Modicon

MCSESM, MCSESM-E, MCSESP Managed Switch Configuration User Manual

QGH59056.02

The information provided in this documentation contains general descriptions and/or technical characteristics of the performance of the products contained herein. This documentation is not intended as a substitute for and is not to be used for determining suitability or reliability of these products for specific user applications. It is the duty of any such user or integrator to perform the appropriate and complete risk analysis, evaluation and testing of the products with respect to the relevant specific application or use thereof. Neither Schneider Electric nor any of its affiliates or subsidiaries shall be responsible or liable for misuse of the information contained herein. If you have any suggestions for improvements or amendments or have found errors in this publication, please notify us.

You agree not to reproduce, other than for your own personal, noncommercial use, all or part of this document on any medium whatsoever without permission of Schneider Electric, given in writing. You also agree not to establish any hypertext links to this document or its content. Schneider Electric does not grant any right or license for the personal and noncommercial use of the document or its content, except for a non-exclusive license to consult it on an "as is" basis, at your own risk. All other rights are reserved.

All pertinent state, regional, and local safety regulations must be observed when installing and using this product. For reasons of safety and to help ensure compliance with documented system data, only the manufacturer must perform repairs to components.

When devices are used for applications with technical safety requirements, the relevant instructions must be followed.

Failure to use Schneider Electric software or approved software with our hardware products may result in injury, harm, or improper operating results.

Failure to observe this information can result in injury or equipment damage.

As part of a group of responsible, inclusive companies, we are updating our communications that contain non-inclusive terminology. Until we complete this process, however, our content may still contain standardized industry terms that may be deemed inappropriate by our customers.

© 2022 Schneider Electric. All Rights Reserved.

Contents

Safety information

Note: Read these instructions carefully, and look at the equipment to become familiar with the device before trying to install, operate, 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 imminently hazardous situation which, if not avoided, **will result in** death or serious injury.

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

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

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

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.

© 2022 Schneider Electric. All Rights Reserved.

About this Manual

Validity Note

The data and illustrations found in this book are not binding. We reserve the right to modify our products in line with our policy of continuous product development. The information in this document is subject to change without notice and should not be construed as a commitment by Schneider Electric.

User Comments

We welcome your comments about this document. You can reach us by e-mail at techpub@schneider-electric.com

Related Documents

The “Configuration” user manual 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.

The “Installation” user manual contains a device description, safety instructions, a description of the display, and the other information that you need to install the device.

The “Graphical User Interface” reference manual contains detailed information on using the graphical user interface to operate the individual functions of the device.

The “Command Line Interface” reference manual contains detailed information on using the Command Line Interface to operate the individual functions of the device.

The ConneXium Network Manager Network Management software provides you with additional options for smooth configuration and monitoring:
- Auto-topology discovery
- Browser interface
- Client/server structure
- Event handling
- Event log
- Simultaneous configuration of multiple devices
- Graphical user interface with network layout
- SNMP/OPC gateway

Key

The designations used in this manual have the following meanings:

▶	List
☐	Work step
Link	Cross-reference with link
Note:	A note emphasizes a significant fact or draws your attention to a dependency.
`Courier`	Representation of a CLI command or field contents in the graphical user interface

Execution in the Graphical User Interface

Execution in the Command Line Interface

Replacing a device

The device provides the following plug-and-play solutions for replacing a device with a device of the same type, for instance, if a failure was detected or for preventive maintenance:

- 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 102.
- The new device gets its IP address using DHCP *Option 82*.
  See “DHCP L2 Relay” on page 310.
  See “Setting up a DHCP server with Option 82” on page 355.

With each solution, upon reboot, the new device gets the same IP settings that the replaced device had.

- For accessing 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 361.
- For accessing 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 358.

1 User interfaces

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

Table 1: User interfaces for accessing the device management

User interface	Can be reached through …	Prerequisite
Graphical User Interface	Ethernet (In-Band)	Web browser
Command Line Interface	Ethernet (In-Band) Serial interface (Out-of-Band)	Terminal emulation software
System monitor	Serial interface (Out-of-Band)	Terminal emulation software

1.1 Graphical User Interface

System requirements

To open the Graphical User Interface, 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 current cryptographic parameter recommendations. Outdated certificates may cause issues due to invalid or outdated information. Example: An expired certificate or changed cryptographic recommendations. 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 Graphical User Interface

The prerequisite for starting the Graphical User Interface is that the IP parameters are configured in the device. See “Specifying the IP parameters” on page 43.

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 Graphical User Interface, 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 Graphical User Interface.

1.2 Command Line Interface

The Command Line Interface enables you to use the functions of the device through a local or remote connection.

The Command Line Interface 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.

1.2.1 Preparing the data connection

Information for assembling and starting up your device can be found in the “Installation” user manual.

- ☐ 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 Command Line Interface for example, with the freeware program *PuTTY*.

- ☐ Install the *PuTTY* program on your computer.

1.2.2 Access to the Command Line Interface using Telnet

Telnet connection using Windows

Telnet is only installed as standard in Windows versions before Windows Vista.

Perform the following steps:

- ☐ Start the *Command Prompt* program on your computer.
- ☐ Enter the command `telnet <IP_address>`.

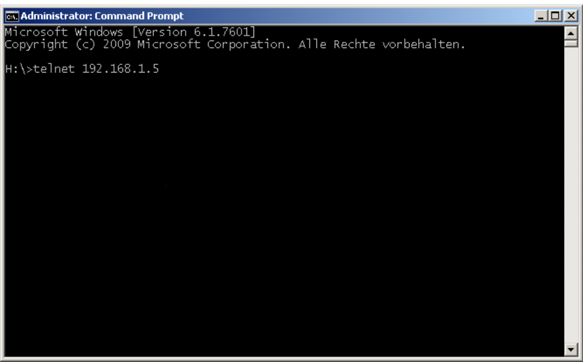


Figure 1: Command Prompt: Setting up the Telnet connection to the device

Telnet connection using PuTTY

Perform the following steps:

- Start the *PuTTY* program on your computer.

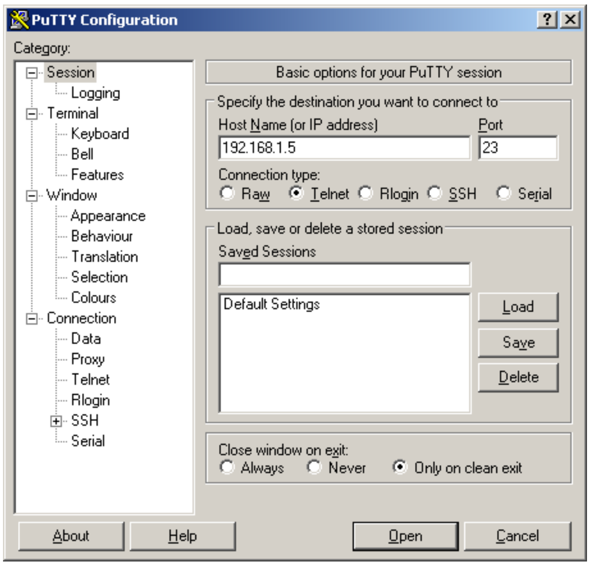


Figure 2: PuTTY input screen

- 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 select 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 Command Line Interface appears on the screen with a window for entering the user name.
  The device enables up to 5 users to have access to the Command Line Interface 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) 2011-2022 Schneider Electric

                               All rights reserved

                            MCSESM-E Release 08.7.00

                          (Build date 2022-06-25 09:36)


              System Name   :  MCSESM-646038d5e846
              Management IP :  192.168.1.5
              Subnet Mask   :  255.255.255.0
              Base MAC      :  64:60:38:01:02:03
              USB IP        :  91.0.0.100
              USB Mask      :  255.255.255.0
              System Time   :  2022-06-27 12:48:08


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.

MCSESM-E>
```

Figure 3: Start screen of the Command Line Interface

1.2.3 Access to the Command Line Interface 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.

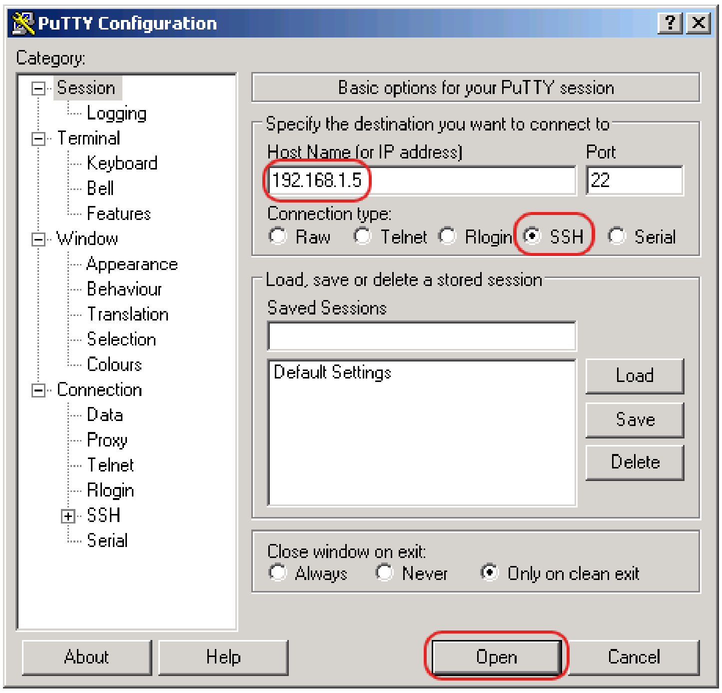


Figure 4: PuTTY input screen

- 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 security alert message and lets you check the fingerprint of the key.

Figure 5: Security alert prompt for the fingerprint

- Check the fingerprint.
  This helps protect yourself from unwelcome guests.
- 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 Command Line Interface appears on the screen with a window for entering the user name. The device enables up to 5 users to have access to the Command Line Interface 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) 2011-2022 Schneider Electric

                                     All rights reserved

                                 MCSESM-E Release 08.7.00

                              (Build date 2022-06-25 09:36)


                    System Name   :  MCSESM-646038d5e846
                    Management IP :  192.168.1.5
                    Subnet Mask   :  255.255.255.0
                    Base MAC      :  64:60:38:01:02:03
                    USB IP        :  91.0.0.100
                    USB Mask      :  255.255.255.0
                    System Time   :  2022-06-27 12:48:08


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.

MCSESM-E>
```

Figure 6: Start screen of the Command Line Interface

1.2.4 Access to the Command Line Interface 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 Command Line Interface 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.

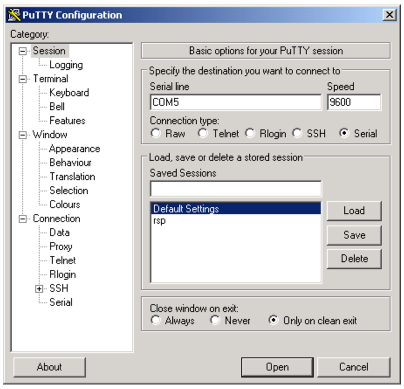


Figure 7: Serial data connection with the serial interface using the PuTTY program

- 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) 2011-2022 Schneider Electric

                              All rights reserved

                          MCSESM-E Release 08.7.00

                        (Build date 2022-06-25 09:36)


              System Name   :  MCSESM-646038d5e846
              Management IP :  192.168.1.5
              Subnet Mask   :  255.255.255.0
              Base MAC      :  64:60:38:01:02:03
              USB IP        :  91.0.0.100
              USB Mask      :  255.255.255.0
              System Time   :  2022-06-27 12:48:08


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.

MCSESM-E>
```

Figure 8: Start screen of the Command Line Interface

1.2.5 Mode-based command hierarchy

In the Command Line Interface, the commands are grouped in the related modes, according to the type of the command. Every command mode supports specific Schneider Electric software commands.

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 currently 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 Command Line Interface also enables you to execute these commands in the Privileged Exec mode.

The following figure displays the modes of the Command Line Interface.

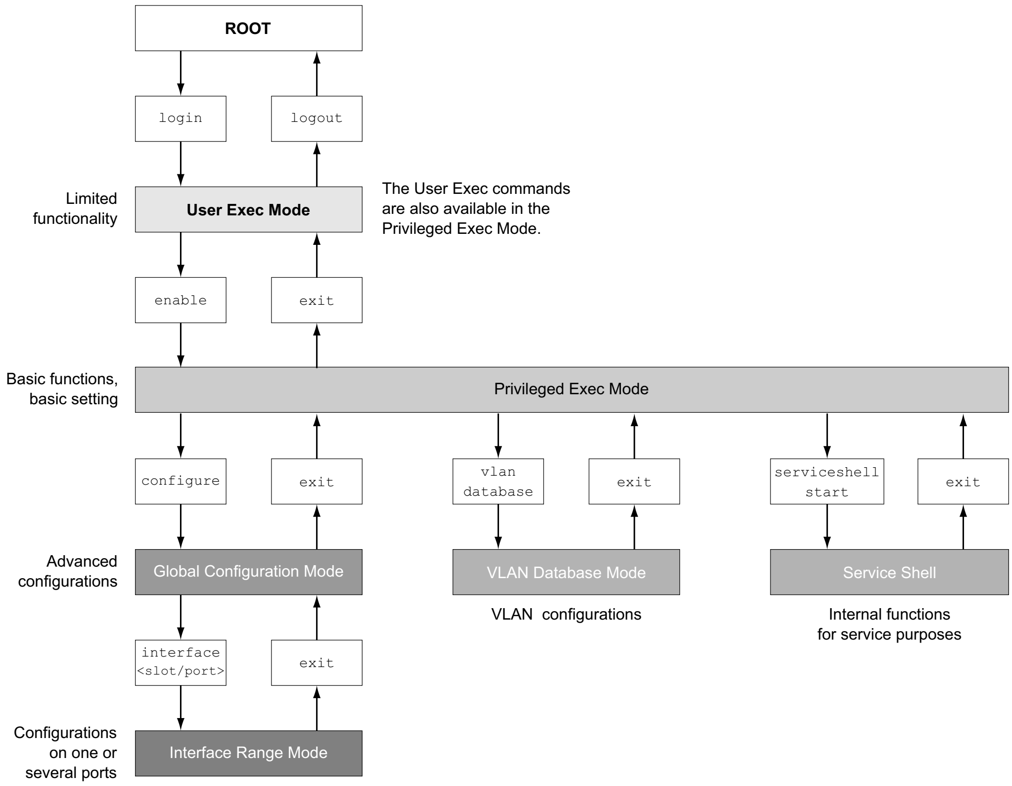


Figure 9: Structure of the Command Line Interface

The Command Line Interface supports, depending on the user level, the following modes:

- User Exec mode
  When you log in with the Command Line Interface, you enter the User Exec mode. The User Exec mode contains a limited range of commands.
  Command prompt: `(MCSESM-E) >`
- Privileged Exec mode
  To access the entire range of commands, you enter the Privileged Exec mode. If you log in as a privileged user, then you are able to enter the Privileged Exec mode. In the Privileged Exec mode, you are able to execute the User Exec mode commands, too.
  Command prompt: `(MCSESM-E) #`
- VLAN mode
  The VLAN mode contains VLAN-related commands.
  Command prompt: `(MCSESM-E) (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 current configuration. This mode groups general setup commands.
  Command prompt: `(MCSESM-E) (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: `(MCSESM-E) ((interface) all)#`
    Example: When you switch from the Global Config mode to the Interface Range mode, the command prompt changes as follows:
    ```
    (MCSESM-E) (config)#interface all
    (MCSESM-E) ((Interface)all)#
    ```
  – A single port on one interface
    Command prompt: `(MCSESM-E) (interface <slot/port>)#`
    Example: When you switch from the Global Config mode to the Interface Range mode, the command prompt changes as follows:
    ```
    (MCSESM-E) (config)#interface 2/1
    (MCSESM-E) (interface 2/1)#
    ```
  – A range of ports on one interface
    Command prompt: `(MCSESM-E) (interface <interface range> )#`
    Example: When you switch from the Global Config mode to the Interface Range mode, the command prompt changes as follows:
    ```
    (MCSESM-E) (config)#interface 1/2-1/4
    (MCSESM-E) ((Interface)1/2-1/4)#
    ```
  – A list of single ports
    Command prompt: `(MCSESM-E) (interface <interface list>)#`
    Example: When you switch from the Global Config mode to the Interface Range mode, the command prompt changes as follows:
    ```
    (MCSESM-E) (config)#interface 1/2,1/4,1/5
    (MCSESM-E) ((Interface)1/2,1/4,1/5)#
    ```
  – A list of port ranges and single ports
    Command prompt: `(MCSESM-E) (interface <complex range>)#`
    Example: When you switch from the Global Config mode to the Interface Range mode, the command prompt changes as follows:
    ```
    (MCSESM-E) (config)#interface 1/2-1/4,1/6-1/9
    (MCSESM-E) ((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.

Table 2: Command modes

Command mode	Access method	Quit or start next mode

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

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

Table 2: Command modes

Command mode	Access method	Quit or start next mode

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

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

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

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

```
(MCSESM-E)>
  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.

(MCSESM-E)>
```

Figure 10: Commands in the User Exec mode

1.2.6 Executing the commands

Syntax analysis

When you log in with the Command Line Interface, you enter the User Exec mode. The Command Line Interface displays the prompt `(MCSESM-E)>` on the screen.

When you enter a command and press the <Enter> key, the Command Line Interface starts the syntax analysis. The Command Line Interface searches the command tree for the desired command.

When the command is outside the Command Line Interface 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 Command Line Interface then displays a message:

```
(MCSESM-E)>show system ino

Error: Invalid command 'ino'
```

Command tree

The commands in the Command Line Interface 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 Command Line Interface checks the input. When you entered the command and the parameters correctly and completely, you 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 unknown, the Command Line Interface 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.

1.2.7 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 Command Line Interface 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.

Table 3: Parameter and command syntax

`<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 (3 points in sequence without spaces) 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>`	Small letters are wild cards. You enter parameters with the notation a.b.c.d with decimal points (for example IP addresses)
`<cr>`	You press the <Enter> key to create a line break (carriage return).

The following list displays the possible parameter values within the Command Line Interface:

Table 4: Parameter values in the Command Line Interface

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. MAC addresses are unique worldwide.

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

Table 5: Format and range of network addresses

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. You enter a space character in a parameter between quotation marks.

Example:

```
*(MCSESM-E)#cli prompt Device name
Error: Invalid command 'name'

*(MCSESM-E)#cli prompt 'Device name'
```

```
*(Device name)#
```

1.2.8 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.

```
(MCSESM-E) (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.

```
(MCSESM-E) (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.

1.2.9 Input prompt

Command mode

With the input prompt, the Command Line Interface displays which of the three modes you are in:

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

- Asterisk `*`
  An asterisk `*` in the first or second position of the input prompt displays you 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.
  `*(MCSESM-E)>`
- Pound sign `#`
  A pound sign `#` at the beginning of the input prompt displays you that the boot parameters and the parameters during the boot phase are different.
  *# `(MCSESM-E)>`
- Exclamation point `!`
  An exclamation point `!` at the beginning of the input prompt displays: the password for the `user` or `admin` user account corresponds with the default setting.
  `!(MCSESM-E)>`

Wildcards

The device lets you change the command line prompt.

The Command Line Interface supports the following wildcards:

Table 6: Using wildcards within the Command Line Interface input prompt

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

Table 6: Using wildcards within the Command Line Interface input prompt

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

```
!(MCSESM-E)>enable

!(MCSESM-E)#cli prompt %i

!192.168.1.5#cli prompt (MCSESM-E)%d

!*(MCSESM-E)2022-06-27#cli prompt (MCSESM-E)%d%t

!*(MCSESM-E)2022-06-27 12:48:08#cli prompt %m

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

1.2.10 Key combinations

The following key combinations make it easier for you to work with the Command Line Interface:

Table 7: Key combinations in the Command Line Interface

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>, <SPACE>	Command line completion
`Exit`	Go to next lower command prompt
<?>	List choices

The Help command displays the possible key combinations in Command Line Interface on the screen:

```
(MCSESM-E) #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

(MCSESM-E) #
```

Figure 11: Listing the key combinations with the Help command

1.2.11 Data entry elements

Command completion

To simplify typing commands, the Command Line Interface lets you use command completion (Tab Completion). Thus you are able to abbreviate key words.

- Type in the beginning of a keyword. When the characters entered identify a keyword, the Command Line Interface completes the keyword after you press the tab key or the space key. When there is more than one option for completion, enter the letter or the letters necessary for uniquely identifying the keyword. Press the tab key or the space key again. After that, the system completes the command or parameter.
- When you make a non-unique entry and press <Tab> or <Space> twice, the Command Line Interface provides you with a list of options.
- On a non-unique entry and pressing <Tab> or <Space>, the Command Line Interface completes the command up to the end of the uniqueness. When several commands exist and you press <Tab> or <Space> again, the Command Line Interface provides you with a list of options.
  Example:
  ```
  (MCSESM-E) (Config)#lo
  (MCSESM-E) (Config)#log
  logging logout
  ```
  When you enter `lo` and <Tab> or <Space>, the Command Line Interface completes the command up to the end of the uniqueness to `log`.
  When you press <Tab> or <Space> again, the Command Line Interface 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 `(MCSESM-E) >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:

```
!*#(MCSESM-E)(Config)#show?

   show          Display device options and settings.
```

1.2.12 Use cases

Saving the Configuration

To help ensure that your password settings and your other configuration changes are kept after the device is reset or after an interruption of the voltage supply, you 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 29.

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`

1.2.13 Service Shell

The Service Shell is for service purposes only.

The Service Shell lets users have 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
RISK THAT DEVICE WILL NOT OPERATE Do not execute internal functions such as deleting the non-volatile memory (*NVM*) without service technician instructions. **Failure to follow these instructions possibly leads to an inoperative device.**

Start the Service Shell

The prerequisite is that you are in User Exec mode: `(MCSESM-E) >`

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.

```
!MCSESM-E >enable

!*MCSESM-E #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 (2022-06-27 12:48:08 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 Command Line Interface 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 are still able to configure 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: `(MCSESM-E) >`

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.

```
!MCSESM-E >enable

!*MCSESM-E #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) ?
```

1.3 System monitor

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

1.3.1 Functional scope

In the System Monitor, you carry out the following tasks, for example:
- Managing the operating system and verifying the software image
- Updating the operating system
- Starting the operating system
- Deleting configuration profiles, resetting the device to the factory defaults
- Checking boot code information

1.3.2 Starting the System Monitor

You establish a serial connection to the device using the USB-C interface. During the boot process, the serial interface of the device is unavailable. For this reason, starting the System Monitor works differently from other Schneider Electric devices. To start the System Monitor, you set the device to the Recovery Mode.

Set the device to the Recovery Mode

Required accessories:
- External memory (recommended: ACA22-USB-C)
- USB-C to USB-A adapter (only if you use a different external memory than the recommended one)
- USB cable to connect the USB-C port of the device with the computer
- Computer with VT100 terminal emulation (for example PuTTY) or a serial terminal

Perform the following steps:
- [ ] Plug the external memory into your computer.
- [ ] In the root directory of the external memory, create an empty file named `recovery.txt`.
- [ ] Plug the external memory into the device.
- [ ] Reboot the device.
- [ ] Observe the LEDs while the device boots. When the *Status* LED flashes alternately red and green, the device has successfully booted into the Recovery Mode.

Note: You find the description of the display elements in the “Installation” user manual.

Access the System Monitor

Perform the following steps:
- Remove the external memory from the device.
- Connect your computer to the device using the USB cable.
- Open the VT100 terminal emulation on the computer to display the System Monitor.
  - Select the appropriate COM port.
  - Specify the following transmission parameters:

VT 100 terminal settings	
Speed	`9600 bit/s`
Data bits	`8 bit`
Stop bit	`1 bit`
Software handshake	`off`
Parity	`none`

When the computer and the device are successfully connected, you see a black screen.

Perform the following steps:
- Press the <Enter> key to display the System Monitor.
  You see the following view on your computer:

```
    System Monitor 1
    (Selected OS: ...-8.7 (2022-06-25 09:36))

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






sysMon1>
```

Figure 12: System Monitor view

- To select a menu item, enter the corresponding number.
- To leave a submenu and return to the main menu, press the <ESC> key.

Note: To boot the device normally next time, only add the external memory without the `recovery.txt` file.

2 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 Command Line Interface.
  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, you choose this “In-Band” method.
- Configuration using the external memory.
  When you are replacing a device with a device of the same type and have already saved the configuration in the external memory, you choose this method.
- Using BOOTP.
  To configure the installed device using BOOTP, you 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, you 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.
  When the device already has an IP address and is reachable using the network, the Graphical User Interface provides you with another option for configuring the IP parameters.

2.1 IP parameter basics

2.1.1 IPv4

IP address

The IP addresses consist of 4 bytes. Write these 4 bytes in decimal notation, separated by a decimal point.

RFC 1340 written in 1992, defines 5 IP Address classes.

Table 8: 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 IANA ("Internet Assigned Numbers Authority"). 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:

- APNIC (Asia Pacific Network Information Center)
  Asia/Pacific Region
- ARIN (American Registry for Internet Numbers)
  Americas and Sub-Sahara Africa
- LACNIC (Regional Latin-American and Caribbean IP Address Registry)
  Latin America and some Caribbean Islands
- RIPE NCC (Réseaux IP Européens)
  Europe and Surrounding Regions

0	Net ID - 7 bits				Host ID - 24 bits	Class A
I	0	Net ID - 14 bits			Host ID - 16 bits	Class B
I	I	0	Net ID - 21 bits		Host ID - 8 bit s	Class C
I	I	I	0	Multicast Group ID - 28 bits		Class D
I	I	I	I	reserved for future use - 28 b its		Class E

Figure 13: Bit representation of the IP address

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

When the first bit of an IP address is a one and the second bit is a 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 a 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 alone is responsible for 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.

You 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

Subnetwork mask bits
Class B

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 how the netmask is used

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?

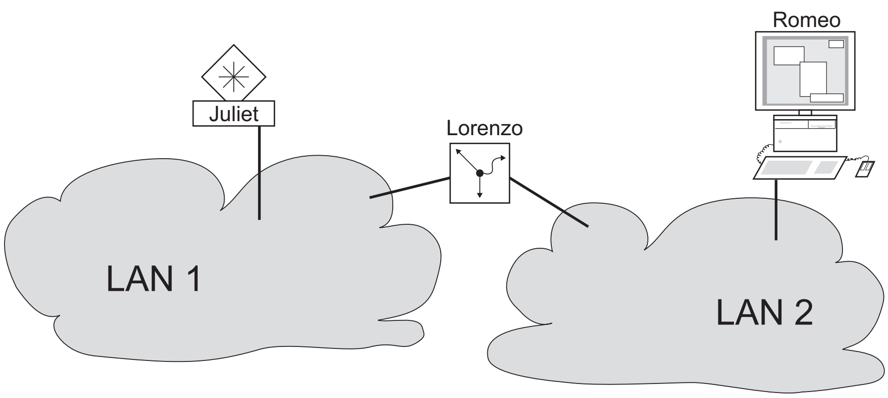


Figure 14: The management agent is separated from its network management station by a router

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 therefore 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 then 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.

Finally, 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 then 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 would now like 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 is she to send the answer? For 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 variable `NetGatewayIPAddr` as a means of communicating with Romeo. She therefore puts the envelope with the IP addresses in a further 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 to a fine degree.

2.1.2 IPv6

IP parameter basics

The Internet Protocol version 6 (IPv6) is the new version of the Internet Protocol version 4 (IPv4). The need to implement IPv6 was due to the fact that IPv4 addresses are not sufficient in the context of the growing Internet today. The IPv6 protocol is described in RFC 8200.

Some of the differences between IPv6 and IPv4 are:
- Address representation and length
- Absence of the broadcast address type
- Simplified header structure
- Fragmentation performed only by the source host
- Added capabilities for packet flow identification in the network

Both IPv4 and IPv6 protocols can operate at the same time in the device. This is possible with the use of the Dual IP Layer technique, also referred to as Dual Stack.

Note: If you want the device to operate only using the IPv4 function, then disable the IPv6 function in the device.

In the device, the IPv6 protocol has the following restrictions:
- You can specify a maximum number of 8 IPv6 unicast addresses as follows:
  - 4 IPv6 addresses using manual configuration
  - 2 IPv6 addresses when the *Auto* radio button is selected
  - 1 IPv6 address using the DHCPv6 server
  - 1 link-local address
- The IPv6 function can be enabled only on the management interface. The total number of configurable IPv6 addresses can be used at the same time on the interface.
- The IPv6 addresses can be used to set the management IP address of the device. Other services where IPv6 addresses can be used include for example, SNTP, SYSLOG, DNS, and LDAP.

Address representation

The IPv6 address consists of 128 bits. It is represented as 8 groups of 4 hexadecimal digits, each group representing 16 bits, further referred to as a hextet. The hextets are separated by colons (:). IPv6 addresses are not case-sensitive and you can write them in either lowercase or uppercase.

In accordance with RFC 4291, the preferred format for an IPv6 address is x:x:x:x:x:x:x:x. Each “x” consists of 4 hexadecimal values and represents a hextet. An example of a preferred format of an IPv6 address is shown in the figure below.

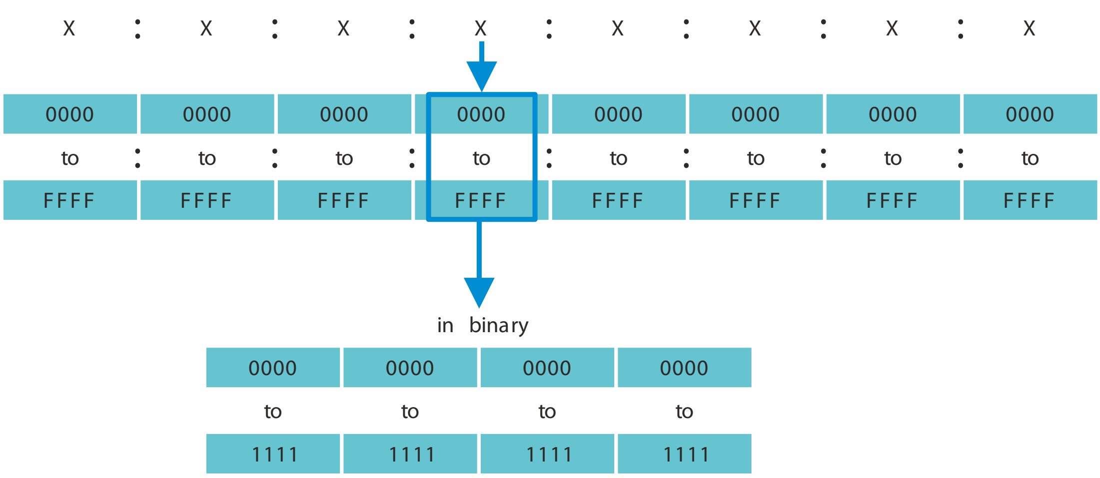


Figure 15: IPv6 address representation

As you can see in the figure above, usually an IPv6 address contains many zeros. In order to shorten IPv6 addresses that contain 0 bits, it is necessary to follow 2 writing rules:

- The first rule is to discard the leading zeros in every hextet. This rule is only applied to leading zeros and not to the trailing zeros of a hextet. If the trailing zeros are also discarded, then the resulting address is ambiguous.
- The second rule uses a special syntax to compress the zeros. You can use 2 adjacent colons “::” to replace a string of adjacent hextets that contain only zeros. The “::” sign can be used only one time in an address. If the “::” sign is used more than one time in an address representation, then there can be more than one possible address expanded from that notation.

When the two rules are applied, the result is commonly known as the compressed format.

In the table below you can find 2 examples of how these rules are applied:

Table 9: IPv6 address compression

Preferred	CC03:0000:0000:0000:0001:AB30:0400:FF02
No leading zeros	CC03: 0: 0: 0: 1:AB30: 400:FF02
Compressed	CC03::1:AB30:400:FF02

Preferred	2008:00B7:0000:DEF0:DDDD:0000:E604:0001
No leading zeros	2008: B7: 0:DEF0:DDDD: 0:E604: 1
Compressed	2008:B7::DEF0:DDDD:0:E604:1

Prefix length

Unlike an IPv4 address, an IPv6 address does not use a subnet mask to identify the network portion of an address. Instead, the IPv6 protocol uses the prefix length.

The text representation of IPv6 address prefixes is similar to the way IPv4 address prefixes are written in Classless Inter-Domain Routing (CIDR):

```
<ipv6-address>/<prefix-length>
```

The prefix length range is `0..128`. The typical IPv6 prefix length for LANs and other types of networks is /64. This means that the network portion of the address is 64 bits in length. The remaining 64 bits represent the Interface ID, similar to the host portion of the IPv4 address.

In the figure below you can find an example of prefix length bits allocation.

64 bits prefix length	**64 bits interface ID**
Address example: 2009:0CB8:0000:0004::10/64	
2009:0CB8:0000:0004	**0000:0000:0000:0010**

Address types

The IPv6 address types are described in RFC 4291.

The IPv6 address types are identified by the high-order bits of the address, as in the table below:

Table 10: IPv6 address types

Address type	Binary prefix	IPv6 notation
Unspecified	00...0 (128 bits)	::/128
Loopback	00...1 (128 bits)	::1/128
Multicast	11111111	FF00::/8
Link-local Unicast	1111111010	FE80::/10
Global Unicast	(everything else)	

The Unspecified address

The IPv6 address with every bit set to 0 is called the Unspecified address, which corresponds to 0.0.0.0 in IPv4. The Unspecified address is used only to indicate the absence of an address. It is typically used as a source address when a unique address is not determined yet.

Note: The Unspecified address cannot be assigned to an interface or used as a destination address.

The Loopback address

The unicast address 0:0:0:0:0:0:0:1 is called the Loopback address. It can be used by a device to send an IPv6 packet to itself. It cannot be assigned to a physical interface.

The Multicast address

IPv6 does not have a broadcast address like IPv4. But there is an IPv6 all-nodes Multicast address that essentially gives the same result.

An IPv6 Multicast address is used to send an IPv6 packet to multiple destinations. The structure of a Multicast address is as follows: The next 4 bits identify the scope of the Multicast address (how far the packet is transmitted):
- The first 8 bits are set to `FF`.
- The next 4 bits are the lifetime of the address: 0 is permanent and 1 is temporary.
- The next 4 bits identify the scope of the Multicast address, meaning how far the packets are transmitted through the network.

The Link-Local address

The Link-Local address is used to communicate with other devices on the same link. The term “link” refers to a subnet. Routers do not forward packets with link-local source or destination addresses to other links.

Link-local addresses are used to transmit packets on a single link for scopes such as automatic address configuration, neighbor discovery, or when no routers are present. They have the following format:

Table 11: Link-Local Address format

10 bits	54 bits	64 bits
1111111010	0	Interface ID

The Link-Local address is always configured and cannot be changed.

The Global Unicast address

A Global Unicast address is globally unique and can be routed over the Internet. This type of addresses are equivalent to public IPv4 addresses. Currently, only Global Unicast addresses with the first three bits of 001 or 2000::/3 are assigned.

A Global Unicast address has 3 parts:
- Global Routing Prefix
- Subnet ID
- Interface ID.

The Global Routing Prefix is the network portion of the address.

The Subnet ID is used by an organization to identify its subnets and it has up to 16 bits in length. The length of the Subnet ID is given by the length of the Global Routing Prefix.

The Interface ID identifies an interface of a particular node. The term Interface ID is used because one host can have multiple interfaces, each having one or more IPv6 addresses.

The general format for IPv6 Global Unicast addresses is represented in the figure below.

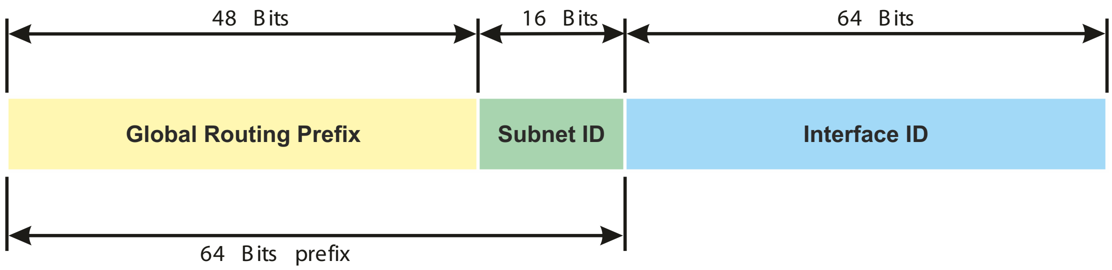


Figure 16: IPv6 Global Unicast address general format

2.2 Specifying the IP parameters using the Command Line Interface

2.2.1 IPv4

There are the following methods you enter the IP parameters:
- BOOTP/DHCP
- Ethernet Switch Configurator protocol
- External memory
- Command Line Interface using the serial connection

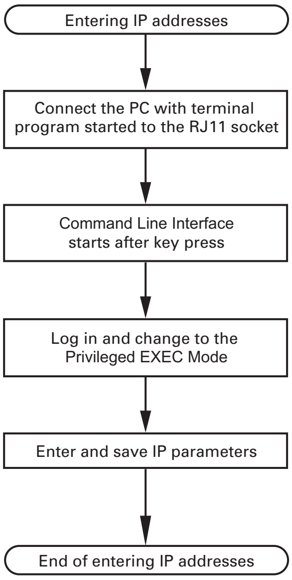
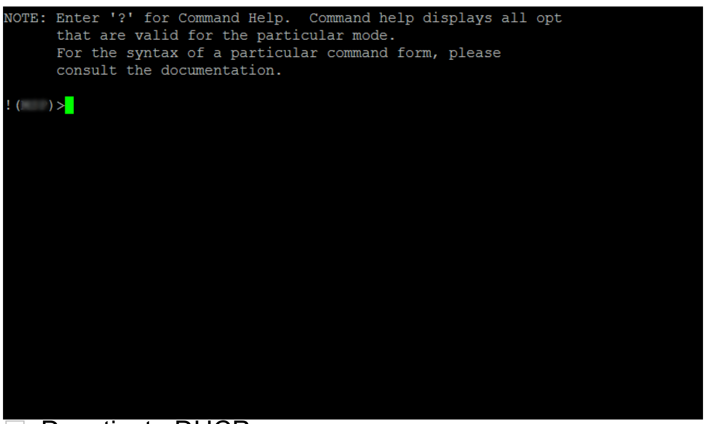


Figure 17: Flow chart for entering IP addresses

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 divided 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 45 “Example of how the netmask is used”).
    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 current settings in the non-volatile memory (`nvm`) in the “selected” configuration profile.

After entering the IP parameters, you easily configure the device using the Graphical User Interface.

2.2.2 IPv6

The device lets you specify the IPv6 parameters using the Command Line Interface over the serial interface. Another option to access the Command Line Interface is using a SSH connection with the use of the IPv4 management address.

Perform the following steps:
- Set up a connection to the device.
  The start screen appears.

- Enable the IPv6 protocol if the protocol is disabled.
- Enter the IPv6 parameters.
  - IPv6 address
    Valid IPv6 address. The IPv6 address is displayed in a compressed format.
  - Prefix length
    Unlike an IPv4 address, the IPv6 address does not use a subnet mask to identify the network part of an address. This role is performed in IPv6 by the prefix length (see on page 49 “Prefix length”).
  - *EUI option* function
    You can use the *EUI option* function to automatically configure the Interface ID of the IPv6 address. The device uses the MAC address of its interface with the values `ff` and `fe` added between byte 3 and byte 4 to generate a 64-bit Interface ID.
    You can only select this option for IPv6 addresses that have a prefix length equal to `64`.
  - IPv6 Gateway address
    The IPv6 Gateway address is the address of a router through which the device accesses other devices outside its own network.
    You can specify any IPv6 address except loopback and *Multicast* addresses.
    In the default setting, the IPv6 Gateway address is `::`.

`enable`	Change to the Privileged EXEC mode.
`network ipv6 operation`	Enable the IPv6 protocol if the protocol is disabled. In the default setting, the IPv6 protocol is enabled.
`network ipv6 address add 2001::1 64 eui-64`	Assign the IPv6 address `2001::1` and the prefix length `64`. The `eui-64` parameter is optional. You have the option of also assigning a Gateway address.
`copy config running-config nvm`	Save the current settings in the non-volatile memory (`nvm`) in the “selected” configuration profile.

After entering the IPv6 parameters, you easily configure the device using the Graphical User Interface. To use an IPv6 address in a URL, use the following URL syntax: `https://[<ipv6_address>]`.

2.3 Specifying the IP parameters using Ethernet Switch Configurator

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

You easily configure other parameters using the Graphical User Interface.

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, Ethernet Switch Configurator automatically searches the network for those devices which 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, you can select the one you desire 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 enables 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 have assigned the IP parameters to the device.

Note: Save the settings so that you will still have the entries after a restart.

2.4 Specifying the IP parameters using the Graphical User Interface

2.4.1 IPv4

Perform the following steps:

- Open the *Basic Settings > Network > Global* dialog.

In this dialog you specify the VLAN in which the device management can be accessed and configure the Ethernet Switch Configurator access.

- In the *VLAN ID* column you specify the VLAN in which the device management can be accessed over the network.

Note here that 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 you specify the settings for accessing 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.
- Open the *Basic Settings > Network > IPv4* dialog.

In this dialog you specify the source from which the device gets its IP parameters after starting.

- In the *Management interface* frame you first specify where the device gets its IP parameters from:
  - In the `BOOTP` mode, the configuration is using a BOOTP or DHCP server on the basis of the MAC address of the device.
  - In the `DHCP` mode, the configuration is using 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, you enter the IP address, the netmask and the Gateway in the *IP parameter* frame.
- Save the changes temporarily. To do this, click the ✓ button.

2.4.2 IPv6

Perform the following steps:

- Open the *Basic Settings > Network > IPv6* dialog.
- The IPv6 protocol is enabled by default. Verify if the `On` radio button is selected in the *Operation* frame.
- In the *Configuration* frame you specify where the device gets its IPv6 parameters from:
- If the *None* radio button is selected, then the device receives its IPv6 parameters manually. You can manually specify a maximum number of 4 IPv6 addresses. You cannot specify loopback, link-local, and *Multicast* addresses as static IPv6 addresses.
- If the *Auto* radio button is selected, then the device receives its IPv6 parameters dynamically for example, with the use of a Router Advertisement Daemon (radvd). The device receives a maximum of 2 IPv6 addresses.
- If the *DHCPv6* radio button is selected, then the device receives its IPv6 parameters from a DHCPv6 server.
  The device can receive only one IPv6 address from the DHCPv6 server.
- If the *All* radio button is selected, then the device receives its IPv6 parameters using every alternative for both dynamic and manual assignments.

Note: When you change the allocation mode of the IPv6 address, the device activates the new mode immediately after you click the ✓ button.

- If necessary, you enter the *Gateway address* in the *IP parameter* frame.

Note: If the *Auto* radio button is selected and you use a Router Advertisement Daemon (radvd), then the device automatically receives a link-local type *Gateway address* with a higher metric than the manually set *Gateway address*.

- In the *Duplicate Address Detection* frame you can specify the number of consecutive *Neighbor Solicitation* messages that the device sends for the *Duplicate Address Detection* function (see on page 63 “Duplicate Address Detection”).

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

Manually specify an IPv6 address. To do this, perform the following steps:

- Open the *Basic Settings > Network > IPv6* dialog.
- Click the button.
  The dialog displays the *Create* window.
- Enter the IPv6 address in the *IP address* field.
- Enter the IPv6 address prefix length in the *PrefixLength* field.
- Click the *Ok* button.
  The device adds a new table entry.

2.5 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 > IPv4* 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.

2.6 Specifying the IP parameters using DHCP

2.6.1 IPv4

The DHCP (Dynamic Host Configuration Protocol) is a further development of BOOTP, which it has replaced. The DHCP additionally lets the configuration of a DHCP client using 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 Graphical User Interface (see dialog *Basic Settings > System*), the Command Line Interface 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 Sever assigns the IP address, the device permanently saves the configuration data in non-volatile memory.

Table 12: DHCP options which the device requests

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 this 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 > IPv4* dialog lets you activate or deactivate DHCP.

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

The appendix contains an example configuration 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 further information, please refer to the DHCP server manual.

2.6.2 IPv6

The Dynamic Host Configuration Protocol version 6 (DHCPv6) is a network protocol that is used to dynamically specify IPv6 addresses. This protocol is the IPv6 equivalent of the DHCP protocol for IPv4. DHCPv6 protocol is described in RFC 8415.

The device uses a DHCP Unique Identifier (DUID) to send a request to the DHCPv6 server. In the device, the DUID represents the *Client ID* that the DHCPv6 server uses to identify the device that requested an IPv6 address.

The *Client ID* is displayed in the *Basic Settings > Network > IPv6* dialog, in the *DHCP* frame.

The device can receive only one IPv6 address from the DHCPv6 server, with a *PrefixLength* of `128`. No *Gateway address* information is provided. If needed, you can manually specify *Gateway address* information.

In the default setting, DHCPv6 protocol is deactivated. You can activate or deactivate the protocol in the *Basic Settings > Network > IPv6* dialog. Verify that the *DHCPv6* radio button is selected in the *Configuration* frame.

If you want to dynamically get an IPv6 address with a *PrefixLength* other than `128`, then select the *Auto* radio button. An example here is the use of a Router Advertisement Daemon (radvd). The radvd uses *Router Solicitation* and *Router Advertisement* messages to automatically configure an IPv6 address.

In the default setting, the *Auto* radio button is selected. You can select or deselect the *Auto* radio button in the *Basic Settings > Network > IPv6* dialog, in the *Configuration* frame.

If the *All* radio button is selected, then the device receives its IPv6 parameters using every alternative for both dynamic and manual assignments.

2.7 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 checks 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*: `marked`
- *Detection delay [ms]*: `200`
- *Release delay [s]*: `15`
- *Address protections*: `3`
- *Protection interval [ms]*: `200`
- *Send trap*: `marked`

2.7.1 Active and passive detection

Actively checking 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 checks if its IP address exists within the network. To check the network for address conflicts, the device sends 4 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 check after the configured release delay time.

When you disable active detection, the device sends 2 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, if the remote device remains connected to the network, then 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. This has the following advantages:
- ARP caches on other devices remain unchanged
- the method is robust through multiple ARP probe transmissions

2.8 Duplicate Address Detection

The *Duplicate Address Detection* function determines the uniqueness of an IPv6 unicast address on an interface. The function is performed when an IPv6 address is configured using manual, *DHCPv6*, or *Auto* methods. The function is also triggered by a change in a link status for example, a link status change from down to up.

The *Duplicate Address Detection* function uses *Neighbor Solicitation* and *Neighbor Advertisement* messages. You have the option to set the number of consecutive *Neighbor Solicitation* messages that the device sends. To do this, perform the following steps:

- Open the *Basic Settings > Network > IPv6* dialog.
- In the *Duplicate Address Detection* frame set the necessary value in the *Number of neighbor solicitants* field.
  Possible values:
  - `0`
    The function is disabled.
  - `1..5` (default setting: `1`)
- Save the changes temporarily. To do this, click the ✓ button.

`enable`	Change to the Privileged EXEC mode.
`network ipv6 dad-transmits <0..5>`	Set the number of *Neighbor Solicitation* messages that the device sends. The value `0` disables the function.

Note: If the *Duplicate Address Detection* function discovers that an IPv6 address is not unique on a link, then the device does not log this event in the log file (System Log).

3 Access to the device

3.1 Access roles

The device functions available to you as a user 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 Command Line Interface mode in which you are currently working. See “Mode-based command hierarchy” on page 25.

The device offers the following access roles:

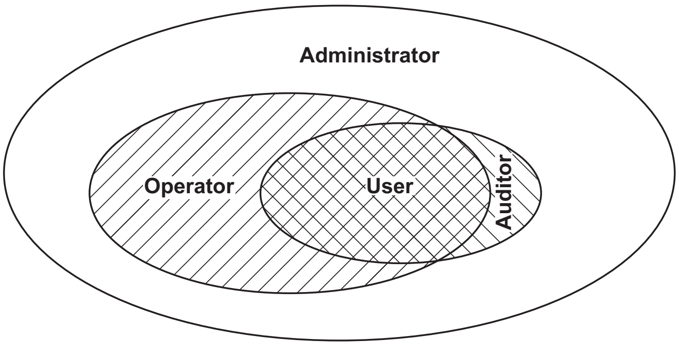


Table 13: Access roles and scope of user authorizations

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 – with the exception of 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, then the device assigns this access role to the user account.

3.2 First login (Password change)

To help prevent undesired access to the device, it is imperative that you change the default password during initial setup.

Perform the following steps:
- Open the Graphical User Interface, the SE View application, or the Command Line Interface the first time you log in.
- Log in with the default password.
  The device prompts you to type in a new password.
- Type in your new password.
  To help increase security, choose a password that contains at least 8 characters which includes upper-case characters, lower-case characters, numerical digits, and special characters.
- When you log in with the Command Line Interface, the device prompts you to confirm your new password.
- Log in again with your new password.

Note: If you lost your password, then contact your local support team.

3.3 Authentication lists

When a user accesses the device using a specific connection, the device verifies the login credentials of the user in an authentication list which contains the policies that the device applies for authentication.

The prerequisite for a user's 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.

3.3.1 Applications

The device provides an application for each type of connection through which someone accesses the device:
- Access to the Command Line Interface using a serial connection: `Console(V.24)`
- Access to the Command Line Interface using SSH: `SSH`
- Access to the Command Line Interface using Telnet: `Telnet`
- Access to the Graphical User Interface: `WebInterface`

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

3.3.2 Policies

When a user logs in with valid login data, the device lets the user have access to its device management. The device authenticates the users using the following policies:
- User management of the device
- LDAP
- 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
- IAS (Integrated Authentication Server)

The device gives you the option of a fall-back solution. For this, you specify more than one policy in the authentication list. When authentication is unsuccessful using the current policy, the device applies the next specified policy.

3.3.3 Managing authentication lists

You manage the authentication lists in the Graphical User Interface or in the Command Line Interface. 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 those applications by means of which no access to the device is performed, for example `8021x`.

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

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

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

3.3.4 Adjust the settings

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

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

☐ Create an authentication list `loginGUI`.

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

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

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

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

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

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

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

☐ In the *Active* column, mark the checkbox.

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

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

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

- In the *Device Security > Authentication List* dialog, highlight the authentication list `loginGUI`.
- Click the ☰ button and then the *Allocate applications* item.
  The dialog displays the *Allocate applications* window.
- In the left column, highlight the application `WebInterface`.
- Click the ➔ button.
  The right column now displays the application `WebInterface`.
- Click the *Ok* button.
  The dialog displays the updated settings:
  – The *Dedicated applications* column of authentication list `loginGUI` displays the application `WebInterface`.
  – The *Dedicated applications* column of authentication list `defaultLoginAuthList` does not display the application `WebInterface` anymore.
- Save the changes temporarily. To do this, click the ✓ button.

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

3.4 User management

When a user logs in with valid login data, the device lets the user have access to its device management. The device authenticates the users either using the local user management or with 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, you manage the user accounts. One user account is usually allocated to each user.

3.4.1 Access roles

The device lets you use a role-based authorization model to specifically control the access to the device management. Users to whom a specific authorization profile is allocated are allowed to use commands and functions from 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, you assign a pre-defined access role to the user. The device differentiates between the following access roles.

Table 14: Access roles for user accounts

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 every password ▶ Configure password management ▶ Set or change system time ▶ Load files to the device, for example device configurations, certificates or software images ▶ Reset settings and security-related settings to the state on delivery ▶ Configure RADIUS server and authentication lists ▶ Apply scripts using the Command Line Interface ▶ Enable/disable CLI logging and SNMP logging ▶ External memory activation and deactivation ▶ System monitor activation and deactivation ▶ Enable/disable the services for the access to the device management (for example SNMP). ▶ Configure access restrictions to the Graphical User Interface or the Command Line Interface based on the IP addresses
Operator	The user is authorized to monitor and configure the device - with the exception of security-related settings.	All activities with read/write access, with the exception of the above-named activities, which are reserved for an administrator:
Auditor	The user is authorized to monitor the device and to save the log file in the *Diagnostics > Report > Audit Trail* dialog.	Monitoring activities with read access.
Guest	The user is authorized to monitor the device - with the exception of security-related settings.	Monitoring 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, then the device assigns this access role to the user account.	No activities allowed.

3.4.2 Managing user accounts

You manage the user accounts in the Graphical User Interface or in the Command Line Interface. To do this, perform the following steps:

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

The dialog displays the user accounts that are set up.

`show users`	Displays the user accounts that are set up.

3.4.3 Default setting

In the state on delivery, the user accounts `admin` and `user` are set up in the device.

Table 15: Default settings for the factory setting user accounts

Parameter	Default setting	
User name	`admin`	`user`
Password	`private`	`public`
Role	`administrator`	`guest`
User locked	`unmarked`	`unmarked`
Policy check	`unmarked`	`unmarked`
SNMP auth type	`hmacmd5`	`hmacmd5`
SNMP encryption type	`des`	`des`

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

3.4.4 Changing default passwords

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

- Change the passwords for the `admin` and `user` user accounts.

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

The dialog displays the user accounts that are set up.

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

Note: The password check can lead to a message in the *Security status* frame in the *Basic Settings > System* dialog. You specify the settings that cause this message in the *Basic Settings > System* dialog.

- ☐ Click the row of the relevant user account in the *Password* field. Enter a password of at least 6 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 checks 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`	Activates the checking of the password for the `<user>` user account based on the specified policy. In this way, you obtain a higher level of complexity for the password.

Note: When you display the security status, the password check can lead to a message (`show security-status all`). You specify the settings that cause this message with the command `security-status monitor pwd-policy-inactive`.

`users password <user> SECRET`	Specifies the password `SECRET` for the`<user>` user account. Enter at least 6 characters.
`save`	Save the settings in the non-volatile memory (`nvm`) in the “selected” configuration profile.

3.4.5 Setting up a new user account

Allocate a separate user account to each user that accesses the device management. In this way you can specifically control the authorizations for the access.

In the following example, we will set up the user account for a `USER` user with the role `operator`. Users with the `operator` role are authorized to monitor and configure the device - with the exception of 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 give the user account the name `USER`.
- ☐ Click the *Ok* button.
- ☐ To obtain a higher level of complexity for the password, mark the checkbox in the *Policy check* column.
  Before saving it, the device checks the password according to the policy specified in the *Password policy* frame.

- In the *Password* field, enter a password of at least 6 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 checks the minimum length of the password.
- In the *Role* column, select the user role.
  In this example, we select the value `operator`.
- To activate the user account, mark the checkbox in the *Active* column.
- Save the changes temporarily. To do this, click the ✓ button.
  The dialog displays the user accounts that are set up.

`enable`	Change to the Privileged EXEC mode.
`configure`	Change to the Configuration mode.
`users add USER`	Creates the `USER` user account.
`users password-policy-check USER enable`	Activates the checking of the password for the `USER` user account based on the specified policy. In this way, you obtain a higher level of complexity for the password.
`users password USER SECRET`	Specifies the password `SECRET` for the user account `USER`. Enter at least 6 characters.
`users access-role USER operator`	Assign the user role `operator` to the user account `USER`.
`users enable USER`	Activates the user account `USER`.
`show users`	Displays the user accounts that are set up.
`save`	Save the settings in the non-volatile memory (`nvm`) in the “selected” configuration profile.

Note: When you are setting up a new user account in the Command Line Interface, remember to allocate the password.

3.4.6 Deactivating the user account

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

- Open the *Device Security > User Management* dialog.
  The dialog displays the user accounts that are set up.
- In the row for the relevant user account, unmark 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>	To disable user account.
show users	Displays the user accounts that are set up.
save	Save the settings in the non-volatile memory (nvm) in the “selected” configuration profile.

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

☐ Highlight the row for the relevant user account.

☐ Click the button.

users delete <user>	Deletes the user account <user>.
show users	Displays the user accounts that are set up.
save	Save the settings in the non-volatile memory (nvm) in the “selected” configuration profile.

3.4.7 Adjusting policies for passwords

The device lets you check if the passwords for the user accounts adhere to the specified policy. When the passwords adhere to the policy, you obtain a higher level of complexity for the passwords.

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

In the default settings, practical values for the policy are set up in the device. You have the option of adjusting 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 user login attempts before the device locks out the user. You also specify the minimum number of characters that defines a password.

Note: The device lets only users with the `administrator` authorization remove the lock.

The number of login attempts as well as the possible lockout of the user apply only when accessing the device management through:
- the Graphical User Interface
- the SSH protocol
- the Telnet protocol

Note: When accessing the device management using the Command Line Interface through the 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 attempts to log in.
    The field lets you define this value in the range `0..5`.
    In the above example, 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 set up 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, mark 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 policies that are set up.
`save`	Save the settings in the non-volatile memory (`nvm`) in the “selected” configuration profile.

3.5 LDAP

Server administrators manage Active Directorys which contain user login credentials for applications used in the office environment. The Active Directory is hierarchical in nature, containing user names, passwords, and the authorized read/write permission levels for each user.

This device uses the Lightweight Directory Access Protocol (LDAP) to retrieve user login information and permission levels from a Active Directory. This provides a “single sign on“ for network devices. Retrieving the login credentials from an Active Directory lets the user log in with the same login credentials used in the office environment.

An LDAP session starts with the device contacting the Directory System Agent (DSA) to search the Active Directory of an LDAP server. If the server finds multiple entries in the Active Directory for a user, then the server sends the higher permission level found. The DSA listens for information requests and sends responses on TCP port `389` for LDAP, or on TCP port `636` for LDAP over SSL (LDAPS). Clients and servers encode LDAPS requests and responses using the Basic Encoding Rules (BER). The device opens a new connection for every request and closes the connection after receiving a response from the server.

The device lets you upload a CA certificate to validate the server for Secure Socket Level (SSL) and Transport Layer Security (TLS) sessions. Whereby, the certificate is optional for TLS sessions.

The device is able to cache login credentials for up to 1024 users in memory. If the active directory servers are unreachable, then the users are still able to log in using their office login credentials.

3.5.1 Coordination with the server administrator

Configuring the *LDAP* function requires that the network administrator request the following information from the server administrator:
- The server name or IP address
- The location of the Active Directory on the server
- The type of connection used
- The TCP listening port
- When required, the location of the CA certificate
- The name of the attribute containing the user login name
- The names of the attribute containing the user permission levels

The server administrator can assign permission levels individually using an attribute such as `description`, or to a group using the `memberOf` attribute. In the *Device Security > LDAP > Role Mapping* dialog you specify which attributes receive the various permission levels.

You also have the option to retrieve the name of the attributes containing the user login name and permission levels using a LDAP browser such as JXplorer or Softerra.

3.5.2 Example configuration

The device is able to establish an encrypted link to a local server using only the server name or to a server on a different network using an IP address. The server administrator uses attributes to identify login credentials of a user and assign individual and group permission levels.

Using information received from the server administrator, specify which attributes in the Active Directory contain the user login credentials and permission level. The device then compares the user login credentials with the permission levels specified in the device and lets the user log in at the assigned permission level.

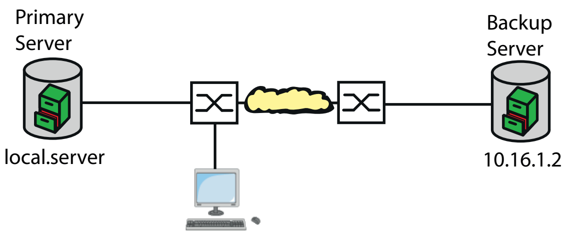


Figure 18: LDAP Example Configuration

For this example, the server administrator sent the following information:

Information	Primary Server	Backup Server
The server name or IP address	`local.server`	`10.16.1.2`
The location of the Active Directory on the server	`Country/City/User`	`Country/Company/User`
The type of connection used	`TLS` (with certificate)	`SSL`
The server administrator sent the CA certificate in an email.	CA certificate for primary server saved locally	CA certificate for backup server saved locally
The TCP listening port	`389 (tls)`	`636 (ssl)`
Name of the attribute containing the user name	`userPrincipalName`	`userPrincipalName`
The names of the attribute containing the user permission levels	`OPERATOR` `ADMINISTRATOR`	`OPERATOR` `ADMINISTRATOR`

Perform the following steps:

- ☐ Open the *Device Security > Authentication List* dialog.
- ☐ To configure the device to retrieve the user login credentials, during login using the Graphical User Interface, from the Active Directory first, specify for the `defaultLoginAuthList` list the value `ldap` in the*Policy 1* column.
- ☐ Open the *Device Security > LDAP > Configuration* dialog.
- ☐ The device lets you specify the length of time that it saves the user login credentials in the cache. To cache user login credentials for a day, in the *Configuration* frame, *Client cache timeout [min]* field, enter the value `1440`.
- ☐ The *Bind user* entry is optional. When specified, users enter only their user name to log in. The service user can be anyone with login credentials listed in the Active Directory under the attribute specified in the *User name attribute* column. In the *Bind user* column, enter the user name and the domain.

- The *Base DN* is a combination of the domain component (dc) and the organizational unit (ou). The *Base DN* lets the device locate a server in a domain (dc) and find the Active Directory (ou). Specify the location of the Active Directory. In the *Base DN* column, specify the value `ou=Users,ou=City,ou=Country,dc=server,dc=local`.
- In the *User name attribute* column, enter the value `userPrincipalName` to specify the attribute under which the server administrator lists the users.

The device uses a CA certificate to verify the server.

- 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.
- To transfer the CA certificate onto the device, click the *Start* button.
- To add a table entry, click the button.
- To specify a description, enter the value `Primary AD Server` in the *Description* column.
- To specify the server name and domain of the primary server, in the *Address* column, enter the value `local.server`.
- The primary server uses the TCP port `389` for communication which is the *Destination TCP port* default value.
- The primary server uses TLS for encrypting communication and a CA certificate for server validation. In the *Connection security* column, specify the value `startTLS`.
- To activate the entry, mark the checkbox in the *Active* column.
- Using the information received from the server administrator for the Backup server, add, configure and activate another row.

- Open the *Device Security > LDAP > Role Mapping* dialog.
- To add a table entry, click the button.

When a user logs in, with LDAP configured and enabled, the device searches the Active Directory for the login credentials of the user. If the device finds the user name and the password is correct, then the device searches for the value specified in the *Type* column. If the device finds the attribute and the text in the *Parameter* column matches the text in the Active Directory, then the device lets the user log in with the assigned permission level. When the value `attribute` is specified in the *Type* column, specify the value in the *Parameter* column in the following form: `attributeName=attributeValue`.

- In the *Role* column, enter the value `operator` to specify the user role.
- To activate the entry, mark the checkbox in the *Active* column.
- Click the button.
  The dialog displays the *Create* window.
  Enter the values received from the server administrator for the `administrator` role.
  To activate the entry, mark the checkbox in the *Active* column.
- Open the *Device Security > LDAP > Configuration* dialog.
- To enable the function, select the `On` radio button in the *Operation* frame.

The following table describes how to configure the *LDAP* function in the device using the Command Line Interface. The table displays the commands for `Index 1`. To configure `Index 2`, use the same commands and substitute the appropriate information.

`enable`	Change to the Privileged EXEC mode.
`configure`	Change to the Configuration mode.
`ldap cache-timeout 1440`	Specify the device to flush the non-volatile memory after a day.

`ldap client server add 1 local.server port 389`	Add a connection to the remote authentication client server with the host name `local.server` and the UDP port `389`.
`ldap client server modify 1 security startTLS`	Specify the type of security used for the connection.
`ldap client server modify 1 description Primary_AD_Server`	Specify the configuration name of the entry.
`ldap basedn ou=Users,ou=City,ou=Country,dc=server, dc=local`	Specify the Base Domain Name used to find the Active Directory on the server.
`ldap search-attr userPrincipalName`	Specify the attribute to search for in the Active Directory which contains the login credential of the users.
`ldap bind-user user@company.com`	Specify the name and domain of the service user.
`ldap bind-passwd Ur-123456`	Specify the password of the service user.
`ldap client server enable 1`	Enable the remote authentication client server connection.
`ldap mapping add 1 access-role operator mapping-type attribute mapping-parameter OPERATOR`	Add a remote authentication role mapping entry for the `Operator` role. Map the `operator` role to the attribute containing the word `OPERATOR`.
`ldap mapping enable 1`	Enable the remote authentication role mapping entry.
`ldap operation`	Enable the remote authentication function.

3.6 SNMP access

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

3.6.1 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.

Make undesired access to the device more difficult. To do this, 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.
- ☐ We recommend using SNMPv3 and disabling the access using SNMPv1 and SNMPv2 in the device.

3.6.2 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 Graphical User Interface, in the Command Line Interface, 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 user accounts that are set up.

- 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.

3.7 Out of Band access

The device comes with a separate port that lets you access the device management out-of-band. When there is a high in-band load on the switching ports, you can still use this separate port to access the device management.

The prerequisite is that you connect the management station directly to the USB port. When you use Microsoft Windows, install the RNDIS driver, where necessary. Once you connect the management station, it can communicate with the device management over a virtual network connection.

In the default setting, you can access the device management through this port using the following IP parameters:
- *IP address* `91.0.0.100`
- *Netmask* `255.255.255.0`

The device lets you access the device management using the following protocols:
- SNMP
- Telnet
- SSH
- HTTP
- HTTPS
- FTP
- SCP
- TFTP
- SFTP

3.7.1 Specifying the IP parameters

When you connect the management station through the USB port, the device assigns the IP address of the USB network interface, increased by 1, to the management station (`91.0.0.101` in the default setting). The device lets you change the IP parameters to adapt the device to the requirements of your environment.

Verify that the IP subnet of this network interface is not overlapping with any subnet connected to another interface of the device:
- Management interface

If the management station accesses the device management through the USB port, then the device disconnects the Graphical User Interface and Command Line Interface immediately after you have performed the changes.

Perform the following steps:

- ☐ Open the *Basic Settings > Out of Band over USB* dialog.
- ☐ Overwrite the IP address in the *IP parameter* frame, *IP address* field.
- ☐ Save the changes temporarily. To do this, click the ✓ button.

`enable`	Change to the Privileged EXEC mode.
`network usb parms 192.168.1.1 255.255.255.0`	Specify the IP address `192.168.1.1` and the netmask `255.255.255.0` for the USB network interface.
`show network usb`	Display the USB network interface settings.

```
Out-of-band USB management settings
-----------------------------------
Management operation........................enabled
IP address..................................192.168.1.1
Subnet mask.................................255.255.255.0
Host MAC address............................64:60:38:1f:85:85
Device MAC address..........................64:60:38:1f:85:86
```

`save`	Save the settings in the non-volatile memory (`nvm`) in the “selected” configuration profile.

3.7.2 Disable the USB network interface

In the default setting, the USB network interface is enabled. If you don’t want someone to access device management through the USB port, then the device lets you disable the USB network interface.

If the management station accesses the device management through the USB port, then the device disconnects the Graphical User Interface and Command Line Interface immediately after you have performed the changes.

Perform the following steps:

- ☐ Open the *Basic Settings > Out of Band over USB* dialog.
- ☐ To disable the USB network interface, 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.
`no network usb operation`	Disable the USB network interface.

```
Out-of-band USB management settings
-----------------------------------
Management operation........................disabled
IP address..................................192.168.1.1
Subnet mask.................................255.255.255.0
Host MAC address............................64:60:38:1f:85:85
Device MAC address..........................64:60:38:1f:85:86
```

`save`	Save the settings in the non-volatile memory (`nvm`) in the “selected” configuration profile.

4 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 simple 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.

4.1 Basic settings

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

4.1.1 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 current time from a PTP clock or from an SNTP server.

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

Perform the following steps:

- Open the *Time > Basic Settings* dialog.
- The *System time (UTC)* field displays the current 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.

4.1.2 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.

4.2 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.

In an IPv6 environment, the *Broadcast* operation mode operates as follows:
- The SNTP client listens only for SNTP server messages that have the IPv6 *Multicast* address set to `ff05::101` as the IPv6 destination address.
- The SNTP server sends only SNTP messages to the *Multicast* address `ff05::101`. The SNTP server does not send SNTP messages with the link-local address as the IPv6 source address.

Table 16: Target IPv4 address classes for Broadcast operation mode

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.

4.2.1 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.

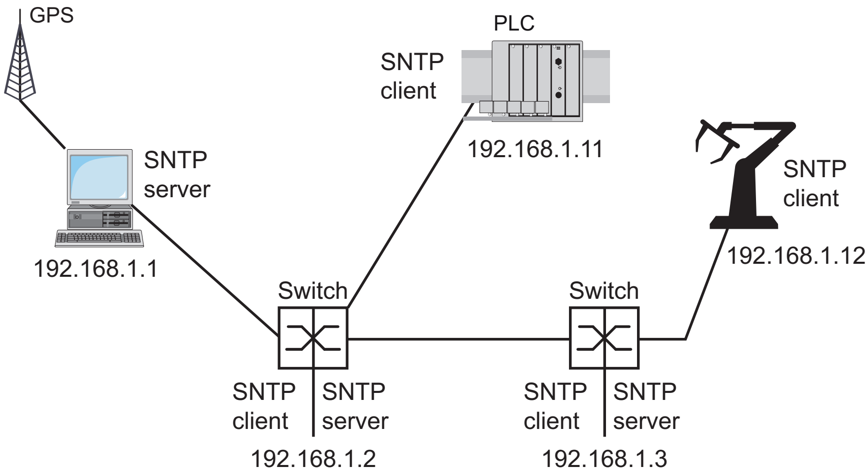


Figure 19: Example of SNTP cascade

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.

4.2.2 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, mark 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 current status of the *SNTP Client* function.

Table 17: SNTP client settings for the example

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`	`192.168.1.2`
			`192.168.1.1`
				`192.168.1.2`
				`192.168.1.1`
					`192.168.1.3`
					`192.168.1.2`
					`192.168.1.1`

4.2.3 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 an IPv6 environment, you cannot set the IPv6 address to which the SNTP server sends the SNTP packets. The SNTP server uses the *Multicast* address `ff05::101` as the IPv6 destination 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.

Note: Except for the *Broadcast destination address* field, the remaining settings are applicable for both IPv4 and IPv6 SNTP servers.

- Save the changes temporarily. To do this, click the ✓ button.
- ▶ The *State* field displays the current status of the *SNTP Server* function.

Table 18: Settings for the example

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	`unmarked`	`unmarked`	`unmarked`	`unmarked`	`unmarked`
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`
Broadcast VLAN ID	`1`	`1`	`1`	`1`	`1`
Broadcast send interval [s]	`128`	`128`	`128`	`128`	`128`
Disable server at local time source	`unmarked`	`unmarked`	`unmarked`	`unmarked`	`unmarked`

4.3 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.

4.3.1 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).

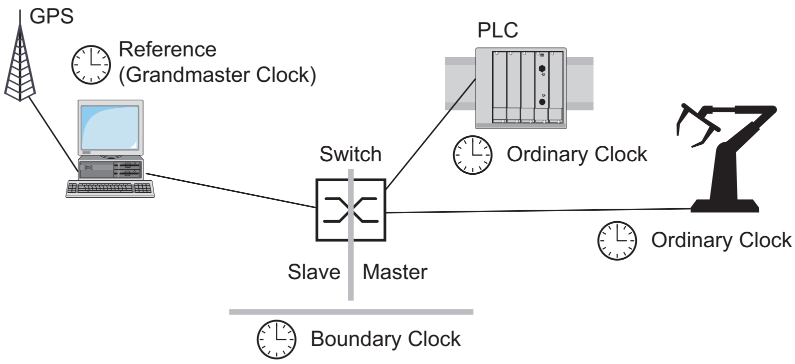


Figure 20: Position of the boundary clock in a network

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.

4.3.2 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 decides 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.

4.3.3 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 knows no master clock, 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 know the delay in the other direction.

4.3.4 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.

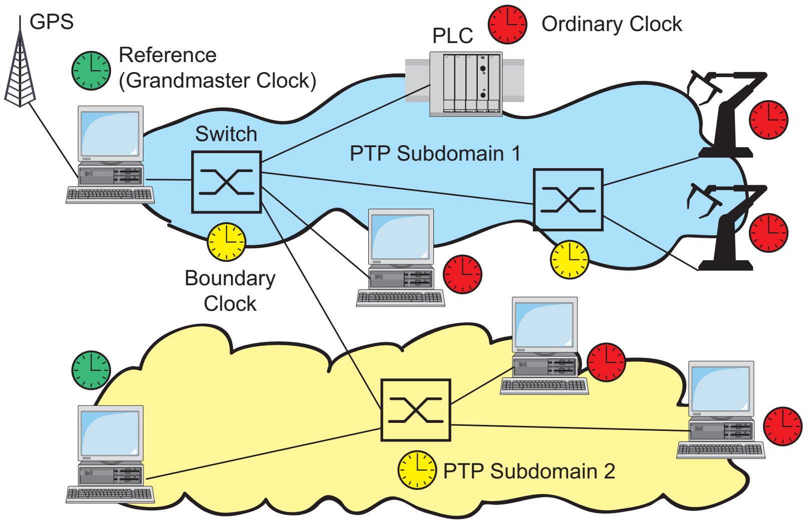


Figure 21: Example of PTP domains

4.3.5 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*.

Table 19: Possible settings for 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*.

5 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 quickly 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.

5.1 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.

5.1.1 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:

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

Or:

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

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

5.1.2 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.
- ☐ Check the status of the checkbox in the *Information* frame:
  - When the checkbox is unmarked, the configuration profiles differ.
  - When the checkbox is marked, the configuration profiles match.

```
show config status

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

5.2 Saving the settings

5.2.1 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 marked.
- ☐ 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 designated as “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 current 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 designated as “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 marked.

- ☐ 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 `marked`.

`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.

5.2.2 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.
- ☐ Mark 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, unmark 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.

5.2.3 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).

5.2.4 Exporting a configuration profile

The device lets you save a configuration profile to a server as an XML file. If you use the Graphical User Interface, 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 for accessing 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 current 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.

5.3 Loading settings

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

5.3.1 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 Graphical User Interface. The device immediately uses the settings of the configuration profile.

- ☐ Reload the Graphical User Interface.
- ☐ Log in again.

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

`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 Command Line Interface. The device immediately uses the settings of the configuration profile `config3`.

5.3.2 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 Command Line Interface, 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).

5.3.3 Importing a configuration profile

The device lets you import from a server a configuration profile saved as an XML file. If you use the Graphical User Interface, 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 for accessing 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 Graphical User Interface 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 Graphical User Interface 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 Command Line Interface. 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 Command Line Interface. 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 Command Line Interface. 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`).

5.4 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.

5.4.1 Using the Graphical User Interface or Command Line Interface

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.

5.4.2 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.

6 Loading software updates

Schneider Electric is continually working on improving and developing their software. Check regularly if there is an updated version of the software that provides you with additional benefits. You find information and software downloads on the Schneider Electric product pages on the Internet at www.schneider-electric.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 see the version of the installed device software in the login dialog of the Graphical User Interface.

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 currently 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 currently running.

6.1 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.

6.2 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 currently 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.

6.3 Software update from the external memory

6.3.1 Manually—initiated by the administrator

The device lets you update the device software with a few mouse clicks. 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 currently 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.

6.3.2 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 mark 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 checks 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 currently running in the device?
  When the criteria are fulfilled, the device starts the update procedure.
  The device copies the currently 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.
- ☐ Check 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 wrong image file
  – `S_watson_AUTOMATIC_SWUPDATE_ABORTED_SAVING_FILE`
    Software update aborted because the device did not save the image file.

6.4 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.

7 Configuring the ports

The following port configuration functions are available.
- Enabling/disabling the port
- Selecting the operating mode
- Gigabit Ethernet mode for ports

7.1 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, mark the checkbox in the *Port on* column.
- [ ] To disable a port, unmark 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.

7.2 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. Unmark 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

7.3 Gigabit Ethernet mode for ports

The device supports 2.5 Gbit/s on several interfaces with one of the following SFP transceivers:
- M-SFP-2.5-MM/LC EEC
- M-SFP-2.5-SM-/LC EEC
- M-SFP-2.5-SM/LC EEC
- M-SFP-2.5-SM+/LC EEC

The type of the transceiver plugged into the slot determines the port speed. The device has no option to set the speed manually. Ports with 2.5 Gbit/s port speed are unable to support data rates of 100 Mbit/s.

Note: You find more information about the transceiver order numbers in the “Accessories” chapter of the “Installation” user manual.

7.3.1 Example

You use the Gigabit Ethernet mode to get a higher bandwidth for uplinks. To use this function, insert an applicable transceiver type in the appropriate slot.

Perform the following steps:

- [ ] Open the *Basic Settings > Port* dialog, *Configuration* tab.

The column *Manual configuration* displays the value `2.5 Gbit/s FDX` for the ports that have a 2.5 Gbit/s SFP transceiver inserted.

You cannot change the speed.

```
show port 1/1
```

Displays the parameters for slot `1` port `1`. The `Physical Mode` list entry displays the value `2500 full` for the ports that have a 2.5 Gbit/s SFP transceiver inserted.

```
Interface....................1/1
Name.........................My interface
--
Cable-crossing Setting........-
Physical Mode................2500 full
Physical Status...............-
```

8 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

8.1 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.

8.2 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. We recommend using SNMPv3 in the device and disabling 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 unmark the *SNMPv1* checkbox.
- To deactivate the SNMPv2 protocol, you unmark 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.

8.3 Disabling HTTP

The web server provides the Graphical User Interface 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 Graphical User Interface 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 Graphical User Interface 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 Graphical User Interface is unaccessible. To work with the Graphical User Interface, enable the HTTPS server using the Command Line Interface. 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.

8.4 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 Command Line Interface 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 Command Line Interface is only possible through the serial interface of the device. To work remotely with the Command Line Interface, 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.

8.5 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, we recommend to set Ethernet Switch Configurator to read-only or to 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.

8.6 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 Graphical User Interface. 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 knows the fingerprint of the RSA key.

Table 20: Parameters for the IP access restriction

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.
- ☐ Unmark 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 marked.

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 marked.

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 Command Line Interface 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.

8.7 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:
- Command Line Interface sessions using an SSH connection
- Command Line Interface sessions using a Telnet connection
- Command Line Interface sessions using a serial connection
- Graphical User Interface

Timeout for Command Line Interface 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 Command Line Interface sessions using an SSH connection.

Timeout for Command Line Interface 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 Command Line Interface sessions using a Telnet connection.

Timeout for Command Line Interface 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, *Serial interface 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 Command Line Interface sessions using a serial connection.

Session timeout for the Graphical User Interface

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 Graphical User Interface sessions

9 Controlling the data traffic

The device checks 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. 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)
- Denying access to devices based on their IP or MAC address (Access Control List)

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 what is known as a status table. Based on this status table, the device decides whether to accept, drop or reject data.

The data packets go through the filter functions of the device in the following sequence:
- DoS … if `permit` or `accept`, then progress to the next rule
- ACL … if `permit` or `accept`, then progress to the next rule

9.1 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 restrict data stream for protection against denial-of-service attacks. The activated filters check 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, mark 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:

Table 21: DoS filters for TCP packets

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.

Table 21: DoS filters for TCP packets

Filter	Action
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.

9.2 ACL

In this menu you can enter the parameters for the Access Control Lists (ACLs).

The device uses ACLs to filter data packets received on VLANs or on individual or multiple ports. In a ACL, you specify rules that the device uses to filter data packets. When such a rule applies to a packet, the device applies the actions specified in the rule to the packet. The available actions are as follows:
- allow (`permit`)
- discard (`deny`)
- redirect to a certain port (see *Redirection port* field)
- mirror (see *Mirror port* field)

The list below contains criteria that you can apply to filter the data packets:
- Source or destination address of a packet (MAC)
- Source or destination address of a data packet (IPv4)
- Source or destination port of a data packet (IPv4)

You can specify the following ACL types:
- IP ACLs for VLANs
- IP ACLs for ports
- MAC ACLs for VLANs
- MAC ACLs for ports

When you assign both an IP ACL and MAC ACL to the same interface, the device first uses the IP ACL to filter the data stream. The device applies the MAC ACL rules only after the packets are filtered through the IP ACL. The priority of an ACL is independent of the index of a rule.

Within an ACL, the device processes the rules in order. The index of the respective rule determines the order in which the device filters the data stream. When you assign an ACL to a port or VLAN, you can specify its priority with the index. The lower the number, the higher the priority. The device processes the rule with the higher priority first.

If none of the rules specified in an ACL applies to a data packet, then the implicit `deny` rule applies. As a result, the device drops the received data packets.

Keep in mind that the device directly implements the implicit `deny` rule.

Note: The number of available ACLs depends on the device. You find more information about the ACL values in the chapter “Technical Data” on page 369.

Note: You can assign a single ACL to any number of ports or VLANs.

The *ACL* menu contains the following dialogs:
- *ACL IPv4 Rule*
- *ACL MAC Rule*
- *ACL Assignment*

These dialogs provide the following options:
- To specify the rules for the various ACL types.
- To provide the rules with the required priorities.
- To assign the ACLs to ports or VLANs.

9.2.1 Creating and editing IPv4 rules

When filtering IPv4 data packets, the device lets you:
- create new groups and rules
- add new rules to existing groups
- edit an existing rule
- activate and deactivate groups and rules
- delete existing groups and rules
- change the order of existing rules

Perform the following steps:

- [ ] Open the *Network Security > ACL > IPv4 Rule* dialog.
- [ ] Click the button.
  The dialog displays the *Create* window.
- [ ] To create a group, specify a meaningful name in the *Group name* field. You can combine several rules in one group.
- [ ] To add a rule to an existing group, select the name of the group in the *Group name* field.
- [ ] In the *Index* field you specify the number for the rule within the ACL.
  This number defines the priority of the rule.
- [ ] Click the *Ok* button.
  The device adds the rule to the table.
  Group and role are active immediately.
  To deactivate group or rules, unmark the checkbox in the *Active* column.
  To remove a rule, highlight the affected table entry and click the button.
- [ ] Edit the rule parameters in the table.
  To change a value, double-click the relevant field.
- [ ] Save the changes temporarily. To do this, click the button.

Note: The device lets you use wildcards with the *Source IP address* and *Destination IP address* parameters. If you enter for example, `192.168.?.?`, then the device allows addresses that start with `192.168`.

Note: The prerequisite for changing the values in the *Source TCP/UDP port* and *Destination TCP/UDP port* column is that you specify the value `tcp` or `udp` in the *Protocol* column.

Note: The prerequisite for changing the value in the *Redirection port* and *Mirror port* column is that you specify the value `permit` in the *Action* column.

9.2.2 Creating and configuring an IP ACL using the Command Line Interface

In the following example, you configure ACLs to block communications from computers B and C, to computer A via IP (TCP, UDP, etc.).

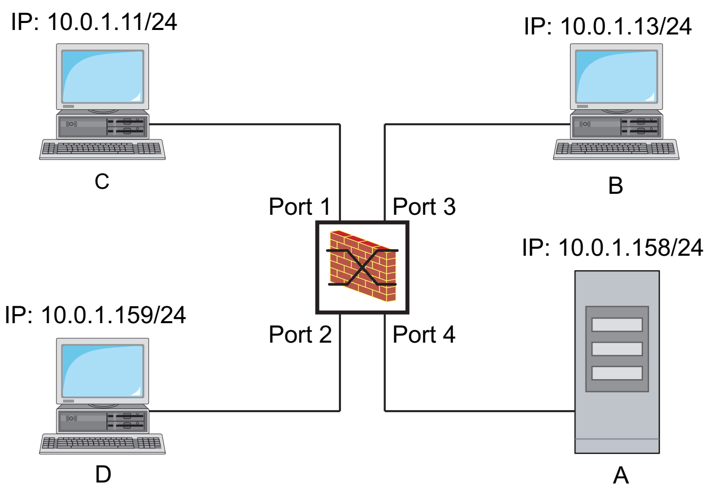


Figure 22: Example of an IP ACL

Perform the following steps:

`enable`	Change to the Privileged EXEC mode.
`configure`	Change to the Configuration mode.
`ip access-list extended name filter1 deny src 10.0.1.11-0.0.0.0 dst 10.0.1.158-0.0.0.0 assign-queue 1`	Add IP ACL with name `filter1`. Add rule denying IP data packets from `10.0.1.11` to `10.0.1.158`. Priority `1` (highest priority).
`ip access-list extended name filter1 permit src any dst any`	Add rule to the IP ACL admitting IP data packets.
`show access-list ip filter1`	Display rules of the IP ACL `filter1`.
`ip access-list extended name filter2 deny src 10.0.1.13-0.0.0.0 dst 10.0.1.158-0.0.0.0 assign-queue 1`	Add IP ACL with name `filter2`. Add rule denying IP data packets from `10.0.1.13` to `10.0.1.158`. Priority `1` (highest priority).
`show access-list ip filter2`	Display rules of the IP ACL `filter2`.

9.2.3 Creating and editing MAC rules

When filtering MAC data packets, the device lets you:

- create new groups and rules
- add new rules to existing groups
- edit an existing rule
- activate and deactivate groups and rules
- delete existing groups and rules
- change the order of existing rules

Perform the following steps:

- Open the *Network Security > ACL > MAC Rule* dialog.
- Click the button.
  The dialog displays the *Create* window.
- To create a group, specify a meaningful name in the *Group name* field. You can combine several rules in one group.
- To add a rule to an existing group, select the name of the group in the *Group name* field.
- In the *Index* field you specify the number for the rule within the ACL.
  This number defines the priority of the rule.
- Click the *Ok* button.
  The device adds the rule to the table.
  Group and role are active immediately.
  To deactivate group or rules, unmark the checkbox in the *Active* column.
  To remove a rule, highlight the affected table entry and click the button.
- Edit the rule parameters in the table.
  To change a value, double-click the relevant field.
- Save the changes temporarily. To do this, click the ✓ button.

Note: In the *Source MAC address* and *Destination MAC address* fields you can use wildcards in the `FF:??:??:??:??:??` or `??:??:??:??:00:01` form. Use capital letters here.

9.2.4 Creating and configuring a MAC ACL using the Command Line Interface

In the following example, AppleTalk and IPX are to be filtered out from the entire network. To do this, perform the following steps:

`enable`	Change to the Privileged EXEC mode.
`configure`	Change to the Configuration mode.
`mac acl add 1 macfilter`	Adds an MAC ACL with the ID `1` and the name `macfilter`.
`mac acl rule add 1 1 deny src any any dst any any etype appletalk`	Adds a rule to position `1` of the MAC ACL with the ID `1` rejecting packets with EtherType `0x809B (AppleTalk)`.
`mac acl rule add 1 2 deny src any any dst any any etype ipx-old`	Adds a rule to position `2` of the MAC ACL with the ID `1` rejecting packets with EtherType `0x8137 (IPX alt)`.
`mac acl rule add 1 3 deny src any any dst any any etype ipx-new`	Adds a rule to position `3` of the MAC ACL with the ID `1` rejecting packets with EtherType `0x8138 (IPX)`.
`mac acl rule add 1 4 permit src any any dst any any`	Adds a rule to position `4` of the MAC ACL with the ID `1` forwarding packets.
`show acl mac rules 1`	Displays the rules of the MAC ACL with the ID `1`.
`interface 1/1,1/2,1/3,1/4,1/5,1/6`	Change to the interface configuration mode of the interfaces `1/1` to `1/6`.

`acl mac assign 1 in 1`	Assigns the MAC ACL with the ID `1` to incoming data packets (`1/1`) on interfaces `1/6` to `in`.
`exit`	Leaves the interface mode.
`show acl mac assignment 1`	Displays the assignment of the MAC ACL with the ID `1` to interfaces or VLANs.

9.2.5 Assigning ACLs to a port or VLAN

When you assign ACLs to a port or VLAN, the device gives you the following options:
- To select the port or VLAN.
- To specify the ACL priority.
- To select the ACL using the group name.

Perform the following steps:

- Open the *Network Security > ACL > Assignment* dialog.
- Click the button.
  The dialog displays the *Create* window.
  - In the *Port/VLAN* field, specify the desired port or the desired VLAN.
  - In the *Priority* field, specify the priority.
  - In the *Direction* field, specify the data packets to which the device applies the rule.
  - In the *Group name* field, specify the rule the device assigns to the port or the VLAN.
- Click the *Ok* button.
- Save the changes temporarily. To do this, click the ✓ button.

9.3 MAC authentication bypass

The *MAC authorized bypass* function lets clients that do not support 802.1X, such as printers and fax machines, authenticate to the network using their MAC address. The device lets you specify the format of the MAC address used to authenticate the clients on the RADIUS server.

Example:

Split the MAC address into 6 groups of 2 characters. Use uppercase letters and a colon character as separator: `AA:BB:CC:DD:EE:FF`

Use the passwort `xY-45uM_e`. To do this, perform the following steps:

- Open the *Network Security > 802.1X Port Authentication > Global* dialog.
  In the *MAC authentication bypass format options* frame, perform the following steps:
- In the *Group size* drop-down list, select the value *2*.
  The device splits the MAC address into 6 groups of 2 characters.
- In the *Group separator* drop-down list, select the *:* character.
- In the *Upper or lower case* drop-down list, select the *upper-case* item.
- In the *Password* field, enter the password `xY-45uM_e`.
  The device uses this password for every client that authenticates to the RADIUS server. If you leave the field empty, then the device uses the formatted MAC address also as the password.
- To temporarily save the settings, click the ✓ button.

`enable`	Change to the Privileged EXEC mode.
`configure`	Change to the Configuration mode.
`dot1x mac-authentication-bypass format group-size 2`	Specify the group size `2`.
`dot1x mac-authentication-bypass format group-separator :`	Specify the group separator `:`.
`dot1x mac-authentication-bypass format letter-case upper-case`	Specify that the device formats the authentication data in uppercase letters.
`dot1x mac-authentication-bypass password xY-45uM_e`	Specify the password `xY-45uM_e`. The device uses this password to authenticate every client on the RADIUS server.

10 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

10.1 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 “port and MAC address” in its MAC address table (FDB).

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

10.1.1 Learning MAC addresses

When the device receives a data packet, it checks 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.

10.1.2 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).

10.1.3 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 survive 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 Graphical User Interface or in the Command Line Interface.

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).

10.2 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 “interested” in Multicast are connected.

10.2.1 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.

10.2.2 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 higher), 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, mark 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, mark 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 itself 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, mark the checkbox in the *Active* column for the relevant VLAN.
- ▶ The device carries out a simple 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.

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.
- 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.

10.3 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, mark 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.

10.4 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.

10.4.1 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 great deal of data traffic in higher traffic classes.

10.4.2 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.

10.4.3 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”).

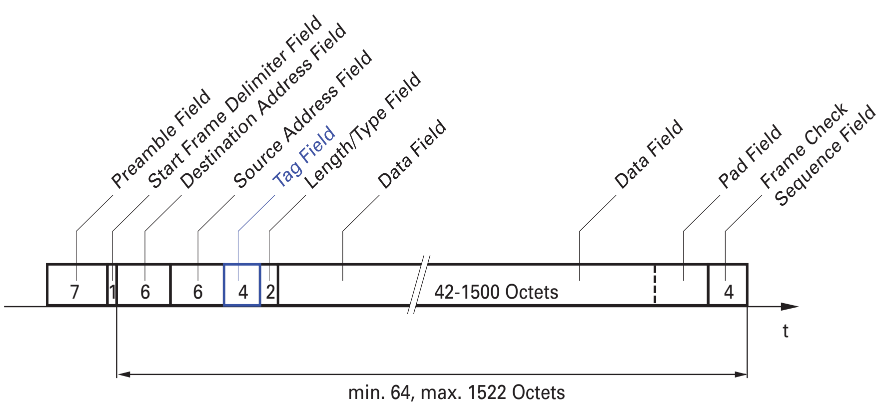


Figure 23: Ethernet data packet with tag

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

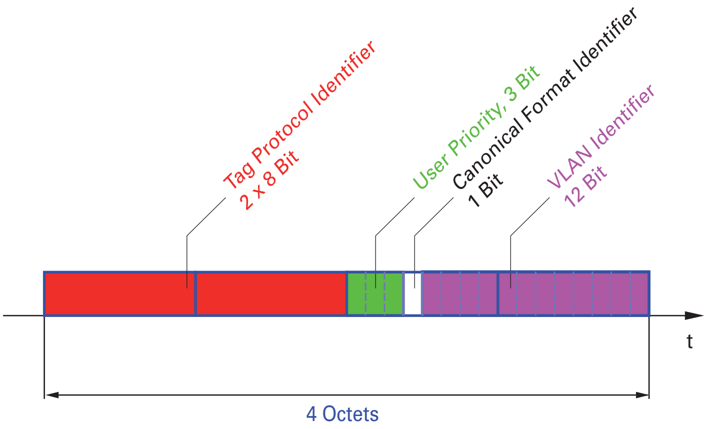


Figure 24: Structure of the VLAN tagging

Data packets with VLAN tags containing priority information but no VLAN information (VLAN ID = 0), are known as 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.

10.4.4 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.

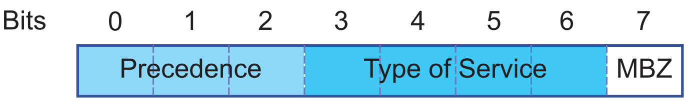


Table 22: ToS field in the IP header

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	

Table 22: ToS field in the IP header (cont

Bits (0-2): IP Precedence Defined	Bits (3-6): Type of Service Defined	Bit (7)
100 - Flash Override	0010 - [maximize reliability]	
011 - Flash	0001 - [minimize monetary cost]	
010 - Immediate		
001 - Priority		
000 - Routine		

10.4.5 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 unfortunate 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.

10.4.6 Queue management

Queue Shaping

Queue Shaping throttles the rate at which queues transmit packets. For example, using Queue Shaping, you rate-limit a higher strict-priority queue so that it lets a lower strict-priority queue to send packets even though higher priority packets are still available for transmission. The device lets you setup Queue Shaping for any queue. You specify Queue Shaping as the maximum rate at which traffic passes through a queue by assigning a percentage of the available bandwidth.

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:
  - Unmark 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:
  - Unmark 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:
  - Unmark the checkbox in the *Strict priority* column.
  - In the *Min. bandwidth [%]* column, specify the value `30`.
- To activate Weighted Fair Queuing for *Traffic class* = `3`, proceed as follows:
  - Unmark the checkbox in the *Strict priority* column.
  - In the *Min. bandwidth [%]* column, specify the value `20`.
- To activate Weighted Fair Queuing and Queue Shaping for *Traffic class* = `4`, proceed as follows:
  - Unmark the checkbox in the *Strict priority* column.
  - In the *Min. bandwidth [%]* column, specify the value `10`.
  - In the *Max. bandwidth [%]* column, specify the value `10`.

  When using a Weighted Fair Queuing and Queue Shaping combination for a specific traffic class, specify a higher value in the *Max. bandwidth [%]* column than the value specified in the *Min. bandwidth [%]* column.
- To activate Weighted Fair Queuing for *Traffic class* = `5`, proceed as follows:
  - Unmark the checkbox in the *Strict priority* column.
  - In the *Min. bandwidth [%]* column, specify the value `5`.
- To activate Weighted Fair Queuing for *Traffic class* = `6`, proceed as follows:
  - Unmark the checkbox in the *Strict priority* column.
  - In the *Min. bandwidth [%]* column, specify the value `10`.
- To activate Strict Priority and Queue Shaping for *Traffic class* = `7`, proceed as follows:
  - Mark the checkbox in the *Strict priority* column.
  - In the *Max. 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`.
`cos-queue weighted 3`	Enabling Weighted Fair Queuing for traffic class `3`.
`cos-queue min-bandwidth: 3 20`	Assigning a weight of `20` % to traffic class `3`.

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

Combining Weighted Fair Queuing and Queue Shaping

Perform the following steps:

`enable`	Change to the Privileged EXEC mode.
`configure`	Change to the Configuration mode.
`cos-queue weighted 4`	Enabling Weighted Fair Queuing for traffic class `4`.
`cos-queue min-bandwidth: 4 10`	Assigning a weight of `10` % to traffic class `4`.
`cos-queue max-bandwidth: 4 10`	Assigning a weight of `10` % to traffic class `4`.
`cos-queue weighted 5`	Enabling Weighted Fair Queuing for traffic class `5`.
`cos-queue min-bandwidth: 5 5`	Assigning a weight of `5` % to traffic class `5`.
`cos-queue weighted 6`	Enabling Weighted Fair Queuing for traffic class `6`.
`cos-queue min-bandwidth: 6 10`	Assigning a weight of `10` % to traffic class `6`.

```
show cos-queue
Queue Id  Min. bandwidth  Scheduler type
--------  --------------  --------------  --------------
0         5               0               weighted
1         20              0               weighted
2         30              0               weighted
3         20              0               weighted
4         10              10              weighted
5         5               0               weighted
6         10              0               weighted
7         0               0               strict
```

Setting up Queue Shaping

Perform the following steps:

`enable`	Change to the Privileged EXEC mode.
`configure`	Change to the Configuration mode.
`cos-queue max-bandwidth: 7 10`	Assigning a weight of `10` % to traffic class `7`.

```
show cos-queue
Queue Id  Min. bandwidth  Scheduler type
--------  --------------  --------------  --------------
0         5               0               weighted
1         20              0               weighted
2         30              0               weighted
3         20              0               weighted
4         10              10              weighted
5         5               0               weighted
6         10              0               weighted
7         0               10              strict
```

10.4.7 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.

10.4.8 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`	Displaying the IP DSCP assignments

```
    IP DSCP       Traffic Class
 -------------    -------------
   be                   2
   1                    2
   .                    .
   .                    .
   (cs1)                1
   .                    .
```

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

`exit`	Change to the Configuration mode.
`show classofservice trust`	Displaying the Trust mode of the ports/interfaces.

Configuring traffic shaping on a port

Perform the following steps:

`enable`	Change to the Privileged EXEC mode.
`configure`	Change to the Configuration mode.
`interface 1/2`	Change to the interface configuration mode of interface `1/2`.
`traffic-shape bw 50`	Limiting the maximum bandwidth of the port `1/2` to 50%.
`exit`	Change to the Configuration mode.
`exit`	Change to the Privileged EXEC mode.
`show traffic-shape`	Display the Traffic Shaping configuration.

```
Interface  Shaping rate
---------  ------------
1/1        0  %
1/2        50 %
1/3        0  %
1/4        0  %
```

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
```

10.5 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.

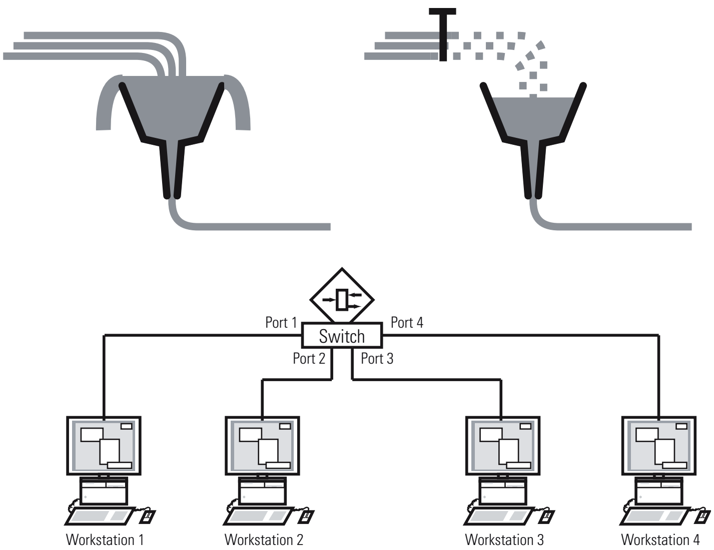


Figure 25: Example of flow control

10.5.1 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 small break in the sending transmission.

10.5.2 Setting up the Flow Control

Perform the following steps:

- ☐ Open the *Switching > Global* dialog.
- ☐ Mark 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, mark 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.

11 Configuring template-based TSN

11.1 Underlying facts

When you use the *TSN* function, the following basic conditions apply:
- The device operates using the "Store and Forward" method. Thus, the device has to receive the complete data packet before it makes a forwarding decision.
- You specify the Base time and Cycle time once in the device. Both settings are valid for each port participating in TSN.
- You configure a Gate Control List per port based on predefined templates for easier setup.
- Verify that the sum of the Gate Control List entry times is less than or equal to the specified Cycle time.
- The device uses a guard band to help protect the time slot for high priority packets from packets that "leak" from the previous time slot. The decisive factor for the interval length of the guard band is the port speed of the sending port.
  We recommend the following interval lengths for the guard band. The values are based on the port speed and the maximum allowed size of Ethernet packets:
  - 2.5 Gbit/s: 5 µs
  - 1 Gbit/s: 13 µs
  - 100 Mbit/s: 124 µs
- The Cycle time range is 50 000..10 000 000 ns.
- The Gate Control List interval range is 1 000..10 000 000 ns.
- Verify that the Cycle time as well as the Gate Control List intervals are multiples of 1 µs, 2 µs or 4 µs.

Table 23: Dependency between Cycle time and granularity

Cycle time	Granularity
50 µs..4 ms	1 µs
4.002 ms..8 ms	2 µs
8.004 ms..10 ms	4 µs

11.2 Example

This example describes how to set up the devices for a scenario with the following conditions:
- Cycle time = 1 ms
- Time slot for high priority packets = 500 µs
- Time slot for low priority packets = 487 µs

In this example, each device is connected to the network with a port speed of 1 Gbit/s.

Table 24: Structure of the cycle

Time slot	Traffic classes	Duration
High priority packets	7	500 µs
Low priority packets	0,1,2,3,4,5,6	487 µs
Guard band	–	13 µs

11.2.1 Time calculation

The device automatically calculates the duration of the time slot for the low priority packets. The calculation is based on the following parameters:
- Cycle time
- Duration of the time slot for high priority packets
- Duration of the guard band

11.2.2 Set up the devices

Using the previously specified times, you set up the devices using the Graphical User Interface or the Command Line Interface. For each device involved, perform the following steps.

Check and adjust the Cycle time

Perform the following steps:

- ☐ Open the *Switching > TSN > Configuration* dialog.
- ☐ Check in the *Configuration* frame the value in the *Cycle time [ns]* field.
- ☐ If necessary, adjust the value.

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

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

```
show tsn configuration
Port  Status                Conf. cycle time[ns]  Conf. base time
      Default gate states   Curr. cycle time[ns]  Curr. base time
      Config change pending                       Time of last activation
----  --------------------- --------------------  -----------------------------
 1/1  [x]           disabled             1000000  1970-01-01 00:00:00.000000000
      7,6,5,4,3,2,1,0                    1000000  1970-01-01 00:00:00.000000000
      [ ]                                         2018-07-12 08:10:58.813000000

 1/2  [x]           disabled             1000000  1970-01-01 00:00:00.000000000
      7,6,5,4,3,2,1,0                    1000000  1970-01-01 00:00:00.000000000
      [ ]                                         2018-07-11 07:24:35.204000000

 1/3  [ ]          disabled              1000000  1970-01-01 00:00:00.000000000
      7,6,5,4,3,2,1,0                          0  1970-01-01 00:00:00.000000000
      [ ]                                         1970-01-01 00:00:00.000000000

 1/4  [ ]          disabled              1000000  1970-01-01 00:00:00.000000000
      7,6,5,4,3,2,1,0                          0  1970-01-01 00:00:00.000000000
      [ ]                                         1970-01-01 00:00:00.000000000
```

`tsn cycle-time 1000000`	If necessary, adjust the value.

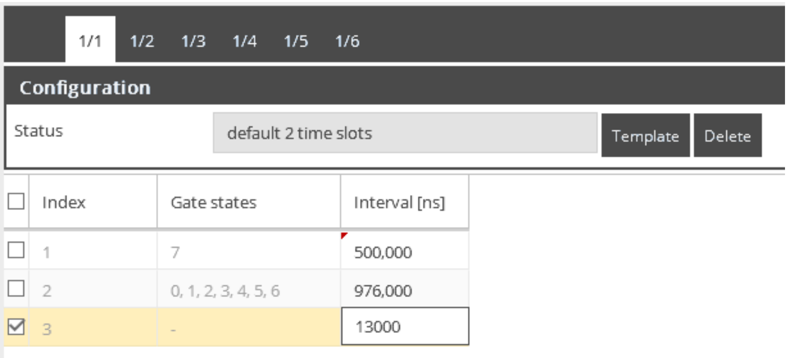
Select a template and set up the Gate Control List

The device provides predefined templates to help you set up the Gate Control List. In this example, we use the template *default 2 time slots*. After you select the template, you can adjust the duration of the time slots. Perform the following steps for each port for which you want to use the *TSN* function.

Perform the following steps:

- ☐ Open the *Switching > TSN > Gate Control List > Configured* dialog.
- ☐ Select the tab for the port for which you want to specify the settings.

- Select a template in the *Configuration* frame.
  Perform the following steps:
  – Click the *Template* button.
  – Select the `default 2 time slots` item.
  – Click the *Ok* button.
- Adjust the values in the *Interval [ns]* column:
  – Enter the value `500000` in the row for high priority packets.
  – Enter the value `13000` in the row for the guard band.
  – The device calculates the third value automatically when saving the changes.



- 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`.
`tsn gcl modify 1 interval 500000`	Adjust the duration in nanoseconds of the time slot for high priority packets.
`tsn gcl modify 3 interval 13000`	Adjust the duration in nanoseconds of the time slot for the guard band. The device automatically calculates the duration of the time slot for low priority packets. You cannot set the time slot for low priority packets.

12 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.

12.1 Examples of VLANs

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

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

12.1.1 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.

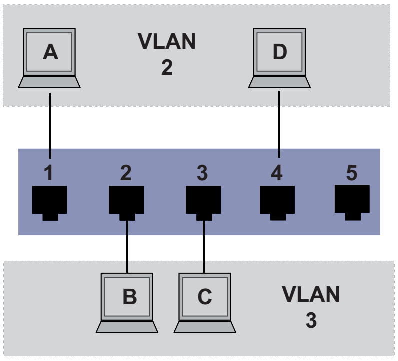


Figure 26: Example of a simple port-based VLAN

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`.

Table 25: Ingress table

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

Table 26: Egress table

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 current VLAN configuration.

```
Max. VLAN ID.................................. 4042
Max. supported VLANs.......................... 128
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.
    Changes using the *GVRP* function are disabled.
  - `-` = The port is not a member of this VLAN.
    Changes using the *GVRP* function are allowed.

  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
```

12.1.2 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 2nd Switch (on the right in the example).

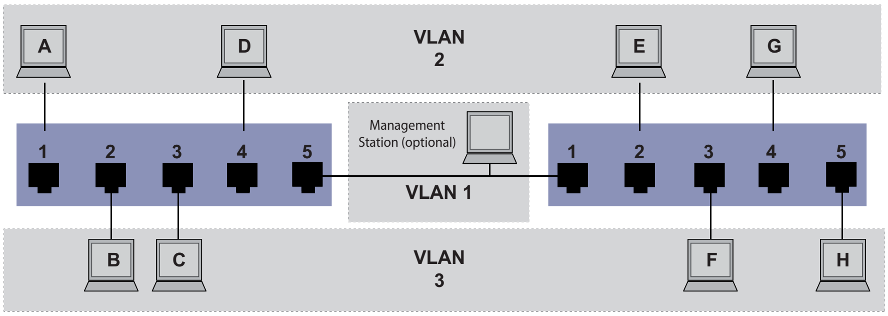


Figure 27: Example of a more complex VLAN configuration

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.

Table 27: Ingress table for device on left

Terminal	Port	Port VLAN identifier (PVID)
A	1	2
B	2	3
C	3	3
D	4	2
Uplink	5	1

Table 28: Ingress table for device on right

Terminal	Port	Port VLAN identifier (PVID)
Uplink	1	1
E	2	2
F	3	3
G	4	2
H	5	3

Table 29: Egress table for device on left

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

Table 30: Egress table for device on right

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 “see” 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 current VLAN configuration.

```
Max. VLAN ID................................ 4042
Max. supported VLANs........................ 128
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.
    Changes using the *GVRP* function are disabled.
  - `-` = The port is not a member of this VLAN.
    Changes using the *GVRP* function are disabled.

  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`.
- Mark 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
```

12.2 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.

12.3 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.

12.4 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 safeguard 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.

13 Redundancy

13.1 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

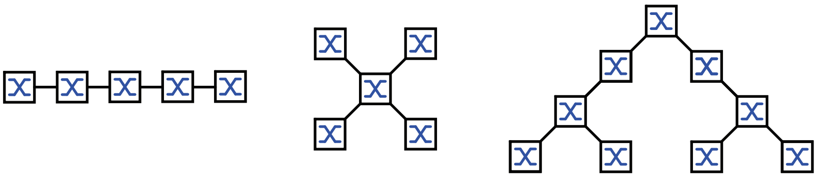


Figure 28: Network with line, star and tree topologies

To maintain communication in case a connection failure 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 working. When a connection failure 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.

13.1.1 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.

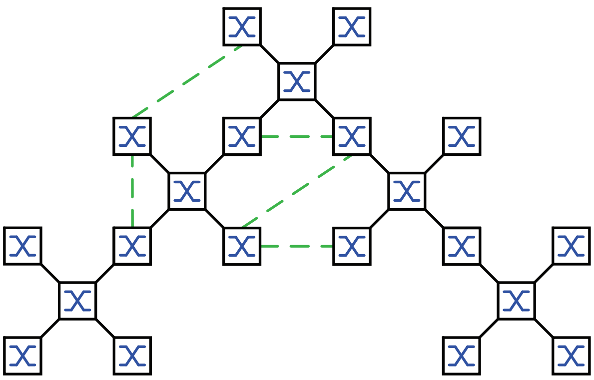


Figure 29: Meshed topology: Tree topology with physical loops

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.

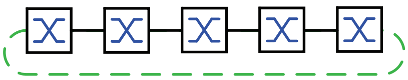


Figure 30: Ring topology: Line topology with connected ends

For operating in this network topology, the device provides you with the following redundancy protocols:
- Media Redundancy Protocol (MRP)
- Rapid Spanning Tree (RSTP)

13.1.2 Redundancy Protocols

For operating in different network topologies, the device provides you with the following redundancy protocols:

Table 31: Overview of 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.
Subring	Ring	The *Sub Ring* function enables you to easily couple network segments to existing redundancy rings.
Ring/Network coupling	Ring	
RCP	Ring	
RSTP	Random structure	The switching time depends on the network topology and the number of devices. ▶ typ. < 1 s with RSTP ▶ typ. < 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.

Table 31: Overview of redundancy protocols (cont

Redundancy protocol	Network topology	Comments
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.
HIPER Ring Client	Ring	Extend an existing HIPER ring or replace a device already participating as a client in a HIPER ring.
HIPER Ring over LAG	Ring	Link devices together over a Link Aggregation Group (LAG). The ring clients and Ring Manager behave in the same manner as a ring without a LAG instance.

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.

13.1.3 Combinations of Redundancies

Table 32: Overview of redundancy protocols

	MRP	RSTP	Link Aggreg.	Link Backup	Subring	HIPER Ring
MRP	▲	– – –	– – –	– – –	– – –	– – –
RSTP	▲ 1)	▲	– – –	– – –	– – –	– – –
Link Aggreg.	▲ 2)	▲ 2)	▲	– – –	– – –	– – –
Link Backup	▲	▲	▲	▲	– – –	– – –
Subring	▲	▲	▲ 2)	▲	▲	– – –
HIPER Ring	▲	▲ 1)	▲ 2)	▲	▲	▲

▲ Combination applicable

1) A redundant coupling between these network topologies will possibly lead to loops. To redundantly couple these topologies, refer to chapter “FuseNet” on page 216.

2) Combination applicable on the same port

13.2 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 failure 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.

13.2.1 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.

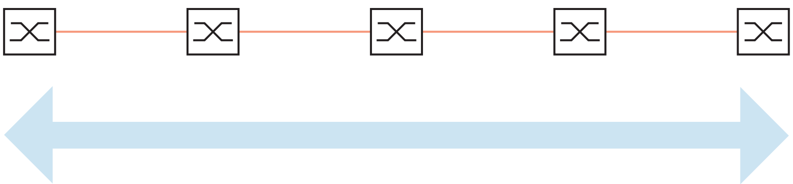


Figure 31: Line structure

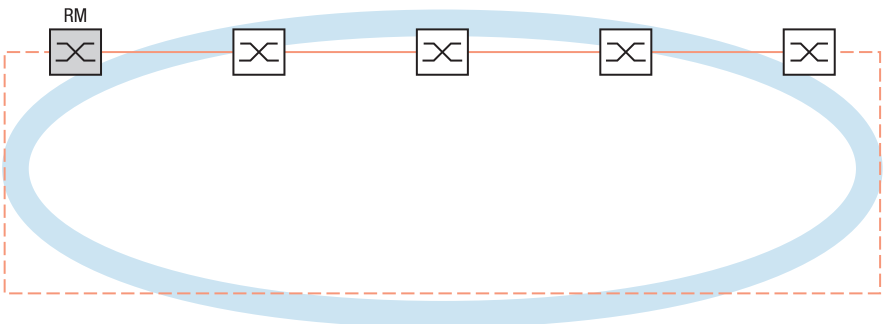


Figure 32: Redundant ring structure
RM = Ring Manager
—— main line
- - - redundant line

13.2.2 Reconfiguration time

When a line section failure 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.

13.2.3 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 failure recognition.

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.

13.2.4 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).

13.2.5 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 failure 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.

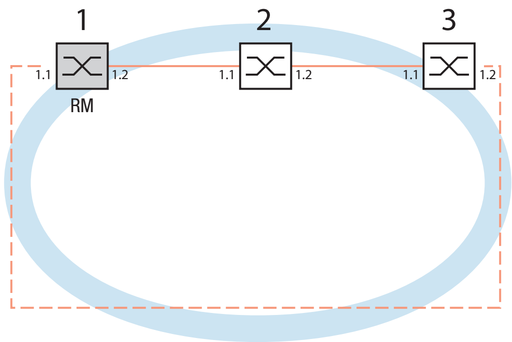


Figure 33: Example of MRP-Ring
RM = Ring Manager
—— main line
- - - redundant line

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:

Table 33: Port settings for ring ports

Port type	Bit rate	Port on	Automatic configuration	Manual configuration
TX	100 Mbit/s	`marked`	`unmarked`	*100 Mbit/s FDX*
TX	1 Gbit/s	`marked`	`marked`	–
Optical	100 Mbit/s	`marked`	`unmarked`	*100 Mbit/s FDX*
Optical	1 Gbit/s	`marked`	`marked`	–
Optical	2.5 Gbit/s	`marked`	–	*2.5 Gbit/s FDX*

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 Command Line Interface 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 Graphical User Interface, 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, mark the *Fixed backup* checkbox.

Note: When the device reverts back to the primary port, the maximum ring recovery time can be exceeded.

When you unmark 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, leave 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.

Check 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.

13.2.6 MRP over LAG

Schneider Electric devices allow you to combine Link Aggregation Groups (LAG) to increase bandwidth with the Media Redundancy Protocol (MRP) providing redundancy. The function lets you increase the bandwidth on individual segments or on the entire network.

The *Link Aggregation* function helps you overcome bandwidth limitations of individual ports. LAG lets you combine 2 or more links in parallel, creating one logical link between 2 devices. The parallel links increase the bandwidth for the data stream between the 2 devices.

An MRP ring consists of up to 50 devices that support the MRP protocol according to IEC 62439. When you use only Schneider Electric devices, the protocol lets you configure MRP rings with up to 100 devices.

You use MRP over LAG in the following cases:
- to increase bandwidth only on specific segments of an MRP ring
- to increase bandwidth on the entire MRP ring

Network Structure

When configuring an MRP ring with LAGs, the Ring Manager (RM) monitors both ends of the backbone for continuity. The RM blocks data on the secondary (redundant) port as long as the backbone is intact. When the RM detects an interruption of the data stream on the ring, it begins forwarding data on the secondary port, which restores backbone continuity.

You use LAG instances in MRP rings to increase bandwidth only, in this case MRP provides the redundancy.

In order for the RM to detect an interruption on the ring, MRP requires a device to block every port in the LAG instance in cases where a port in the instance is down.

LAG on a single segment of an MRP ring

The device lets you configure a LAG instance on specific segments of an MRP ring.

You use the LAG Single Switch method for devices in the MRP ring. The Single Switch method provides you an inexpensive way to grow your network by using only one device on each side of a segment to provide the physical ports. You group the ports of the device into a LAG instance to provide increased bandwidth on specific segments where needed.

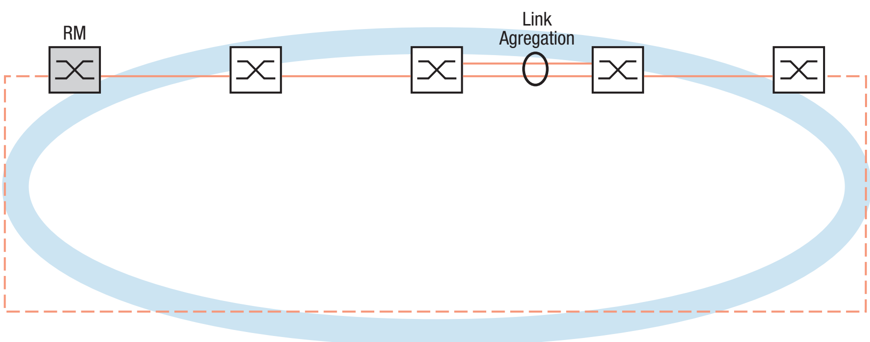


Figure 34: Link Aggregation over a single link of an MRP ring.

LAG on an entire MRP ring

Besides being able to configure a LAG instance on specific segments of an MRP ring, Schneider Electric devices also allow you to configure LAG instances on every segment, which increases bandwidth on the entire MRP ring.

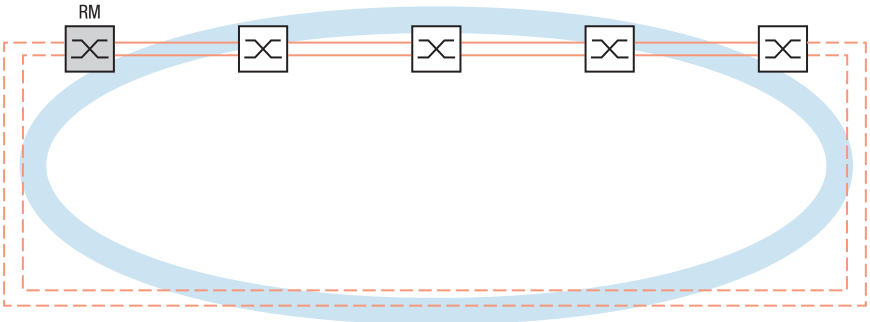


Figure 35: Link Aggregation over the entire MRP ring.

Detecting interruptions on the ring

When configuring the LAG instance, specify the *Active ports (min.)* value to equal the total number of ports used in the LAG instance. When a device detects an interruption on a port in the LAG instance, it blocks data on the other ports of the instance. With every port of an instance blocked, the RM senses that the ring is open and begins forwarding data on the secondary port. This way the RM is able to restore continuity to the devices on the other side of the interrupted segment.

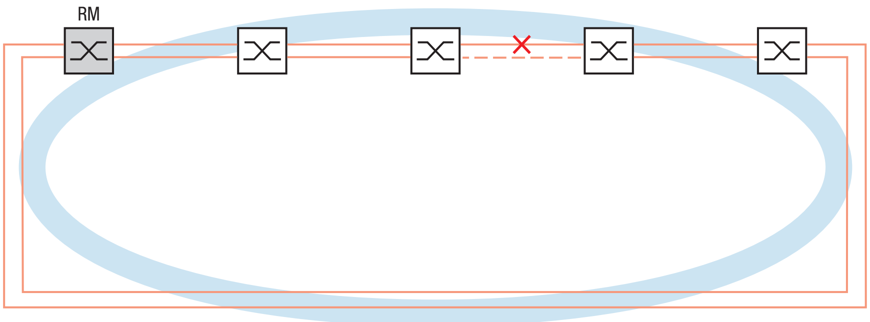


Figure 36: Interruption of a link in an MRP ring.

Example Configuration

In the following example, switch A and switch B link two departments together. The departments produce traffic too high for the individual port bandwidth to handle. You configure a LAG instance for the single segment of the MRP ring, increasing the bandwidth of the segment.

The prerequisite for the example configuration is that you begin with an operational MRP ring.

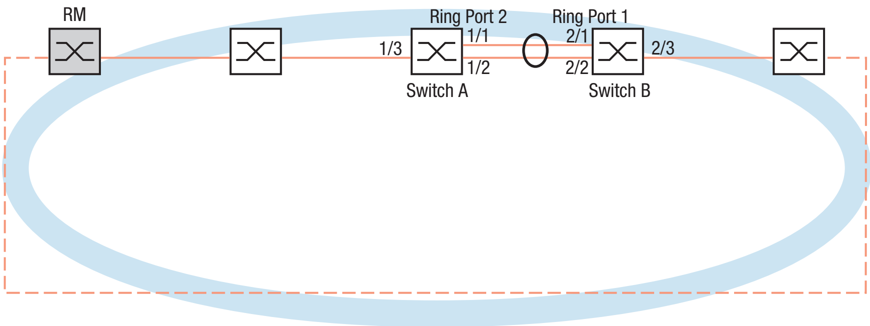


Figure 37: MRP over LAG Configuration Example

Configure switch A first. To do this, perform the following steps. Then configure switch B using the same steps, substituting the appropriate port and ring port numbers.

- ☐ 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.
- ☐ In the *Active ports (min.)* column enter `2`, which in this case is the total number of ports in the instance. When combining MRP and LAG you specify the total number of ports as the *Active ports (min.)*. When the device detects an interruption on a port, it blocks the other ports in the instance causing the ring to open. The Ring Manager senses that the ring is open, then begins forwarding data on its secondary ring port which restores the connectivity to the other devices in the network.
- ☐ Save the changes temporarily. To do this, click the ✓ button.
- ☐ Open the *Switching > L2-Redundancy > MRP* dialog.
- ☐ In the *Ring port 2* frame, select port `lag/1` in the *Port* drop-down list.
- ☐ 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.
`mrp domain modify port secondary lag/1`	Specifies port `lag/1` as ring port `2`.
`copy config running-config nvm`	Save the current settings in the non-volatile memory (`nvm`) in the “selected” configuration profile.

13.3 HIPER Ring Client

⚠ WARNING

UNINTENDED EQUIPMENT OPERATION

To help avoid loops during the configuration phase, configure each device of the *HIPER Ring* 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.

The concept of HIPER Ring Redundancy enables the construction of high-availability, ring-shaped network structures. The *HIPER Ring* Client function lets the network administrator extend an existing HIPER Ring or replace a client device already participating in a HIPER Ring.

When the device senses that the link on a ring port goes down, the device sends a LinkDown packet to the Ring Manager (RM) and flushes the FDB table. Once the RM receives the LinkDown packet, it immediately forwards the data stream over both the primary and secondary ring ports. Thus, the RM is able to maintain the integrity of the HIPER Ring.

The device only supports Fast Ethernet and Gigabit Ethernet ports as ring ports. Furthermore, you can include the ring ports in a LAG instance.

In the default state, the HIPER Ring client is inactive, and the primary and secondary ports are set to `no Port`.

Note: Deactivate the Spanning Tree Protocol (STP) for the ring ports in the *Switching > L2-Redundancy > Spanning Tree > Port* dialog, because STP and HIPER Ring have different reaction times.

Table 34: Port settings for ring ports

Port type	Bit rate	Port on	Automatic configuration	Manual configuration
TX	100 Mbit/s	`marked`	`unmarked`	*`100 Mbit/s FDX`*
TX	1 Gbit/s	`marked`	`marked`	–
Optical	100 Mbit/s	`marked`	`unmarked`	*`100 Mbit/s FDX`*
Optical	1 Gbit/s	`marked`	`marked`	–
Optical	2.5 Gbit/s	`marked`	–	*`2.5 Gbit/s FDX`*

13.3.1 VLANS on the HIPER Ring

The device lets you forward VLAN data over the HIPER Ring. Thus the device provides redundancy for your VLAN data. The ring device forwards management data around the ring for example, on VLAN 1. In order for the data to reach the management station, the ring devices forward the untagged management data on the ring ports. Also, specify the ring ports as members in VLAN 1.

When you have other VLANs traversing your ring devices, the ring devices forward the other VLAN data as tagged.

Specify the VLAN settings. To do this, perform the following steps:

- ☐ Open the *Switching > VLAN > Configuration* dialog.
- ☐ Forward untagged VLAN management data on the ring ports.
  In the VLAN 1 row, select the `U` item in the drop-down list in the columns related to the ring port.
- ☐ Block management packets from being forwarded to the non-ring ports.
  In the VLAN 1 row, select the `-` item in the drop-down list in the columns **not** related to the ring port.
- ☐ Allow a ring device to forward VLAN data to and from ports with VLAN membership.
  In the VLAN row, select the `T` item in the drop-down list in the columns related to the ring port.
- ☐ Open the *Switching > VLAN > Port* dialog.
- ☐ Assign VLAN 1 membership to the ring ports.
  Enter the value `1` in the *Port-VLAN ID* column of the ring port rows.
- ☐ Assign VLAN membership to the non-ring ports.
  Enter the appropriate VLAN ID in the *Port-VLAN ID* column of the non-ring port rows.

13.3.2 HIPER Ring over LAG

The *HIPER Ring* function lets you link the devices together over a Link Aggregation Group (LAG). The ring clients and Ring Manager behave in the same manner as a ring without a LAG instance.

If a LAG link goes down, then the other link in the instance also goes down making a break in the ring. After detecting a break in the ring, the affected ports send a Link Down packet to the Ring Manager. The Ring Manager unblocks the secondary port, sending data in both directions around the ring, and replies with a Delete packet. Upon receiving a Delete packet the ring participates flush their FDB.

13.4 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. In order 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* for the current root bridge. 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).

13.4.1 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.

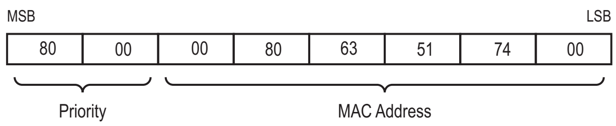


Figure 38: Bridge Identifier, Example (values in hexadecimal notation)

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 (see table 35). 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 has a tool with which he 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.

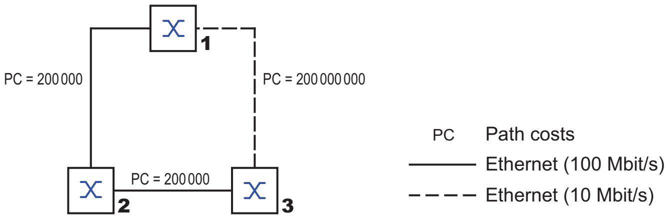


Figure 39: Path costs

Table 35: Recommended path costs for RSTP based on the data rate.

Data rate	Recommended value	Recommended range	Possible range
≤100 kbit/s	200 000000[1]	20000000-200000000	1-200000000
1 Mbit/s	20000000[a]	2000000-200000000	1-200000000
10 Mbit/s	2000000[a]	200000-20000000	1-200000000
100 Mbit/s	200000[a]	20000-2000000	1-200000000
1 Gbit/s	20000	2000-200000	1-200000000
10 Gbit/s	2000	200-20000	1-200 000000
100 Gbit/s	200	20-2000	1-200000000
1 TBit/s	20	2-200	1-200000000
10 TBit/s	2	1-20	1-200000000

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.

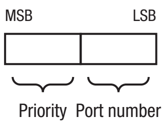


Figure 40: Port Identifier

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.

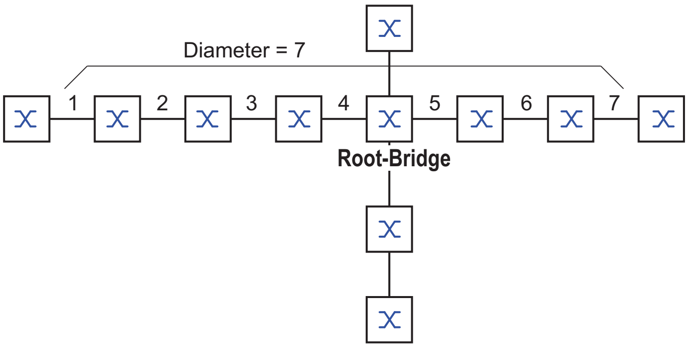


Figure 41: Definition of diameter

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.

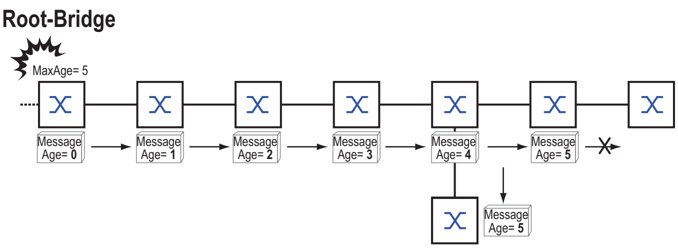


Figure 42: Transmission of an STP-BPDU depending on MaxAge

13.4.2 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 decides 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 figure 40). 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.

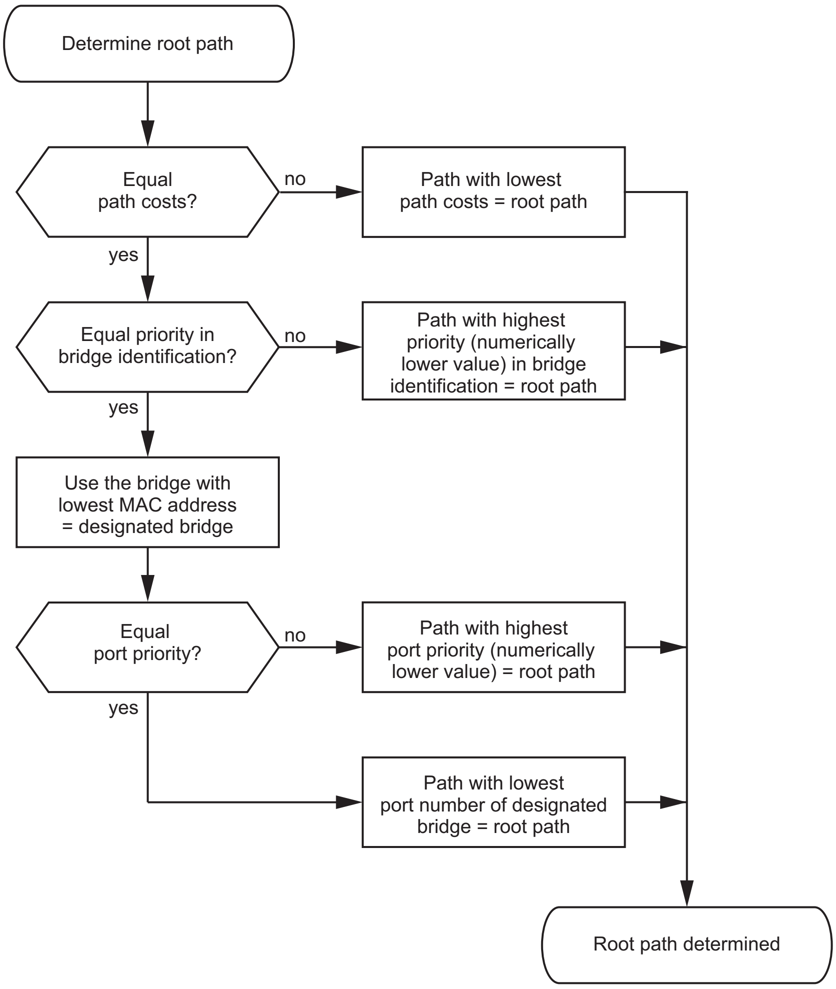


Figure 43: Flow diagram for specifying the root path

13.4.3 Examples

Example of determining the root path

You can use the network plan (see figure 44) to follow the flow chart (see figure 43) 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).

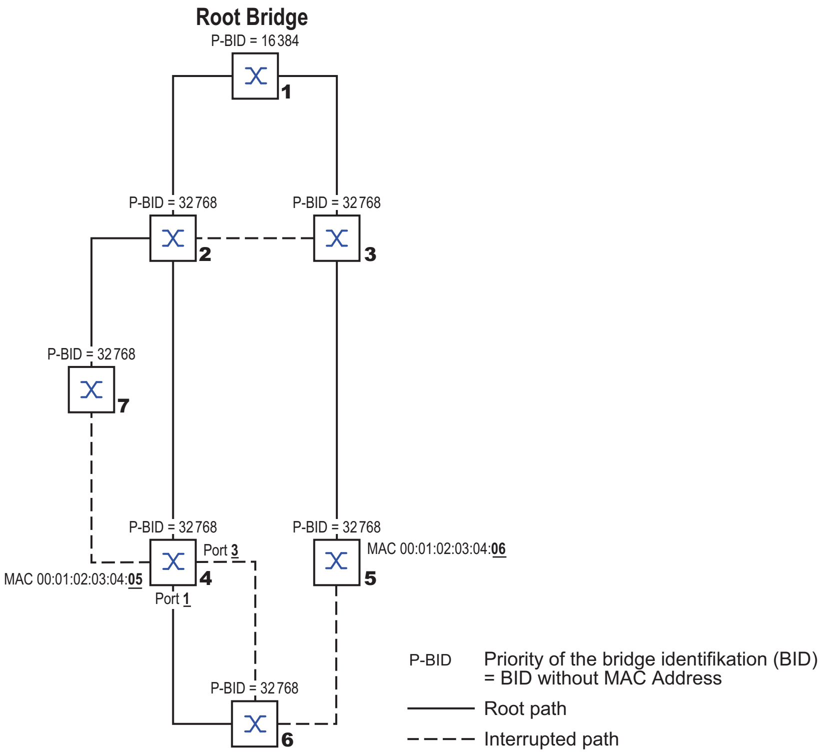


Figure 44: Example of determining the root path

Note: When the current 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 (see figure 45) to follow the flow chart (see figure 43) 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 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.

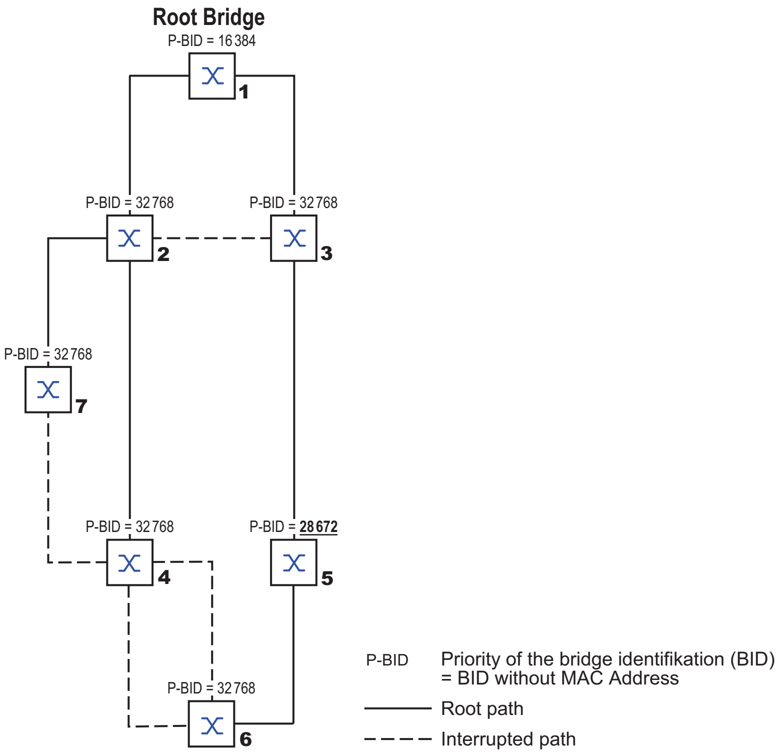


Figure 45: Example of manipulating the root path

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 shown here (see figure 46). The path costs for most of the bridges to the root bridge have decreased.

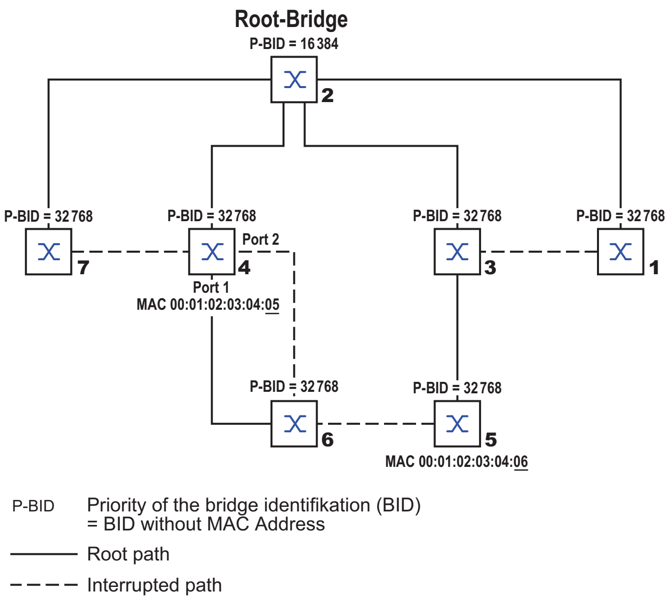


Figure 46: Example of manipulating the tree structure

13.5 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.

13.5.1 Port roles

RSTP assigns each bridge port one of the following roles (see figure 47):

- 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) decides 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 decide which port it selects locally as the root port (see figure 43).
  The root bridge itself 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.

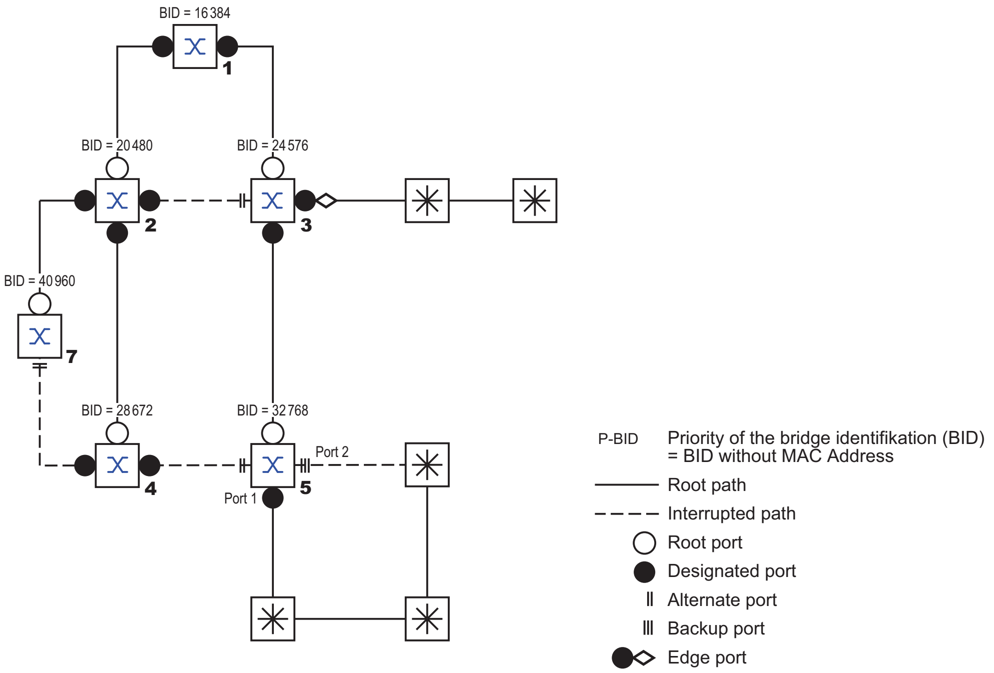


Figure 47: Port role assignment

13.5.2 Port states

Depending on the tree structure and the state of the selected connection paths, the RSTP assigns the ports their states.

Table 36: Relationship between port state values for STP and RSTP

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)

13.5.3 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.

13.5.4 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 at the recipient in the wrong order 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.

13.5.5 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 marked.
- 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.

Check 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:

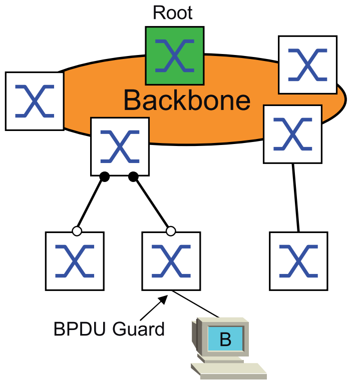
`show spanning-tree global`	Displays the parameters for checking.

13.5.6 Guards

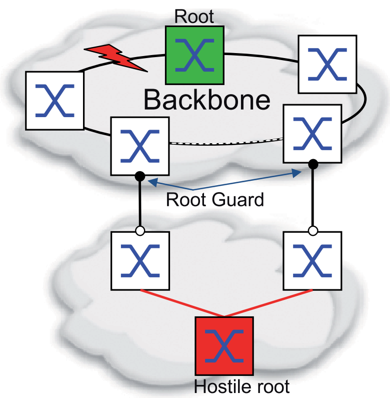
The device lets you activate various protection functions (guards) in the device ports.

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.

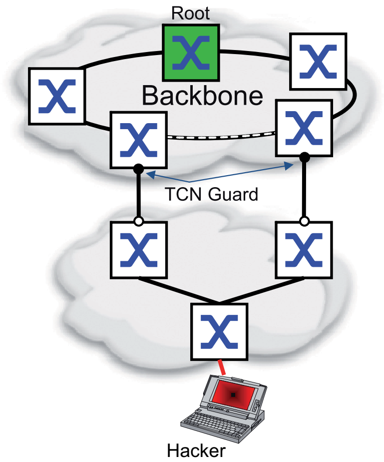


  Terminal device ports do not normally receive any STP-BPDUs. If an attacker still attempts to feed in STP-BPDUs on this port, then the device deactivates the device port.
- Root Guard – for designated ports
  You activate this protection function separately for every device port.

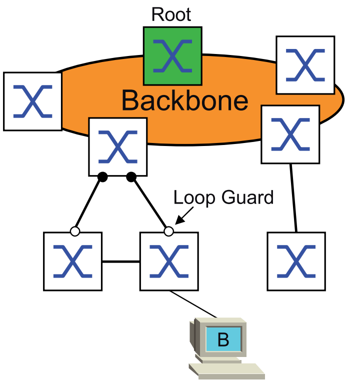


  When a designated port receives an STP-BPDU with better path information to the root bridge, the device discards the STP-BPDU and sets the transmission state of the port to `discarding` instead of `root`.
  When there are no STP-BPDUs with better path information to the root bridge, after 2 × *Hello 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.
- ☐ Mark 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, mark 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 unmarked.
- 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 marked.

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, mark 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.

13.6 Dual RSTP (MCSESM-E)

Industrial applications require your networks to have high availability. This also involves maintaining deterministic, short interruption times for the communication in cases where one of the network components becomes inoperable.

A ring topology helps provide short interruption times with a minimal use of ressources. Using the *Spanning Tree* protocol, the interruption time depends on the size of the network. To optimize the interruption time, you can split large *Spanning Tree* networks into smaller ring segments.

The *Dual RSTP* function is used together with the *RCP* function. Using the *RCP* function you have the option of coupling one or more RSTP rings with the RSTP instance in a primary ring. When coupling two *Spanning Tree* segments, the secondary ring represents a separate RSTP instance for which the settings of the *Dual RSTP* function apply. This *Dual RSTP* instance works independently of the RSTP instance of the primary ring and of the other secondary rings. When RSTP is the protocol used in only one of the rings to be coupled, you do not need the *Dual RSTP* function.

13.7 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 with a seamless failover. 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 marked.
- In the *Send trap (Link up/down)* column, the checkbox is marked.
- In the *Static link aggregation* column, the checkbox is unmarked.
- In the *Active ports (min.)* column, the value is `1`.

13.7.1 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 2 Link Aggregation groups. The number of useable ports per Link Aggregation group depends on the device.

13.7.2 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.

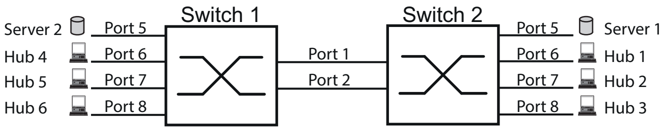


Figure 48: Link Aggregation Switch to Switch Network

Configure Switch 1 and 2 in the Graphical User Interface. 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.

13.8 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.

13.8.1 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 relearn the MAC addresses.

13.8.2 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.

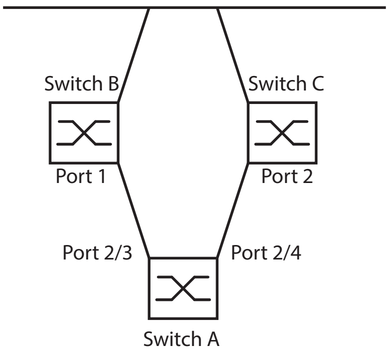


Figure 49: Link Backup example network

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, mark the *Fail back* checkbox.

- ☐ Set the fail back timer for the link backup pair, enter `30` s in *Fail back delay [s]*.
- ☐ To activate the link backup pair, mark 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 timer.
`link-backup modify 2/4 failback-time 30`	Specify the fail back delay time 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.

13.9 FuseNet

The *FuseNet* protocols let you couple rings that are operating with one of the following redundancy protocols:
- MRP
- HIPER ring
- RSTP

Note: The prerequisite for coupling a network to the main ring using the *Ring/Network Coupling* protocol is that the connected network contains only network devices that support the *Ring/Network Coupling* protocol.

Use the following table to select the *FuseNet* coupling protocol to be used in your network:

Main Ring	Connected Network		
	MRP	**HIPER ring**	**RSTP**
MRP	*Sub Ring*[1)]	– *Redundant Coupling Protocol* – *Ring/Network Coupling*	– *Redundant Coupling Protocol* – *Ring/Network Coupling*
HIPER ring	*Sub Ring*	*Ring/Network Coupling*	– *Redundant Coupling Protocol* – *Ring/Network Coupling*
RSTP	*Redundant Coupling Protocol*	*Redundant Coupling Protocol*	*Dual RSTP* + *Redundant Coupling Protocol*

– no suitable coupling protocol

1) with *MRP* configured on different VLANs

13.10 Subring

The *Sub Ring* function is an extension of the Media Redundancy Protocol (MRP). This function lets you couple a subring to a main ring using various network structures.

The Subring protocol provides redundancy for devices by coupling both ends of an otherwise flat network to a main ring.

Setting up subrings has the following advantages:

- Through the coupling process, you include the new network segment in the redundancy concept.
- Subrings allow easy integration of new areas into existing networks.
- Subrings allow you easy mapping of the organizational structure of an area in a network topology.
- In an MRP ring, the failover times of the subring in redundancy cases are typically < 100 ms.

13.10.1 Subring description

The subring concept lets you couple new network segments to suitable devices in an existing ring (main ring). The devices with which you couple the subring to the main ring are Subring Managers (SRM).

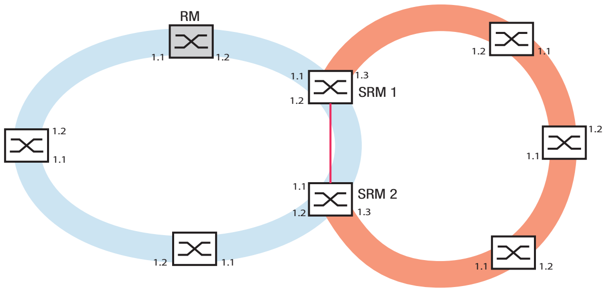


Figure 50: Example of a subring structure
blue ring = Main ring
orange ring = Subring
red line = Redundant link of Subring
SRM = Subring Manager
RM = Ring Manager

The Subring Manager capable devices support up to 8 instances and thus manage up to 8 subrings at the same time.

The *Sub Ring* function lets you integrate devices that support MRP as participants. The devices with which you couple the subring to the main ring require the *Sub Ring* Manager function.

Each subring can consist of up to 200 participants, excluding the Subring Managers themselves and the devices between the Subring Managers in the main ring.

The following figures display examples of possible subring topologies:

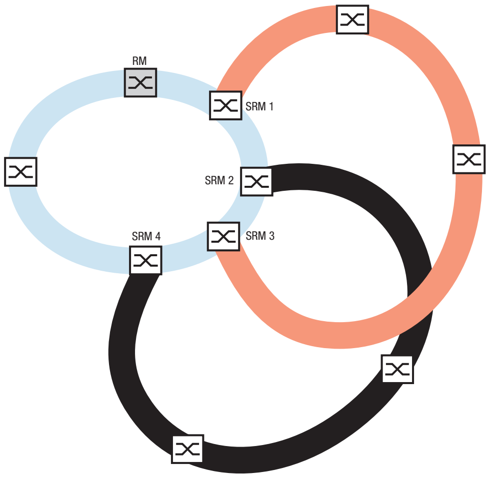


Figure 51: Example of an overlapping subring structure

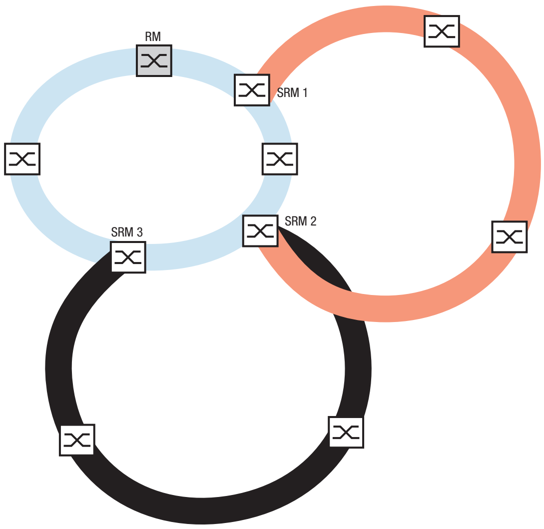


Figure 52: Special case: A Subring Manager manages 2 subrings (2 instances). The Subring Manager is capable of managing up to 8 instances.

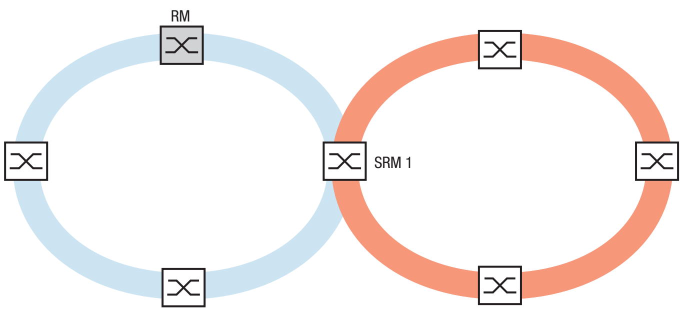


Figure 53: Special case: a Subring Manager manages both ends of a subring on different ports (Single Subring Manger).

Note: In the previous examples, the Subring Managers only couple subrings to existing main rings. The *Sub Ring* function prohibits cascaded subrings, for example coupling a new subring to another existing subring.

If you use MRP for the main ring and the subring, then specify the VLAN settings as follows:

- VLAN `X` for the main ring
  – on the ring ports of the main ring participants
  – on the main ring ports of the Subring Manager
- VLAN `Y` for the Subring
  – on the ring ports of the Subring participants
  – on the subring ports of the Subring Manager

  You can use the same VLAN for multiple subrings.

13.10.2 Subring example

In the following example, you couple a new network segment with 3 devices to an existing main ring which uses the MRP protocol. When you couple the network at both ends instead of one end, the subring provides increased availability with the corresponding configuration.

You couple the new network segment as a subring. You couple the subring to the existing devices of the main ring using the following configuration types.

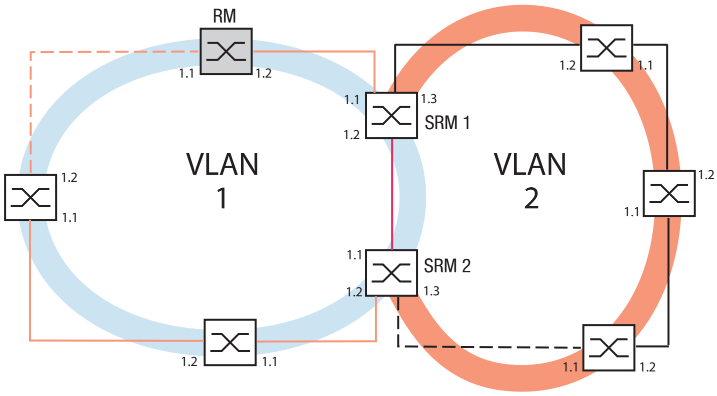


Figure 54: Example of a subring structure
orange line= Main ring members in VLAN 1
black line= Subring members in VLAN 2
orange dash line= Main ring loop open
black dash line= Subring loop open
red line = Redundant link member in VLAN 1
SRM = Subring Manager
RM = Ring Manager

To configure the subring, perform the following steps:

☐ Configure the three devices of the new network segment as participants in an MRP ring:
  – Configure the transmission rate and the duplex mode for the ring ports in accordance with the following table:

Table 37: Port settings for subring ports

Port type	Bit rate	Port on	Automatic configuration	Manual configuration
TX	100 Mbit/s	marked	unmarked	*100 Mbit/s FDX*
TX	1 Gbit/s	marked	marked	–
Optical	100 Mbit/s	marked	unmarked	*100 Mbit/s FDX*
Optical	1 Gbit/s	marked	marked	–
Optical	2.5 Gbit/s	marked	–	*2.5 Gbit/s FDX*

The following steps contain additional settings for subring configuration:

- To help prevent loops during configuration, deactivate the Subring Manager function on the main ring and subring devices. After you completely configure every device participating in the main ring and subrings activate the global *Sub Ring* function and Subring Managers.
- Disable the RSTP function on the MRP ring ports used in the subring.
- Verify that the *Link Aggregation* function is inactive on ports participating in the main ring and subring.
- Specify a different VLAN membership for the main ring ports and subring ports although the main ring is using the MRP protocol. For example, use VLAN ID `1` for the main ring and the redundant link, then use VLAN ID `2` for the subring.
  - For the devices participating in the main ring for example, open the *Switching > VLAN > Configuration* dialog. Create VLAN `1` in the static VLAN table. To tag the main ring ports for membership in VLAN `1`, select the `T` item in the drop-down list of the appropriate port columns.
  - For the devices participating in the subring use the step above and add the ports to VLAN `2` in the static VLAN table.
- Activate the *MRP* function for the main ring and subring devices.
  - In the *Switching > L2-Redundancy > MRP* dialog, configure the 2 ring ports participating in the main ring on the main ring devices.
  - For the devices participating in the subring use the step above and configure the 2 ring ports participating in the subring on the subring devices.
  - Assign the same MRP domain ID to the main ring and subring devices. When you only use Schneider Electric devices, the default values suffice for the MRP domain ID.

Note: The *MRP domain* is a sequence of 16 numbers in the range from `0` to `255`. The default value is `255 . 255 . 255 . 255 . 255 . 255 . 255 . 255 . 255 . 255 . 255 . 255 . 255 . 255 . 255 . 255`. A *MRP domain* consisting entirely of zeroes is invalid.

The *Sub Ring* dialog lets you change the MRP domain ID. Alternatively, use the Command Line Interface. To do this, perform the following steps:

`enable`	Change to the Privileged EXEC mode.
`configure`	Change to the Configuration mode.
`mrp domain delete`	Deletes the current MRP domain.
`mrp domain add domain-id 0.0.1.1.2.2.3.4.4.111. 222.123.0.0.66.99`	Creates a new MRP domain with the specified MRP domain ID. Any subsequent MRP domain changes apply to this domain ID.

13.10.3 Subring example configuration

⚠ WARNING

UNINTENDED EQUIPMENT OPERATION

To help avoid loops during the configuration phase, configure each device of the *Sub Ring* 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.

Note: Help avoid loops during configuration. Configure every device of the subring individually. Before you activate the redundant link, completely configure every subring device.

Configure the 2 Subring Managers in the example. To do this, perform the following steps:

- Open the *Switching > L2-Redundancy > Sub Ring* dialog.
- To add a table entry, click the button.
- In the *Port* column, select the port that couples the device to the subring.
  Use port *1/3* for this example.
  For coupling, use one of the available ports with the exception of the ports which are already connected to the main ring.
- In the *Name* column, assign a name to the subring.
  For this example enter `Test`.
- In the *SRM mode* column, select Subring Manager mode.
  You thus specify which port for coupling the subring to the main ring becomes the redundant manager.
  The options for the coupling are:
  - `manager`
    When you specify both Subring Managers with the same value, the device with the higher MAC address manages the redundant link.
  - `redundant manager`
    This device manages the redundant link, as long as you have specified the other Subring Manager as a `manager`. Otherwise the device with the higher MAC address manages the redundant link.

  Specify Subring Manager 1 as `manager`, in accordance with the figure depicting this example.
- Leave the values in the *VLAN* column and *MRP domain* column unchanged.
  The default values are correct for the example configuration.
- Save the changes temporarily. To do this, click the button.

`enable`	Change to the Privileged EXEC mode.
`configure`	Change to the Configuration mode.
`sub-ring add 1`	Creates a new subring with the subring ID `1`.
`sub-ring modify 1 port 1/3`	Specify port *1/3* as subring port.
`sub-ring modify 1 name Test`	Assign the name `Test` to the subring `1`.
`sub-ring modify 1 mode manager`	Assign the `manager` mode to the subring `1`.
`show sub-ring ring`	Display the subrings state on this device.
`show sub-ring global`	Display the subring global state on this device.

- Configure the 2nd Subring Manager in the same way.
  Specify Subring Manager 2 as `redundant manager`, in accordance with the figure depicting this example.

- To activate the Subring Manager function, mark the *Active* checkbox in the appropriate row.
- After you have configured both Subring Managers and the devices participating in the subring, enable the function and close the redundant link.
- Save the changes temporarily. To do this, click the ✓ button.

`enable`	Change to the Privileged EXEC mode.
`configure`	Change to the Configuration mode.
`sub-ring enable 1`	Activate subring `1`.
`sub-ring enable 2`	Activate subring `2`.
`exit`	Change to the Privileged EXEC mode.
`show sub-ring ring <Domain ID>`	Display the settings of the selected subrings.
`show sub-ring global`	Display global subring settings.
`copy config running-config nvm profile Test`	Save the current settings in the configuration profile named `Test` in non-volatile memory (`nvm`).

13.11 Subring with LAG

⚠ WARNING

UNINTENDED EQUIPMENT OPERATION

To help avoid loops during the configuration phase, configure each device of the *Sub Ring* 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.

When at least two parallel redundant connecting lines exist (known as a trunk) between two devices, and these lines are combined into one logical connection, this is a Link Aggregation (LAG) connection.

The device lets you use the LAG ports as ring ports with the *Sub Ring* protocol.

13.11.1 Example

The following example is a simple setup between an MRP ring and a Subring.

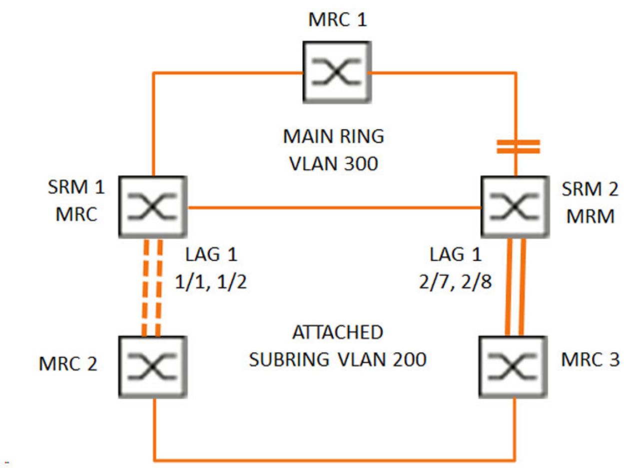


Figure 55: Subring with Link Aggregation

The following table describes the device roles as seen in the figure above. The table provides information of how you use the ring ports and Subring ports as LAG ports.

Table 38: Devices, Ports and Roles

Device Name	Ring Port	Main Ring Role	Sub Ring Role	Subring Port
MRC1	1/3, 1/4	MRP client	-	-
SRM1	1/3, 1/4	MRP client	Redundant Manager	lag/1
SRM2	2/4, 2/5	MRP manager	Manager	lag/1
MRC2	lag/1, 1/3	-	MRP client	-
MRC3	lag/1, 1/3	-	MRP client	-

MRP ring configuration

The devices participating in the Main ring are members of VLAN 300.

Perform the following steps:

`SRM2`

`enable`	Change to the Privileged EXEC mode.
`configure`	Change to the Configuration mode.
`mrp domain add default-domain`	Creates a new MRP domain with the ID `default-domain`.
`mrp domain modify port primary 2/4`	Specifies port *2/4* as ring port `1`.
`mrp domain modify port secondary 2/5`	Specifies port *2/5* as ring port `2`.
`mrp domain modify mode   manager`	Specifies that the device operates as the *Ring manager*. Do not activate the *Ring manager* function on any other device.
`mrp domain modify operation   enable`	Activates the MRP-Ring.
`mrp domain modify vlan 300`	Specifies the VLAN ID as `300`.
`mrp operation`	Enable the *MRP* function in the device.

`MRC1, SRM1`

`enable`	Change to the Privileged EXEC mode.
`configure`	Change to the Configuration mode.
`mrp domain add default-domain`	Creates a new MRP domain with the ID `default-domain`.
`mrp domain modify port primary 1/3`	Specifies port *1/3* as ring port `1`.
`mrp domain modify port secondary 1/4`	Specifies port *1/4* as ring port `2`.
`mrp domain modify mode client`	Specifies the device role as ring client.
`mrp domain modify operation   enable`	Activates the MRP-Ring.
`mrp domain modify vlan 300`	Specifies the VLAN ID as `300`.
`mrp operation`	Enable the *MRP* function in the device.

Subring configuration

The devices participating in the attached Sub-ring are members of VLAN 200.

Perform the following steps:

SRM1

`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-aggregation modify lag/1 adminmode`	Activate the Link Aggregation Group.

`enable`	Change to the Privileged EXEC mode.
`configure`	Change to the Configuration mode.
`sub-ring add 1`	Creates a new subring with the subring ID `1`.
`sub-ring modify 1 name SRM1`	Assign the name `SRM1` to the subring `1`.
`sub-ring modify 1 mode redundant-manager vlan 200 port lag/1`	Assign the device the role of `Sub-ring redundant manager`in subring `1`. If the subring is closed, then the device blocks the ring port. VLAN `200` is the set for the VLAN ID of the domain. The `lag/1` port is set as a member in VLAN `200`.
`sub-ring enable 1`	Activate subring `1`.
`sub-ring operation`	Enable the global Subring Manager functionality on this device.

SRM2

`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 2/7`	Adds port *2/7* to the Link Aggregation Group.
`link-aggregation modify lag/1 addport 2/8`	Adds port *2/8* to the Link Aggregation Group.
`link-aggregation modify lag/1 adminmode`	Activate the Link Aggregation Group.

`enable`	Change to the Privileged EXEC mode.
`configure`	Change to the Configuration mode.
`sub-ring add 1`	Creates a new subring with the subring ID `1`.
`sub-ring modify 1 mode manager vlan 200 port lag/1`	Assign the device the role of `Subring manager` in subring `1`. VLAN `200` is the set for the VLAN ID of the domain. The `lag/1` port is set as a member in VLAN `200`.

`sub-ring modify 1 name SRM2`	Assign the name `SRM2` to the subring `1`.
`sub-ring enable 1`	Activate subring `1`.
`sub-ring operation`	Enable the global Subring Manager functionality on this device.

`MRC 2, 3`

`enable`	Change to the Privileged EXEC mode.
`configure`	Change to the Configuration mode.
`mrp domain add default-domain`	Creates a new MRP domain with the ID `default-domain`.
`mrp domain modify port primary lag/1`	Specifies port `lag/1` as ring port `1`.
`mrp domain modify port secondary 1/3`	Specifies port *1/3* as ring port `2`.
`mrp domain modify mode client`	Specifies the device role as ring client.
`mrp domain modify operation enable`	Activates the MRP-Ring.
`mrp domain modify vlan 200`	Specifies the VLAN ID as `200`.
`mrp operation`	Enable the *MRP* function in the device.

Disable STP

Disable the *Spanning Tree* function on every port that you specified as an MRP or Sub-ring port. The following example uses port *1/3*.

Perform the following steps:

`enable`	Change to the Privileged EXEC mode.
`configure`	Change to the Configuration mode.
`interface 1/3`	Change to the interface configuration mode of interface *1/3*.
`no spanning-tree operation`	Disable the *Spanning Tree* function on the port.

13.12 Ring/Network Coupling

Based on a ring, the *Ring/Network Coupling* function couples rings or network segments redundantly. *Ring/Network Coupling* connects 2 rings/network segments through 2 separate paths.

When the devices in the coupled network are Schneider Electric devices, the *Ring/Network Coupling* function supports the coupling following ring protocols in the primary and secondary rings:
- HIPER Ring
- Fast HIPER Ring
- MRP

The *Ring/Network Coupling* function can also couple network segments of a bus and mesh structures.

13.12.1 Methods of Ring/Network Coupling

The One-Switch coupling

Two ports of **one** device in the first ring/network connect to one port each of two devices in the second ring/network (see figure 56). In the One-Switch coupling method, the main line forwards data and the device blocks the redundant line.

When the main line no longer functions, the device immediately unblocks the redundant line. When the main line is restored, the device blocks data on the redundant line. The main line forwards data again.

The ring coupling detects and handles an error within 500 ms (typically 150 ms).

The Two-Switch coupling

One port each from **two** devices in the first ring/network connect to one port each of two devices in the second ring/network segment (see figure 58).

The device in the redundant line and the device in the main line use control packets to inform each other about their operating states, using the Ethernet or a control line.

When the main line no longer functions, the redundant device (Stand-by) immediately unblocks the redundant line. As soon as the main line is restored, the device on the main line informs the redundant device of this. The Stand-by device blocks data on the redundant line. The main line forwards data again.

The ring coupling detects and handles an error within 500 ms (typically 150 ms).

The type of coupling configuration is primarily determined by the network topological and the desired level of availability (see table 39).

Table 39: Selection criteria for the configuration types for redundant coupling

	One-Switch coupling	**Two-Switch coupling**	**Two-Switch coupling with Control line**
Application	The 2 devices are in impractical topological positions. Therefore, putting a link between them would involve a lot of effort for two-Switch coupling.	The 2 devices are in practical topological positions. Installing a control line would involve a lot of effort.	The 2 devices are in practical topological positions. Installing a control line would not involve much effort.
Disadvantage	If the Switch configured for the redundant coupling becomes inoperable, then no connection remains between the networks.	More effort for connecting the 2 devices to the network (compared with one-Switch coupling).	More effort for connecting the two devices to the network (compared with one-Switch and two-Switch coupling).
Advantage	Less effort involved in connecting the 2 devices to the network (compared with two-Switch coupling).	When one of the devices configured for the redundant coupling becomes inoperable, the coupled networks are still connected.	When one of the devices configured for the redundant coupling becomes inoperable, the coupled networks are still connected. The partner determination between the coupling devices occurs more secure and faster than without the control line.

13.12.2 Prepare the Ring/Network Coupling

⚠ WARNING

UNINTENDED EQUIPMENT OPERATION

To help avoid loops during the configuration phase, configure each device of the *Ring/Network Coupling* configuration individually. Before you connect the redundant lines, complete the configuration of the other devices of the ring configuration.

To help avoid loops, use the *Ring/Network Coupling* function only on ports on which the Rapid Spanning Tree Protocol is inactive.

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

Using the images in the dialog you define the role of the devices within the *Ring/Network Coupling*.

In the following screen shots and diagrams, the following conventions are used:
- Blue boxes and lines indicate devices or connections of the items currently being described.
- Solid lines indicate a main connection.

- Dash lines indicate a stand-by connection.
- Dotted lines indicate the control line.

Perform the following steps:

- ☐ Open the *Switching > L2-Redundancy > Ring/Network Coupling* dialog.
- ☐ In the *Mode* frame, *Type* option list, select the required radio button.
  - `one-switch coupling`
  - `two-switch coupling, master`
  - `two-switch coupling, slave`
  - `two-switch coupling with control line, master`
  - `two-switch coupling with control line, slave`

One-Switch coupling

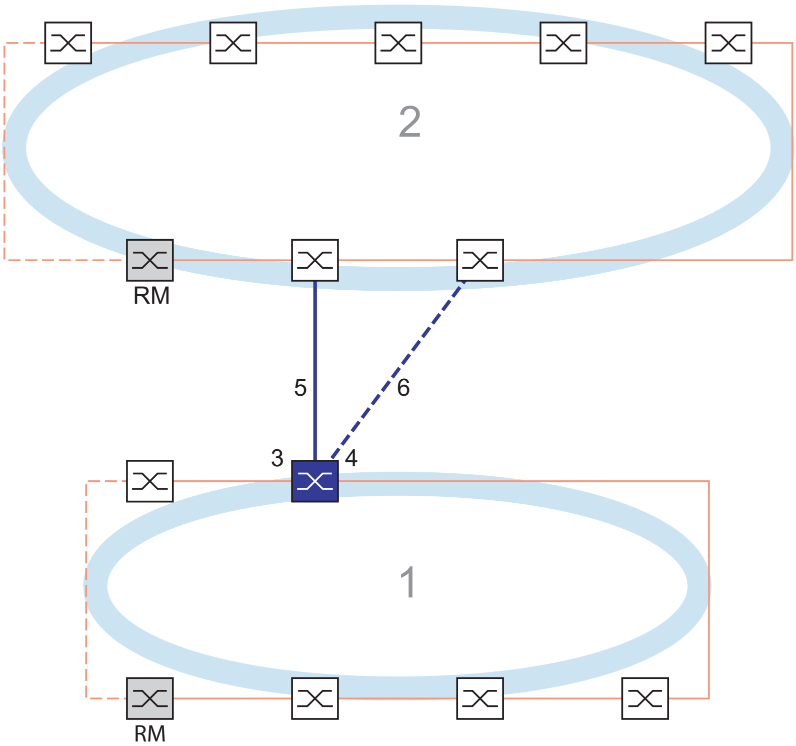


Figure 56: Example of One-Switch coupling
1: Ring
2: Backbone
3: Partner coupling port
4: Coupling port
5: Main line
6: Redundant line

The main line, indicated by the solid blue line, which is connected to the partner coupling port provides coupling between the two networks in the normal mode of operation. If the main line is inoperable, then the redundant line, indicated by the dashed blue line, which is connected to the coupling port takes over the ring/network coupling. **One** switch performs the coupling switch-over.

The following settings apply to the device displayed in blue in the selected graphic.

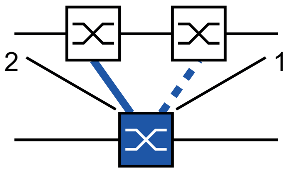


Figure 57: One-switch-coupling
1: Coupling port
2: Partner coupling port

Perform the following steps:

- ☐ Open the *Switching > L2-Redundancy > Ring/Network Coupling* dialog.
- ☐ In the *Mode* frame, *Type* option list, select the `one-switch coupling` radio button.

Note: Configure the *Partner coupling port* and the ring ports on different ports.

- ☐ In the *Coupling port* frame, select the port on which you connect the redundant line in the *Port* drop-down list.
- ☐ In the *Partner coupling port* frame, select the port on which you connect the main line in the *Port* drop-down list.
- ☐ To enable the function, select the *On* radio button in the *Operation* frame.
- ☐ Save the changes temporarily. To do this, click the ✓ button.
- ☐ Connect the redundant line to the Partner coupling port.
  In the *Partner coupling port* frame, the *State* field displays the status of the Partner coupling port.
- ☐ Connect the main line to the Coupling port.
  In the *Coupling port* frame, the *State* field displays the status of the Coupling port.

In the *Information* frame, the *Redundancy available* field displays if the redundancy is available.
The *Configuration failure* field displays if the settings are complete and correct.

For the coupling ports, perform the following steps:

Note: The following settings are required for the coupling ports.

- ☐ Open the *Basic Settings > Port* dialog, *Configuration* tab.
- ☐ For the ports selected as the coupling ports, specify the settings according to the parameters in the following table.
- ☐ Save the changes temporarily. To do this, click the ✓ button.

Table 40: Port settings for ring ports

Port type	Bit rate	Port on	Automatic configuration	Manual configuration
TX	100 Mbit/s	`marked`	`unmarked`	*`100 Mbit/s FDX`*
TX	1 Gbit/s	`marked`	`marked`	–
Optical	100 Mbit/s	`marked`	`unmarked`	*`100 Mbit/s FDX`*
Optical	1 Gbit/s	`marked`	`marked`	–
Optical	2.5 Gbit/s	`marked`	–	*`2.5 Gbit/s FDX`*

If you have configured VLANs on the coupling ports, then you specify the VLAN settings on the coupling and partner coupling ports. To do this, perform the following steps:

- ☐ Open the *Switching > VLAN > Port* dialog.
- ☐ Change the *Port-VLAN ID* setting to the value of the VLAN ID configured on the ports.
- ☐ Unmark the *Ingress filtering* checkbox for both coupling ports.
- ☐ Open the *Switching > VLAN > Configuration* dialog.
- ☐ To tag the redundant connections for `VLAN 1` and VLAN Membership, enter the value `T` in the cells corresponding to both coupling ports on the `VLAN 1` row.
- ☐ Save the changes temporarily. To do this, click the ✓ button.

The coupling devices send the redundancy packets with the highest priority on `VLAN 1`.

- ☐ In the *Configuration*frame, *Redundancy mode* option list, specify the type of redundancy:
  - ▶ With the *redundant ring/network coupling* setting, either the main line or the redundant line is active. The setting lets the devices toggle between both lines.
  - ▶ When you activate the *extended redundancy* setting, the main line and the redundant line are active simultaneously. The setting lets you add redundancy to the coupling network. When the connection between the coupling devices in the second network becomes inoperable the coupling devices continue to transmit and receive data.

Note: During the reconfiguration period, packet duplications can occur. Therefore, if your devices detect package duplications, then select this setting.

The *Coupling mode* describes the type of the backbone network to which you connect the ring network (see figure 56).

- ☐ In the *Configuration* frame, *Coupling mode* option list, specify the type of the second network:
  - ☐ If you connect to a ring network, then select the *ring coupling* radio button.
  - ☐ If you connect to a bus or mesh structure, then select the *network coupling* radio button.
- ☐ Save the changes temporarily. To do this, click the ✓ button.

Reset the coupling settings to the default state. To do this, perform the following steps:

- ☐ Click the ☰ button and then the *Reset* item.

Two-Switch coupling

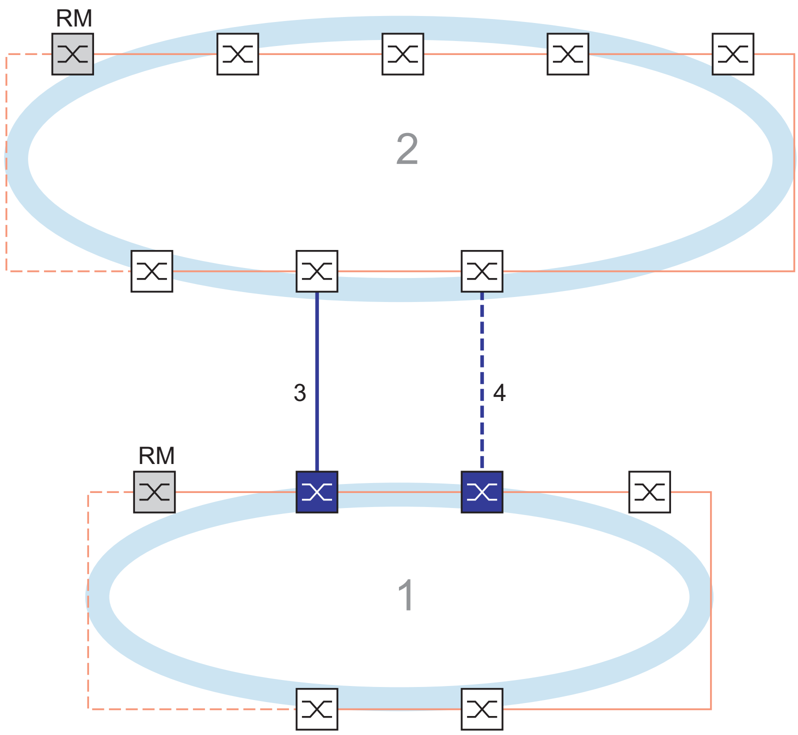


Figure 58: Example of Two-Switch coupling
1: Ring
2: Backbone
3: Main line
4: Redundant line

The coupling between 2 networks is performed by the main line, indicated by the solid blue line. If the main line or one of the adjacent devices becomes inoperable, then the redundant line, indicated by the dashed black line, takes over the network coupling. The coupling is performed by 2 devices.

The devices send control packages to each other over the Ethernet.

The primary device connected to the main line, and the stand-by device connected to the redundant line are partners with regard to the coupling.

- ☐ Connect the 2 partners using the ring ports.

Two-Switch coupling, Primary device

The following settings apply to the device displayed in blue in the selected graphic.

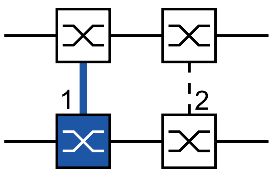


Figure 59: Two-Switch coupling, Primary device
1: Coupling port
2: Partner coupling port

Perform the following steps:

- ☐ Open the *Switching > L2-Redundancy > Ring/Network Coupling* dialog.
- ☐ In the *Mode* frame, *Type* option list, select the `two-switch coupling, master` radio button.
- ☐ In the *Coupling port* frame, select the port on which you connect the network segments in the *Port* drop-down list.
  Configure the *Coupling port* and the ring ports on different ports.
- ☐ To enable the function, select the *On* radio button in the *Operation* frame.
- ☐ Save the changes temporarily. To do this, click the ✓ button.
- ☐ Connect the main line to the *Coupling port*.
  In the *Coupling port* frame, the *State* field displays the status of the Coupling port.
  When the partner is already operating in the network, the *IP address* field in the *Partner coupling port* frame displays the IP address of the partner port.

In the *Information* frame, the *Redundancy available* field displays if the redundancy is available. The *Configuration failure* field displays if the settings are complete and correct.

Note: If you operate the *Ring manager* function and a two-switch coupling function on the same device, then there is the possibility of creating a loop.

To help prevent continuous loops while the connections are in operation on the ring coupling ports, perform one of the following actions. The device sets the port state of the coupling port to “off”:
- disable the operation
- change the configuration

For the coupling ports, perform the following steps:

- ☐ Open the *Basic Settings > Port* dialog, *Configuration* tab.
- ☐ For the ports selected as the coupling ports, specify the settings according to the parameters in the following table.
- ☐ Save the changes temporarily. To do this, click the ✓ button.

Table 41: Port settings for ring ports

Port type	Bit rate	Port on	Automatic configuration	Manual configuration
TX	100 Mbit/s	`marked`	`unmarked`	`100 Mbit/s FDX`
TX	1 Gbit/s	`marked`	`marked`	–
Optical	100 Mbit/s	`marked`	`unmarked`	`100 Mbit/s FDX`
Optical	1 Gbit/s	`marked`	`marked`	–
Optical	2.5 Gbit/s	`marked`	–	`2.5 Gbit/s FDX`

If you have configured VLANs on the coupling ports, then you specify the VLAN settings on the coupling and partner coupling ports. To do this, perform the following steps:

- ☐ Open the *Switching > VLAN > Port* dialog.
- ☐ Change the *Port-VLAN ID* setting to the value of the VLAN ID configured on the ports.
- ☐ Unmark the *Ingress filtering* checkbox for both coupling ports.
- ☐ Open the *Switching > VLAN > Configuration* dialog.

- To tag the redundant connections for `VLAN 1` and VLAN Membership, enter the value `T` in the cells corresponding to both coupling ports on the `VLAN 1` row.
- Save the changes temporarily. To do this, click the ✓ button.

The coupling devices send the redundancy packets with the highest priority on `VLAN 1`.

Two-Switch coupling, Stand-by device

The following settings apply to the device displayed in blue in the selected graphic.

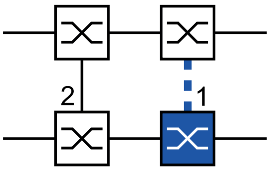


Figure 60: Two-Switch coupling, Stand-by device
1: Coupling port
2: Partner coupling port

Perform the following steps:

- Open the *Switching > L2-Redundancy > Ring/Network Coupling* dialog.
- In the *Mode* frame, *Type* option list, select the *`two-switch coupling, slave`* radio button.
- In the *Coupling port* frame, select the port on which you connect the network segments in the *Port* drop-down list.
  Configure the *Coupling port* and the ring ports on different ports.
- To enable the function, select the *On* radio button in the *Operation* frame.
- Save the changes temporarily. To do this, click the ✓ button.
- Connect the redundant line to the *Coupling port*.
  In the *Coupling port* frame, the *State* field displays the status of the Coupling port.
  When the partner is already operating in the network, the *IP address* field in the *Partner coupling port* frame displays the IP address of the partner port.

In the *Information* frame, the *Redundancy available* field displays if the redundancy is available.
The *Configuration failure* field displays if the settings are complete and correct.

Note: If you operate the *Ring manager* function and a two-switch coupling function on the same device, then there is the possibility of creating a loop.

To help prevent continuous loops while the connections are in operation on the ring coupling ports, perform one of the following actions. The device sets the port state of the coupling port to “off”:
- disable the operation
- change the configuration

For the coupling ports, perform the following steps:

- Open the *Basic Settings > Port* dialog, *Configuration* tab.
- For the ports selected as the coupling ports, specify the settings according to the parameters in the following table.
- Save the changes temporarily. To do this, click the ✓ button.

Table 42: Port settings for ring ports

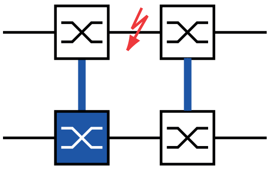
Port type	Bit rate	Port on	Automatic configuration	Manual configuration
TX	100 Mbit/s	`marked`	`unmarked`	*`100 Mbit/s FDX`*
TX	1 Gbit/s	`marked`	`marked`	–
Optical	100 Mbit/s	`marked`	`unmarked`	*`100 Mbit/s FDX`*
Optical	1 Gbit/s	`marked`	`marked`	–
Optical	2.5 Gbit/s	`marked`	–	*`2.5 Gbit/s FDX`*

If you have configured VLANs on the coupling ports, then you specify the VLAN settings on the coupling and partner coupling ports. To do this, perform the following steps:

- Open the *Switching > VLAN > Port* dialog.
- Change the *Port-VLAN ID* setting to the value of the VLAN ID configured on the ports.
- Unmark the *Ingress filtering* checkbox for both coupling ports.
- Open the *Switching > VLAN > Configuration* dialog.
- To tag the redundant connections for `VLAN 1` and VLAN Membership, enter the value `T` in the cells corresponding to both coupling ports on the `VLAN 1` row.
- Save the changes temporarily. To do this, click the ✓ button.

The coupling devices send the redundancy packets with the highest priority on `VLAN 1`.

Specify the *Redundancy mode* and *Coupling mode* settings. To do this, perform the following steps:

- Open the *Switching > L2-Redundancy > Ring/Network Coupling* dialog.
- In the *Configuration* frame, *Redundancy mode* option list, select one of the following radio buttons:
  - `redundant ring/network coupling`
    With this setting, either the main line or the redundant line is active. The setting lets the devices toggle between both lines.
  - `extended redundancy`
    With this setting, the main line and the redundant line are active simultaneously. The setting lets you add redundancy to the second network. When the connection between the coupling devices in the second network becomes inoperable, the coupling devices continue to transmit and receive data.
    
    During the reconfiguration period, packet duplications can occur. Therefore, select this setting only if your devices detect package duplications.
- In the *Configuration* frame, *Coupling mode* option list, select one of the following radio buttons:
  - If you connect to a ring network, then select the *ring coupling* radio button.
  - If you connect to a bus or mesh structure, then select the *network coupling* radio button.

  The *Coupling mode* describes the type of the backbone network to which you connect the ring network (see figure 58).
- Save the changes temporarily. To do this, click the ✓ button.

Reset the coupling settings to the default state. To do this, perform the following steps:

- Click the ☰ button and then the *Reset* item.

Two-Switch Coupling with Control Line

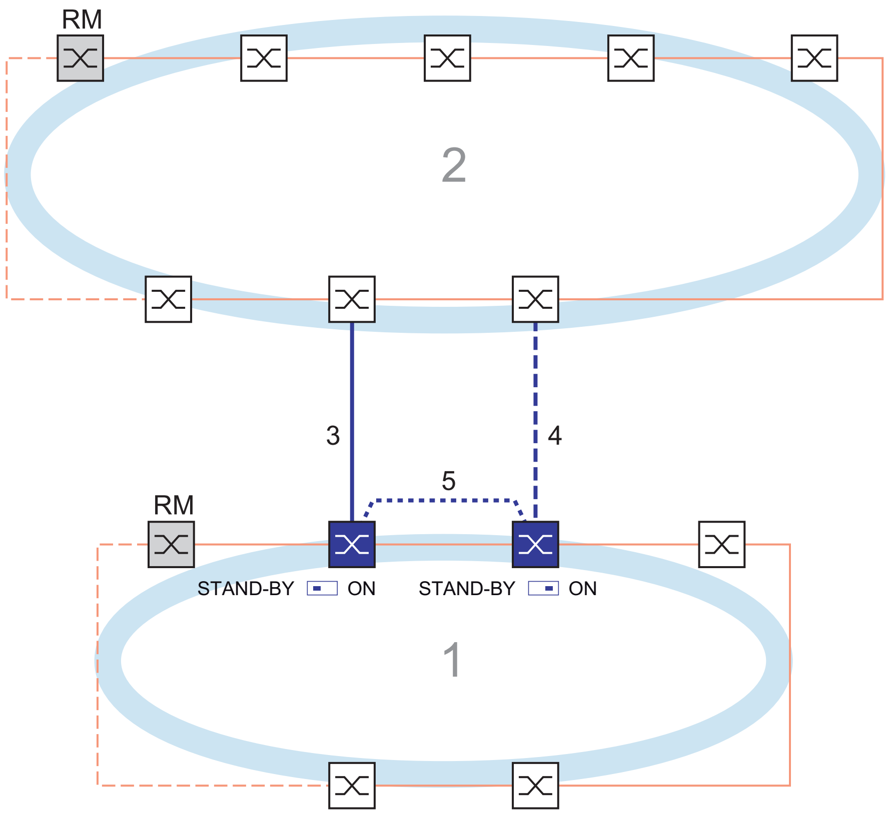


Figure 61: Example of Two-Switch coupling with control line
1: Ring
2: Backbone
3: Main line
4: Redundant line
5: Control line

The coupling between 2 networks is performed by the main line, indicated by the solid blue line. If the main line or one of the adjacent devices become inoperable, then the redundant line, indicated by the dashed blue line, takes over coupling the 2 networks. The ring coupling is performed by 2 devices.

The devices send control packets over a control line indicated by the dotted blue line in the figure below (see figure 62).

The primary device connected to the main line, and the stand-by device connected to the redundant line are partners with regard to the coupling.

- Connect the 2 partners using the ring ports.

Two-Switch coupling with Control Line, Primary device

The following settings apply to the device displayed in blue in the selected graphic.

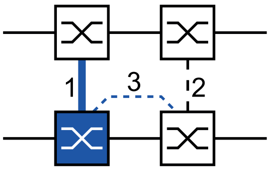


Figure 62: Two-Switch coupling with Control Line, Primary device
1: Coupling port
2: Partner coupling port
3: Control line

Perform the following steps:

- Open the *Switching > L2-Redundancy > Ring/Network Coupling* dialog.
- In the *Mode* frame, *Type* option list, select the `two-switch coupling with control line, master` radio button.
- In the *Coupling port* frame, select the port on which you connect the network segments in the *Port* drop-down list.
  Configure the *Coupling port* and the ring ports on different ports.
- In the *Control port* frame, select the port on which you connect the control line in the *Port* drop-down list.
  Configure the *Coupling port* and the ring ports on different ports.
- To enable the function, select the *On* radio button in the *Operation* frame.
- Save the changes temporarily. To do this, click the ✓ button.
- Connect the redundant line to the Coupling port.
  In the *Coupling port* frame, the *State* field displays the status of the Coupling port.
  When the partner is already operating in the network, the *IP address* field in the *Partner coupling port* frame displays the IP address of the partner port.
- Connect the control line to the Control port.
  In the *Control port* frame, the *State* field displays the status of the Control port.
  When the partner is already operating in the network, the *IP address* field in the *Partner coupling port* frame displays the IP address of the partner port.

In the *Information* frame, the *Redundancy available* field displays if the redundancy is available.
The *Configuration failure* field displays if the settings are complete and correct.

Note: If you operate the *Ring manager* function and a two-switch coupling function on the same device, then there is the possibility of creating a loop.

To help prevent continuous loops while the connections are in operation on the ring coupling ports, perform one of the following actions. The device sets the port state of the coupling port to “off”:

- disable the operation
- change the configuration

For the coupling ports, perform the following steps:

- ☐ Open the *Basic Settings > Port* dialog, *Configuration* tab.
- ☐ For the ports selected as the coupling ports, specify the settings according to the parameters in the following table.
- ☐ Save the changes temporarily. To do this, click the ✓ button.

Table 43: Port settings for ring ports

Port type	Bit rate	Port on	Automatic configuration	Manual configuration
TX	100 Mbit/s	`marked`	`unmarked`	*`100 Mbit/s FDX`*
TX	1 Gbit/s	`marked`	`marked`	–
Optical	100 Mbit/s	`marked`	`unmarked`	*`100 Mbit/s FDX`*
Optical	1 Gbit/s	`marked`	`marked`	–
Optical	2.5 Gbit/s	`marked`	–	*`2.5 Gbit/s FDX`*

If you have configured VLANs on the coupling ports, then you specify the VLAN settings on the coupling and partner coupling ports. To do this, perform the following steps:

- ☐ Open the *Switching > VLAN > Port* dialog.
- ☐ Change the *Port-VLAN ID* setting to the value of the VLAN ID configured on the ports.
- ☐ Unmark the *Ingress filtering* checkbox for both coupling ports.
- ☐ Open the *Switching > VLAN > Configuration* dialog.
- ☐ To tag the redundant connections for `VLAN 1` and VLAN Membership, enter the value `T` in the cells corresponding to both coupling ports on the `VLAN 1` row.
- ☐ Save the changes temporarily. To do this, click the ✓ button.

The coupling devices send the redundancy packets with the highest priority on `VLAN 1`.

Two-Switch coupling with Control Line, Stand-by device

The following settings apply to the device displayed in blue in the selected graphic.

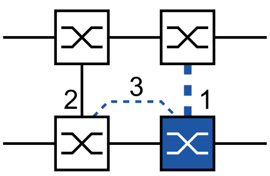


Figure 63: Two-Switch coupling with Control Line, Stand-by device
1: Coupling port
2: Partner coupling port
3: Control line

Perform the following steps:

- ☐ Open the *Switching > L2-Redundancy > Ring/Network Coupling* dialog.
- ☐ In the *Mode* frame, *Type* option list, select the `two-switch coupling with control line, slave` radio button.
- ☐ In the *Coupling port* frame, select the port on which you connect the network segments in the *Port* drop-down list.
  Configure the *Coupling port* and the ring ports on different ports.
- ☐ In the *Control port* frame, select the port on which you connect the control line in the *Port* drop-down list.
  Configure the *Coupling port* and the ring ports on different ports.
- ☐ To enable the function, select the *On* radio button in the *Operation* frame.
- ☐ Save the changes temporarily. To do this, click the ✓ button.
- ☐ Connect the redundant line to the Coupling port.
  In the *Coupling port* frame, the *State* field displays the status of the Coupling port.
  When the partner is already operating in the network, the *IP address* field in the *Partner coupling port* frame displays the IP address of the partner port.
- ☐ Connect the control line to the Control port.
  In the *Control port* frame, the *State* field displays the status of the Control port.
  When the partner is already operating in the network, the *IP address* field in the *Partner coupling port* frame displays the IP address of the partner port.

In the *Information* frame, the *Redundancy available* field displays if the redundancy is available.
The *Configuration failure* field displays if the settings are complete and correct.

Note: If you operate the *Ring manager* function and a two-switch coupling function on the same device, then there is the possibility of creating a loop.

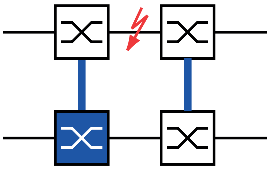
To help prevent continuous loops while the connections are in operation on the ring coupling ports, perform one of the following actions. The device sets the port state of the coupling port to “off”:
- disable the operation
- change the configuration

For the coupling ports, perform the following steps:

- ☐ Open the *Switching > VLAN > Port* dialog.
- ☐ Change the *Port-VLAN ID* setting to the value of the VLAN ID configured on the ports.
- ☐ Unmark the *Ingress filtering* checkbox for both coupling ports.
- ☐ Open the *Switching > VLAN > Configuration* dialog.
- ☐ To tag the redundant connections for `VLAN 1` and VLAN Membership, enter the value `T` in the cells corresponding to both coupling ports on the `VLAN 1` row.
- ☐ Save the changes temporarily. To do this, click the ✓ button.

The coupling devices send the redundancy packets with the highest priority on `VLAN 1`.

Specify the *Redundancy mode* and *Coupling mode* settings. To do this, perform the following steps:

- Open the *Switching > L2-Redundancy > Ring/Network Coupling* dialog.
- In the *Configuration* frame, *Redundancy mode* option list, select one of the following radio buttons:
  - `redundant ring/network coupling`
    With this setting, either the main line or the redundant line is active. The setting lets the devices toggle between both lines.
  - `extended redundancy`
    With this setting, the main line and the redundant line are active simultaneously. The setting lets you add redundancy to the second network. When the connection between the coupling devices in the second network becomes inoperable, the coupling devices continue to transmit and receive data.
    
    During the reconfiguration period, packet duplications can occur. Therefore, select this setting only if your devices detect package duplications.
- In the *Configuration* frame, *Coupling mode* option list, select one of the following radio buttons:
  - If you connect to a ring network, then select the *ring coupling* radio button.
  - If you connect to a bus or mesh structure, then select the *network coupling* radio button.

  The *Coupling mode* describes the type of the backbone network to which you connect the ring network (see figure 61).
- Save the changes temporarily. To do this, click the ✓ button.

Reset the coupling settings to the default state. To do this, perform the following steps:

- Click the ≡ button and then the *Reset* item.

13.13 RCP

Industrial applications require your networks to have high availability. This also involves maintaining deterministic, short interruption times for the communication in cases where a network device becomes inoperable.

A ring topology provides short transition times with a minimal use of resources. However, ring topology brings the challenge of coupling these rings together redundantly.

The Redundant Coupling Protocol *RCP* lets you couple rings that are operating with one of the following redundancy protocols:
- MRP
- HIPER ring
- RSTP

The *RCP* function also lets you couple multiple secondary rings to a primary ring (see figure 64). Only the switches which couple the rings require the *RCP* function.

You can also use devices other than Schneider Electric devices within the coupled networks.

The *RCP* function uses a master and a slave device to transport data between the networks. Only the master device forwards frames between the rings.

Using Schneider Electric proprietary multicast messages, the *RCP* master and slave devices inform each other about their operating state. Configure the devices in the ring which are not coupling devices to forward the following multicast addresses:
- `01:80:63:07:00:09`
- `01:80:63:07:00:0A`

Connect the master and slave devices as direct neighbors.

You use 4 ports per device to create the redundant coupling. Install the coupling devices with 2 inner and 2 outer ports in each network.
- The inner port connects the master and slave devices together.
- The outer port connects the devices to the network.

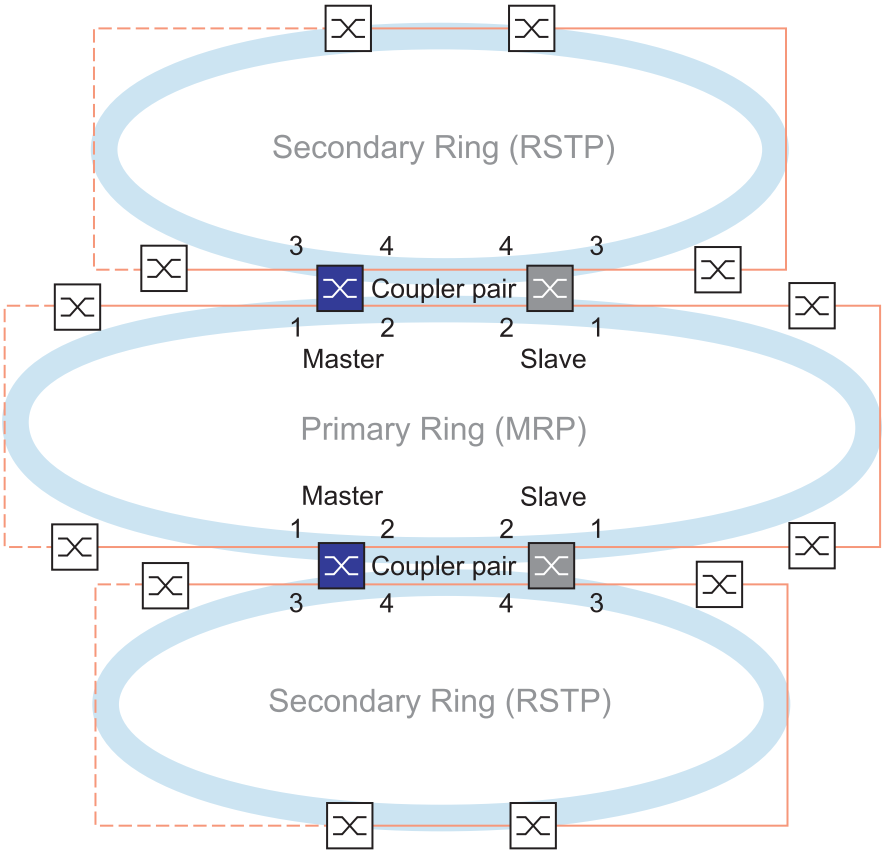


Figure 64: Example of a two-switch redundant coupling
1: Outer coupling port in the primary ring
2: Inner coupling port in the primary ring
3: Outer coupling port in the secondary ring
4: Inner coupling port in the secondary ring

When the role is set to the value *auto*, the coupler devices automatically selects its role as *master* or *slave*. When you want a permanent master or slave device, configure the roles manually.

Note: The `single` role is only used together with the *Dual RSTP* function. See “Coupling 2 RSTP rings using the Dual RSTP function” on page 248.

If the master is no longer reachable using the inner coupling ports, then the slave device waits for the timeout period to expire before taking over the master role. During the specified timeout period, the slave attempts to reach the master using the outer coupling ports. When the master is still not reachable, the slave assumes the master role. To maintain stability in the network connected to the outer coupling ports, configure the timeout period for a longer duration than the recovery time in the coupled rings.

Note: Disable RSTP on the *RCP* redundant coupling inner and outer ports not connected to the RSTP ring. In the example configuration, you disable RSTP on ports `1` and `2` of every device.

13.13.1 Application example for RCP coupling

> **⚠ WARNING**
>
> **UNINTENDED EQUIPMENT OPERATION**
>
> To help avoid loops during the configuration phase, configure each device of the *RCP* 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.**

The Schneider Electric devices support the two switch Redundant Coupling Protocol method. You can use the *RCP* function to provide a network installed in a train for example. The network provides information for the passengers about the train location or the different stops on the line. The network can also help provide passenger safety, for example using video surveillance.

The primary rings in the figure represent an *MRP* ring network within a car. The secondary rings in the figure are RSTP ring networks. Each ring contains 4 devices (see figure 65).

To simplify the train topology in the figure, the *MRP* ring ports and the *RCP* inner and outer ports are assigned the same port numbers. Specify the same values for the parameters of the ports according to their function in the network. For example, specify ports *1/1* and *1/2* on Switch 1D and 1C as MRP ring ports. Port *1/4* as an *RCP* inner port, and port *1/3* as an *RCP* outer port.

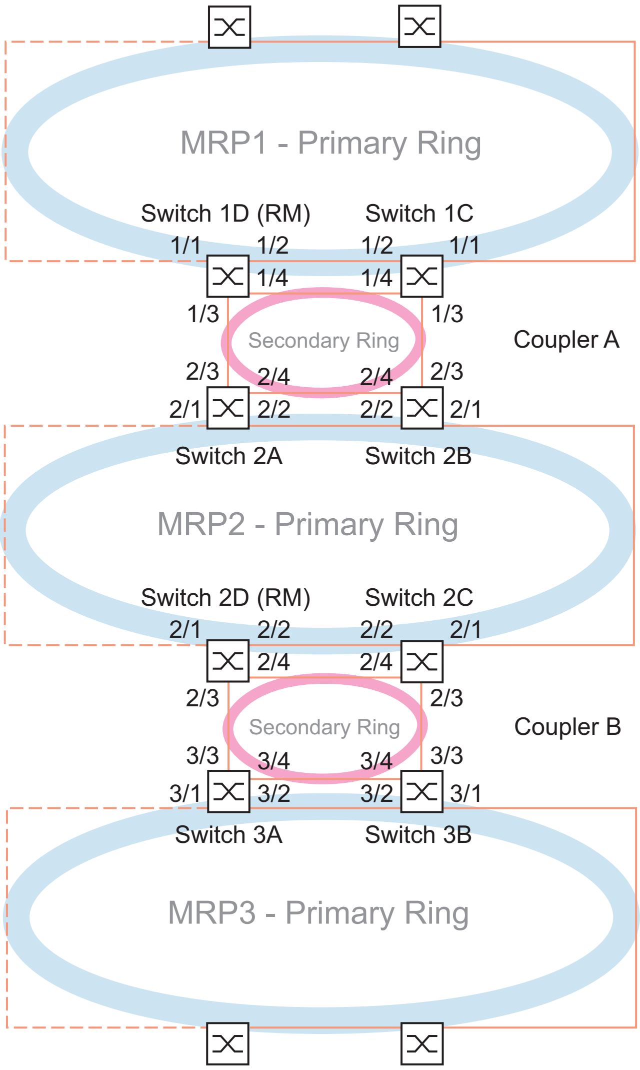


Figure 65: Redundant Coupling Protocol Train Topology

The following list specifies roles of the ports on each device.
1: ports 1 and 2 are MRP ring ports
2: port 3 is an RCP outer port
3: port 4 is an RCP inner port

The following steps describe how to specify the parameters for Switch 1D in Coupler A. Configure the other devices used for Coupler A and the devices used in Coupler B in the same manner.

Disable the RSTP function in the MRP Ring

MRP and RSTP do not work together. Therefore, deactivate the RSTP function on the *RCP* ports used in the *MRP* ring. In the example configuration, ports `x/1` and `x/2` are used for the *MRP* ring. Activate the RSTP function only on the *RCP* inner and outer ports used in the secondary ring. For example, activate the RSTP function on ports `x/3` and `x/4`.

Perform the following steps:

- ☐ Open the *Switching > L2-Redundancy > Spanning Tree > Port* dialog, *CIST* tab.
- ☐ In the default setting, the RSTP function is active on the ports. To deactivate the RSTP function on the *MRP* ring ports, unmark the *STP active* checkboxes for ports `x/1` and `x/2`.
- ☐ Open the *Switching > L2-Redundancy > Spanning Tree > 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.

`enable`	Change to the Privileged EXEC mode.
`configure`	Change to the Configuration mode.
`interface x/1`	Change to the interface configuration mode of interface `x/1`.
`no spanning-tree mode`	Disable the *Spanning Tree* function on the port.
`exit`	Change to the Configuration mode.
`interface x/2`	Change to the interface configuration mode of interface `x/2`.
`no spanning-tree mode`	Disable the *Spanning Tree* function on the port.
`exit`	Change to the Configuration mode.
`spanning-tree operation`	Enable the *Spanning Tree* function.

Specify the Ring Master in the MRP ring

In the figure, Switch D of each *MRP* ring is designated as the ring manger (see figure 65). Specify the other switches in the rings as ring clients.

Perform the following steps:

- ☐ Open the *Switching > L2-Redundancy > MRP* dialog.
- ☐ Specify the first ring port in the *Ring port 1* frame.
  In the *Port* drop-down list, select port `x/1`.
- ☐ Specify the second ring port in the *Ring port 2* frame.
  In the *Port* drop-down list, select port `x/2`.
- ☐ To designate the device as the Ring Manager, activate the function in the *Ring manager* frame.
- ☐ 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.
`mrp domain add default-domain`	Create a new *MRP* domain with the ID `default-domain`.
`mrp domain modify port primary x/1`	Specify port `x/1` as ring port `1`.
`mrp domain modify port secondary x/2`	Specify port `x/2` as ring port `2`.
`mrp domain modify mode manager`	Specify that the device operates as the *Ring manager*. For the other devices in the ring, leave the default setting.
`mrp domain modify operation enable`	Enable the *MRP* function.

Specify the devices in the redundant coupler

Perform the following steps:

- ☐ Open the *Switching > L2-Redundancy > RCP* dialog.
- ☐ Specify the *Inner port* in the *Primary ring/network* frame.
  Select port `x/2`.
- ☐ Specify the *Outer port* in the *Primary ring/network* frame.
  Select port `x/1`.
- ☐ Specify the *Inner port* in the *Secondary ring/network* frame.
  Select port `x/4`.
- ☐ Specify the *Outer port* in the *Secondary ring/network* frame.
  Select port `x/3`.

- ☐ 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.
`redundant-coupling port primary inner x/2`	Specify port `x/2` as the primary inner port.
`redundant-coupling port primary outer x/1`	Specify port `x/1` as the primary outer port.
`redundant-coupling port secondary inner x/4`	Specify port `x/4` as the secondary inner port.
`redundant-coupling port secondary outer x/3`	Specify port `x/3` as the secondary outer port.
`redundant-coupling operation`	Enable the *RCP* function in the device.
`copy config running-config nvm`	Save the current settings in the non-volatile memory (`nvm`) in the “selected” configuration profile.

13.13.2 Coupling 2 RSTP rings using the Dual RSTP function

If you want to use RSTP for the primary and secondary rings, then the *RCP* function assigns the ports of the secondary ring to the *Dual RSTP* instance. This creates two independent RSTP networks coupled by *RCP*.

You have the option of operating up to 16 MCSESM-E devices in a secondary ring. This includes the 2 devices of the primary ring that connect the secondary ring. When a network component becomes inoperable in the secondary ring, the *RCP* function can typically get a reconfiguration time of below 50 ms.

You also have the option of operating up to 16 MCSESM-E devices in a primary ring. Thus, the *RCP* and the *Dual RSTP* function can also typically get a reconfiguration time of below 50 ms in the primary ring. You can connect up to 8 secondary rings to a primary ring. Thus, you can connect up to 128 bridges (8 × 14 + 16). In this network, you can typically get an end-to-end reconfiguration time of below 50 ms with device redundancy.

When the requirements for the reconfiguration time in the primary ring are lower, you have the following options:
- Increase the number of bridges in the primary ring.
- Connect more secondary rings to the primary ring.

You can also use devices other than MCSESM-E in the rings, but only in cases where the devices update the RSTP topology changes fast enough. For example, when a network component becomes inoperable.

Properties of the primary and secondary ports of the instance

For ports of a primary or a secondary instance, consider the following notes:
- Only those ports of the *RCP* bridge that are configured as the outer or inner ring ports of the secondary ring belong to the *Dual RSTP* instance. The other ports belong to the primary instance of the bridge.
- You have the option to connect end devices or networks that do not run *Spanning Tree* to a port that implicitly belongs to a primary instance of the *RCP* bridge.
  These topologies provide neither device redundancy nor link redundancy.
- You have the option to make a meshed network in the primary or the secondary ring by establishing more links between ports of the same instance.
  In these topologies, a defined maximum end-to-end reconfiguration time of 50 ms does not apply.

Coupling 2 RSTP rings using only one RCP bridge

If you want to couple two RSTP rings using only one bridge, then use the `single` role.

If you want to couple 2 RSTP rings using only one bridge, then use the `single` role.

For the *RCP* bridge with the `single` role, the inner and outer ports have the same function. You can interchange the inner and outer ports of a specific instance.

When using one bridge to connect the rings, you can connect up to 16 secondary rings to a primary ring. This includes the *RCP* bridge that connects the rings. Thus, you can connect up to 256 bridges (16 × 15 + 16). In this network, you can get a maximum end-to-end reconfiguration time of 50 ms in a network with connection redundancy.

When the requirements for the reconfiguration time in the primary ring are lower, you have the following options:
- Increase the number of bridges in the primary ring.
- Connect more secondary rings to the primary ring.

Topology options for the Dual RSTP function

The following example shows the basic structure of a primary ring that is connected with 3 secondary rings. Secondary rings 1 and 2 are connected to the primary ring using 2 *RCP* bridges each, and secondary ring 3 with 1 *RCP* bridge. The path costs for every connection in a ring are assumed to be the same.

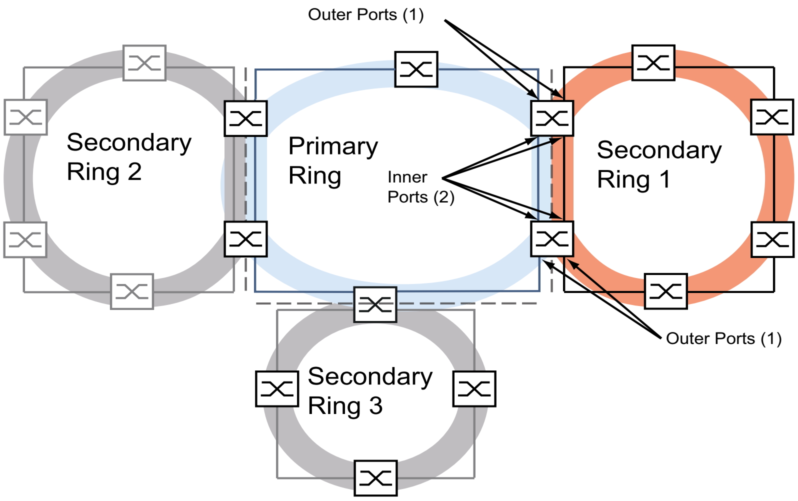


Figure 66: Primary ring with 3 secondary rings connected using RCP

Configuration of the primary ring

The following chapters describe the configuration in principle, and thus do not include work steps.

⚠ WARNING

UNINTENDED EQUIPMENT OPERATION

When performing an actual configuration, take steps to help avoid generating loops.

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

To specify the root bridge and the backup root bridge in the primary ring, configure their global RSTP bridge priorities. When the root bridge and the backup root bridge are opposite each other in the primary ring, you get an optimally short reconfiguration time in the primary ring. This is the case when the backup root bridge has 2 paths to the root bridge whose number of devices to the root bridge is different by a maximum of 1.

Configure the other bridges in the primary ring that are located between the root bridge and the backup root bridge so that the bridge priorities decrease (i.e. increase numerically) as their distance from the root bridge increases.

The figure shows an example with the RSTP details for the primary ring. The topology is reduced to the primary ring and one secondary ring. During the course of the configuration, the management station is connected to the primary ring in order to help avoid interruptions of the communication to the bridges in the secondary ring.

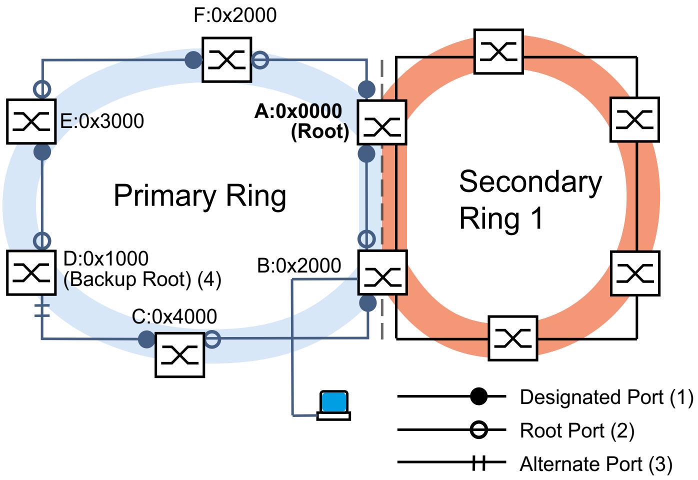


Figure 67: Primary ring with one connected secondary ring, with details for the primary ring
A..F: bridge identifiers
0x0000..0x4000: bridge priorities in the primary ring

Configuration of the secondary ring

To specify the root bridge and the backup root bridge in the secondary ring, configure the *Dual RSTP* bridge priority for the *RCP* bridges. For the other bridges in the secondary ring, only configure their global RSTP bridge priority. When the root bridge and the backup root bridge are opposite each other in the secondary ring, you get an optimally short reconfiguration time in the secondary ring.

Also configure the other bridges in the secondary ring so that the bridge priorities decrease (i.e. increase numerically) as their distance from the root bridge increases.

The figure shows an example with the RSTP details for the secondary ring.

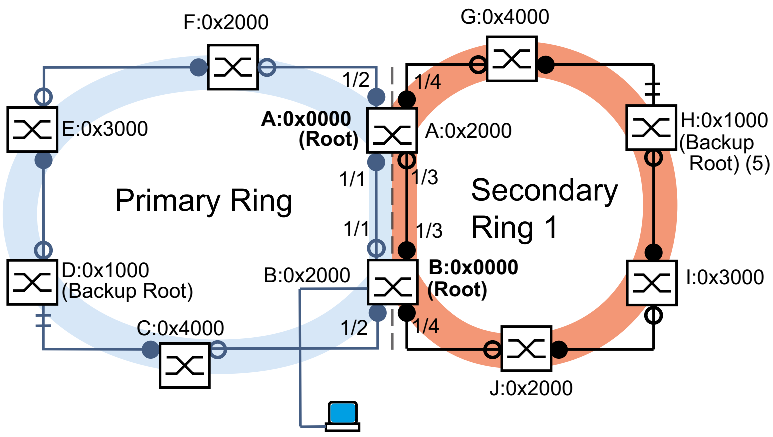


Figure 68: Primary ring with one connected secondary ring, with details for the secondary ring
A, B, G to J: bridge identifiers in the secondary ring
0x0000..0x4000: bridge priorities
for the bridges A and B: Dual RSTP bridge priority
for the bridges G to J: Global RSTP bridge priority
5: backup root bridge for secondary ring

The root bridge roles in the primary ring and in the secondary ring are independent of each other. A bridge can be the RSTP root for:
- Both rings
- One ring
- No ring

Operate the secondary ring only with RSTP.

Configuring the coupling of the rings

For the *RCP* bridges, define the inner and outer ports for both the primary and secondary rings.

Table 44: Ring ports for the RCP bridges

Ports	RCP master (B)	RCP slave (A)
Primary ring		
Inner port	1/1	1/1
Outer port	1/2	1/2
Secondary ring		
Inner port	1/3	1/3
Outer port	1/4	1/4

Afterwards, configure the role for each *RCP* bridge.

The figure shows an example.

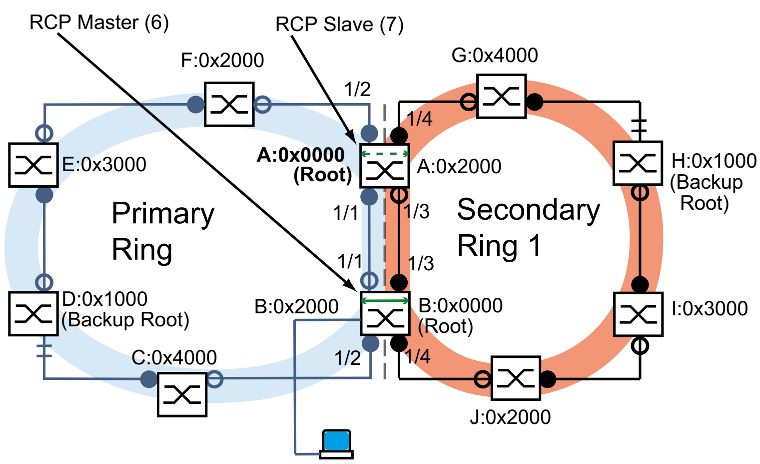


Figure 69: Primary ring with one connected secondary ring, with port numbers and RCP roles
6: RCP master
7: RCP slave

The root bridge roles and the coupling roles are independent of each other. A bridge can be *RCP* master and operate at the same time as the RSTP root for:
- Both rings
- One ring
- No ring

The same applies to the *RCP* slave.

Afterwards, enable the *RCP* function.

13.13.3 Application example for RCP coupling using Dual RSTP

In a production hall, there are multiple production cells. The devices in a production cell are connected in a line network structure. This network is connected to the higher-level network in the production hall. The network of the production hall is redundantly interconnected and works with RSTP. Every device is of the MCSESM-E type.

Your requirements:
- Set up the existing line network in the production cells with a fast device redundancy.
- Connect the production cells redundantly to the network of the production hall.
- Reconfigure the network of the production hall so that it helps provide deterministic, short reconfiguration times.

Existing network topology, reduced to one production cell:

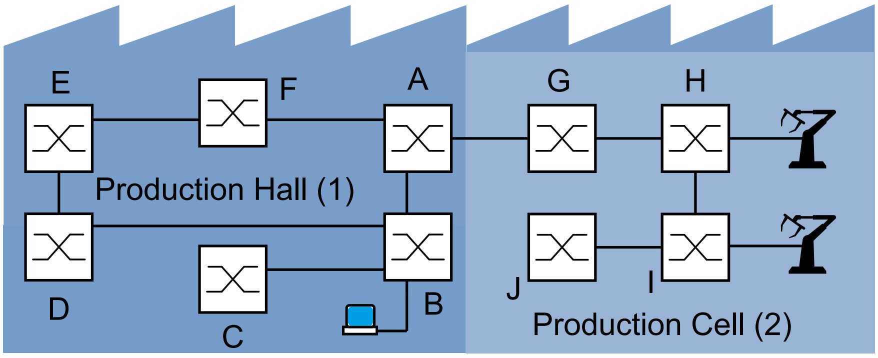


Figure 70: Example of a production cell in a production hall, topology before using the RCP and Dual RSTP function
1: production hall
2: production cell

Desired *Dual RSTP* network topology:

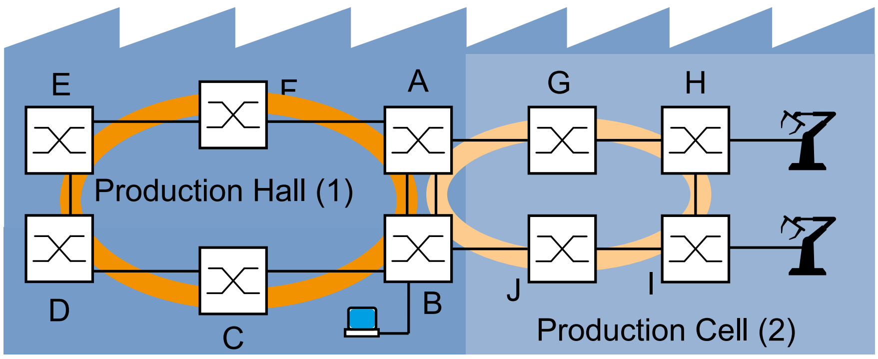


Figure 71: Example of a production cell in a production hall, topology when using the RCP and Dual RSTP function
1: production hall
2: production cell

Schematic representation of desired *Dual RSTP* network topology:

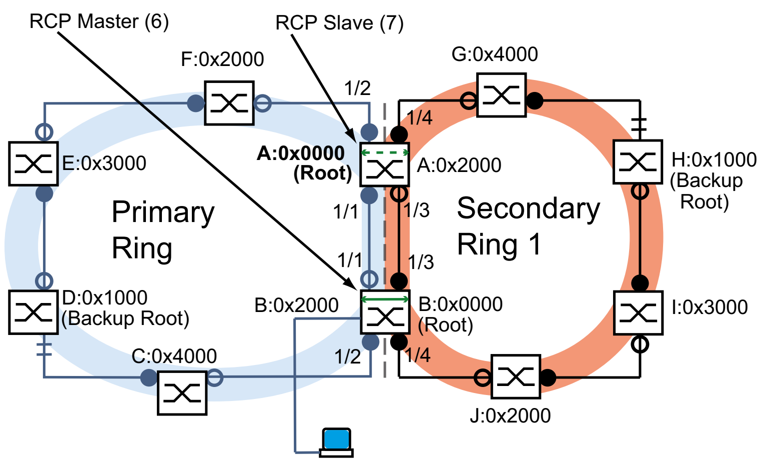


Figure 72: Schematic representation of Dual RSTP network topology
6: RCP master
7: RCP slave

The following table shows that a small number of settings are sufficient to configure the new topology. You only enter the *Dual RSTP* settings on devices A and B.

Table 45: Values for the configuration of the Switches of the Dual RSTP example

Parameter	A	B	C	D	E	F	G	H	I	J
RSTP settings										
Bridge priority (hex.)[1]	0x0000	0x2000	0x4000	0x1000	0x3000	0x2000	0x4000	0x1000	0x3000	0x2000
Dual RSTP settings										
Bridge priority (hex.)[a]	0x2000	0x0000	-	-	-	-	-	-	-	-
RCP settings										
Primary ring, inner port	1/1	1/1	-	-	-	-	-	-	-	-
Primary ring, outer port	1/2	1/2	-	-	-	-	-	-	-	-
Secondary ring, inner port	1/3	1/3	-	-	-	-	-	-	-	-
Secondary ring, outer port	1/4	1/4	-	-	-	-	-	-	-	-
Coupling role	Slave	Master	-	-	-	-	-	-	-	-

1. For the bridge priorities in hexadecimal and decimal notation, see table 46.

Table 46: Possible bridge priorities in hexadecimal and decimal notation

Bridge priority								
Hexadecimal	0x0000	0x1000	0x2000	0x3000	0x4000	0x5000	0x6000	0x7000
Decimal	0	4096	8192	12288	16384	20480	24576	28672

Table 46: Possible bridge priorities in hexadecimal and decimal notation

Bridge priority								
Hexadecimal	0x8000	0x9000	0xA000	0xB000	0xC000	0xD000	0xE000	0xF000
Decimal	32768	36864	40960	45056	49152	53248	57344	61440

Prerequisites for further configuration:
- The connection for the existing interconnection between bridges B and D is inactive, in the old topology, of the secondary ring. You can do this for example, by manually deactivating the corresponding ports on bridges B and D or by unplugging the link.
- The connections between bridges C and D and between bridges J and B are inactive. You can do this for example, by manually deactivating the corresponding ports on the bridges before plugging in the links.
- The connection for the secondary ring between bridges A and B is inactive.
- RSTP is active on every device and the parameters are in the state on delivery.
- Your management station is connected to the primary ring.
- You have opened the Graphical User Interface or the Command Line Interface for devices A and B.
- You have access to the user interfaces of devices C to J.

⚠ WARNING

LOOP HAZARD
- Configure each device of the *RCP* and *Dual RSTP* configuration individually. Before you connect the redundant lines, complete the configuration of the other devices of the ring configuration.
- Configure the timeout in the *RCP* coupling configuration longer than the longest assumable interruption time for the faster instance of the redundancy protocol.
- In a topology with 2 coupling bridges, configure the coupling roles of the two devices only as `master`, `slave` or `auto`.
- Couple the primary and the secondary instance only by means of 1 *RCP* bridge (for a topology with 1 *RCP* bridge) or by means of 2 *RCP* bridges (for a topology with 2 *RCP* bridges). Keep the ports of the primary instance separated from the ports of each secondary instance.
- Activate the *Admin edge port* setting on a port only in cases where a terminal device is connected to the port.

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

Configuring the global RSTP parameters of the RCP bridges

From the task specifications in table 45, you require the RSTP bridge priorities for bridge A and bridge B. The following table contains a summary of these values.

Table 47: RSTP bridge priorities for bridges A and B

RSTP parameter	A	B
Bridge priority (hex.)	0x0000	0x2000
Bridge priority (dec.)	0	8192

Note: The following instructions describe the configuration of the *RCP* bridges (A and B) in detail; those of the other bridges (C to J) only in abbreviated form.

Configure device A. To do this, perform the following steps:

- ☐ Open the *Switching > L2-Redundancy > Spanning Tree > Global* dialog.
- ☐ In the *Bridge configuration* frame, select the value `0` in the *Priority* drop-down list.
- ☐ 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 mst priority 0 0`	Set the RSTP bridge priority of MST instance `0` to the value `0`. The MST instance `0` is the global MST instance or the default instance.

Configure device B. To do this, perform the following steps:

- ☐ Open the *Switching > L2-Redundancy > Spanning Tree > Global* dialog.
- ☐ In the *Bridge configuration* frame, select the value `8192` in the *Priority* drop-down list.
- ☐ 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 mst priority 0 8192`	Set the RSTP bridge priority of the global MST instance to the value `8192`.

Configuring the global RSTP parameters of the other bridges

Now configure the other bridges. From the task specifications, you require the RSTP bridge priorities. The following table contains a summary of these values.

Table 48: RSTP bridge priorities for bridges C to J

RSTP parameter	C	D	E	F	G	H	I	J
Bridge priority (hex.)	0x4000	0x1000	0x3000	0x2000	0x4000	0x1000	0x3000	0x2000
Bridge priority (dec.)	16384	4096	12288	8192	16384	4096	12288	8192

Perform the following steps:

- ☐ Set the RSTP bridge priority of device C to `16384 (0x4000)` and activate the setting.
- ☐ Set the RSTP bridge priority of device D to `4096 (0x1000)` and activate the setting.
- ☐ Set the RSTP bridge priority of device E to `12288 (0x3000)` and activate the setting.
- ☐ Set the RSTP bridge priority of device F to `8192 (0x2000)` and activate the setting.
- ☐ Set the RSTP bridge priority of device G to `16384 (0x4000)` and activate the setting.
- ☐ Set the RSTP bridge priority of device H to `4096 (0x1000)` and activate the setting.
- ☐ Set the RSTP bridge priority of device I to `12288 (0x3000)` and activate the setting.
- ☐ Set the RSTP bridge priority of device J to `8192 (0x2000)` and activate the setting.

Configuring the Dual RSTP parameters of the RCP bridges

From the task specifications, you require the specific *Dual RSTP* parameters for bridges A and B. These are the *Dual RSTP* bridge priorities, the ring ports, and the coupling roles. The following tables contain a summary of these values.

Table 49: Dual RSTP parameters for bridges A and B

Dual RSTP parameter	A	B
Dual RSTP bridge priority (hex.)	`0x2000`	`0x0000`
Dual RSTP bridge priority (dec.)	`8192`	`0`

Table 50: RCP parameters for bridges A and B

Dual RSTP parameter	A	B
Primary ring, inner port	`1/1`	`1/1`
Primary ring, outer port	`1/2`	`1/2`
Secondary ring, inner port	`1/3`	`1/3`
Secondary ring, outer port	`1/4`	`1/4`
Coupling role	`Slave`	`Master`

Configure device A. To do this, perform the following steps:

- ☐ Open the *Switching > L2-Redundancy > FuseNet > RCP* dialog.
- ☐ In the *Primary ring/network* frame, select the value `1/1` in the *Inner port* drop-down list.
- ☐ In the *Primary ring/network* frame, select the value `1/2` in the *Outer port* drop-down list.
- ☐ In the *Secondary ring/network* frame, select the value `1/3` in the *Inner port* drop-down list.
- ☐ In the *Secondary ring/network* frame, select the value `1/4` in the *Outer port* drop-down list.
- ☐ In the *Coupler configuration* frame, select the value *`slave`* in the *Role* drop-down list.
- ☐ 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 *Switching > L2-Redundancy > Spanning Tree > Dual RSTP* dialog.
- ☐ In the *Bridge configuration* frame, select the value `8192` in the *Priority* drop-down list.
- ☐ Save the changes temporarily. To do this, click the ✓ button.

`spanning-tree drstp mst priority 0 8192`	Set the RSTP bridge priority of the *Dual RSTP* instance to the value `8192`.
`redundant-coupling port primary inner 1/1`	Select port *1/1* as the inner port for the *RCP* primary ring.
`redundant-coupling port primary outer 1/2`	Select port *1/2* as the outer port for the *RCP* primary ring.
`redundant-coupling port secondary inner 1/3`	Select port *1/3* as the inner port for the *RCP* secondary ring.
`redundant-coupling port secondary outer 1/4`	Select port *1/4* as the outer port for the *RCP* secondary ring.
`redundant-coupling role slave`	Configure this device as the *RCP* slave.
`exit`	Change to the Privileged EXEC mode.

Configure device B. To do this, perform the following steps:

- ☐ Open the *Switching > L2-Redundancy > FuseNet > RCP* dialog.
- ☐ In the *Primary ring/network* frame, select the value `1/1` in the *Inner port* drop-down list.
- ☐ In the *Primary ring/network* frame, select the value `1/2` in the *Outer port* drop-down list.
- ☐ In the *Secondary ring/network* frame, select the value `1/3` in the *Inner port* drop-down list.
- ☐ In the *Secondary ring/network* frame, select the value `1/4` in the *Outer port* drop-down list.
- ☐ In the *Coupler configuration* frame, select the value *`master`* in the *Role* drop-down list.
- ☐ 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 *Switching > L2-Redundancy > Spanning Tree > Dual RSTP* dialog.
- ☐ In the *Bridge configuration* frame, select the value `0` in the *Priority* drop-down list.
- ☐ Save the changes temporarily. To do this, click the ✓ button.

`spanning-tree drstp mst priority 0 0`	Set the RSTP bridge priority of the *Dual RSTP* instance to the value `0`.
`redundant-coupling port primary inner 1/1`	Select port *1/1* as the inner port for the *RCP* primary ring.
`redundant-coupling port primary outer 1/2`	Select port *1/2* as the outer port for the *RCP* primary ring.
`redundant-coupling port secondary inner 1/3`	Select port *1/3* as the inner port for the *RCP* secondary ring.
`redundant-coupling port secondary outer 1/4`	Select port *1/4* as the outer port for the *RCP* secondary ring.
`redundant-coupling role master`	Configure this device as the *RCP* master.
`exit`	Change to the Privileged EXEC mode.

Checking the configuration

Activate the new redundant connections:
- The connection of the inner ports for the secondary ring between device A, port *1/3* and device B, port *1/3*.
- The ring closure for the secondary ring between devices G and H.
- The ring closure for the primary ring between devices C and D.

Compare the current bridge roles in the primary ring with the necessary bridge roles:

Bridge A ought to be the root bridge.

Perform the following steps:

- ☐ Open the *Switching > L2-Redundancy > Spanning Tree > Global* dialog.
- ☐ In the *Topology information* frame, check the setting of the *Bridge is root* checkbox.

```
show spanning-tree global
Spanning Tree Information:
--------------------------
Spanning Tree Mode.........................RSTP
Spanning Tree Trap Mode....................enabled
Bridge is root.............................true
...
```

Compare the 4 ports that you configured as the inner and outer ports in the primary and secondary rings with the specifications in table 45.

Perform the following steps:

- ☐ Open the *Switching > L2-Redundancy > FuseNet > RCP* dialog.
- ☐ In the *Primary ring/network* and *Secondary ring/network* frames, check the displayed ports.

```
show redundant-coupling global
Redundant coupling protocol global settings
-------------------------------------------
RCP global state...........................enabled
RCP device configured role.................slave
RCP inner primary interface................1/1
RCP outer primary interface................1/2
RCP inner secondary interface..............1/3
RCP outer secondary interface..............1/4
RCP timeout................................45 milliseconds
```

Compare the current bridge roles in the secondary ring with the necessary bridge roles. Bridge B shall be the root bridge.

Perform the following steps:

- ☐ Open the *Switching > L2-Redundancy > Spanning Tree > Dual RSTP* dialog.
- ☐ In the *Topology information* frame, check the setting of the *Bridge is root* checkbox.

```
show spanning-tree drstp
Dual Spanning Tree Information:
-------------------------------
Spanning Tree Mode.........................RSTP
Spanning Tree Trap Mode....................enabled
Bridge is root.............................true
...
```

Compare the current port roles of the bridges in the primary ring with the necessary port roles:
- For the ports of bridge D that lead to bridge C:
  Role `alternate`
- For the other ports of the bridges that lead in the direction of root bridge A:
  Role `root`
- For the other ports of the bridges that lead in the direction of backup root bridge D:
  Role `designated`

Perform the following steps:

- ☐ Open the *Switching > L2-Redundancy > Spanning Tree > Port* dialog.
- ☐ In the *Port role* column, check the value `alternate`, `root` or `designated` as mentioned above.

```
show spanning-tree mst port 0 1/<port>
```

Compare the current port roles of the bridges in the secondary ring with the necessary port roles:
- For the ports of bridge H that lead to bridge G:
  Role `alternate`
- For the other ports of the bridges that lead in the direction of root bridge B:
  Role `root`
- For the other ports of the bridges that lead in the direction of backup root bridge H:
  Role `designated`

Perform the following steps:

- ☐ Open the *Switching > L2-Redundancy > Spanning Tree > Port* dialog.
- ☐ In the *Port role* column, check the value `alternate`, `root` or `designated` as mentioned above.

```
show spanning-tree mst port 0 1/<port>
```

If either the *RCP* or *Spanning Tree* function is disabled, then the device automatically disables the *Dual RSTP* function.

Check the status of the *Dual RSTP* function.

Perform the following steps:

- ☐ Open the *Switching > L2-Redundancy > Spanning Tree > Dual RSTP* dialog.
  In the *Operation* frame, the *Off* radio button is selected.

```
show redundant-coupling status
Redundant coupling protocol status
-------------------------------------------
RCP global state...........................forwarding
RCP device actual role.....................disabled
Redundancy state availability..............redNotAvailable
Primary ring protocol......................NONE
Secondary ring protocol....................NONE
```

Completing the configuration

For devices A to J, save the settings in the non-volatile memory. Follow the instructions in section “Saving a configuration profile” on page 97.

14 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
- Help protect against layer 2 network loops
- Reports
- Monitoring data traffic on a port (port mirroring)
- Syslog
- Event log
- Cause and action management during selftest

14.1 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.

14.1.1 List of SNMP traps

The following table displays possible SNMP traps sent by the device.

Table 51: Possible SNMP traps

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 current 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.

14.1.2 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.

14.1.3 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
- *Basic Settings > Power over Ethernet > Global* 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
- *Advanced > Digital IO Module* dialog

14.1.4 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.

14.2 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 current 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 Graphical User Interface
- query the device status in the Command Line Interface

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.

14.2.1 Events which can be monitored

Table 52: Device Status 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.

14.2.2 Configuring the Device Status

Perform the following steps:

- Open the *Diagnostics > Status Configuration > Device Status* dialog, *Global* tab.
- For the parameters to be monitored, mark 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 fault, 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, mark the checkbox in the *Monitor* column.
- ☐ Open the *Diagnostics > Status Configuration > Device Status* dialog, *Port* tab.
- ☐ For the *Propagate connection error* parameter, mark 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 Command Line Interface console. To display the help in Command Line Interface, insert a question mark `?` and press the <Enter> key.

14.2.3 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.

14.3 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 current 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 Graphical User Interface
- query the security status in the Command Line Interface

14.3.1 Events which can be monitored

Perform the following steps:
- ☐ Specify the events that the device monitors.
- ☐ For the corresponding parameter, mark the checkbox in the *Monitor* column.

Table 53: Security Status events

Name	Meaning
Password default settings unchanged	After installation change the passwords to increase security. When active and the default passwords remain unchanged, the device displays an alarm.
Min. password length < 8	Create passwords more than 8 characters long to maintain a high security posture. 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.
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 serial interface 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.

Table 53: *Security Status* events (cont

Name	Meaning
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.

14.3.2 Configuring the Security Status

Perform the following steps:

- Open the *Diagnostics > Status Configuration > Security Status* dialog, *Global* tab.
- For the parameters to be monitored, mark 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`	Monitors the password for the locally set up user accounts `user` and `admin`. When the password for the `user` or `admin` user accounts 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, mark 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, mark 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`.

14.3.3 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.

14.4 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.

14.4.1 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`.

14.4.2 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, mark 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 fault, 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.

Events which can be monitored

Table 54: Device Status 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 Graphical User Interface
- Query in the Command Line Interface

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 currently exists, the frame is highlighted.

`show signal-contact 1 all`	Displays signal contact settings for the specified signal contact.

14.5 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 current 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.

Table 55: Symbols identifying the status of the ports

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.

14.6 Port event counter

The port statistics table lets experienced network administrators identify possible detected problems 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.

Table 56: Examples indicating known weaknesses

Counter	Indication of known 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 fault 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.

14.6.1 Detecting non-matching duplex modes

Problems occur when 2 ports directly connected to each other have mismatching duplex modes. These problems are difficult to track down. The automatic detection and reporting of this situation has the benefit of recognizing mismatching duplex modes before problems 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 fault events. The meanings of terms used in the table are as follows:

- Collisions
  In half-duplex mode, collisions mean normal operation.

- Duplex problem
  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.

Table 57: Evaluation of non-matching of the duplex mode

No.	Automatic configuration	Current duplex mode	Detected error events (≥ 10 after link up)	Duplex modes	Possible causes
1	`marked`	Half duplex	None	OK	
2	`marked`	Half duplex	Collisions	OK	
3	`marked`	Half duplex	Late Collisions	Duplex problem detected	Duplex problem, EMI, network extension
4	`marked`	Half duplex	CRC Error	OK	EMI
5	`marked`	Full duplex	None	OK	
6	`marked`	Full duplex	Collisions	OK	EMI
7	`marked`	Full duplex	Late Collisions	OK	EMI
8	`marked`	Full duplex	CRC Error	OK	EMI
9	`unmarked`	Half duplex	None	OK	
10	`unmarked`	Half duplex	Collisions	OK	
11	`unmarked`	Half duplex	Late Collisions	Duplex problem detected	Duplex problem, EMI, network extension
12	`unmarked`	Half duplex	CRC Error	OK	EMI
13	`unmarked`	Full duplex	None	OK	
14	`unmarked`	Full duplex	Collisions	OK	EMI
15	`unmarked`	Full duplex	Late Collisions	OK	EMI
16	`unmarked`	Full duplex	CRC Error	Duplex problem detected	Duplex problem, EMI

14.7 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 blinks 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)
- *DHCP Snooping*
- *Dynamic ARP Inspection*
- *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, mark 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, highlight 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, mark 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.

14.8 Displaying the SFP status

The SFP status display lets you look at the current 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.

14.9 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
- System capabilities currently active
- 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.

14.9.1 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.

14.9.2 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

14.10 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 check if the device has detected a loop, perform the following steps:

- ☐ Open the *Switching > L2-Redundancy > Spanning Tree > Port* dialog, *CIST* tab.
- ☐ Check 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.
- ☐ Check the value in the *Loop state* column. If the field displays the value `true`, then the port is in a loop status.

14.11 Help protect against layer 2 network loops

The device helps protect against layer 2 network loops.

A network loop can lead to a standstill of the network due to overload. A possible reason is the continuous duplication of data packets due to a misconfiguration. The cause could be, for example, a poorly connected cable or an incorrect setting in the device.

For example, a layer 2 network loop can occur in the following cases, if no redundancy protocols are active:
- Two ports of the same device are directly connected to each other.
- More than one active connection is established between two devices.

⚠ WARNING

UNINTENDED EQUIPMENT OPERATION

To help avoid loops during the configuration phase, configure each device of the layer 2 network individually. Before you connect the redundant lines, complete the configuration of the other devices of the layer 2 network.

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

14.11.1 Application example

The figure displays examples for possible layer 2 loops in a network. The *Loop Protection* function is enabled in every device.

▶ **A**: *Active mode*
Ports that are intended to connect end devices operate in the *active* mode. The device evaluates and sends *loop detection* packets on these ports.

- **P**: *Passive mode*
  Ports which belong to the redundant rings operate in the *passive* mode. The device only evaluates *loop detection* packets on these ports.
- **Loop 1..Loop 4**
  Unintentionally configured layer 2 network loops.

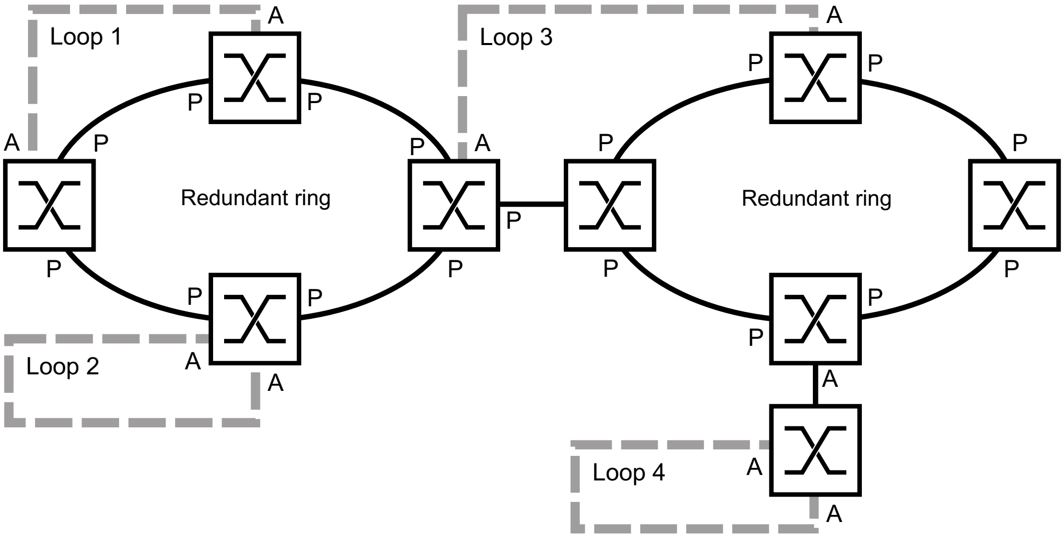


Figure 73: Examples for unintended layer 2 network loops

Assign the Loop Protection settings to the ports

For each *active* and each *passive* port, assign the settings of the *Loop Protection* function.

Perform the following steps:

- ☐ Open the *Diagnostics > Loop Protection* dialog.
- ☐ In the *Global* frame, *Transmit interval* field, adjust the value, if necessary.
- ☐ In the *Global* frame, *Receive threshold* field, adjust the value, if necessary.
- ☐ In the *Mode* column, specify the behavior of the *Loop Protection* function on the port:
  – `active` for ports that are intended to connect end devices
  – `passive` for ports which belong to the redundant rings
- ☐ In the *Action* column, specify the value *all*.
  When the device detects a layer 2 loop on this port, then it sends a trap and disables the port using the *Auto-Disable* function. If necessary, adjust the value.
- ☐ In the *Active* column, mark the checkbox.
- ☐ Save the changes temporarily. To do this, click the ✓ button.

`enable`	Change to the Privileged EXEC mode.
`configure`	Change to the Configuration mode.
`loop-protection tx-interval 5`	Specify the transmit interval, if necessary.
`loop-protection rx-threshold 1`	Specify the receive threshold, if necessary.
`interface 1/1`	Change to the Interface mode. Example: port *1/1*.

`loop-protection mode active`	Specify the mode `active` for ports that are intended to connect end devices.
`loop-protection mode passive`	Specify the mode `passive` for ports which belong to the redundant rings.
`loop-protection action all`	Specify the action that the device performs when it detects a layer 2 network loop on this port.
`loop-protection operation`	Activate the *Loop Protection* function on the port.
`exit`	Change to the Configuration mode.

Activate the Auto-Disable function

After you assigned the *Loop Protection* settings to the ports, activate the *Auto-Disable* function.

Perform the following steps:

- In the*Configuration* frame, mark the *Auto-disable* checkbox.
- Save the changes temporarily. To do this, click the ✓ button.

`loop-protection auto-disable`	Activate the *Auto-Disable* function.

Enable the Loop Protection function in the device

When finished, enable the *Loop Protection* function in the device.

Perform the following steps:

- In the*Operation* frame, select the *On* radio button.
- Save the changes temporarily. To do this, click the ✓ button.

`loop-protection operation`	Enable the *Loop Protection* function in the device.

14.11.2 Recommendations for redundant ports

Depending on the *Loop Protection* settings, the device disables ports using the *Auto-Disable* function when the device detects a layer 2 network loop.

If any redundancy function is active on a port, then do not activate the *active* mode on this port. Otherwise, port shutdowns on redundant network paths can be the result. In the example above these are the ports which belong to the redundant rings.

Verify that a redundant network path is available as backup media. The device changes to the redundant path in case of the outage of the primary path.

The following settings help avoid port shutdowns on redundant network paths:

- Disable the *Loop Protection* function on redundant ports.
  or
- Enable the *passive* mode on redundant ports.

The *Loop Protection* function and the *Spanning Tree* function have an effect on each other. The following steps help avoid unexpected behavior of the device:

- Disable the *Spanning Tree* function on the port on which you want to enable the *Loop Protection* function. See the *Switching > L2-Redundancy > Spanning Tree > Port* dialog, *STP active* column.
- Disable the*Spanning Tree* function on the connected port of each connected device. See the *Switching > L2-Redundancy > Spanning Tree* dialog.

14.12 Using the Email Notification function

The device lets you inform users by email about events that have occurred. Prerequisite is that a mail server is available through the network on which the device transfers the emails.

To set up the device to send emails, perform the steps in the following chapters:
- Specify the sender address
- Specify the triggering events
- Specify the recipients
- Specify the mail server
- Enable/disable the Email Notification function
- Send a test email

14.12.1 Specify the sender address

The sender address is the email address that indicates the device which sent the email. In the device, the default setting is .

Change the preset value. To do this, perform the following steps:

- Open the *Diagnostics > Email Notification > Global* dialog.
- In the *Sender* frame, change the value in the *Address* field.
  Add a valid email address.
- Save the changes temporarily. To do this, click the ✓ button.

`enable`	Change to the Privileged EXEC mode.
`configure`	Change to the Configuration mode.
`logging email from-addr <user@doma.in>`	Changes the sender address.

14.12.2 Specify the triggering events

The device differentiates between the following severities:

Table 58: Meaning of the severities for events

Severity	Meaning
`emergency`	Device not ready for operation
`alert`	Immediate user intervention required
`critical`	Critical status
`error`	Error status
`warning`	Warning
`notice`	Significant, normal status
`informational`	Informal message
`debug`	Debug message

You have the option of specifying the events of which the device informs you. For this, assign the desired minimum severity to the notification levels of the device.

The device informs the recipients as follows:
- *Notification immediate*
  When an event of the severity assigned or more severe occurs, the device sends an email immediately.
- *Notification periodic*
  – When an event of the severity assigned or more severe occurs, the device logs the event in a buffer.
  – The device sends an email with the log file periodically or if the buffer is full.
  – When an event of a lower severity occurs, the device does not log this event.

Perform the following steps:

- [ ] Open the *Diagnostics > Email Notification > Global* dialog.

In the *Notification immediate* frame, you specify the settings for emails which the device sends immediately.
- [ ] In the *Severity* field, you specify the minimum severity.
- [ ] In the *Subject* field, you specify the subject of the email.

In the *Notification periodic* frame, you specify the settings for emails which the device sends periodically.
- [ ] In the *Severity* field, you specify the minimum severity.
- [ ] In the *Subject* field, you specify the subject of the email.

- [ ] Save the changes temporarily. To do this, click the ✓ button.

`enable`	Change to the Privileged EXEC mode.
`configure`	Change to the Configuration mode.
`logging email severity immediate <level>`	Specifies the minimum severity for events for which the device sends an email immediately.
`logging email severity periodic <level>`	Specifies the minimum severity for events for which the device sends an email periodically.
`logging email subject add <immediate | periodic> TEXT`	Creates a subject line with the content `TEXT`.

14.12.3 Change the send interval

The device lets you specify in which interval it sends emails with the log file. The default setting is `30` minutes.

Perform the following steps:

- [ ] Open the *Diagnostics > Email Notification > Global* dialog.

In the *Notification periodic* frame, you specify the settings for emails which the device sends periodically.
- [ ] Change the value in the *Sending interval [min]* field to change the interval.

- [ ] Save the changes temporarily. To do this, click the ✓ button.

`enable`	Change to the Privileged EXEC mode.
`configure`	Change to the Configuration mode.
`logging email duration <30..1440>`	Specifies the interval at which the device sends emails with log file.

14.12.4 Specify the recipients

The device lets you specify up to 10 recipients.

Perform the following steps:

- Open the *Diagnostics > Email Notification > Recipients* dialog.
- To add a table entry, click the button.
- In the *Notification type* column, specify if the device sends the emails to this recipient immediately or periodically.
- In the *Address* column, specify the email address of the recipient.
- In the *Active* column, mark the checkbox.
- Save the changes temporarily. To do this, click the button.

`enable`	Change to the Privileged EXEC mode.
`configure`	Change to the Configuration mode.
`logging email to-addr add <1..10> addr <user@doma.in> msgtype <immediately | periodically>`	Specifies the recipient with the email address `user@doma.in`. The device manages the settings in memory `1..10`.

14.12.5 Specify the mail server

The device supports encrypted and unencrypted connections to the mail server.

Perform the following steps:

- Open the *Diagnostics > Email Notification > Mail Server* dialog.
- To add a table entry, click the button.
- In the *IP address* column, specify the IP address or the DNS name of the server.
- In the *Encryption* column, specify the protocol which encrypts the connection between the device and the mail server.
- When the mail server uses a port other than the well-known port, specify the TCP port in the *Destination TCP port* column.

When the mail server requests an authentication:
- In the *User name* and *Password* columns, specify the account credentials which the device uses to authenticate on the mail server.

- In the *Description* column, enter a meaningful name for the mail server.
- In the *Active* column, mark the checkbox.
- Save the changes temporarily. To do this, click the ✓ button.

`enable`	Change to the Privileged EXEC mode.
`configure`	Change to the Configuration mode.
`logging email mail-server add <1..5> addr <IP ADDRESS> [security <none|tlsv1>] [username <USER NAME>] [password <PASSWORD>] [port <1..65535>]`	Specifies the mail server with the IP address `IP ADDRESS`. The device manages the settings in memory `1..5`.

14.12.6 Enable/disable the Email Notification function

Perform the following steps:

- Open the *Diagnostics > Email Notification > 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.

`enable`	Change to the Privileged EXEC mode.
`configure`	Change to the Configuration mode.
`logging email operation`	Enables the sending of emails.
`no logging email operation`	Disables the sending of emails.

14.12.7 Send a test email

The device lets you check the settings by sending a test email.

Prerequisite:
- The email settings are completely specified.
- The *Email Notification* function is enabled.

Perform the following steps:

- Open the *Diagnostics > Email Notification > Mail Server* dialog.
- Click the ☰ button and then the *Connection test* item.
  The dialog displays the *Connection test* window.
- In the *Recipient* drop-down list, select to which recipients the device sends the test email.
- In the *Message text* field, specify the text of the test email.
- Click the *Ok* button to send the test email.

`enable`	Change to the Privileged EXEC mode.
`configure`	Change to the Configuration mode.
`logging email test msgtype <urgent|non-urgent> TEXT`	Sends an email with the content `TEXT` to the recipients.

When you do not see any detected error messages and the recipients obtain the email, the device settings are correct.

14.13 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 Command Line Interface 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.

14.13.1 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 Command Line Interface. 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 Command Line Interface, 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.

14.13.2 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 or *Hostname* of the Syslog server.
  You can specify a valid IPv4 or IPv6 address for the Syslog server.
- ☐ In the *Destination UDP port* column, specify the TCP or 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.
- ☐ Mark 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 host add 2 addr 2001::1 severity 4`	Add a new IPv6 recipient in the Syslog servers list. The value `4` means `warning`.
`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
2     2001::1        514   warning        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
```

14.13.3 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.

14.13.4 Syslog over TLS

The Transport Layer Security (TLS) is a cryptographic protocol designed to provide communications security over a computer network. The primary goal of the TLS protocol is to provide privacy and data integrity between two communicating computer applications.

After initiating a connection with a Syslog server, using a TLS handshake, the device validates the certificate received from the server. For this purpose, you transfer the PEM certificate from a remote server or from the external memory onto the device. Verify that the configured IP address or DNS name of the server matches the information provided in the certificate. You find the information in the Common Name or in the Subject Alternative Name fields of the certificate.

The device sends the TLS encrypted Syslog messages over the TCP port specified in the *Destination UDP port* column.

Note: Specify the IP address or DNS name on the server to match the IP Address or DNS name provided in the server certificate. You find the values entered in the certificate as the Common Name or the Subject Alternative Name.

Example

The given example describes the configuration of the *Syslog* function. By following these steps, the device lets you send the TLS encrypted Syslog messages over the TCP port specified in the *Destination UDP port* column.

The Syslog messages that are sent from a device to a syslog server can pass through unsecured networks. To configure a Syslog server over TLS, transfer the Certificate Authority (CA) certificate onto the device.

Note: In order for the changes to take effect after loading a new certificate, restart the *Syslog* function.

Perform the following steps:

- Open the *Diagnostics > Syslog* dialog.
- To initiate a connection with the Syslog servers, select the *On* radio button in the *Operation* frame.
- Save the changes temporarily. To do this, click the ✓ button.

The device validates the certificate received. The device also authenticates the server and starts sending Syslog messages.

- Transfer the PEM certificate from the remote server or from the external memory onto the device.

`enable`	Change to the Privileged EXEC mode.
`configure`	Change to the Configuration mode.
`logging host add 1 addr 192.168.3.215`	Add index `1` to the Syslog server with IPv4 address `192.168.3.215`.
`logging host add 2 addr 2001::1`	Add index `2` to the Syslog server with IPv6 address `2001::1.`
`logging host modify 1 port 6512 type systemlog`	Specifying the port number `6512` and logging the events in the system log.
`logging host modify 1 transport tls`	Specify the type of transmission as `tls`.
`logging host modify 1 severity informational`	Specifying the type of event to log into the system log as `informational`.
`exit`	Change to the Privileged EXEC mode.
`copy syslogcacert evmm`	Copy CA certificates from external memory to the device.
`show logging host`	Display the Syslog host settings.

14.13.5 Audit Trail

The *Diagnostics > Report > Audit Trail* dialog contains system information and changes to the device configuration performed through the Command Line Interface 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 Command Line Interface
- Command `logging audit-trail <string>` using the Command Line Interface 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 Command Line Interface
- Manual, user-initiated, logout
- Timed logout after a user-defined period of inactivity in the Command Line Interface
- 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 failures

14.14 Network analysis with TCPdump

Tcpdump is a packet-sniffing UNIX utility used by network administrators to sniff 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 in the device provides the possibility to decode or capture packets received and transmitted by the Management CPU. This function is available using the `debug` command. Refer to the “Command Line Interface” reference manual for further information about the TCPDump function.

14.15 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

14.15.1 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.

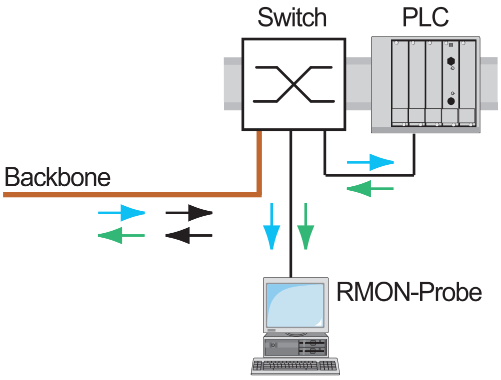


Figure 74: Example

On the destination port, the device only forwards the data packets copied from the source ports.

Before you switch on the *Port Mirroring* function, mark 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.

Enabling the Port Mirroring function

Perform the following steps:

- Open the *Diagnostics > Ports > Port Mirroring* dialog.
- Specify the source ports.
  Mark 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.
- When needed, specify a second destination port.
  In the *Destination port* frame, select the desired port in the *Secondary port* drop-down list.
  The prerequisite is that you have already specified the primary destination port.
- In order to access the device management via the destination port:
  In the *Destination port* frame, mark 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.

14.16 Self-test

The device checks its assets during the boot process and occasionally thereafter. The device checks system task availability or termination and the available amount of memory. Furthermore, the device checks 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 unmarked.
- The *Load default config on error* checkbox is unmarked.

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.

14.17 Copper cable test

Use this feature to test copper cables attached to an interface for a short or open circuit. The test interrupts traffic flow, when in progress, on this port.

The table displays the state and lengths of each individual pair. The device returns a result with the following meaning:

- normal - indicates that the cable is operating properly
- open - indicates an interruption in the cable
- short circuit - indicates a short circuit in the cable
- untested - indicates an untested cable
- Unknown - cable unplugged

15 Advanced functions of the device

15.1 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.

15.1.1 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.

15.1.2 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`.
- Mark the checkbox in the *Active* column.
- Open the *Advanced > DHCP Server > Global* dialog.
- For port `1/1`, mark 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.

15.1.3 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`.
- Mark the checkbox in the *Active* column.
- Open the *Advanced > DHCP Server > Global* dialog.
- For port `1/2`, mark 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.

15.2 DHCP L2 Relay

On the front panel of the device you find the following hazard message:

⚠ WARNING

UNINTENDED OPERATION

Do not change cable positions if DHCP Option 82 is enabled. Check the user manual before servicing.

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

A network administrator uses the DHCP Layer 2 *Relay Agent* to add DHCP client information. This information is required by Layer 3 *Relay Agents* and DHCP servers to assign an address and configuration to a client.

When a DHCP client and server are in the same IP subnet, they exchange IP address requests and replies directly. However, having a DHCP server on each subnet is expensive and often impractical. An alternative to having a DHCP server in every subnet is to use the network devices to relay packets between a DHCP client and a DHCP server located in a different subnet.

A Layer 3 *Relay Agent* is generally a router that has IP interfaces in both the client and server subnets and routes traffic between them. However, in Layer 2 switched networks, there are one or more network devices, switches for example, between the client and the Layer 3 *Relay Agent* or DHCP server. In this case, this device provides a Layer 2 *Relay Agent* to add the information that the Layer 3 *Relay Agent* and DHCP server require to perform their roles in address and configuration assignment.

The following list contains the default settings for this function:
- Global setting:
  - Active setting: disable
- Interface settings:
  - Active setting: disable
  - Trusted Port: disable
- VLAN settings:
  - Active setting: disable
  - *Circuit ID*: enable
  - *Remote ID* Type: mac
  - *Remote ID*: blank

For the DHCPv6 protocol, a *Relay Agent* is used to add *Relay Agent* options to DHCPv6 packets exchanged between a client and a DHCPv6 server. The Lightweight DHCPv6 Relay Agent (LDRA) is described in RFC 6221.

The LDRA processes 2 types of messages:

- The first type of message is the *Relay-Forward* message which contains unique information about the client.
- The second type of message is the *Relay-Reply* message which the DHCPv6 server sends to the *Relay Agent*. The *Relay Agent* then validates the message to include the information encapsulated in the initial *Relay-Forward* message and if valid, sends the packet to the client.

The *Relay-Forward* message contains *Interface-ID* information, also known as *Option 18*. This option provides information that identifies the interface on which the client request was sent. The device discards DHCPv6 packets that do not contain *Option 18* information.

15.2.1 Circuit and Remote IDs

In an IPv4 environment, before forwarding the request of a client to the DHCP server, the device adds the *Circuit ID* and the *Remote ID* to the *Option 82* field of the DHCP request packet.

- The *Circuit ID* stores on which port the device received the request of the client.
- The *Remote ID* contains the MAC address, the IP address, the system name, or a user-defined character string. Using it, the participating devices identify the *Relay Agent* that received the request of the client.

The device and other *Relay Agents* use this information to re-direct the answer from the DHCP *Relay Agent* to the original client. The DHCP server is able to analyze this data for example to assign the client an IP address from a specific address pool.

Also, the replay packet of the DHCP server contains the *Circuit ID* and the *Remote ID*. Before forwarding the answer to the client, the device removes the information from the *Option 82* field.

15.2.2 DHCP L2 Relay configuration

The *Advanced > DHCP L2 Relay > Configuration* dialog lets you activate the function on the active ports and on the VLANs. In the *Operation* frame, select the *On* radio button. Then click the ✓ button.

The device forwards DHCPv4 packets with *Option 82* information and DHCPv6 packets with *Option 18* information on those ports for which the checkbox in the *DHCP L2 Relay* column and in the *Trusted port* column is marked. Typically, these are ports in the network of the DHCP server.

The ports to which the DHCP clients are connected, you activate the *DHCP L2 Relay* function, but leave the *Trusted port* checkbox unmarked. On these ports, the device discards DHCPv4 packets with *Option 82* information and DHCPv6 packets with *Option 18* information.

An example configuration for the DHCPv4 L2 Relay function is shown below. The configuration steps for DHCPv6 L2 Relay function are similar, except for the *Circuit ID* and *Remote ID* entries that can only be specified for *Option 82*.

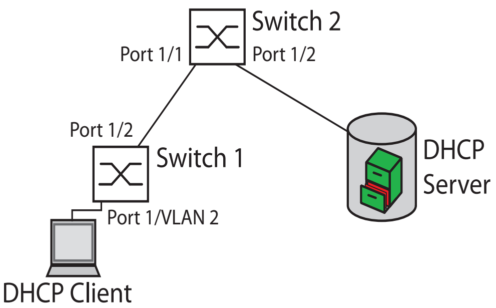


Figure 75: DHCP Layer 2 Example Network

Perform the following steps on Switch 1:

- Open the *Advanced > DHCP L2 Relay > Configuration* dialog, *Interface* tab.
- For port `1/1`, specify the settings as follows:
  – Mark the checkbox in the *Active* column.
- For port `1/2`, specify the settings as follows:
  – Mark the checkbox in the *Active* column.
  – Mark the checkbox in the *Trusted port* column.
- Open the *Advanced > DHCP L2 Relay > Configuration* dialog, *VLAN ID* tab.
- Specify the settings for VLAN 2 as follows:
  – Mark the checkbox in the *Active* column.
  – Mark the checkbox in the *Circuit ID* column.
  – To use the IP address of the device as the *Remote ID*, in the *Remote ID type* column, specify the value `ip`.
- To enable the function, select the `On` radio button in the *Operation* frame.
- Save the changes temporarily. To do this, click the ✓ button.

Perform the following steps on Switch 2:

- Open the *Advanced > DHCP L2 Relay > Configuration* dialog, *Interface* tab.
- For port `1/1` and `1/2`, specify the settings as follows:
  – Mark the checkbox in the *Active* column.
  – Mark the checkbox in the *Trusted port* column.
- To enable the function, select the `On` radio button in the *Operation* frame.
- Save the changes temporarily. To do this, click the ✓ button.

Verify that VLAN 2 is present. Then perform the following steps on Switch 1:
- Configure VLAN 2, and specify port `1/1` as a member of VLAN 2.

`enable`	Change to the Privileged EXEC mode.
`vlan database`	Change to the VLAN configuration mode.
`dhcp-l2relay circuit-id 2`	Activate the Circuit ID and the DHCP Option 82 on VLAN `2`.
`dhcp-l2relay remote-id ip 2`	Specify the IP address of the device as the Remote ID on VLAN `2`.

`dhcp-l2relay mode 2`	Activate the *DHCP L2 Relay* function on VLAN `2`.
`exit`	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`.
`dhcp-l2relay mode`	Activate the *DHCP L2 Relay* function on the port.
`exit`	Change to the Configuration mode.
`interface 1/2`	Change to the interface configuration mode of interface `1/2`.
`dhcp-l2relay trust`	Specify the port as *Trusted port*.
`dhcp-l2relay mode`	Activate the *DHCP L2 Relay* function on the port.
`exit`	Change to the Configuration mode.
`dhcp-l2relay mode`	Enable the *DHCP L2 Relay* function in the device.

Perform the following steps on Switch 2:

`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`.
`dhcp-l2relay trust`	Specify the port as *Trusted port*.
`dhcp-l2relay mode`	Activate the *DHCP L2 Relay* function on the port.
`exit`	Change to the Configuration mode.
`interface 1/2`	Change to the interface configuration mode of interface `1/2`.
`dhcp-l2relay trust`	Specify the port as *Trusted port*.
`dhcp-l2relay mode`	Activate the *DHCP L2 Relay* function on the port.
`exit`	Change to the Configuration mode.
`dhcp-l2relay mode`	Enable the *DHCP L2 Relay* function in the device.

15.3 Using the device as a DNS client

The Domain Name System (DNS) client queries DNS servers to resolve host names and IP addresses of network devices. Much like a telephone book, the DNS client converts names of devices into IP addresses. When the DNS client receives a request to resolve a new name, the DNS client first queries its internal static database, then the assigned DNS servers for the information. The DNS client saves the queried information in a cache for future requests.

The device lets you configure the DNS client from the DHCP server using the device management VLAN. The device also lets you assign host names to IP addresses statically.

The DNS client provides the following user functions:
- DNS server list, with space for 4 domain name server IP addresses
- static hostname to IP address mapping, with space for 64 configurable static hosts
- host cache, with space for 128 entries

15.3.1 Configuring a DNS server example

Name the DNS client and configure it to query a DNS server to resolve host names. To do this, perform the following steps:

- ☐ Open the *Advanced > DNS > Client > Static* dialog.
- ☐ In the *Configuration* frame, *Configuration source* field, specify the value `user`.
- ☐ In the *Configuration* frame, *Domain name* field, specify the value `device1`.
- ☐ To add a table entry, click the button.
- ☐ In the *Address* column, specify the value `192.168.3.5` as the IPv4 address of the DNS server. You can also specify a valid IPv6 address as the IP address of the DNS server.
- ☐ Mark the checkbox in the *Active* column.
- ☐ Open the *Advanced > DNS > Client > 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.

`enable`	Change to the Privileged EXEC mode.
`configure`	Change to the Configuration mode.
`dns client source user`	Specifying that the user manually configures the DNS client settings.
`dns client domain-name device1`	Specifying the string `device1` as a unique domain name for the device.
`dns client servers add 1 ip 192.168.3.5`	To add a DNS name server with an IPv4 address of `192.168.3.5` as index `1`.
`dns client servers add 2 ip 2001::1`	Add a DNS server with an IPv6 address of `2001::1` as index `2`.
`dns client adminstate`	Enable the *DNS Client* function globally.

Configure the DNS client to map static hosts with IP addresses. To do this, perform the following steps:

- Open the *Advanced > DNS > Client > Static Hosts* dialog.
- To add a table entry, click the button.
- In the *Name* column, enter the value `example.com`.
  This is a name of a device in the network.
- In the *IP address* column, specify the value `192.168.3.9`.
- Mark 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.
`dns client host add 1 name example.com ip 192.168.3.9`	Add `example.com` as a static host with an IP address of `192.168.3.9`.
`dns client adminstate`	Enable the *DNS Client* function globally.

15.4 GARP

The Generic Attribute Registration Protocol (*GARP*) is defined by the IEEE to provide a generic framework so switches can register and deregister attribute values, such as VLAN identifiers and Multicast group membership.

If an attribute for a participant is registered or deregistered according to the *GARP* function, then the participant is modified according to specific rules. The participants are a set of reachable end stations and network devices. The defined set of participants at any given time, along with their attributes, is the reachability tree for the subset of the network topology. The device forwards the data frames only to the registered end stations. The station registration helps prevent attempts to send data to the end stations that are unreachable.

15.4.1 Configuring GMRP

The GARP Multicast Registration Protocol (*GMRP*) is a Generic Attribute Registration Protocol (*GARP*) that provides a mechanism allowing network devices and end stations to dynamically register group membership. The devices register group membership information with the devices attached to the same LAN segment. The *GARP* function also lets the devices disseminate the information across the network devices that support extended filtering services.

Note: Before you enable the *GMRP* function, verify that the *MMRP* function is disabled.

The following example describes the configuration of the *GMRP* function. The device provides a constrained multicast flooding facility on a selected port. To do this, perform the following steps:

- ☐ Open the *Switching > GARP > GMRP* dialog.
- ☐ To provide constrained Multicast Flooding on a port, mark the checkbox in the *GMRP 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.
`interface 1/1`	Change to the interface configuration mode of interface `1/1`.
`garp gmrp operation`	Enabling the *GMRP* function on the port.
`exit`	Change to the Configuration mode.
`garp gmrp operation`	Enabling the *GMRP* function globally.

15.4.2 Configuring GVRP

You use the *GVRP* function to allow the device to exchange VLAN configuration information with other *GVRP* devices. Thus reducing unnecessary Broadcast and unknown Unicast traffic. Besides the *GVRP* function dynamically creates and manages VLANs on devices connected through 802.1Q trunk ports.

The following example describes the configuration of the *GVRP* function. The device lets you exchange VLAN configuration information with other *GVRP* devices. To do this, perform the following steps:

- ☐ Open the *Switching > GARP > GVRP* dialog.
- ☐ To exchange VLAN configuration information with other *GVRP* devices, mark checkbox in the *GVRP active* column for the 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 3/1`	Change to the interface configuration mode of interface `3/1`.
`garp gvrp operation`	Enabling the *GVRP* function on the port.
`exit`	Change to the Configuration mode.
`garp gvrp operation`	Enabling the *GVRP* function globally.

15.5 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.

15.5.1 MRP operation

Each participant contains an applicant component and an MRP Attribute Declaration (MAD) component. The applicant component is responsible for forming 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.

15.5.2 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.

15.5.3 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.

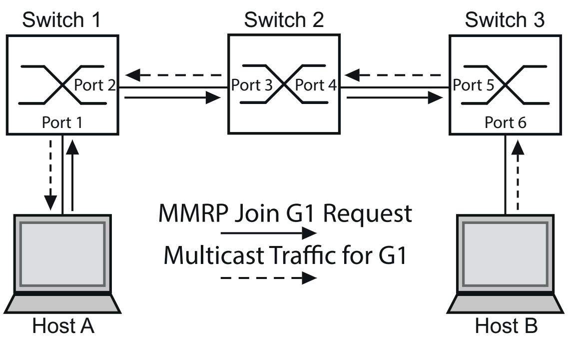


Figure 76: MMRP Network for MAC address Registration

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, mark 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, mark 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, mark 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.

15.5.4 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.

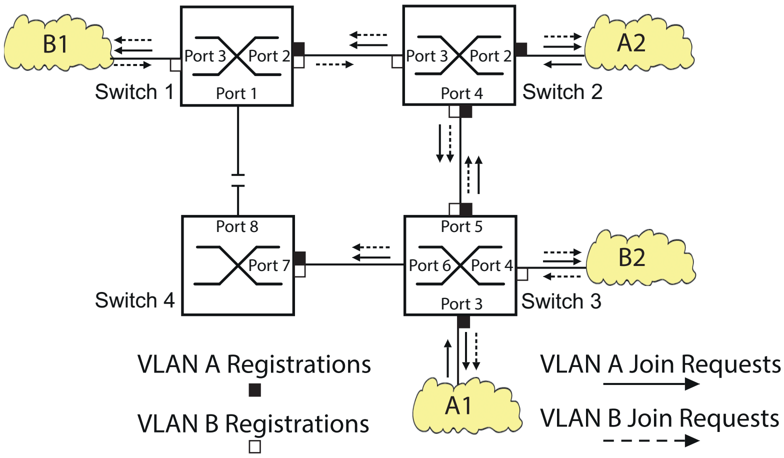


Figure 77: MVRP Example Network for VLAN Registration

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, mark 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, mark 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, mark 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, mark 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.

16 Industry Protocols

16.1 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.

16.1.1 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.

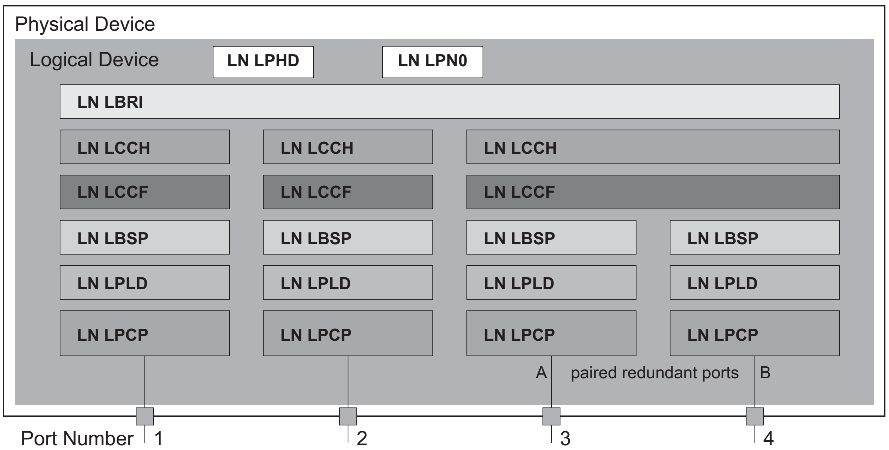


Figure 78: Bridge model based on Technical Report IEC 61850 90-4

Table 59: Classes of the bridge model based on TR IEC61850 90-4

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.
`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.

16.1.2 Integration into a Control System

Preparation of the device

Perform the following steps:
- ☐ Check 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 to failures 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, mark the *Write access* checkbox, and click the ✓ button.

Offline configuration

The device lets you download the ICD file using the Graphical User Interface. 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:

Table 60: Statuses of the device that can be monitored with IEC 61850/MMS

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.

Table 60: Statuses of the device that can be monitored with IEC 61850/MMS (cont

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.

16.2 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.

16.2.1 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.

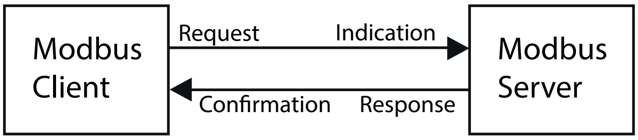


Figure 79: Client/Server Modbus TCP/IP Mode

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.

16.2.2 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 failure 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 table below lists addresses that allow the client to reset port counters and retrieve specific information from the device registers.

Port Information

Table 61: 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
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

Table 62: Port Statistics

Address	Qty	Description	MIn	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
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

16.2.3 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 to potential issues 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 marked.
- ☐ Activate the IP address range. To do this, mark 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 marked.
- ☐ 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]
```

16.3 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.

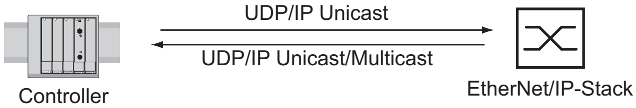


Figure 80: EtherNet/IP network

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.

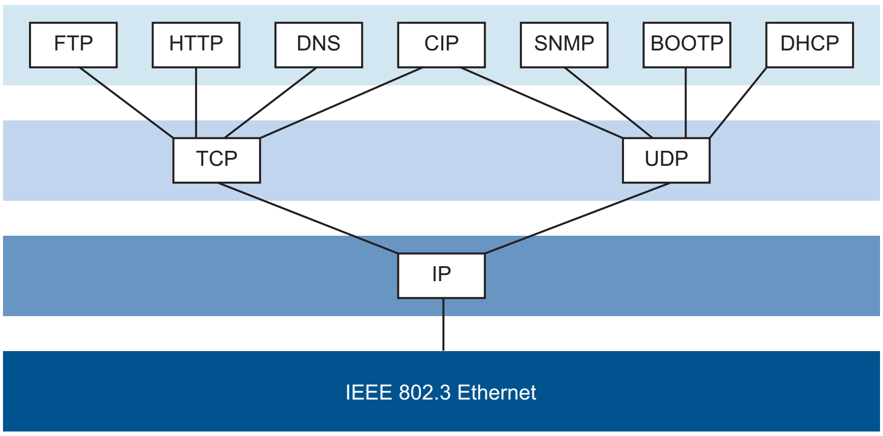


Figure 81: IEEE802.3 EtherNet/IP

For detailed information on *EtherNet/IP*, see the ODVA website at www.odva.org.

16.3.1 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.

16.3.2 EtherNet/IP Entity Parameters

The following paragraphs identify the objects and operations supported by the device.

Supported operations

Table 63: Overview of the supported EtherNet/IP requests for the objects instances

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".

Table 64: Instance attributes (only instance 1 is available)

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:	Revision of the EtherNet/IP implementation, 2.1.
			USINT Major	
			USINT Minor	
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.

Table 65: Class attributes

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 currently created: 1

Table 66: Attributes of Instance 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 fault (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:	Path to the Physical Link Object, always {0x20, 0xF6, 0x24, 0x01} describing instance 1 of the Ethernet Link Object.
			UINT PathSize	
			EPATH Path	
0x5	Interface Configuration	Set/Get	STRUCT of:	IP Stack Configuration (IP-Address, Netmask, Gateway, 2 Name servers (DNS, if supported) and the domain name).
			UDINT IpAddress	
			UDINT Netmask	
			UDINT GatewayAddress	
			UDINT NameServer1	
			UDINT NameServer2	
			STRING DomainName	
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)

Table 66: Attributes of Instance 1 (cont

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

Table 67: Schneider Electric extensions to the TCP/IP Interface Object

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=Failure, 4=Uninitialized)
0x65	Cable Pair Size	Get	USINT	Size of the Cable Test Result STRUCT of: 2 Pair for 100BASE 4 Pair for 1000BASE

Table 67: Schneider Electric extensions to the TCP/IP Interface Object (cont

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

Table 68: Instance attributes and Schneider Electric extensions to the Ethernet Link Object

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=Auto-Negotiation failed 0x2=Failed 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

Table 68: Instance attributes and Schneider Electric extensions to the Ethernet Link Object (cont

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: Unknown interface type 1: The interface is internal 2: Twisted-pair 3: Optical fiber
0x8	Interface state	Get	USINT	Current state of the interface: 0: Unknown 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.
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

Table 68: Instance attributes and Schneider Electric extensions to the Ethernet Link Object (cont

Id	Attribute	Access Rule	Data type	Description
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.
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

Table 69: Assignment of ports to Ethernet Link Object Instances

Ethernet Port	Ethernet Link Object Instance
CPU	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.

Table 70: Class attributes

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=failed)
				1:	Device Security Status (0=ok, 1=failed)
				2:	Power Supply 1 (0=ok, 1=failed)
				3:	Power Supply 2 (0=ok, 1=failed or not existing)
				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=failure)
				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
				20:	Reserved
				21:	Reserved
				22:	Reserved
				23:	MRP (0=disabled, 1=enabled)
				24:	Reserved
				25:	Reserved
				26:	RSTP (0=disabled, 1=enabled)
				27:	LAG (0=disabled, 1=enabled)
				28:	Reserved
				29:	Reserved
				30:	Reserved
				31:	Connection Error (1=failure)

Table 70: Class attributes (cont

Id	Attribute	Access Rule	Data type	Description
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: 5: 6: 7: IGMP Querier Packet Version Off=0 IGMP Querier disabled V1=1 V2=2 V3=3
				8: 9: 10: Treatment of Unknown Multicasts: 0=Send To All Ports 2=Discard
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

Table 70: Class attributes (cont

Id	Attribute	Access Rule	Data type	Description	
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 Failed/Flash Write Failed
				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.

Table 71: Instance attributes

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

Table 71: Instance attributes (cont

Id	Attribute	Access Rule	Data type	Description
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

RSTP Bridge Object (MCSESM-E)

RSTP is a layer 2 protocol that enables the use of a redundant Ethernet topology (for example, a ring topology). RSTP is specified in Chapter 17 of IEEE 802.1D-2004.

The device supports the Schneider Electric-specific RSTP Bridge Object (class code 64_H, 100) for the device configuration and information parameters.

The device supports 2 instances:
- Instance 1 represents the bridge's primary RSTP instance, and
- instance 2 represents the secondary (Dual) RSTP instance.

You will find further information on these parameters and how to set them in the “Graphical User Interface” reference manual.

Table 72: Schneider Electric RSTP Bridge Object

Id	Attribute	Access rule	Data type	Description
1	Bridge Identifier Priority	Set	UDINT	Range: 0 to 61,440 in steps of 4,096, default: 32,768 (refer to IEEE, 802.1D-2004, § 17.13.7)
2	Transmit Hold Count	Set	UINT	Range: 1 to 40, default: 10 (refer to IEEE 802.1D-2004, §17.13.12)
3	Force Protocol Version	Set	UINT	Default:2 (refer to IEEE 802.1D-2004, §17.13.4 and dot1dStpVersion in RFC 4318)
4	Bridge Hello Time	Set	UDINT	Range: 100 to 200, unit: centi-seconds (1/100 of a second), default: 200 (refer to IEEE 802.1D-2004, §17.13.6 and dot1dStpHoldTime in RFC 4188)
5	Bridge Forward Delay	Set	UDINT	Range: 400 to 3000, unit: centi-seconds, default: 2100 (refer to IEEE 802.1D-2004, §17.13.5 and dot1dStpForwardDelay in RFC 4188)
6	Bridge Max. Age	Set	UINT	Range: 600 to 4000, unit: centi-seconds, default: 4000 (refer to IEEE 802.1D-2004, §17.13.8 and dot1dStpBridgeMaxAge in RFC 4188)
7	Time Since Topology Change	Get	UDINT	Unit: centi-seconds (refer to dot1dStpTimeSinceTopologyChange in RFC 4188)

Table 72: Schneider Electric RSTP Bridge Object (cont

Id	Attribute	Access rule	Data type	Description
8	Topology Change	Get	UDINT	Refer to dot1dStpTopChanges in RFC 4188
100	InnerPort	Get	UINT	Schneider Electric-specific object. ▶ For instance 1, it holds the port number of the DRSTP Primary instance‘s inner port. ▶ For instance 2, it holds the port number of the DRSTP Secondary instance‘s inner port.
101	OuterPort	Get	UINT	Schneider Electric-specific object. ▶ For instance 1, it holds the port number of the DRSTP Primary instance‘s outer port. ▶ For instance 2, it holds the port number of the DRSTP Secondary instance‘s outer port.

RSTP Port Object (MCSESM-E)

The device supports the Schneider Electric-specific RSTP Port Object (class code 65_H, 101) for the RSTP port configuration and information parameters with at least one instance.

Instance 1 represents the CPU‘s Ethernet Interface, instance 2 represents the first physical port, instance 3 the second physical port, and so on.

You will find further information on these parameters and how to set them in the “Graphical User Interface” reference manual.

Table 73: Schneider Electric RSTP Port Object

Id	Attribute	Access rule	Data type	Description
1	Port Identifier Priority	Set	UDINT	Range: 0 to 240 in steps of 16, default: 128 (refer to IEEE, 802.1D-2004, § 17.13.10).
2	mcheck	Set	BOOL	True (1), False (2) (refer to IEEE 802.1D-2004, §17.19.13 and dot1dStpPortProtocolMigration in RFC 4318).
3	Port Path Cost	Set	UDINT	Range: 1 to 200,00,000, default:auto (0) (refer to IEEE 802.1D-2004, §17.13.11 and dot1dStpPortAdminPathCost in RFC 4318).
4	Port Admin Edge Port	Set	BOOL	True (1), False (2) (refer to IEEE 802.1D-2004, §17.13.1 and dot1dStpPortAdminEdgePort in RFC 4318).
5	Port Oper Edge Port	Get	BOOL	True (1), False (2) (refer to dot1dStpPortOperEdgePort in RFC 4318).
6	Port Admin PointToPoint	Set	UINT	forceTrue (0), forceFalse (1), auto (2) (refer to dot1dStpPortAdminPointToPoint in RFC 4318).
7	Port Oper PointToPoint	Get	UINT	True (1), False (2) (refer to dot1dStpPortOperPointToPoint in RFC 4318).
8	Port Enable	Set	UINT	Enabled (1), Disabled (2) (Refer to dot1dStpPortEnable in RFC 4188).

Table 73: Schneider Electric RSTP Port Object (cont

Id	Attribute	Access rule	Data type	Description
9	Port State	Get	UINT	Disabled (1), Blocking (2), Listening (3), Learning (4), Forwarding (5), Broken (6) (refer to dot1dStpPortState in RFC 4188).
10	Port Role	Get	UNT	Unknown (0), Alternate/Backup (1), Root (2), Designated (3) (refer to dot1dStpTopChanges in RFC 4188).
100	DRSTP	Get	UINT	Schneider Electric-specific object. True (1), False (2).

Services, Connections and I/O Data

The device supports the following connection types and parameters.

Table 74: Settings for integrating a new module

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

Table 75: Device I/O data structure

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

Table 75: Device I/O data structure (cont

I/O Data	Value (data types and sizes to be defined)	Direction	Size[1]
TCP/IP Connections	Integer, number of connections	Input	DINT
Quick Connect Mask	Bitmask (1 Bit per port) (0=Quick Connect disabled, 1=Quick Connec 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.

Table 76: Mapping of the data types to bit sizes

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

A Setting up the configuration environment

A.1 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.

Figure 82: Start window of 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.

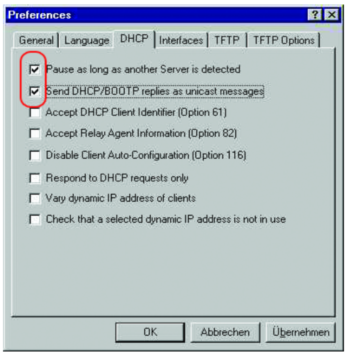


Figure 83: DHCP setting

- 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.

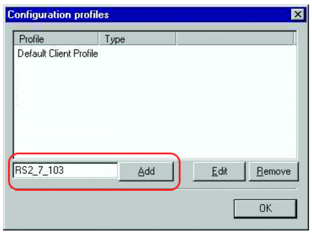


Figure 84: Adding configuration profiles

- Click the *Add* button.
- Specify the netmask.

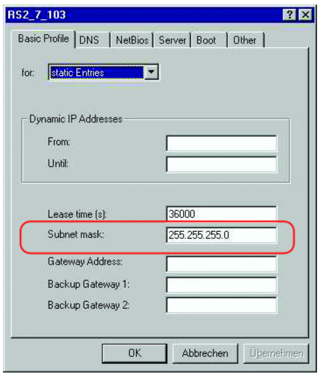


Figure 85: Netmask in the configuration profile

- 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.

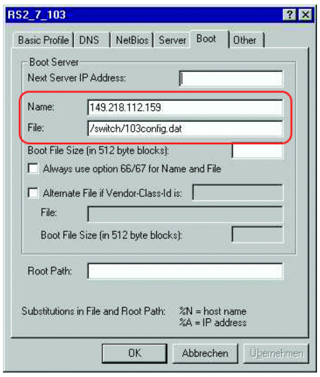


Figure 86: Configuration file on the tftp server

- 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.

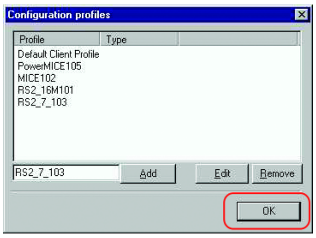


Figure 87: Managing configuration profiles

- 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.

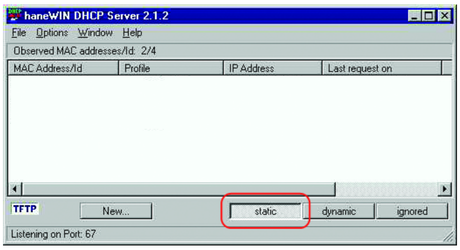


Figure 88: Static address input

- Click the *Add* button.

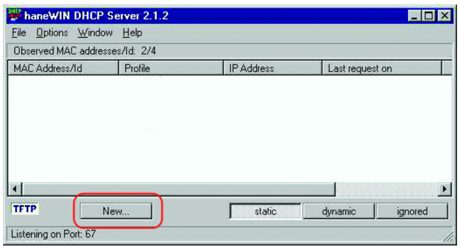


Figure 89: Adding static addresses

- Enter the MAC address of the device.
- Enter the IP address of the device.

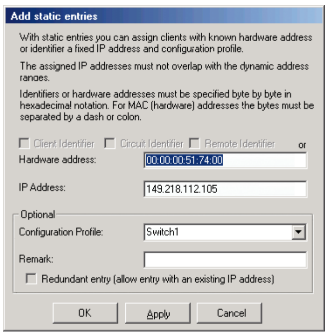


Figure 90: Entries for static addresses

- 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.

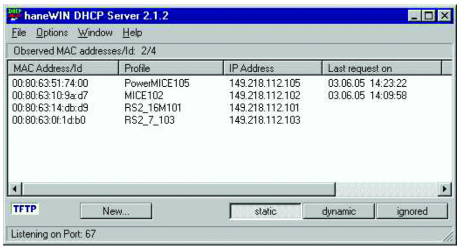


Figure 91: DHCP server with entries

A.2 Setting up a DHCP server with Option 82

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.

Figure 92: Start window of 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.

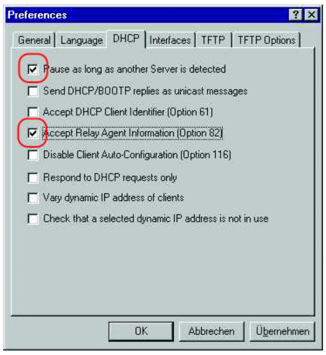


Figure 93: DHCP setting

- To enter the static addresses, click the *Add* button.

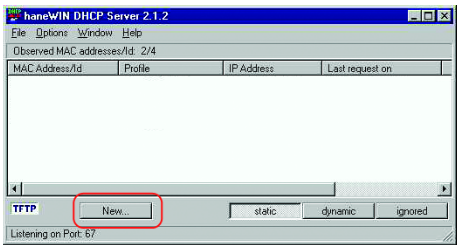


Figure 94: Adding static addresses

- Mark the *Circuit Identifier* checkbox.
- Mark the *Remote Identifier* checkbox.

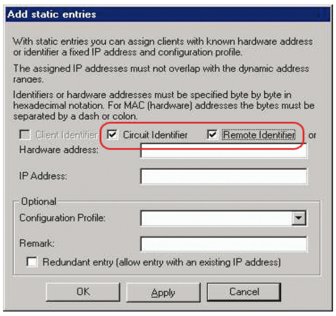


Figure 95: Default setting for the fixed address assignment

- In the *Hardware address* field, specify the value *Circuit Identifier* and the value *Remote Identifier* for the switch and port.
  The DHCP server assigns the IP address specified in the *IP address* field to the device that you connect to the port specified in the *Hardware address* field.
  The hardware address is in the following form:
  `ciclvvvvssmmpprirlxxxxxxxxxxxx`
  - `ci`
    Sub-identifier for the type of the Circuit ID
  - `cl`
    Length of the Circuit ID.
  - Schneider Electric identifier:
    `01` when a Schneider Electric device is connected to the port, otherwise `00`.
  - `vvvv`
    VLAN ID of the DHCP request.
    Default setting: `0001` = VLAN 1
  - `ss`
    Socket of device at which the module with that port is located to which the device is

connected. Specify the value `00`.

- `mm`
  Module with the port to which the device is connected.
- `pp`
  Port to which the device is connected.
- `ri`
  Sub-identifier for the type of the Remote ID
- `rl`
  Length of the Remote ID.
- `xxxxxxxxxxxx`
  Remote ID of the device (for example MAC address) to which a device is connected.

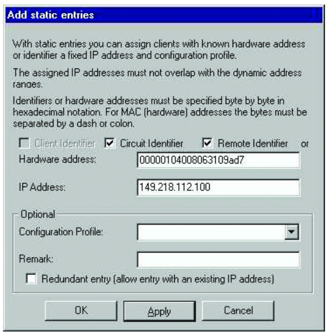


Figure 96: Specifying the addresses

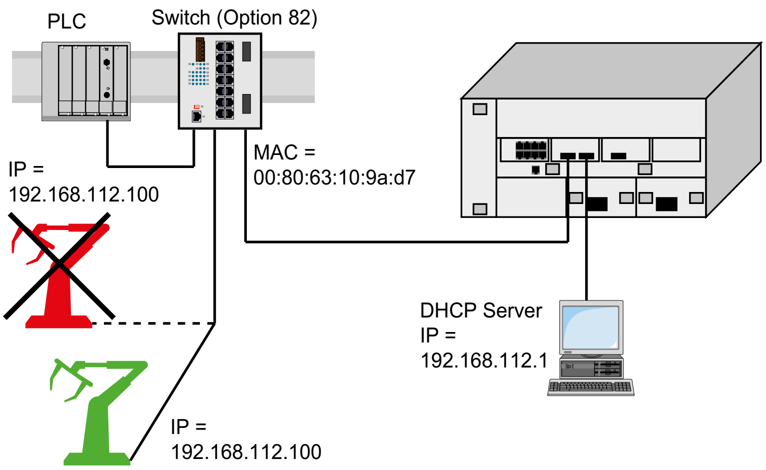


Figure 97: Application example of using Option 82

A.3 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.

A.3.1 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.

A.3.2 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.

A.3.3 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.

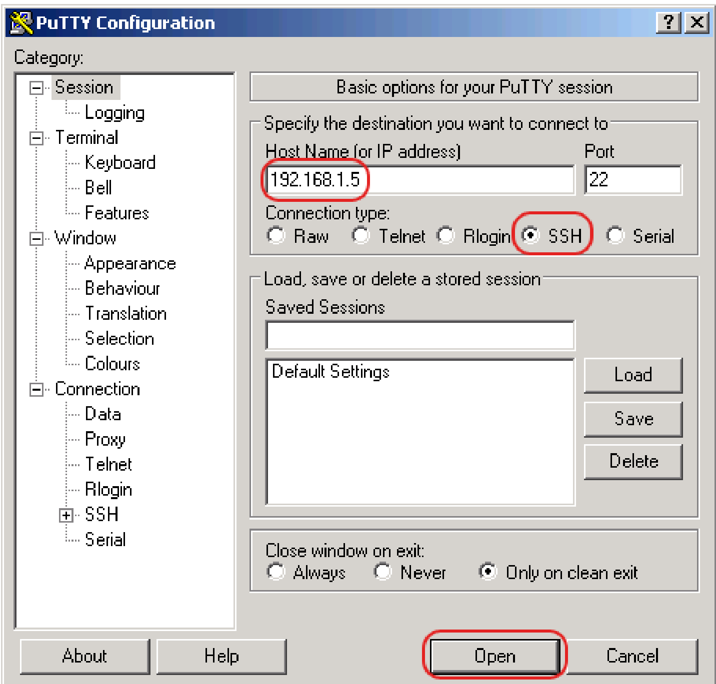


Figure 98: *PuTTY input screen*

- 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 security alarm message and lets you check the key fingerprint.

Figure 99: Security alert prompt for the fingerprint

Before the connection is established, the *PuTTY* program displays a security alarm message and lets you check the key fingerprint.

- Check 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.

A.4 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 current cryptographic parameter recommendations. Outdated certificates may cause issues due to invalid or outdated information. Example: An expired certificate or changed cryptographic recommendations. 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.

A.4.1 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 Command Line Interface.

`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 Command Line Interface.

A.4.2 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.

B Appendix

B.1 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`.

B.2 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 3621	Power Ethernet MIB
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 4291	IPv6 Addressing 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)
RFC 4861	Neighbor Discovery for IPv6
RFC 5321	Simple Mail Transfer Protocol
RFC 6221	Leightweight DHCPv6 Relay Agent
RFC 8200	IPv6 Specification
RFC 8415	DHCPv6

B.3 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

B.4 Underlying IEC Norms

IEC 62439	High availability automation networks MRP – Media Redundancy Protocol based on a ring topology

B.5 Underlying ANSI Norms

ANSI/TIA-1057	Link Layer Discovery Protocol for Media Endpoint Devices, April 2006

B.6 Technical Data

16.3.3 Switching

Size of the MAC address table (incl. static filters)	16384
Max. number of statically configured MAC address filters	100
Max. number of MAC address filters learnable through IGMP Snooping	1024
Max. number of MAC address entries (MMRP)	64
Number of priority queues	8 Queues
Port priorities that can be set	0..7
MTU (Max. allowed length of packets a port can receive or transmit)	9720 Bytes

16.3.4 VLAN

VLAN ID range	1..4042
Number of VLANs	max. 128 simultaneously per device max. 128 simultaneously per port

16.3.5 Access Control Lists (ACL)

Max. number of ACLs	50
Max. number of rules per ACL	256
Max. number of rules per port	256
Number of total configurable rules	2048 (8 × 256)
Max. number of VLAN assignments	12
Max. number of rules which log an event	128
Max. number of Ingress rules	514

B.7 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 Graphical User Interface in the *Help > Licenses* dialog.

B.8 Abbreviations used

ACL	Access Control List
BOOTP	Bootstrap Protocol
CLI	Command Line Interface
DHCP	Dynamic Host Configuration Protocol
DHCPv6	Dynamic Host Configuration Protocol for IPv6
DUID	DHCP Unique Identifier
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
IPv6	Internet Protocol version 6
LDRA	Lightweight DHCPv6 Relay Agent
LED	Light Emitting Diode
LLDP	Link Layer Discovery Protocol
MAC	Media Access Control
MIB	Management Information Base
MRP	Media Redundancy Protocol
NDP	Neighbor Discovery 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

C Index

R

S

T

U