92` to `192.168.23.142`.
`dhcp-server pool modify 2 leasetime {seconds | infinite}`	Entering the Lease Time in seconds or infinite.
`dhcp-server pool add 3 dynamic 192.198.23.172 192.168.23.180`	Add a dynamic pool with an IP range from `192.168.23.172` to `192.168.23.180`.
`dhcp-server pool modify 3 leasetime {seconds | infinite}`	Entering the Lease Time in seconds or infinite.
`dhcp-server pool mode 2`	Enable the index `2` pool entry.
`dhcp-server pool mode 3`	Enable the index `3` pool entry.
`dhcp-server operation`	Enable the DHCP server globally.
`interface 2/1`	Change to the interface configuration mode of interface `2/1`.
`dhcp-server operation`	Activate the *DHCP Server* server function on this port.

MRP-IEEE

The IEEE 802.1ak amendment to the IEEE 802.1Q standard introduced the Multiple Registration Protocol (MRP) to replace the Generic Attribute Registration Protocol (*GARP*). The IEEE also modified and replaced the *GARP* applications, *GARP* Multicast Registration Protocol (*GMRP*) and *GARP* VLAN Registration Protocol (*GVRP*), with the Multiple MAC Registration Protocol (*MMRP*) and the Multiple VLAN Registration Protocol (*MVRP*).

To confine traffic to the required areas of a network, the MRP applications distribute attribute values to MRP enabled devices across a LAN. The MRP applications register and de-register Multicast group memberships and VLAN identifiers.

NOTE: The Multiple Registration Protocol (MRP) requires a loop free network. To help prevent loops in your network, use a network protocol such as the Media Redundancy Protocol, Spanning Tree Protocol, or Rapid Spanning Tree Protocol with MRP.

MRP Operation

Each participant contains an applicant component and an MRP Attribute Declaration (MAD) component. The applicant component forms the attribute values and their registration and de-registration. The MAD component generates MRP messages for transmission and processes messages received from other participants. The MAD component encodes and transmits the attributes to other participants in MRP Data Units (MRPDU). In the switch, an MRP Attribute Propagation (MAP) component distributes the attributes to participating ports.

A participant exists for each MRP application and each LAN port. For example, a participant application exists on an end device and another application exists on a switch port. The Applicant state machine records the attribute and port for each MRP participant declaration on an end device or switch. Applicant state machine variable changes trigger the transmission of MRPDUs to communicate the declaration or withdrawal.

To establish an *MMRP* instance, an end device first sends a Join empty (JoinMt) message with the appropriate attributes. The switch then floods the JoinMt to the participating ports and to the neighboring switches. The neighboring switches flood the message to their participating port, and so on, establishing a path for the group traffic.

MRP Timers

The default timer settings help prevent unnecessary attribute declarations and withdraws. The timer settings allow the participants to receive and process MRP messages before the Leave or LeaveAll timers expire.

When you reconfigure the timers, maintain the following relationships:
- To allow for re-registration after a Leave or LeaveAll event, although there is a lost message, set the value of the LeaveTime as follows: ≥ (2x JoinTime) + 60 in 1/100 s
- To minimize the volume of rejoining traffic generated following a LeaveAll, specify the value for the LeaveAll timer larger than the LeaveTime.

The following list contains various MRP events that the device transmits:
- Join - Controls the interval for the next Join message transmission
- Leave - Controls the length of time that a switch waits in the Leave state before changing to the withdraw state
- LeaveAll - Controls the frequency with which the switch generates LeaveAll messages

When expired, the Periodic timer initiates a Join request MRP message that the switch sends to participants on the LAN. The switches use this message to help prevent unnecessary withdraws.

MMRP

When a device receives Broadcast, Multicast or unknown traffic on a port, the device floods the traffic to the other ports. This process causes unnecessary use of bandwidth on the LAN.

The Multiple MAC Registration Protocol (*MMRP*) lets you control the traffic flooding by distributing an attribute declaration to participants on a LAN. The attribute values that the MAD component encodes and transmits on the LAN in MRP messages are Group service requirement information and 48-bit MAC addresses.

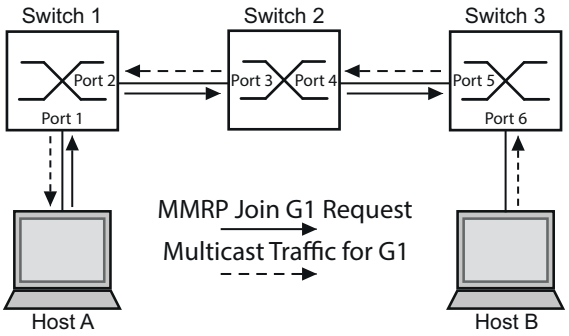
The switch stores the attributes in a filtering database as MAC address registration entries. The forwarding process uses the filtering database entries only to transmit data through those ports necessary to reach Group member LANs.

Switches facilitate the group distribution mechanisms based on the Open Host Group concept, receiving packets on the active ports and forwarding only to ports with group members. This way, any *MMRP* participants requiring packets transmitted to a particular group or groups, requests membership in the group. MAC service users send packets to a particular group from anywhere on the LAN. A group receives these packets on the LANs attached to registered *MMRP* participants. *MMRP* and the MAC Address Registration Entries thus restrict the packets to required segments of a loop-free LAN.

In order to maintain the registration and deregistration state and to receive traffic, a port declares interest periodically. Every device on a LAN with the *MMRP* function enabled maintains a filtering database and forwards traffic having the group MAC addresses to listed participants.

MMRP Example

In this example, Host A intends to listen to traffic destined to group G1. Switch A processes the *MMRP* Join request received from host A and sends the request to both of the neighboring switches. The devices on the LAN now recognize that there is a host interested in receiving traffic destined for group G1. When Host B starts transmitting data destined for group G1, the data flows on the path of registrations and Host A receives it.



Enable the *MMRP* function on the switches. To do this, perform the following steps:

- ☐ Open the *Switching* > *MRP-IEEE* > *MMRP* dialog, *Configuration* tab.
- ☐ To activate port `1` and port `2` as *MMRP* participants, select the checkbox in the *MMRP* column for port `1` and port `2` on switch 1.
- ☐ To activate port `3` and port `4` as *MMRP* participants, select the checkbox in the *MMRP* column for port `3` and port `4` on switch 2.
- ☐ To activate port `5` and port `6` as *MMRP* participants, select the checkbox in the *MMRP* column for port `5` and port `6` on switch 3.
- ☐ To send periodic events allowing the device to maintain the registration of the MAC address group, enable the *Periodic state machine*. Select the `On` radio button in the *Configuration* frame.
- ☐ Save the changes temporarily. To do this, click the button.

To enable the *MMRP* ports on switch 1, use the following commands. Substituting the appropriate interfaces in the commands, enable the *MMRP* functions and ports on switches 2 and 3.

`enable`	Change to the Privileged EXEC mode.
`configure`	Change to the Configuration mode.
`interface 1/1`	Change to the interface configuration mode of interface `1/1`.
`mrp-ieee mmrp operation`	Enabling the *MMRP* function on the port.
`interface 1/2`	Change to the interface configuration mode of interface `1/2`.
`mrp-ieee mmrp operation`	Enabling the *MMRP* function on the port.
`exit`	Change to the Configuration mode.
`mrp-ieee mrp periodic-state-machine`	Enabling the *Periodic state machine* function globally.
`mrp-ieee mmrp operation`	Enabling the *MMRP* function globally.

MVRP

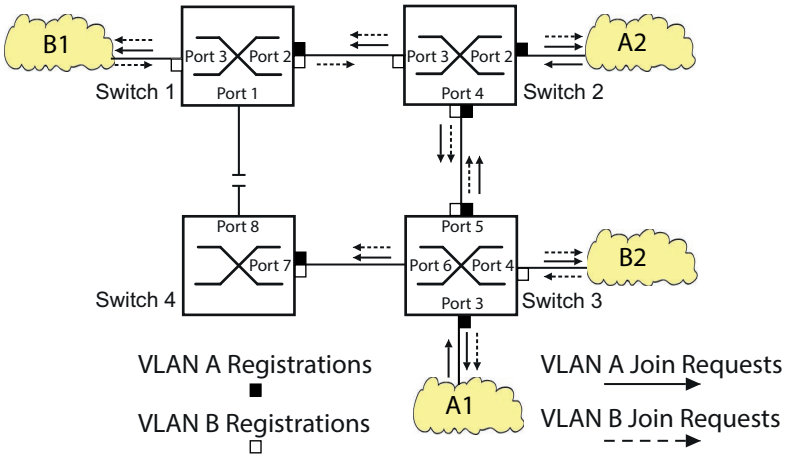
The Multiple VLAN Registration Protocol (*MVRP*) is an MRP application that provides dynamic VLAN registration and withdraw services on a LAN.

The *MVRP* function provides a maintenance mechanism for the Dynamic VLAN Registration Entries, and for transmitting the information to other devices. This information lets *MVRP*-aware devices establish and update their VLAN membership information. When members are present on a VLAN, the information indicates through which ports the switch forwards traffic to reach those members.

The main purpose of the *MVRP* function is to allow switches to discover some of the VLAN information that you otherwise manually set up. Discovering this information lets switches overcome the limitations of bandwidth consumption and convergence time in large VLAN networks.

MVRP Example

Set up a network comprised of MVRP aware switches (1 - 4) connected in a ring topology with end device groups, A1, A2, B1, and B2 in 2 different VLANs, A and B. With STP enabled on the switches, the ports connecting switch 1 to switch 4 are in the discarding state, helping prevent a loop condition.



In the MVRP example network, the LANs first send a Join request to the switches. The switch enters the VLAN registration in the forwarding database for the port receiving the frames.

The switch then propagates the request to the other ports, and sends the request to the neighboring LANs and switches. This process continues until the switches have registered the VLANs in the forwarding database of the receive port.

Enable MVRP on the switches. To do this, perform the following steps:

- ☐ Open the *Switching* > *MRP-IEEE* > *MVRP* dialog, *Configuration* tab.
- ☐ To activate the ports 1 through 3 as *MVRP* participants, select the checkbox in the *MVRP* column for the ports 1 through 3 on switch 1.
- ☐ To activate the ports 2 through 4 as *MVRP* participants, select the checkbox in the *MVRP* column for the ports 2 through 4 on switch 2.
- ☐ To activate the ports 3 through 6 as *MVRP* participants, select the checkbox in the *MVRP* column for the ports 3 through 6 on switch 3.

- ☐ To activate port 7 and port 8 as *MVRP* participants, select the checkbox in the *MVRP* column for port 7 and port 8 on switch 4.
- ☐ To maintain the registration of the VLANs, enable the *Periodic state machine*. Select the *On* radio button in the *Configuration* frame.
- ☐ To enable the function, select the *On* radio button in the *Operation* frame.
- ☐ Save the changes temporarily. To do this, click the button.

To enable the *MVRP* ports on switch 1, use the following commands. Substituting the appropriate interfaces in the commands, enable the *MVRP* functions and ports on switches 2, 3 and 4.

`enable`	Change to the Privileged EXEC mode.
`configure`	Change to the Configuration mode.
`interface 1/1`	Change to the interface configuration mode of interface `1/1`.
`mrp-ieee mvrp operation`	Enabling the *MVRP* function on the port.
`interface 1/2`	Change to the interface configuration mode of interface `1/2`.
`mrp-ieee mvrp operation`	Enabling the *MVRP* function on the port.
`exit`	Change to the Configuration mode.
`mrp-ieee mvrp periodic-state-machine`	Enabling the *Periodic state machine* function globally.
`mrp-ieee mvrp operation`	Enabling the *MVRP* function globally.

Industry Protocols

IEC 61850/MMS

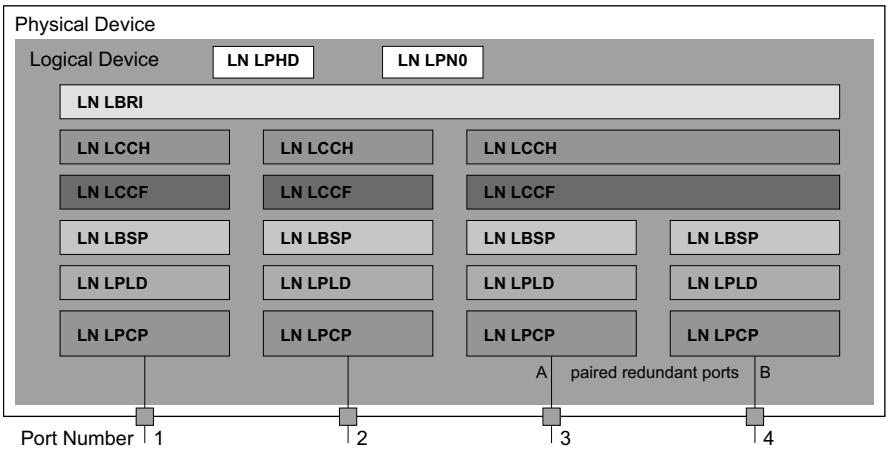
IEC 61850/MMS is an industrial communication protocol standardized by the International Electrotechnical Commission (IEC). The protocol is to be found in substation automation, for example in the control technology of energy suppliers.

This protocol, which works in a packet-oriented way, is based on the TCP/IP transport protocol and uses the Manufacturing Messaging Specification (MMS) for the client-server communication. The protocol is object-oriented and defines a standardized configuration language that comprises, among other things, functions for SCADA, Intelligent Electronic Devices (IED) and for the network control technology.

Part 6 of the IEC 61850 standard defines the configuration language SCL (Substation Configuration Language). SCL describes the properties of the device and the system structure in an automatically processable form. The properties of the device described with SCL are stored in the ICD file in the device.

Switch Model for IEC 61850

The Technical Report, IEC 61850 90-4, specifies a bridge model. The bridge model represents the functions of a switch as objects of an Intelligent Electronic Device (IED). An MMS client (for example the control room software) uses these objects to monitor and configure the device.



Class	Description
LN LLN0	Zero logical node of the Bridge IED: Defines the logical properties of the device.
LN LPHD	Physical Device logical node of the Bridge IED: Defines the physical properties of the device.
LN LBRI	Bridge logical node: Represents general settings of the bridge functions of the device.

Class	Description
LN LCCH	Communication Channel logical node: Defines the logical Communication Channel that consists of one or more physical device ports.
LN LCCF	Channel Communication Filtering logical node: Defines the VLAN and Multicast settings for the higher-level Communication Channel.
LN LBSP	Port Spanning Tree Protocol logical node: Defines the Spanning Tree statuses and settings for the respective physical device port.
LN LPLD	Port Layer Discovery logical node: Defines the LLDP statuses and settings for the respective physical device port.
LN LPCP	Physical Communication Port logical node: Represents the respective physical device port.

Integration into a Control System

Preparation of the Device

Perform the following steps:

- ☐ Verify that the device has an IP address assigned.
- ☐ Open the *Advanced > Industrial Protocols > IEC61850-MMS* dialog.
- ☐ To start the MMS server, select in the *Operation* frame the On radio button, and click ✓ button.
  Afterwards, an MMS client is able to connect to the device and to read and monitor the objects defined in the bridge model.

IEC61850/MMS does not provide any authentication mechanisms. If the write access for IEC61850/MMS is activated, then every client that can access the device using TCP/IP is capable of changing the settings of the device. This in turn can result in an incorrect configuration of the device and possible issues detected in the network.

NOTICE
RISK OF UNAUTHORIZED ACCESS TO THE DEVICE Only activate the write access if you have taken additional measures (for example Firewall, VPN, etc.) to reduce possible unauthorized access. **Failure to follow these instructions can result in equipment damage.**

☐ To allow the MMS client to change the settings, select the *Write access* checkbox, and click the ✓ button.

Offline Configuration

The device lets you download the ICD file using the GUI. This file contains the properties of the device described with SCL and enables you to configure the substation without directly connecting to the device.

☐ Open the *Advanced > Industrial Protocols > IEC61850-MMS* dialog.

☐ To load the ICD file to your PC, click the ☰ button and then the *Download* item.

Monitoring the Device

The IEC61850/MMS server integrated into the device lets you monitor multiple statuses of the device by means of the Report Control Block (RCB). Up to 5 MMS clients can register for a Report Control Block at the same time.

The device lets you monitor the following statuses:

Class	RCB Object	Description
LN LPHD	TmpAlm	When the temperature measured in the device exceeds or falls below the set temperature thresholds, the status changes.
	PhyHealth	When the status of the LPHD.TmpAlm RCB object changes, the status changes.
LN LPHD	TmpAlm	When the temperature measured in the device exceeds or falls below the set temperature thresholds, the status changes.
	PwrSupAlm	When one of the redundant power supplies becomes inoperative or starts operating again, the status changes.
	PhyHealth	When the status of the LPHD.PwrSupAlm or LPHD.TmpAlm RCB object changes, the status changes.

Class	RCB Object	Description
LN LBRI	RstpRoot	When the device takes over or relinquishes the role of the root bridge, the status changes.
	RstpTopoCnt	When the topology changes due to a change of the root bridge, the status changes.
LN LCCH	ChLiv	When the link status of the physical port changes, the status changes.
LN LPCP	PhyHealth	When the link status of the physical port changes, the status changes.

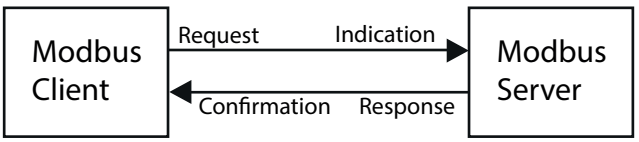
Modbus TCP

Modbus TCP is an application layer messaging protocol providing client/server communication between the client and devices connected in Ethernet TCP/IP networks.

The *Modbus TCP* function lets you install the device in networks already using *Modbus TCP* and retrieve information saved in the registers in the device.

Client/Server Modbus TCP/IP Mode

The device supports the client/server model of Modbus TCP/IP. This device operates as a server in this constellation and responds to requests from a client for information saved in the registers.



The client / server model uses four types of messages to exchange data between the client and server:

- Modbus TCP/IP Request, the client creates a request for information and sends it to the server.
- Modbus TCP/IP Indication, the server receives a request as an indication that a client requires information.
- Modbus TCP/IP Response, when the required information is available, the server sends a reply containing the requested information. When the requested information is unavailable, the server sends an Exception Response to notify the client of the error detected during the processing. The Exception Response contains an exception code indicating the reason for the detected error.
- Modbus TCP/IP Confirmation, the client receives a response from the server, containing the requested information.

Supported Functions and Memory Mapping

The device supports functions with the public codes `0x03` (`Read Holding Registers`) and `0x05` (`Write Single Coil`). The codes let you read the information saved in the registers such as the system information, including the system name, system location, software version, IP address, MAC address. The codes also let you read the port information and port statistics. The `0x05` code lets you reset the port counters individually or globally.

The following list contains definitions for the values entered in the `Format` column:

- Bitmap: a group of 32-bits, encoded into the Big-endian byte order and saved in 2 registers. Big-endian systems save the most significant byte of a word in the smallest address and save the least significant byte in the largest address.
- F1: 16-bit unsigned integer
- F2: Enumeration - power supply alarm
  - 0 = power supply good
  - 1 = power supply error detected
- F3: Enumeration - OFF/ON
  - 0 = Off
  - 1 = On
- F4: Enumeration - port type
  - 0 = Giga - Gigabit Interface Converter (GBIC)
  - 1 = Copper - Twisted Pair (TP)
  - 2 = Fiber - 10 Mb/s
  - 3 = Fiber - 100 Mb/s
  - 4 = Giga - 10/100/1000 Mb/s (triple speed)
  - 5 = Giga - Copper 1000 Mb/s TP
  - 6 = Giga - Small Form-factor Pluggable (SFP)
- F9: 32-bit unsigned long
- String: octets, saved in sequence, 2 octets per register.

Modbus TCP/IP Codes

The following table lists addresses that allow the client to reset port counters and retrieve specific information from the device registers.

Port Information

Address	Qty	Description	Min	Max	Step	Unit	Format
0400	1	Port 1 Type	0	6	1	-	F4
0401	1	Port 2 Type	0	6	1	-	F4
		...					
043F	1	Port 64 Type	0	6	1	-	F4
0440	1	Port 1 Link Status	0	1	1	-	F1
0441	1	Port 2 Link Status	0	1	1	-	F1
		...					
047F	1	Port 64 Link Status	0	1	1	-	F1
0480	1	Port 1 STP State	0	1	1	-	F1
0481	1	Port 2 STP State	0	1	1	-	F1
		...					
04BF	1	Port 64 STP State	0	1	1	-	F1
04C0	1	Port 1 Activity	0	1	1	-	F1

Address	Qty	Description	Min	Max	Step	Unit	Format
04C1	1	Port 2 Activity	0	1	1	-	F1
		...					
04FF	1	Port 64 Activity	0	1	1	-	F1
0500	1	Port 1 Counter Reset	0	1	1	-	F1
0501	1	Port 2 Counter Reset	0	1	1	-	F1
		...					
053F	1	Port 64 Counter Reset	0	1	1	-	F1

Port Statistics

Address	Qty	Description	Mln	Max	Step	Unit	Format
0800	1	Port1 - Number of bytes received	0	4294967295	1	-	F9
0802	1	Port1 - Number of bytes sent	0	4294967295	1	-	F9
0804	1	Port1 - Number of frames received	0	4294967295	1	-	F9
0806	1	Port1 - Number of frames sent	0	4294967295	1	-	F9
0808	1	Port1 - Total bytes received	0	4294967295	1	-	F9
080A	1	Port1 - Total frames received	0	4294967295	1	-	F9
080C	1	Port1 - Number of broadcast frames received	0	4294967295	1	-	F9
080E	1	Port1 - Number of multicast frames received	0	4294967295	1	-	F9
0810	1	Port1 - Number of frames with CRC error	0	4294967295	1	-	F9
0812	1	Port1 - Number of oversized frames received	0	4294967295	1	-	F9
0814	1	Port1 - Number of bad fragments rcvd(<64 bytes)	0	4294967295	1	-	F9
0816	1	Port1 - Number of jabber frames received	0	4294967295	1	-	F9
0818	1	Port1 - Number of collisions occurred	0	4294967295	1	-	F9
081A	1	Port1 - Number of late collisions occurred	0	4294967295	1	-	F9
081C	1	Port1 - Number of 64-byte frames rcvd/sent	0	4294967295	1	-	F9
081E	1	Port1 - Number of 65-127 byte frames rcvd/sent	0	4294967295	1	-	F9
0820	1	Port1 - Number of 128-255 byte frames rcvd/sent	0	4294967295	1	-	F9
0822	1	Port1 - Number of 256-511 byte frames rcvd/sent	0	4294967295	1	-	F9
0824	1	Port1 - Number of 512-1023 byte frames rcvd/sent	0	4294967295	1	-	F9
0826	1	Port1 - Number of 1023-MAX byte frames rcvd/sent	0	4294967295	1	-	F9
0828	1	Port1 - Number of Mac Error Packets	0	4294967295	1	-	F9
082A	1	Port1 - Number of dropped received packets	0	4294967295	1	-	F9

Address	Qty	Description	Min	Max	Step	Unit	Format
082C	1	Port1 - Number of multicast frames sent	0	4294967295	1	-	F9
082E	1	Port1 - Number of broadcast frames sent	0	4294967295	1	-	F9
0830	1	Port1 - Number of <64 byte fragments w/ good CRC	0	4294967295	1	-	F9
		...					
147E	1	Port64 - Number of <64 byte fragments w/ good CRC	0	4294967295	1	-	F9

Example Configuration

In this example, you configure the device to respond to client requests. The prerequisite for this configuration is that the client device is configured with an IP address within the given range. The *Write access* function remains inactive for this example. When you activate the *Write access* function, the device lets you reset the port counters only. In the default configuration the *Modbus TCP* and *Write access* functions are inactive.

The *Modbus TCP* protocol does not provide any authentication mechanisms. If the write access for *Modbus TCP* is activated, then every client that can access the device using TCP/IP is capable of changing the settings of the device. This in turn can result in an incorrect configuration of the device and possible issues detected in the network.

NOTICE

RISK OF UNAUTHORIZED ACCESS TO THE DEVICE

Only activate the write access if you have taken additional measures (for example Firewall, VPN, etc.) to reduce possible unauthorized access.

Failure to follow these instructions can result in equipment damage.

Perform the following steps:

- ☐ Open the *Device Security > Management Access > IP Access Restriction* dialog.
- ☐ Add a table entry. To do this, click the button.
- ☐ Specify the IP address range in the row where the *Index* column has the value `2`. To do this, enter the following values:
  - In the *Address* column: `10.17.1.0`
  - In the *Netmask* column: `255.255.255.248`
- ☐ Verify that the checkbox in the *Modbus TCP* column is selected.
- ☐ Activate the IP address range. To do this, select the checkbox in the *Active* column.
- ☐ Save the changes temporarily. To do this, click the button.
- ☐ Open the *Diagnostics > Status Configuration > Security Status* dialog, *Global* tab.
- ☐ Verify that the checkbox related to the parameter *Modbus TCP active* is selected.

- ☐ Open the *Advanced > Industrial Protocols > Modbus TCP* dialog.
- ☐ The standard *Modbus TCP* listening port, port `502`, is the default value. However, when you wish to listen on another TCP port, enter the value for the listening port in the *TCP port* field.
- ☐ To enable the function, select the `On` radio button in the *Operation* frame.
- ☐ Save the changes temporarily. To do this, click the ✓ button.

When you enable the *Modbus TCP* function, the *Security Status* function detects the activation and displays an alarm in the *Basic Settings > System* dialog, *Security status* frame.

`enable`	Change to the Privileged EXEC mode.
`network management access add 2`	Creates the entry for the address range in the network. Number of the next available index in this example: `2`.
`network management access modify 2 ip 10.17.1.0`	Specifies the IP address.
`network management access modify 2 mask 29`	Specifies the netmask.
`network management access modify 2 modbus-tcp enable`	Specifies that the device lets *Modbus TCP* have access to the device management.
`network management access operation`	Enables the IP access restriction.
`configure`	Change to the Configuration mode.
`security-status monitor modbus-tcp-enabled`	Specifies that the device monitors the activation of the *Modbus TCP* server.
`modbus-tcp operation`	Activates the *Modbus TCP* server.
`modbus-tcp port <1..65535>`	Specify the TCP port for *Modbus TCP* communication (optionally). The default value is port `502`.
`show modbus-tcp`	Display the *Modbus TCP* Server settings.

```
Modbus TCP/IP server settings
-------------------------
Modbus TCP/IP server operation.................enabled
Write-access...................................disabled
Listening port.................................502
Max number of sessions.........................5
Active sessions................................0
```

`show security-status monitor`	Display the security-status settings.

```
Device Security Settings
Monitor
---------------------------------
Password default settings unchanged...........monitored
...
Write access using Ethernet Switch Configurator is possible....monitored
Loading unencrypted configuration from ENVM...monitored
IEC 61850 MMS is enabled......................monitored
Modbus TCP/IP server active...................monitored
```

`show security-status event`	Display occurred security status events.

```
Time stamp             Event                       Info
--------------------   ----------------------    ------
2014-01-01 01:00:39   password-change(10)           -
.................................................
2014-01-01 01:00:39   ext-nvm-load-unsecure(21)     -
2014-01-01 23:47:40   modbus-tcp-enabled(23)        -
```

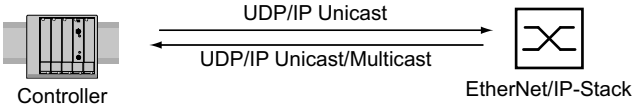
```
show network management access
rules 1
```

Display the restricted management access rules for index 1.

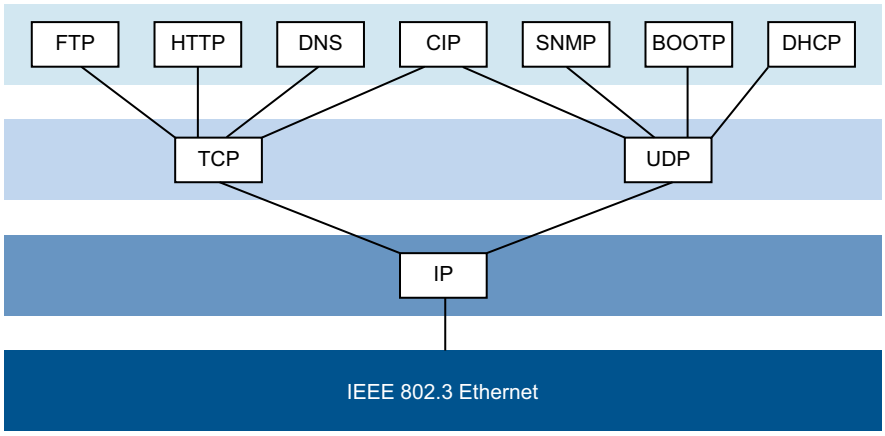
```
Restricted management access settings
-------------------------------------
Index.....................................1
IP Address................................10.17.1.0
Prefix Length.............................29
HTTP......................................yes
SNMP......................................yes
Telnet....................................yes
SSH.......................................yes
HTTPS.....................................yes
IEC61850-MMS..............................yes
Modbus TCP/IP.............................yes
Active....................................[x]
```

EtherNet/IP

EtherNet/IP is accepted worldwide as a standardized industrial communication protocol and is maintained by the Open DeviceNet Vendor Association (ODVA). The protocol is based on the widely used standard Ethernet transport protocols TCP/IP and UDP/IP. *EtherNet/IP* is supported by leading manufacturers, thus providing a wide base for effective data communication in the industry sector.



EtherNet/IP adds the industry protocol CIP (Common Industrial Protocol) to the standard Ethernet protocols. *EtherNet/IP* implements CIP at the Session layer and above and adapts CIP to the specific *EtherNet/IP* technology at the Transport layer and below. In the case of automation applications, *EtherNet/IP* implements CIP on the application level. Therefore, *EtherNet/IP* is ideally suited to the industrial control technology sector.



For detailed information on *EtherNet/IP*, see the ODVA website at www.odva.org.

Integration into a Control System

Perform the following steps:

- ☐ Open the *Switching > IGMP Snooping > Global* dialog.
  Verify that the *IGMP Snooping* function is enabled.
- ☐ Open the *Advanced > Industrial Protocols > EtherNet/IP* dialog.
  Verify that the *EtherNet/IP* function is enabled.
- ☐ Open the *Advanced > Industrial Protocols > EtherNet/IP* dialog.
- ☐ To save the EDS as a ZIP archive on your PC, click *Download*.
  The ZIP archive contains the *EtherNet/IP* configuration file and the icon used to configure the controller to connect to the device.

EtherNet/IP Entity Parameters

The following paragraphs identify the objects and operations supported by the device.

Supported Operations

Service Code	Identity Object	TCP/IP Interface Object	Ethernet Link Object	Switch Agent Object	Base Switch Object
0x01 Get Attribute All	All attributes	All attributes	All attributes	All attributes	All attributes
0x02 Set Attribute All	–	Settable attributes (0x3, 0x5, 0x6, 0x8, 0x9, 0xA)	Settable attributes (0x6, 0x9)	–	–
0x0e Get Attribute Single	All attributes	All attributes	All attributes	All attributes	All attributes
0x10 Set Attribute Single	–	Settable attributes (0x3, 0x5, 0x6, 0x8, 0x9, 0xA, 0x64)	Settable attributes (0x6, 0x9, 0x65, 0x67, 0x68, 0x69, 0x6C)	Settable attributes (0x5, 0x7)	–
0x05 Reset	Parameter (0x0, 0x1)	–	–	–	–
0x35 Save Configuration Vendor specific	–	–	–	Save switch configuration	–
0x36 Mac Filter Vendor specific	–	–	–	Add MAC filter STRUCT of: USINT VlanId ARRAY of: 6 USINT Mac DWORD PortMask	–

Identity Object

The device supports the identity object (Class Code 0x01) of *EtherNet/IP*. The Schneider Electric manufacturer ID is 634. Schneider Electric uses the ID 44 (0x2C) to indicate the product type "Managed Ethernet Switch".

ID	Attribute	Access Rule	Data Type	Description
0x1	Vendor ID	Get	UINT	Schneider Electric634
0x2	Device Type	Get	UINT	Managed Ethernet Switch 44 (0x2C) (0x2C)
0x3	Product Code	Get	UINT	Product Code: mapping is defined for every device type
0x4	Revision	Get	STRUCT of: USINT Major USINT Minor	Revision of the EtherNet/IP implementation, 2.1.
0x5	Status	Get	WORD	Support for the following Bit status only: 0: Owned (always 1) 2: Configured (always 1) 4: Extend Device Status 5: 0x3: No I/O connection established 6: 0x7: At least one I/O connection established, all in idle mode. 7:
0x6	Serial number	Get	UDINT	Serial number of the device (contains last 3 Bytes of MAC address).
0x7	Product name	Get	SHORT-STRING	Displayed as "Schneider Electric" + product family + product ID + software variant.

TCP/IP Interface Object

The device supports only Instance 1 of the TCP/IP Interface Object (Class Code 0xF5) of *EtherNet/IP*.

Depending on the write access status, the device stores the complete configuration in its flash memory. Saving the configuration file can take up to 10 seconds. If the saving process is interrupted for example, due to an inoperative power supply, then the operation of the device might be impossible.

NOTE: The device replies to the configuration change `Get Request` with a `Response` although the configuration has not yet been saved completely.

ID	Attribute	Access Rule	Data Type	Description
0x1	Revision	Get	UINT	Revision of this object: 3
0x2	Max Instance	Get	UINT	Maximum instance number: 1
0x3	Number of instance	Get	UINT	Number of object instances created: 1

ID	Attribute	Access Rule	Data Type	Description
0x1	Status	Get	DWORD	0: Interface Status (0=Interface not configured, 1=Interface contains valid config)
				6: ACD status (default 0)
				7: ACD error (default 0)
0x2	Interface Capability flags	Get	DWORD	0: BOOTP Client
				1: DNS Client
				2: DHCP Client
				3: DHCP-DNS Update
				4: Configuration setable (within CIP) Other bits reserved (0)
				7: ACD capable (0=not capable, 1=capable)
0x3	Config Control	Set/ Get	DWORD	0: 0x0=using stored config 1: 0x1=using BOOTP 2: 0x2=using DHCP 3:
				4: One device uses DNS for name lookup (always 0 because it is not supported) Other bits reserved (0)
0x4	Physical Link Object	Get	STRUCT of: UINT PathSize EPATH Path	Path to the Physical Link Object, always {0x20, 0xF6, 0x24, 0x01} describing instance 1 of the Ethernet Link Object.
0x5	Interface Configuration	Set/ Get	STRUCT of: UDINT IpAddress UDINT Netmask UDINT GatewayAddress UDINT NameServer1 UDINT NameServer2 STRING DomainName	IP Stack Configuration (IP-Address, Netmask, Gateway, 2 Name servers (DNS, if supported) and the domain name).
0x6	Host Name	Set/ Get	STRING	Host Name (for DHCP DNS Update)
0x7	Safety Network Number			Not supported
0x8	TTL Value	Get/ Set	USINT	Time to live value for IP multicast packets Range 1..255 (default = 1)

ID	Attribute	Access Rule	Data Type	Description
0x9	Mcast Config	Get/ Set	STRUCT of: USINT AllocControl USINT reserved UINT NumMcast UDINT McastStartAddr	Alloc Control = 0 Number of IP multicast addresses = 32 Multicast start address = 239.192.1.0
0xA	Selected Acd	Get/ Set	BOOL	0=ACD disable 1=ACD enable (default)
0xB	Last Conflict Detected	Get	STRUCT of: USINT AcdActivity ARRAY of: 6 USINT RemoteMac ARRAY of: 28 USINT ArpPdu	ACD Diagnostic Parameters

ID	Attribute	Access Rule	Data Type	Description
0x64	Cable Test	Set/ Get	STRUCT of: USINT Interface USINT Status	Interface Status (1=Active, 2=Success, 3=Error, 4=Uninitialized)
0x65	Cable Pair Size	Get	USINT	Size of the Cable Test Result STRUCT of: 2 Pair for 100BASE 4 Pair for 1000BASE

ID	Attribute	Access Rule	Data Type	Description

0x66	Cable Test Result	Get	STRUCT of:
			USINT Interface
			USINT CablePair
			USINT CableStatus
			USINT CableMinLength
			USINT CableMaxLength
			USINTCableFailureLocation
				100BASE:{
				{Interface, CablePair1, CableStatus, CableMinLength, CableMaxLength, CableFailureLocation}
				{Interface, CablePair2, CableStatus, CableMinLength, CableMaxLength, CableFailureLocation}
				}
				1000BASE:{
				{Interface, CablePair1, CableStatus, CableMinLength, CableMaxLength, CableFailureLocation}
				{Interface, CablePair2, CableStatus, CableMinLength, CableMaxLength, CableFailureLocation}
				{Interface, CablePair3, CableStatus, CableMinLength, CableMaxLength, CableFailureLocation}
				{Interface, CablePair4, CableStatus, CableMinLength, CableMaxLength, CableFailureLocation}
				}

Ethernet Link Object

The information in the following two tables are part of the Ethernet Link Object. To access the information, use the following values:

- Class(####)
- Instance(###)
- Attribute(#)

For example, the *class*, *instance*, and *attribute* values to access information for the utilization alarm using an explicit message are:
- Class = 0xF6
- Instance = 1
- Attribute = 6

ID	Attribute	Access Rule	Data Type	Description
Instance attributes				
0x1	Interface Speed	Get	UDINT	Used interface speed in Mbit/s (10, 100, 1000, …). 0 is used when the speed has not been determined or is invalid because of detected errors.
0x2	Interface Flags	Get	DWORD	Interface Status Flags: 0: Link State (0=No link, 1=Link) 1: Duplex mode (0=Half, 1=Full) 2:, 3:, 4: Auto-Negotiation Status 0x0=Auto-Negotiation in progress 0x1=Unsuccessful Auto-Negotiation 0x2=Unsuccessful but speed detected 0x3=Auto-Negotiation success 0x4=No Auto-Negotiation 5: Manual configuration require reset (always 0 because it is not needed) 6: Hardware error
0x3	Physical Address	Get	ARRAY of: 6 USINT	MAC address of physical interface
0x4	Interface Counters	Get	STRUCT of: UDINT MibIICounter1 UDINT MibIICounter2 …	InOctets, InUcastPackets, InNUcastPackets, InDiscards, InErrors, InUnknownProtos, OutOctets, OutUcastPackets, OutNUcastPackets, OutDiscards, OutErrors
0x5	Media Counters	Get	STRUCT of: UDINT EthernetMib Counter1 UDINT EthernetMib Counter2 …	Detected errors: Alignment, FCS, single collision, multiple collision, SQE Test, deferred transmissions, late collisions, excessive collisions, MAC TX, carrier sense, frame too long, MAC RX

ID	Attribute	Access Rule	Data Type	Description	
0x6	Interface Control	Get/ Set	STRUCT of:		Control Bits:
			WORD ControlBits	0:	Auto-negotiation enable/ disable (0=disable, 1=enable)
				1:	Duplex mode (0=Half, 1=Full), if Auto-negotiation disabled
			UINT ForcedInterface Speed	Interface speed in MBits/s: 10,100,…, if Auto-negotiation disabled	
0x7	Interface type	Get	USINT	Type of interface: 0: Undefined interface type 1: The interface is internal 2: Twisted-pair 3: Optical fiber	
0x8	Interface state	Get	USINT	State of the interface: 0: Undefined interface state 1: The interface is enabled 2: The interface is disabled 3: The interface is testing	
0x9	Admin State	Set/ Get	USINT	Administrative state: 1: Enable the interface 2: Disable the interface	
0xA	Interface label	Get	SHORT-STRING	Human readable ID	
Schneider Electric extensions to the Ethernet Link Object					
0x64	Ethernet Interface Index	Get	USINT	Interface/Port Index (ifIndex out of MIBII)	
0x65	Port Control	Get/ Set	DWORD	0:	Link state (0=link down, 1=link up)
				1:	Link admin state (0=disabled, 1=enabled)
				8:	Access violation alarm (read-only)
				9:	Utilization alarm (read-only)
0x66	Interface Utilization	Get	USINT	The existing Counter out of the private MIB hm2IDiagfaceUtilization is used. Utilization in percentage (Unit 1%=100, %/100). RX Interface Utilization.	
0x67	Interface Utilization Alarm Upper Threshold	Get/ Set	USINT	Within this parameter the variable hm2DiagIfaceUtilizationAlarmUpperThreshold can be accessed. Utilization in percentage (Unit 1%=100). RX Interface Utilization Upper Limit.	

ID	Attribute	Access Rule	Data Type	Description	
0x68	Interface Utilization Alarm Lower Threshold	Get/ Set	USINT	Within this parameter the variable hm2DiagIfaceUtilizationAlarmLowerThreshold can be accessed. Utilization in percentage (Unit 1%=100). RX Interface Utilization Lower Limit.	
0x69	Broadcast limit	Get/ Set	USINT	Broadcast limiter Service (Egress BC-Frames limitation, 0=disabled), Frames/second	
0x6A	Ethernet Interface Description	Get/ Set	STRING	Interface/Port Description (from MIB II ifDescr), for example "Unit: 1 Slot: 2 Port: 1 - 10/100 Mbit TX" or "unavailable", max. 64 Bytes.	
0x6B	Port Monitor	Get/ Set	DWORD	0:	Link Flap (0=Off, 1=On)
				1:	CRC/Fragment (0=Off, 1=On)
				2:	Duplex Mismatch (0=Off, 1=On)
				3:	Overload-Detection (0=Off, 1=On)
				4:	Link-Speed/ Duplex Mode (0=Off, 1=On)
				5:	Deactivate port action (0=Off, 1=On)
				6:	Send trap action (0=Off, 1=On)
				7: 8: 9: 10: 11:	Active Condition (displays which condition caused an action to occur) 00001_B: Link Flap 00010_B: CRC/Fragments 00100_B: Duplex Mismatch 01000_B: Overload-Detection 10000_B: Link-Speed/ Duplex mode
				12:	Reserved (always 0)
				13:	Reserved (always 0)
				14:	Reserved (always 0)
				15:	Reserved (always 0)
0x6C	Quick Connect	Get/ Set	USINT	Quick Connect on the interface (0=Off, 1=On) If you enable Quick Connect, then the device sets the port speed to 100FD, disables Auto-Negotiation, and Spanning Tree on the interface.	

ID	Attribute	Access Rule	Data Type		Description
0x6D	SFP Diagnostics	Get	STRUCT of:		
				STRING ModuleType	
				SHORT-STRING SerialNumber	
				USINT Connector	
				USINT Supported	
				DINT Temperature	in °C
				DINT TxPower	in mW
				DINT RxPower	in mW
				DINT RxPower	in dBm
				DINT TxPower	in dBm

Ethernet Port	Ethernet Link Object Instance
Controller	1
1	2
2	3
3	4
4	5
…	…

NOTE: The number of ports depends on the type of hardware used. The Ethernet Link Object only exists, if the port is connected.

Switch Agent Object

The device supports the Schneider Electric specific Ethernet Switch Agent Object (Class Code 0x95) for the device configuration and information parameters with Instance 1.

ID	Attribute	Access Rule	Data Type	Description	
0x1	Switch Status	Get	DWORD	0:	Like the signal contact, the value indicates the Device Overall state (0=ok, 1=error detected)
				1:	Device Security Status (0=ok, 1=error detected)
				2:	Power Supply 1 (0=ok, 1=error detected)
				3:	Power Supply 2 (0=ok, 1=error detected or absent)
				4:	Reserved
				5:	Reserved
				6:	Signal Contact 1 (0=closed, 1=open)
				7:	Signal Contact 2 (0=closed, 1=open or not existing)
				8:	Reserved
				9:	Temperature (0=ok, 1=error detected)
				10:	Module removed (1=removed)
				11:	EAM removed (1=removed)
				12:	EAM-SD removed (1=removed)
				13:	Reserved
				14:	Reserved
				15:	Reserved
				16:	Reserved
				17:	Reserved
				18:	Reserved
				19:	Reserved

ID	Attribute	Access Rule	Data Type	Description	
0x1	Switch Status	Get	DWORD	20:	Reserved
				21:	Reserved
				22:	Reserved
				23:	MRP (0=disabled, 1=enabled)
				24:	PRP (0=disabled, 1=enabled)
				25:	Reserved
				26:	RSTP (0=disabled, 1=enabled)
				27:	LAG (0=disabled, 1=enabled)
				28:	Reserved
				29:	Reserved
				30:	Reserved
				31:	Connection Error (1=error detected)
0x2	Switch Temperature	Get	STRUCT of:		
			INT TemperatureF	in °F	
			INT TemperatureC	in °C	
0x3	Reserved	Get	UDINT	Reserved for future use (always 0)	
0x4	Switch Max Ports	Get	UINT	Maximum number of Ethernet Switch Ports	
0x5	Multicast Settings (IGMP Snooping)	Get/ Set	WORD	0:	IGMP Snooping (0=disabled, 1=enabled)
				1:	IGMP Querier (0=disabled, 1=enabled)
				2:	IGMP Querier Mode (read-only) (0=Non-Querier, 1=Querier)
				3:	
				4:	IGMP Querier Packet Version Off=0 IGMP Querier disabled V1=1 V2=2 V3=3
				5:	
				6:	
				7:	
				8:	Treatment of Unknown Multicasts: 0=Send To All Ports 1=Send To Query Ports 2=Discard
				9:	
				10:	

ID	Attribute	Access Rule	Data Type	Description
0x6	Switch Existing Ports	Get	ARRAY of: DWORD	Bitmask of existing switch ports Per bit starting with Bit 0 (=Port 1) (0=Port not available, 1=Port existing) Array (bit mask) size is adjusted to the size of maximum number of switch ports (for max. 28 Ports 1 DWORD is used)
0x7	Switch Port Control	Get/ Set	ARRAY of: DWORD	Bitmask Link Admin Status switch ports Per bit starting with Bit 0 (=Port 1) (0=Port enabled, 1=Port disabled) Array (bit mask) size is adjusted to the size of maximum number of Switch ports (for max. 28 Ports 1 DWORD is used)
0x8	Switch Ports Mapping	Get	ARRAY of: USINT	Instance number of the Ethernet-Link-Object Starting with Index 0 (=Port 1) All Ethernet Link Object Instances for the existing Ethernet Switch Ports (1..N, maximum number of ports). When the entry is 0, the Ethernet Link Object for this port does not exist
0x9	Switch Action Status	Get	DWORD	Status of the last executed action (for example config save, software update, etc.) 0: Flash Save Configuration In Progress/Flash Write In Progress 1: Flash Save Configuration error detected/Flash Write error detected 4: Configuration changed (configuration not in sync. between running configuration

The Schneider Electric specific Ethernet Switch Agent Object provides you with the additional vendor specific service, with the Service Code 0x35 for saving the Switch configuration. When you send a request from your PC to save a device configuration, the device sends a reply after saving the configuration in the flash memory.

Base Switch Object

The Base Switch object provides the CIP application-level interface to basic status information for a managed Ethernet switch (revision 1).

Only Instance 1 of the Base Switch (Class Code 0x51) is available.

ID	Attribute	Access Rule	Data Type	Description
0x1	Device Up Time	Get	UDINT	Time since the device powered up
0x2	Total port count	Get	UDINT	Number of physical ports
0x3	System Firmware Version	Get	SHORT-STRING	Human readable representation of System Firmware Version
0x4	Power source	Get	WORD	Status of switch power source
0x5	Port Mask Size	Get	UINT	Number of DWORD in port array attributes
0x6	Existing ports	Get	ARRAY of: DWORD	Port Mask
0x7	Global Port Admin State	Get	ARRAY of: DWORD	Port Admin Status
0x8	Global Port link Status	Get	ARRAY of: DWORD	Port Link Status
0x9	System Boot Loader Version	Get	SHORT-STRING	Readable System Firmware Version
0xA	Contact Status	Get	UDINT	Switch Contact Closure
0xB	Aging Time	Get	UDINT	Range 10..1000000 · 1/10 seconds (default=300) 0=Learning off
0xC	Temperature C	Get	UINT	Switch temperature in degrees Celsius
0xD	Temperature F	Get	UINT	Switch temperature in degrees Fahrenheit

Services, Connections and I/O Data

The device supports the following connection types and parameters.

Setting	I/O Connection	Input only	Listen only
Comm Format:	Data - DINT	Data - DINT	Input Data - DINT - Run/Program
IP Address	IP address of the device	IP address of the device	IP address of the device
Input Assembly Instance	100	100	100
Input Size	32	32	32
Output Assembly Instance	150	152	153
Output Size	32	0	0
Configuration Assembly Instance	151	151	151
Data Size	10	10	10

I/O Data	Value (Data Types and Sizes to be Defined)	Direction	Size[1]
Device Status	Bitmask (see Switch Agent Attribute 0x1)	Input	DWORD
Link Status	Bitmask, 1 Bit per port (0=No link, 1=Link up)	Input	DWORD
Output Links Admin State applied	Bitmask (1 Bit per port) to acknowledge output. Link state change can be denied, for example for controller access port. (0=Port enabled, 1=Port disabled)	Input	DWORD
Utilization Alarm[2]	Bitmask, 1 Bit per port (0=No alarm, 1=Alarm on port)	Input	DWORD
Access Violation Alarm[3]	Bitmask, 1 Bit per port (0=No alarm, 1=Alarm on port)	Input	DWORD
Multicast Connections	Integer, number of connections	Input	DINT
TCP/IP Connections	Integer, number of connections	Input	DINT
Quick Connect Mask	Bitmask (1 Bit per port) (0=Quick Connect disabled, 1=Quick Connect enabled)	Input	DINT
Link Admin State	Bitmask, 1 Bit per port (0=Port enabled, 1=Port disabled)	Output	DWORD

1. The default size of the port bit masks is 32 bits (DWORD). For devices with more than 28 ports the port bit masks have been extended to n * DWORD.
2. You specify the utilization alarm settings in the *Basic Settings > Port* dialog, *Utilization* tab. The upper threshold is the limit, where the alarm condition becomes active. The lower threshold is the limit, where an active alarm condition becomes inactive.
3. You specify the Access Violation alarm settings in the *Network Security > Port Security* dialog. The upper threshold is the limit, where the alarm condition becomes active. The lower threshold is the limit, where an active alarm condition becomes inactive.

Object Type	Bit Size
BOOL	1 bit
DINT	32 bit
DWORD	32 bit
SHORT-STRING	max. 32 bytes
STRING	max. 64 bytes
UDINT	32 bit
UINT	16 bit
USINT	8 bit
WORD	16 bit

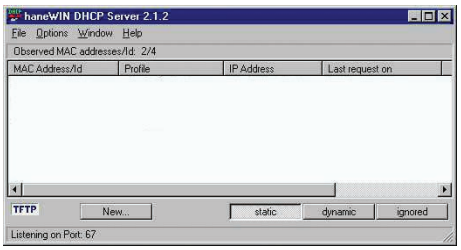
Setting up the Configuration Environment

Setting up a DHCP/BOOTP Server

The following example describes the configuration of a DHCP server using the haneWIN DHCP Server software. This shareware software is a product of IT-Consulting Dr. Herbert Hanewinkel. You can download the software from www.hanewin.net. You can test the software for 30 calendar days from the date of the first installation, and then decide if you want to purchase a license.

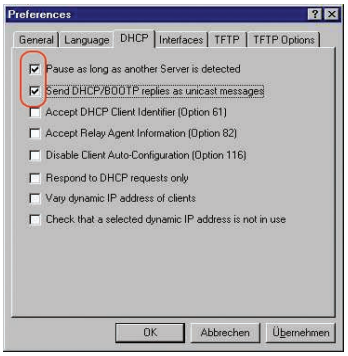
Perform the following steps:

- ☐ Install the DHCP server on your PC.
  To carry out the installation, follow the installation assistant.
- ☐ Start the *haneWIN DHCP Server* program.



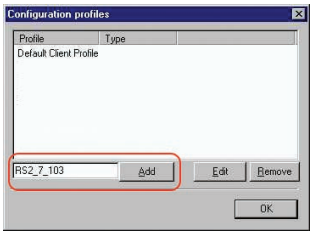
NOTE: When Windows is activated, the installation procedure includes a service that is automatically started in the basic configuration. This service is also active although the program itself has not been started. When started, the service responds to DHCP queries.

- ☐ In the menu bar, click the items *Options > Preferences* to open the program settings window.
- ☐ Select the *DHCP* tab.
- ☐ Specify the settings displayed in the figure.

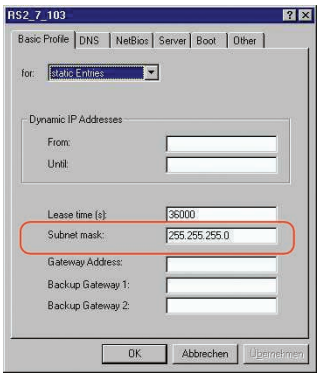


- ☐ Click the *OK* button.
- ☐ To enter the configuration profiles, click in the menu bar the items *Options > Configuration Profiles*.

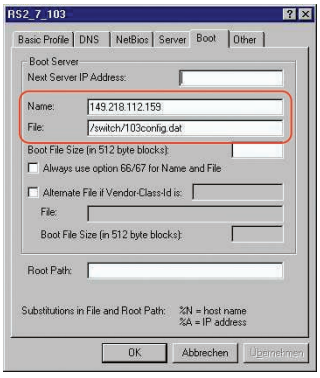
☐ Specify the name for the new configuration profile.



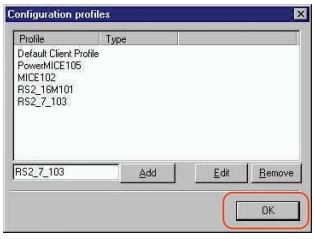
☐ Click the *Add* button.
☐ Specify the netmask.



☐ Click the *Apply* button.
☐ Select the *Boot* tab.
☐ Enter the IP address of your tftp server.
☐ Enter the path and the file name for the configuration file.

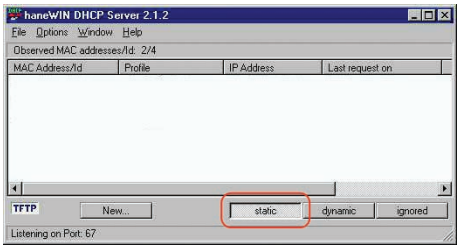


☐ Click the *Apply* button and then the *OK* button.
☐ Add a profile for each device type.
When devices of the same type have different configurations, you add a profile for each configuration.

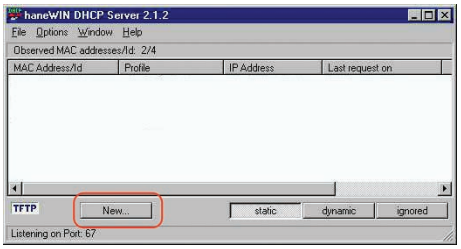


☐ To complete the addition of the configuration profiles, click the *OK* button.

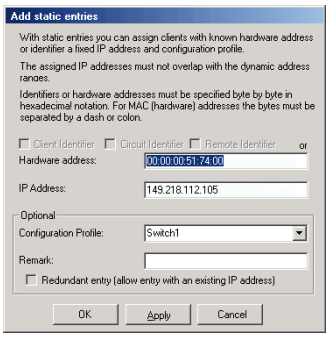
☐ To enter the static addresses, in the main window, click the *Static* button.



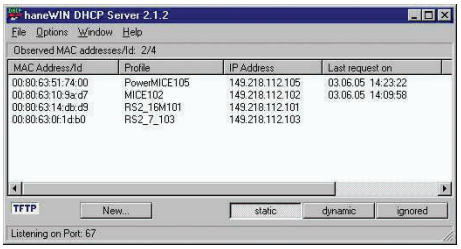
☐ Click the *Add* button.



☐ Enter the MAC address of the device.
☐ Enter the IP address of the device.



☐ Select the configuration profile of the device.
☐ Click the *Apply* button and then the *OK* button.
☐ Add an entry for each device that will get its parameters from the DHCP server.



Preparing Access via SSH

You can connect to the device using SSH. To do this, perform the following steps:

- Generate a key in the device.
  or
- Transfer your own key onto the device.
- Prepare access to the device in the SSH client program.

NOTE: In the default setting, the key is already existing and access using SSH is enabled.

Generating a Key in the Device

The device lets you generate the key directly in the device. To do this, perform the following steps:

- ☐ Open the *Device Security > Management Access > Server* dialog, *SSH* tab.
- ☐ To disable the SSH server, select the *Off* radio button in the *Operation* frame.
- ☐ Save the changes temporarily. To do this, click the ✓ button.
- ☐ To create a RSA key, in the *Signature* frame, click the *Create* button.
- ☐ To enable the SSH server, select the *On* radio button in the *Operation* frame.
- ☐ Save the changes temporarily. To do this, click the ✓ button.

`enable`	Change to the Privileged EXEC mode.
`configure`	Change to the Configuration mode.
`ssh key rsa generate`	Generate a new RSA key.

Loading your own Key onto the Device

OpenSSH gives experienced network administrators the option of generating an own key. To generate the key, enter the following commands on your PC:

```
ssh-keygen(.exe) -q -t rsa -f rsa.key -C '' -N ''
rsaparam -out rsaparam.pem 2048
```

The device lets you transfer your own SSH key onto the device. To do this, perform the following steps:

- ☐ Open the *Device Security > Management Access > Server* dialog, *SSH* tab.
- ☐ To disable the SSH server, select the *Off* radio button in the *Operation* frame.
- ☐ Save the changes temporarily. To do this, click the ✓ button.

- ☐ When the host key is located on your PC or on a network drive, drag and drop the file that contains the key in the area. Alternatively click in the area to select the file.
- ☐ Click the *Start* button in the *Key import* frame to load the key onto the device.
- ☐ To enable the SSH server, select the `On` radio button in the *Operation* frame.
- ☐ Save the changes temporarily. To do this, click the button.

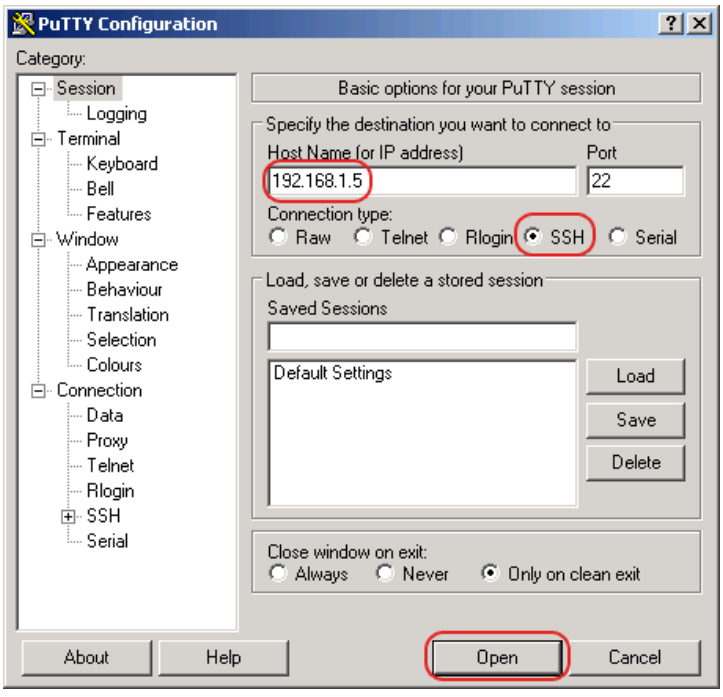
Perform the following steps:
- ☐ Copy the self-generated key from your PC to the external memory.
- ☐ Copy the key from the external memory into the device.

`enable`	Change to the Privileged EXEC mode.
`copy sshkey envm <file name>`	Load your own key onto the device from the external memory.

Preparing the SSH Client Program

The *PuTTY* program lets you access the device using SSH. You can download the software from www.putty.org.

Perform the following steps:
- ☐ Start the program by double-clicking on it.



- ☐ In the *Host Name (or IP address)* field you enter the IP address of your device. The IP address (a.b.c.d) consists of 4 decimal numbers with values from `0` to `255`. The 4 decimal numbers are separated by points.
- ☐ To select the connection type, select the *SSH* radio button in the *Connection type* option list.
- ☐ Click the *Open* button to set up the data connection to your device.

Before the connection is established, the *PuTTY* program displays a message and lets you verify the key fingerprint.

- ☐ Verify the fingerprint of the key to help ensure that you have actually connected to the desired device.
- ☐ When the fingerprint matches your key, click the *Yes* button.

For experienced network administrators, another way of accessing your device through an SSH is by using the OpenSSH Suite. To set up the data connection, enter the following command:

```
ssh admin@10.0.112.53
```

`admin` is the user name.

`10.0.112.53` is the IP address of your device.

HTTPS Certificate

Your web browser establishes the connection to the device using the HTTPS protocol. The prerequisite is that you enable the *HTTPS server* function in the*Device Security > Management Access > Server* dialog, *HTTPS* tab.

NOTE: Third-party software such as web browsers validate certificates based on criteria such as their expiration date and cryptographic parameters. Outdated certificates may cause issues due to invalid or outdated information. Example: An expired certificate or changed cryptographic parameters. To solve validation conflicts with third-party software, transfer your own up-to-date certificate onto the device or regenerate the certificate with the latest firmware.

HTTPS Certificate Management

A standard certificate according to X.509/PEM (Public Key Infrastructure) is required for encryption. In the default setting, a self-generated certificate is already present in the device. To do this, perform the following steps:

- ☐ Open the *Device Security > Management Access > Server* dialog, *HTTPS* tab.
- ☐ To create a X509/PEM certificate, in the *Certificate* frame, click the *Create* button.
- ☐ Save the changes temporarily. To do this, click the ✓ button.
- ☐ Restart the HTTPS server to activate the key. Restart the server using the CLI.

`enable`	Change to the Privileged EXEC mode.
`configure`	Change to the Configuration mode.
`https certificate generate`	Generate a https X.509/PEM Certificate.
`no https server`	Disable the *HTTPS* function.
`https server`	Enable the *HTTPS* function.

☐ The device also enables you to transfer an externally generated X.509/PEM certificate onto the device:

- ☐ Open the *Device Security > Management Access > Server* dialog, *HTTPS* tab.
- ☐ When the certificate is located on your PC or on a network drive, drag and drop the certificate in the area. Alternatively click in the area to select the certificate.
- ☐ Click on the *Start* button to copy the certificate to the device.
- ☐ Save the changes temporarily. To do this, click the ✓ button.

`enable`	Change to the Privileged EXEC mode.
`copy httpscert envm <file name>`	Copy HTTPS certificate from external non-volatile memory device.
`configure`	Change to the Configuration mode.
`no https server`	Disable the *HTTPS* function.
`https server`	Enable the *HTTPS* function.

NOTE: To activate the certificate after you created or transfered it, reboot the device or restart the HTTPS server. Restart the HTTPS server using the CLI.

Access through HTTPS

The default setting for HTTPS data connection is TCP port `443`. If you change the number of the HTTPS port, then reboot the device or the HTTPS server. Thus the change becomes effective. To do this, perform the following steps:

- ☐ Open the *Device Security > Management Access > Server* dialog, *HTTPS* tab.
- ☐ To enable the function, select the `On` radio button in the *Operation* frame.
- ☐ To access the device by HTTPS, enter HTTPS instead of HTTP in your browser, followed by the IP address of the device.

`enable`	Change to the Privileged EXEC mode.
`configure`	Change to the Configuration mode.
`https port 443`	Specifies the number of the TCP port on which the web server receives HTTPS requests from clients.
`https server`	Enable the *HTTPS* function.
`show https`	Displays the status of the *HTTPS* server and the port number.

When you make changes to the HTTPS port number, disable the HTTPS server and enable it again in order to make the changes effective.

The device uses HTTPS protocol and establishes a new data connection. When you log out at the end of the session, the device terminates the data connection.

Appendix

Management Information Base (MIB)

The Management Information Base (MIB) is designed in the form of an abstract tree structure.

The branching points are the object classes. The "leaves" of the MIB are called generic object classes.

When this is required for unique identification, the generic object classes are instantiated, that means the abstract structure is mapped onto reality, by specifying the port or the source address.

Values (integers, time ticks, counters or octet strings) are assigned to these instances; these values can be read and, in some cases, modified. The object description or object ID (OID) identifies the object class. The subidentifier (SID) is used to instantiate them.

Example:

The generic object class `sa2PSState` (`OID` = `1.3.6.1.4.1.3833.1.1.11.11.1.1.2.1`) is the description of the abstract information `power supply status`. However, it is not possible to read any value from this, as the system does not know which power supply is meant.

Specifying the subidentifier `2` maps this abstract information onto reality (instantiates it), thus identifying it as the operating status of power supply `2`. A value is assigned to this instance and can be read. The instance `get 1.3.6.1.4.1.3833.1.1.11.11.1.1.2.1` returns the response `1`, which means that the power supply is ready for operation.

Definition of the Syntax Terms Used:	
Integer	An integer in the range -2^{31} - 2^{31}-1
IP address	`xxx.xxx.xxx.xxx` (`xxx` = integer in the range `0..255`)
MAC address	12-digit hexadecimal number in accordance with ISO/IEC 8802-3
Object Identifier	x.x.x.x… (for example 1.3.6.1.1.4.1.3833...)
Octet String	ASCII character string
PSID	Power supply identifier (number of the power supply unit)
TimeTicks	Stopwatch, Elapsed time = numerical value / 100 (in seconds) numerical value = integer in the range 0-2^{32}-1
Timeout	Time value in hundredths of a second time value = integer in the range 0-2^{32}-1
Type field	4-digit hexadecimal number in accordance with ISO/IEC 8802-3
Counter	Integer (0-2^{32}-1), when certain events occur, the value increases by `1`.

List of RFCs

RFC 768	UDP
RFC 783	TFTP
RFC 791	IP
RFC 792	ICMP
RFC 793	TCP
RFC 826	ARP
RFC 854	Telnet
RFC 855	Telnet Option
RFC 951	BOOTP
RFC 1112	IGMPv1
RFC 1157	SNMPv1
RFC 1155	SMIv1
RFC 1212	Concise MIB Definitions
RFC 1213	MIB2
RFC 1493	Dot1d
RFC 1542	BOOTP-Extensions
RFC 1643	Ethernet-like -MIB
RFC 1757	RMON
RFC 1867	Form-Based File Upload in HTML
RFC 1901	Community based SNMP v2
RFC 1905	Protocol Operations for SNMP v2
RFC 1906	Transport Mappings for SNMP v2
RFC 1945	HTTP/1.0
RFC 2068	HTTP/1.1 protocol as updated by draft-ietf-http-v11-spec-rev-03
RFC 2131	DHCP
RFC 2132	DHCP-Options
RFC 2233	The Interfaces Group MIB using SMI v2
RFC 2236	IGMPv2
RFC 2246	The TLS Protocol, Version 1.0
RFC 2346	AES Ciphersuites for Transport Layer Security
RFC 2365	Administratively Scoped IP Multicast
RFC 2578	SMIv2
RFC 2579	Textual Conventions for SMI v2
RFC 2580	Conformance statements for SMI v2
RFC 2613	SMON
RFC 2618	RADIUS Authentication Client MIB
RFC 2620	RADIUS Accounting MIB
RFC 2674	Dot1p/Q
RFC 2818	HTTP over TLS
RFC 2851	Internet Addresses MIB
RFC 2863	The Interfaces Group MIB
RFC 2865	RADIUS Client
RFC 2866	RADIUS Accounting

RFC 2868	RADIUS Attributes for Tunnel Protocol Support
RFC 2869	RADIUS Extensions
RFC 2869bis	RADIUS support for EAP
RFC 2933	IGMP MIB
RFC 3164	The BSD Syslog Protocol
RFC 3376	IGMPv3
RFC 3410	Introduction and Applicability Statements for Internet Standard Management Framework
RFC 3411	An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks
RFC 3412	Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)
RFC 3413	Simple Network Management Protocol (SNMP) Applications
RFC 3414	User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)
RFC 3415	View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP)
RFC 3418	Management Information Base (MIB) for the Simple Network Management Protocol (SNMP)
RFC 3580	802.1X RADIUS Usage Guidelines
RFC 3584	Coexistence between Version 1, Version 2, and Version 3 of the Internet-standard Network Management Framework
RFC 4022	Management Information Base for the Transmission Control Protocol (TCP)
RFC 4113	Management Information Base for the User Datagram Protocol (UDP)
RFC 4188	Definitions of Managed Objects for Bridges
RFC 4251	SSH protocol architecture
RFC 4252	SSH authentication protocol
RFC 4253	SSH transport layer protocol
RFC 4254	SSH connection protocol
RFC 4293	Management Information Base for the Internet Protocol (IP)
RFC 4318	Definitions of Managed Objects for Bridges with Rapid Spanning Tree Protocol
RFC 4330	Simple Network Time Protocol (SNTP) Version 4 for IPv4, IPv6 and OSI
RFC 4363	Definitions of Managed Objects for Bridges with Traffic Classes, Multicast Filtering, and Virtual LAN Extensions
RFC 4541	Considerations for Internet Group Management Protocol (IGMP) and Multicast Listener Discovery (MLD) Snooping Switches
RFC 4836	Definitions of Managed Objects for IEEE 802.3 Medium Attachment Units (MAUs)

Underlying IEEE Standards

IEEE 802.1AB	Station and Media Access Control Connectivity Discovery
IEEE 802.1D	MAC Bridges (switching function)
IEEE 802.1Q	Virtual LANs (VLANs, MRP, Spanning Tree)
IEEE 802.1X	Port Authentication
IEEE 802.3	Ethernet
IEEE 802.3ac	VLAN Tagging
IEEE 802.3x	Flow Control
IEEE 802.3af	Power over Ethernet

Underlying IEC Norms

IEC 62439	High availability automation networks MRP – Media Redundancy Protocol based on a ring topology PRP – Parallel Redundancy Protocol

Underlying ANSI Norms

ANSI/TIA-1057	Link Layer Discovery Protocol for Media Endpoint Devices, April 2006

Technical Data

Switching

Size of the MAC address table (incl. static filters)	2048
Max. number of statically configured MAC address filters	100
Max. number of MAC address filters learnable through IGMP Snooping	256
Max. number of MAC address entries (MMRP)	64
Number of priority queues	4 Queues
Port priorities that can be set	0..3
MTU (Max. allowed length of packets a port can receive or transmit)	1518 Bytes

VLAN

VLAN ID range	1..4042
Number of VLANs	max. 16 simultaneously per device max. 16 simultaneously per port

Copyright of Integrated Software

The product contains, among other things, Open Source Software files developed by third parties and licensed under an Open Source Software license.

You can find the license terms in the GUI in the *Help > Licenses* dialog.

Abbreviations used

BOOTP	Bootstrap Protocol
CLI	Command Line Interface
DHCP	Dynamic Host Configuration Protocol
EUI	Extended Unique Identifier
FDB	Forwarding Database
GUI	Graphical User Interface
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
ICMP	Internet Control Message Protocol
IEEE	Institute of Electrical and Electronics Engineers
IGMP	Internet Group Management Protocol
IP	Internet Protocol
LED	Light Emitting Diode
LLDP	Link Layer Discovery Protocol
MAC	Media Access Control
MIB	Management Information Base
MRP	Media Redundancy Protocol
NMS	Network Management System
PC	Personal Computer
PTP	Precision Time Protocol
QoS	Quality of Service
RFC	Request For Comment
RM	Redundancy Manager
RSTP	Rapid Spanning Tree Protocol
SCP	Secure Copy
SFP	Small Form-factor Pluggable
SFTP	SSH File Transfer Protocol
SNMP	Simple Network Management Protocol
SNTP	Simple Network Time Protocol
TCP	Transmission Control Protocol
TFTP	Trivial File Transfer Protocol
TP	Twisted Pair
UDP	User Datagram Protocol
URL	Uniform Resource Locator
UTC	Coordinated Universal Time
VLAN	Virtual Local Area Network

A Index

T

U

V

W

Schneider Electric
35 rue Joseph Monier
92500 Rueil Malmaison
France

+ 33 (0) 1 41 29 70 00

www.se.com

As standards, specifications, and design change from time to time, please ask for confirmation of the information given in this publication.

EIO0000005410.00