HIRSCHMANN
A BELDEN BRAND

Hirschmann Automation and Control GmbH

LRS HiEOS Rel. 01100

Reference Manual

Graphical User Interface

User Manual

Configuration

HIRSCHMANN
A BELDEN BRAND

Reference Manual

Graphical User Interface
Lemur Rail Switch
HiEOS

Technical support
https://hirschmann-support.belden.com

You find the latest user documentation for your device at: doc.hirschmann.com

Hirschmann Automation and Control GmbH
Stuttgarter Str. 45-51
72654 Neckartenzlingen
Germany

Contents

Safety instructions

⚠ WARNING

UNCONTROLLED MACHINE ACTIONS

To avoid uncontrolled machine actions caused by data loss, configure all the data transmission devices individually.

Before you start any machine which is controlled via data transmission, be sure to complete the configuration of all data transmission devices.

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

About this Manual

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 Industrial HiVision 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

Notes on the Graphical User Interface

The prerequisite to use the Graphical User Interface of the device is a web browser with HTML5 support.

The responsive Graphical User Interface automatically adapts to the size of your screen. Consequently, you can see more details on a large, high-resolution screen than on a small screen. For example, on a high-resolution screen, the buttons have a label next to the icon. On a screen with a small width, the Graphical User Interface displays only the icon.

Note: On a conventional screen, you click to navigate. On a device with a touchscreen, on the other hand, you tap. For simplicity, we only use "click" in our help texts.

The Graphical User Interface is divided as follows:

- Banner
- Menu pane
- Dialog area

Banner

The banner displays the following information:

Displays and hides the menu. When the web browser window is too narrow, the Graphical User Interface hides the menu pane. The banner displays the button instead.

Brand logo

Click the logo to open the website of the manufacturer of the device in a new window.

Dialog name

Displays the name of the dialog currently displayed in the dialog area.

Displays that the web browser cannot contact the device. The connection to the device is interrupted.

When you click the button, the online help opens in a new window.

When you click the button, a submenu opens with the following menu items:

- User account name
  The account name of the user that is currently logged in.
- *Logout* button
  When you click the button, this logs out the currently logged in user. Then the login dialog opens.

Menu pane

When the web browser window is too narrow, the Graphical User Interface hides the menu pane.

To display the menu pane, click the ☰ button in the banner.

The menu pane is divided as follows:
- Icons bar
- Menu tree

Icons bar

The icons bar displays the following information:

Device software

Displays the version number of the device software that the device loaded during the last system startup and is currently running.

Displays a text field to search for a keyword. When you enter a character or string, the menu tree displays a menu item only for those dialogs that are related to this keyword.

The menu tree displays a menu item only for those dialogs in which at least one parameter differs from the default setting (*Diff to default*). To display the complete menu tree again, click the  button.

Collapses the menu tree. The menu tree then displays only the menu items of the first level.

Expands the menu tree. The menu tree then displays every menu item on every level.

Menu tree

The menu tree contains one item for each dialog in the Graphical User Interface. When you click a menu item, the dialog area displays the corresponding dialog. You can change the view of the menu tree by clicking the buttons in the icons bar at the top. Furthermore, you can change the view of the menu tree by clicking the following buttons:

+

Expands the current menu item to display the menu items of the next lower level. The menu tree displays the button next to each collapsed menu item that contains menu items on the next lower level.

−

Collapses the menu item to hide the menu items of the lower levels. The menu tree displays the button next to each expanded menu item.

Dialog area

The dialog area displays the dialog that you select in the menu tree, including its controls. Here, you can monitor and change the settings of the device depending on your access role.

Below you find useful information on how to use the dialogs.

- Control elements
- Modification mark
- Standard buttons
- Saving the settings
- Updating the display
- Working with tables

Control elements

The dialogs contain different control elements. These control elements are read-only or editable, depending on the parameter and your access role as a user.

The control elements have the following visual properties:

- Input fields
  - An editable input field has a line at the bottom.
  - A read-only input field has no special visual properties.
- Checkboxes
  - An editable checkbox has a bright color.
  - A read-only checkbox has a grey color.
- Radio buttons
  - An editable radio button has a bright color.
  - A read-only radio button has a grey color.

Modification mark

When you modify a value, the corresponding field or table cell displays a red triangle in its top-left corner. The red triangle indicates that you have not yet transferred your modification to the volatile memory (RAM) of the device. The modified settings are not yet effective.

Standard buttons

Here you find the description of the standard buttons. The special dialog-specific buttons are described in the corresponding dialog help text.

✓

Transfers the changes to the volatile memory (RAM) of the device and applies them to the device.

Information on how the device retains the modified settings even after a reboot you find in section “Saving the settings” on page 14.

Undoes the unsaved changes in the current dialog. Resets the values in the fields to the settings saved in the volatile memory (RAM) of the device.

Saving the settings

Saving transfers the modified settings to the volatile memory (RAM) of the device. To do this, perform the following step:

- ☐ Click the ✓ button.

Note: Unintentional changes to the settings can terminate the connection between your PC and the device.

To keep the modified settings even after restarting the device, perform the following steps:

- ☐ Open the *Basic Settings > Load/Save* dialog.
- ☐ Click the  button to save your current changes.

Updating the display

If a dialog remains open for a longer time, then the values in the device have possibly changed in the meantime.

- ☐ To update the display in the dialog, click the  button. Unsaved information in the dialog is lost.

Working with tables

The dialogs display numerous settings in table form. You have the option of customizing the appearance of the tables to fit your needs.

You can find useful information on how to use the tables in the following sections:

- ▶ Filter rows
- ▶ Sort rows
- ▶ Select multiple table rows

Filter rows

The filter lets you reduce the number of displayed table rows.

Displays a second table row in the table header containing a text field for every column. When you enter a string in a field, the table displays only the table rows that contain this string in the corresponding column.

Sort rows

Every column in the table header contains an icon that lets you change the order of the table rows.

Displays that the table rows are sorted by a criterion other than the values in this column.

Click the icon to sort the table rows in descending order based on the entries of the corresponding column. You might be able to restore the initial sorting in the table only after logging off and logging in again.

Displays that the table rows are sorted in descending order based on the entries of the corresponding column.

Click the icon to sort the table rows in ascending order based on the entries of the corresponding column. You might be able to restore the initial sorting in the table only after logging off and logging in again.

Displays that the table rows are sorted in ascending order based on the entries of the corresponding column.

Click the icon to sort the table rows in descending order based on the entries of the corresponding column. You might be able to restore the initial sorting in the table only after logging off and logging in again.

Select multiple table rows

You have the option of selecting multiple table rows at once and then apply an action to the selected table rows. This is useful for example, when you want to remove multiple table rows at the same time.

To select individual table rows, mark the leftmost checkbox in the desired table row.

To select every table row, mark the leftmost checkbox in the table header.

1 Basic Settings

The menu contains the following dialogs:

- System
- Network
- Software
- Load/Save
- Port
- Power over Ethernet
- Restart

1.1 System

[Basic Settings > System]

This dialog displays information about the operating status of the device.

Error

Error

Displays the number of errors detected.

A tooltip displays the cause of the currently existing error and the time at which the device triggered the error. To display the tooltip, hover the mouse pointer over or tap the field. In the *Diagnostics* > Report > *System Log* dialog, the table displays an overview of the errors.

Warning

Warning

Displays the number of warnings. If an action is not taken, then an error could occur.

A tooltip displays the cause of the currently existing warning and the time at which the device triggered the warning. To display the tooltip, hover the mouse pointer over or tap the field. In the *Diagnostics* > *Report* > *System Log* dialog, the table displays an overview of the warnings.

Notice

Notice

Displays the number of notices that are unusual but not specific.

A tooltip displays the cause of the currently existing notice and the time at which the device triggered the notice. To display the tooltip, hover the mouse pointer over or tap the field. In the *Diagnostics > Report > System Log* dialog, the table displays an overview of the notices.

Information

Information

Displays the number of informational message.

A tooltip displays the cause of the currently existing informational message and the time at which the device triggered the informational message. To display the tooltip, hover the mouse pointer over or tap the field. In the *Diagnostics > Report > System Log* dialog, the table displays an overview of the informational message.

System data

The fields in this frame display operating data and system information of the device.

System name

Specifies the name by which the device is known in the network.

Possible values:

- Alphanumeric ASCII character string with 0..255 characters
  `<device family name>-<MAC address>` (default setting)

Location

Specifies the current or planned location.

Possible values:

- Alphanumeric ASCII character string with 0..255 characters

Contact

Specifies the contact name for the device.

Possible values:

- Alphanumeric ASCII character string with 0..255 characters

Device type

Displays the product name of the basic device.

Power supply

Displays the status of the power supply unit.

Possible values:

- *active*
- *standby*
- *not-present*

System uptime

Displays the time that has elapsed since the device was last restarted.

Possible values:

- Time in the format `d hh:mm:ss`

Port status

This frame displays a simplified view of the device ports at the time of the last display update. In the initial view, the frame only displays ports with an active link. When you click the button, the frame displays every port.

You can easily identify the port status from the indicator:

- Ports with an active link:
  - The background color is green.
  - The port speed is displayed next to the port number.
- Ports with an inactive link:
  The background color is gray.

When you hover the mouse pointer over or tap the appropriate port icon, a tooltip displays detailed port state information.

1.2 Network

[Basic Settings > Network]

The menu contains the following dialogs:

- Global
- IPv4

1.2.1 Global

[Basic Settings > Network > Global]

This dialog displays the management VLAN and lets you specify the HiDiscovery settings required for access to the device management through the network.

The dialog contains the following frames:
- Management interface
- HiDiscovery protocol v2

Management interface

This frame displays the details of the management interface.

VLAN ID

Displays the VLAN in which the device management is accessible through the network. The device management is accessible through the ports that are members of the VLAN.

Possible values:
- `1` (default setting)

MAC address

Displays the MAC address of the device. The device management is accessible via the network using the MAC address.

HiDiscovery protocol v2

This frame lets you specify settings for the access to the device using the HiDiscovery protocol.

On a PC, the Provize Explorer application displays the Hirschmann devices that can be accessed on the network on which the HiDiscovery function is enabled. You can access these devices even if they have invalid or no IP parameters assigned. The Provize Explorer application lets you assign or change the IP parameters in the device.

Note: With the Provize Explorer application, you access the device only through ports that are members of the device management VLAN. You specify which VLAN a certain port is assigned to in the *Switching > VLAN > Port* dialog.

Operation

Enables/disables the HiDiscovery function in the device.

Possible values:
- *On* (default setting)
  HiDiscovery function is enabled.
  You can use the Provize Explorer application to access the device from your PC.
- *Off*
  HiDiscovery function is disabled.

Note: Disabling the HiDiscovery function after initial use helps secure your device against possible attacks that use the HiDiscovery protocol.

Access

Enables/disables the write access to the device using the HiDiscovery protocol.

Possible values:

- *read-only*
  The Provize Explorer application is given read-only access to the device.
  With this setting, you can view the IP parameters in the device.
- *read-write* (default setting)
  The Provize Explorer application is given read-write access to the device.
  With this setting, you can change the IP parameters in the device.

Recommendation: Change the setting to the value *read-only* only after putting the device into operation.

Signal

Activates/deactivates the flashing of the port LEDs, which is similar to the signal function in the Provize Explorer application. The function helps you identify the device in the field.

Possible values:

- marked
  The flashing of the port LEDs is active.
  The port LEDs flash until you disable the function again.
- unmarked (default setting)
  The flashing of the port LEDs is inactive.
  The port LEDs resume their standard function.

1.2.2 IPv4

[Basic Settings > Network > IPv4]

This dialog lets you set up the management interface and IPv4 setting on the device.

The dialog contains the following frames:
- Management interface
- Management IP parameter

Management interface

IPv4 address assignment

Specifies the source from which the device management receives its IP parameters.

Possible values:

- *DHCP*
  The device receives its IP parameters from a DHCP server. The server evaluates the MAC address, the DHCP name, or other parameters of the device, then assigns the IP parameters.
- *Local* (default setting)
  The device uses the IP parameters specified in the *Management IP parameter* frame.

Management IP parameter

This frame lets you specify the IP parameters, only when the `Local` radio button is selected in the *IPv4 address assignment* field.

IPv4 address

Specifies the management IPv4 address manually.

Possible values:

- Valid IPv4 address.

Prefix size

Specifies the prefix size of the IPv4 address. The prefix size is equivalent to the length of the network mask. Together with the device's IPv4 address, it specifies the range of the local IP network.

Possible values:

- `1..32`

Gateway address

Specifies the IPv4 address of a router through which the device accesses other devices outside its network.

Possible values:

- Valid IPv4 address.

Table

In this table you can add/remove a VLAN interface only if the VLAN is already created in the *Switching > VLAN* dialog.

Buttons

Add

Opens the *Create* window to add a table row.

- In the *VLAN ID* field, specify the VLAN ID.
  Possible values:
  – `2..4093`
  VLANs `4094` and `4095` are reserved for the internal functions.

Remove

Removes the selected table row.

Client restart

Restarts the *DHCP client enable* setting for the selected interface VLAN.

VLAN ID

Displays the interface VLAN ID.

Possible values:

- `1..4093`

Active

Activates/deactivates the interface VLAN.

Possible values:

- `marked`
  The interface VLAN is active.
- `unmarked`
  The interface VLAN is inactive.

MTU

Specifies the maximum allowed size of the Ethernet packets.

Possible values:

- `1280..1500` (default setting: `1500`)

IPv4 address

Specifies the valid IPv4 address for the interface.

If the *DHCP client enable* column is `marked`, then the IPv4 address you specify in this field becomes the fallback IP. If no IPv4 address is assigned by the *DHCP* before the *DHCP fallback timeout [s]* timer stops, then the device assigns the fallback IP as a primary IP to the node.

Possible values:

- Valid IPv4 address.

Prefix size

Specifies the prefix size for the IPv4 address.

Possible values:

- `0..32`

DHCP client enable

Activates/deactivates the *DHCP* client function.

Possible values:

- `marked`
  The *DHCP* client function is active.
  You activate the *DHCP* client function only if there is no conflict among the values of the *IPv4 address*, the *Prefix size*, and the *DHCP fallback timeout [s]* columns.
- `unmarked`
  The *DHCP* client function is inactive.

DHCP fallback timeout [s]

Specifies the fallback time in seconds.

Possible values:

- `1..4294967295` (default setting: `60`)
  If you deactivate the *DHCP client enable* setting, then the *DHCP fallback timeout [s]* has no effect.
  If you activate the setting and the timeout value is apart from `0`, then the *DHCP fallback timeout [s]* timer stops the *DHCP* process after the specified timeout and assigns the *IPv4 address* to the interface. When this occurs, the *IPv4 address* becomes the fallback IP.
  When you remove the timeout value, clear the values from the following columns as well:
  - *IPv4 address*
  - *Prefix size*

  As a result, the fallback settings get removed.

DHCP host name

Specifies the host name for the *DHCP* client.

Possible values:

- Alphanumeric ASCII character string with 1..63 characters.
  A valid name consists of a sequence of domain labels separated by a dot (.), each domain label starting and ending with an alphanumeric character, and possibly contains the hyphen (-) as well.

DHCP ID type

Specifies the type of *DHCP* client identifier.

Possible values:

- *auto*
- *If MAC*

- *ASCII*
- *hex*

DHCP ID if MAC

Specifies the port number for the *DHCP* client identifier only when the *DHCP* client setting is enabled, and the *DHCP ID type* column contains the value item *If MAC*.

Possible values:

- <port number>

DHCP ID ASCII

Specifies the ASCII string for the *DHCP* client identifier only when the *DHCP* client setting is enabled, and the *DHCP ID type* column contains the value item *ASCII*.

Possible values:

- Alphanumeric ASCII character string with 1..31 characters.

DHCP ID hex

Specifies the hexadecimal string for the *DHCP* client identifier only when the *DHCP* client setting is enabled, and the *DHCP ID type* column contains the value item *hex*.

Possible values:

- 2..64 hexadecimal characters of even length.

DHCP state

Displays the status of the *DHCP* client.

Possible values:

- *stopped*
- *init*
- *selecting*
- *requesting*
- *rebinding*
- *bound*
- *renewing*
- *fallback*
- *arpCheck*

DHCP server IPv4 address

Displays the IPv4 address of the *DHCP* server that provides the *DHCP* functionality.

Possible values:

- Valid IPv4 address.

Active IPv4 address

Displays the current IPv4 address of the interface VLAN.

Possible values:

- Valid IPv4 address.

Broadcast

Displays the broadcast address of the network.

Possible values:

- Valid IPv4 address.

1.3 Software

[Basic Settings > Software]

This dialog lets you update the device software via Web using the *Hypertext Transfer Protocol (HTTP)*, *Hypertext Transfer Protocol Secure (HTTPs)* or *Trivial File Transfer Protocol (TFTP)* servers and display information about the device software. You also have the option to restore a backup of the device software saved in the device. Web interface accepts both firmware and bootloader images of the software.

Note: Before updating the device software, follow the version-specific notes in the `Readme` text file.

Version

Running version

Displays the version number, creation date and time of the device software that the device loaded during the last system startup and is currently running.

Backup version

Displays the version number, creation date and time of the device software saved as a backup in the non-volatile memory (`NVM`). The device copied the running version into the backup partition during the last software update or after you clicked the *Restore* button.

Restore

Lets you restore to the previous version of the software. When you click the *Restore* button the device swaps the images between active and backup partition.

Boot code

Displays the version number, creation date and time of the boot code.

Software update

URL

Specifies the path and the file name of the image file with which you update the device software.

The device gives you the following options for updating the device software:

- Software update from the PC

  When the file is located on your PC or on a network drive, drag and drop the file in the  area.
  As an alternative, click in the area to select the file.
- Software update from an HTTP server
  When the file is located on an HTTP server, enter the URL in the following form:
  `http://<IP address>/<path>/<file name>`
- Software update from an HTTPS server
  The prerequisites for downloading the file from an HTTPS server are:
  - The SSL certificate of the HTTPS server is available in the non-volatile memory (NVM) of the device. See the *Basic Settings > Load/Save* dialog.
  - The HTTPS server domain name is set up on the device. See the *Advanced > DNS Client* dialog.
  - The device is set to the correct time. See the *Time > Basic Settings* dialog.

  When the file is located on an HTTPs server, enter the URL in the following form:
  `https://<IP address>/<path>/<file name>`
- Software update from a TFTP server
  When the file is located on an TFTP server, enter the URL in the following form:
  `tftp://<IP address>/<path>/<file name>`

Image type

Specifies the type of software to be uploaded.

Possible values:

- `firmware` (default setting)
  To upload the software image.
- `bootloader`
  To upload the bootloader image.

Start

Updates the device software.

When you click the *Start* button, the device replaces the backup software file with the new file that you selected for the installation. After installing the new file in the backup partition, the device swaps the active and backup partition so that the new software is loaded after the system startup. This implies that you perform a system restart to activate the new software.

The device copies the existing software into the backup memory.

1.4 Load/Save

[Basic Settings > Load/Save]

This dialog lets you save the device settings in a configuration profile.

The device can hold several configuration profiles. When you activate an alternative configuration profile, you change the existing device settings to the selected configuration profile. You have the option of exporting the configuration profiles to a server. You also have the option of importing the configuration profiles from a server to the device.

Table

For information on how to customize the appearance of the table, see “Working with tables” on page 14.

Buttons

Remove

Removes the configuration profile selected in the table from the non-volatile memory.

Save

Copies the running-config from the volatile memory into the startup-config stored in the non-volatile memory when a table row is not selected. If a table row is selected, then the running-config is saved in the selected configuration profile.

Displays a context menu with further functions for the corresponding dialog.

Save as...

Opens the *Save as...* window to copy the configuration profile selected in the table and saves it with a user-specified name in the non-volatile memory.

- ☐ In the *File name* field, enter the name under which you want to save the configuration profile.
  - ☐ To save the configuration profile under a new name, click the + button.
  - ☐ To overwrite an existing configuration profile, select the corresponding item from the drop-down list.

Activate

Loads the settings of the configuration profile selected in the table to the volatile memory.

- The device terminates the connection to the Graphical User Interface. To access the device management again, perform the following steps:
  - Reload the Graphical User Interface.
  - Log in again.
- The device immediately uses the settings of the configuration profile on the fly.

When you activate an older configuration profile that belongs to an earlier software version, the device takes over the settings of the new functions contained in this software version. The device sets the values of new functions to their default value.

Import...

Opens the *Import...* window to import a configuration profile.

The prerequisite is that you have exported the configuration profile using the *Export...* button.

- In the *URL* field, specify the configuration profile file to be imported.
  - Import from a TFTP server
    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>`
  - Import from an HTTP server
    When the file is located on an HTTP server, specify the URL for the file in the following form:
    `http://<IP address>/<path>/<file name>`
- In the *File name* drop-down list, select the desired file to be imported. The imported file can be saved to either non-volatile memory (NVM) or running-config.
- Mark the *Merge* checkbox to merge the configuration from the imported file into running-config. The prerequisite is that running-config profile is selected in the *File name* drop-down list.

Export...

Exports the configuration profile selected in the table and saves it as a text file on a remote server.

The device gives you the following options for exporting a configuration profile:

- Export to a TFTP server
  To save the file on a TFTP server, specify the URL for the file in the following form:
  `tftp://<IP address>/<path>/<file name>`
- Export to an HTTP server
  To save the file on an HTTP server, specify the URL for the file in the following form:
  `http://<IP address>/<path>/<file name>`

Load running-config from script

Imports a script file which modifies the current `running-config` configuration profile.

- In the *URL* field, specify the script file to be imported.
  - Import from a TFTP server
    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>`
  - Import from an HTTP server
    When the file is located on an HTTP server, specify the URL for the file in the following form:
    `http://<IP address>/<path>/<file name>`
- Mark the *Merge* checkbox to merge the configuration from the imported file into running-config.

When you import a configuration profile, the device takes over the settings as follows:

- If the configuration profile was exported from the same device or from an identically equipped device of the same type, then:
  The device takes over the settings completely.
- If the configuration profile was exported from another device, then:
  The device takes over the settings which it can interpret based on its hardware equipment and software level.
  The remaining settings the device takes over from its `running-config` configuration profile.

Back to factory...

Resets the settings in the device to the default values.

- The device deletes the saved configuration profiles from the volatile memory (RAM) and from the non-volatile memory (NVM).
- After a brief period, the device reboots and loads the default values. It also triggers force password change (FPC) to change the default password of the device.

Back to default

Deletes the current operating (`running-config`) settings from the volatile memory and loads the default-config settings from the non-volatile memory. It also triggers force password change (FPC) to change the default password of the device.

Note: Verify that *Keep IPv4 address* checkbox is marked to retain the IPv4 address configured for the management VLAN.

File name

Displays the file name.

Modification date

Displays the last modified date of the file.

File size

Displays the file size in bytes.

Flash memory access

Displays the access permission of the file.

Possible values:

- *read-write*
  The file has *read-write* access.
- *read-only*
  The file has *read-only* access.

1.5 Port

[Basic Settings > Port]

This dialog lets you specify settings for the individual ports. The dialog also displays the connection status, port speed, and duplex mode for each port.

The dialog contains the following tabs:
- [Configuration]
- [Status]
- [Statistics]

[Configuration]

Table

For information on how to customize the appearance of the table, see “Working with tables” on page 14.

Port

Displays the port number.
- Ports whose name begin with *Fa* are *Fast Ethernet* ports with a maximum port speed of 100 Mbit/s.
- Ports whose name begin with *Gi* are *Gigabit Ethernet* ports with a maximum port speed of 1 Gbit/s.

Description

Specifies the description about the port.

Possible values:
- ASCII character string with 1..200 characters
  The device accepts the following characters:
  - `<Space>`
  - `0..9`
  - `a..z`
  - `A..Z`
  - `!"#$%&'()*+,-./:;<=>?@[\]^_`{|}~`

Enable

Activates/deactivates the port.

Possible values:
- `marked` (default setting)
  The port is active.
- `unmarked`
  The port is inactive. The port does not send or receive any data.

Speed/Duplex mode

Specifies the link speed and duplex mode of the port.

Possible values:

- `10 Mbit/s Full Duplex`
- `10 Mbit/s Half Duplex`
- `100 Mbit/s Full Duplex`
- `100 Mbit/s Half Duplex`
- `1 Gbit/s Full Duplex`
- `Autonegotiation` (default setting)

Half-duplex

Activates/deactivates the half duplex mode on the port.

The prerequisite is that *Autonegotiation* is selected in *Speed/Duplex mode* column.

Possible values:

- `marked` (default setting)
  Half duplex mode is active on the port.
- `unmarked`
  Half duplex mode is inactive on the port.

Full-duplex

Activates/deactivates the full duplex mode on the port.

The prerequisite is that *Autonegotiation* is selected in *Speed/Duplex mode* column.

Possible values:

- `marked` (default setting)
  Full duplex mode is active on the port.
- `unmarked`
  Full duplex mode is inactive on the port.

10 Mbit/s

Activates/deactivates the *10 Mbit/s* link speed.

The prerequisite is that *Autonegotiation* is selected in *Speed/Duplex mode* column.

Possible values:

- `marked` (default setting)
  10 Mbit/s link speed is active on the port.
- `unmarked`
  10 Mbit/s link speed is inactive on the port.

100 Mbit/s

Activates/deactivates the *100 Mbit/s* link speed.

The prerequisite is that *Autonegotiation* is selected in *Speed/Duplex mode* column.

Possible values:

- `marked` (default setting)
  100 Mbit/s link speed is active on the port.
- `unmarked`
  100 Mbit/s link speed is inactive on the port.

1 Gbit/s

Activates/deactivates the *1 Gbit/s* link speed.

The prerequisite is that *Autonegotiation* is selected in *Speed/Duplex mode* column.

Possible values:

- `marked` (default setting)
  1 Gbit/s link speed is active on the port.
- `unmarked`
  1 Gbit/s link speed is inactive on the port.

Media type

Specifies the media type of the port.

Possible values:

- *RJ45*
- *SFP*
- *Dual*

Cable crossing

Specifies the medium-dependent interface configuration of a Twisted Pair (TP) port.

Possible values:

- *mdi*
  If this setting is configured on a port and an end device port is also configured as *mdi*, then use a crossover cable to connect. If an end device port is configured as *mdix*, then use a straight-through cable to connect.
- *mdix*
  If this setting is configured on a port and an end device port is also configured as *mdix*, then use a crossover cable to connect. If an end device port is configured as *mdi*, then use a straight-through cable to connect.
- *auto-mdix* (default setting on TP ports)
  If this setting is configured on a port, then either type of cable (straight-through or crossover) can be used to connect an end device.
- *unsupported* (default setting on optical ports)
  The port does not support this function.

Flow control

Activates/deactivates the flow control according to IEEE 802.3x on the port.

Possible values:

- `marked`
  The flow control on the port is active.
- `unmarked` (default setting)
  The flow control on the port is inactive.

MTU

Specifies the maximum allowed size (in bytes) of Ethernet packets that the port can receive or transmit.

Possible values:

- `1518..10240` (default setting: `10240`)

Excessive restart

Activates/deactivates the excessive restart function on the port.

The excessive restart function is an extension of the backoff algorithm used to avoid collisions on a shared medium like a half-duplex link.

Two end-points transmitting data on a shared medium at same time can result in a collision. The endpoints then backoff and restart the transmission after a randomized amount of time. This restart may lead to another collision in which case the endpoints will extend the wait time. The standard backoff algorithm tries to restart sending the frame up to 16 times and then gives up. If the excessive restart function is active, the algorithm keeps trying indefinitely.

Possible values:

- `marked`
  The excessive restart function is active. The port will continue to try to send the frame even after 16 successive collisions.
- `unmarked` (default setting)
  The excessive restart function is inactive. The device discards the frame after 16 successive collisions.

Frame length check

Activates/deactivates the checking of the length given in the Ethertype field against the actual frame length if the Ethertype field value is less than 1536 bytes. If the value given in the Ethertype field is ≥1536 bytes, the device will consider that an Ethertype value, not a frame length.

Possible values:

- `marked`
  The checking of frame length is active.
  The device compares the length in the Ethertype field to the actual frame length. In case of a mismatch, the device drops the frame. The device then also increments the frame length mismatch counter in port statistics.
- `unmarked` (default setting)
  The checking of frame length is inactive.
  The device does not compare the length in the Ethertype field to the actual frame length. The device forwards the frame even in case of a frame length mismatch.

[Status]

This tab displays the status of each port interface parameter.

Table

For information on how to customize the appearance of the table, see “Working with tables” on page 14.

Port

Displays the port number.

Link status

Displays if the device detects a link for an interface.

Possible values:

- `marked`
  The device detects a link for an interface.
- `unmarked`
  The device detects no link for an interface.

Full-duplex

Displays if an interface is operating at full duplex.

Possible values:

- `marked`
  An interface is operating at full duplex.
- `unmarked`
  An interface is not operating at full duplex.

Speed

Displays the current interface speed.

Fiber

Displays if an interface is a fiber link.

Possible values:

- `marked`
  An interface is a fiber link.
- `unmarked`
  An interface is not a fiber link.

Loss of signal

Displays the loss of an input optical signal of receiver.

Possible values:

- `marked`
  Loss of an input optical signal of receiver.
- `unmarked`
  No loss of the input optical signal of receiver.

Transmitted faults

Displays if a fault is detected on SFP during transmission.

Possible values:

- `marked`
  Fault is detected on SFP.
- `unmarked`
  No fault is detected on SFP.

Present

Displays if SFP is detected on the port.

Possible values:

- `marked`
  An SFP is detected on the port.
- `unmarked`
  No SFP is detected on the port.

Link up count

Displays the number of times the link was up on the port.

Link down count

Displays the number of times the link was down on the port.

[Statistics]

The tab displays the following overview per port:

- Number of data packets/bytes received
  - *Received octets*
  - *Received unicast packets*
  - *Received multicast packets*
  - *Received broadcast packets*
  - *Received non-unicast packets*
  - *Received discards*
  - *Received errors*
- Number of data packets/bytes sent
  - *Transmitted octets*
  - *Transmitted unicast packets*
  - *Transmitted multicast packets*
  - *Transmitted broadcast packets*
  - *Transmitted non-unicast packets*
  - *Transmitted discards*
  - *Transmitted errors*

To sort the table by a specific criterion, click the header of the corresponding column.

For example, to sort the table based on the number of received bytes in ascending order, click the header of the *Received octets* column once. To sort in descending order, click the header again.

To reset the counters for the port statistics in the table to `0`, perform the following steps:

☐ Open the *Basic Settings > Port* dialog, *Statistics* tab.

☐ Clear the port statistics. To do this, click the 🗑 button.

1.6 Power over Ethernet

[Basic Settings > Power over Ethernet]

In Power over Ethernet (PoE), the Power Source Equipment (PSE) supplies current to powered devices (PD) such as IP phones through the twisted pair cable.

The product code and the PoE-specific labeling on the PSE device housing indicates if your device supports *Power over Ethernet*. The PoE ports of the device support Power over Ethernet according to IEEE 802.3af.

The system provides an internal maximum power budget for the ports. The ports reserve power according to the detected class of a connected powered device. The real delivered power is equal to or less than the reserved power.

When you connect a new powered device to the port, verify the difference between the *Total power allocated [W]* and *Total power consumption [W]* is equal to or more than the maximum power class of the new powered device.

You manage the power output with the *Priority* parameter. When the sum of the power required by the connected devices exceeds the power available, the device turns off power supplied to the ports according to configured priority.

The menu contains the following dialogs:

- PoE Global
- PoE Port

1.6.1 PoE Global

[Basic Settings > Power over Ethernet > Global]

This dialog lets you set up the maximum power output of the device and displays the power and current parameters.

System power

User customizable

Displays if the user can set up the PSU power supply.

Possible values:

- `marked`
  The user can set up the PSU power supply.
- `unmarked`
  The user cannot set up the PSU power supply.

Max. power [W]

Displays the maximum available power in watts.

Reserved power [W]

Displays the reserved power in watts required to keep the device operating. This is applicable for the device which is powered by the same PSU and used for PoE functionality.

Configuration

Max. power [W]

Specifies the maximum power that the PSE can deliver in watts.

Possible values:

- The default setting is `0`. The maximum power value is mapped with the *Max. power [W]* field in the *System power* frame.

Status

Total power consumption [W]

Displays the total power consumption that powered devices are consuming currently in watts.

Total current consumption [mA]

Displays the total current consumption that powered devices are consuming currently in milliampere.

Total power allocated [W]

Displays the total power allocated to the powered devices in watts.

1.6.2 PoE Port

[Basic Settings > Power over Ethernet > Port]

When power consumption is higher than deliverable power, the device turns off power to the powered devices (PD) according to the priority levels and port numbers. When the PDs connected require more power than the device provides, the device deactivates the *Power over Ethernet* function on the ports. The device disables the *Power over Ethernet* function on the ports with the lowest priority first. When multiple ports have the same priority, the device first disables the *Power over Ethernet* function on the ports with the higher port number.

The dialog contains the following tabs:
- [Configuration]
- [Status]

[Configuration]

Table

For information on how to customize the appearance of the table, see “Working with tables” on page 14.

Port

Displays the port number.

PoE

Activates/deactivates the *PoE* function on the port.

Possible values:
- `marked` (default setting)
  The *PoE* function is active on the port.
- `unmarked`
  The *PoE* function is inactive on the port.

Priority

Specifies the port priority.

To help prevent current overloads, the device disables ports with low-priority first, so specify a high priority to the ports which are connected to the necessary devices.

Possible values:
- *low* (default setting)
- *high*
- *critical*

LLDP aware

Activates/deactivates the LLDP awareness on the port.

Possible values:

- `marked` (default setting)
  The port determines the reserve power by exchanging the PoE information using LLDP-MED.
- `unmarked`
  The port determines the reserve power as per the class of the connected powered devices.

[Status]

Table

For information on how to customize the appearance of the table, see “Working with tables” on page 14.

Port

Displays the port number.

PoE

Displays if the *PoE* function is active on the port.

Possible values:

- `marked`
  The *PoE* function is active on the port.
- `unmarked`
  The *PoE* function is inactive on the port.

PD class Alt A

Displays the class assigned to PD alternative A, based on the electrical characteristics.

Possible values:

- `-1..4`
  The value `-1` displays any one of the following conditions:
  - PD attached to the interface can not advertise its power class.
  - PD not detected.
  - PoE is not supported.
  - PoE feature is disabled.
  - PD class not supported.

  The value `0..4` displays the supported PD class.
  - The value `0` displays that the maximum power consumption of PD is up to `15.4W`.
  - The value `1` displays that the maximum power consumption of PD is up to `4W`.
  - The value `2` displays that the maximum power consumption of PD is up to `7W`.
  - The value `3` displays that the maximum power consumption of PD is up to `15.4W`.
  - The value `4` displays that the maximum power consumption of PD is up to `30W`.

PD class Alt B

Displays the class assigned to PD alternative B, based on the electrical characteristics.

Possible values:

- `-1..4`
  The value `-1` displays any one of the following conditions:
  - PD attached to the interface can not advertise its power class.
  - PD not detected.
  - PoE is not supported.
  - PoE feature is disabled.
  - PD class not supported.

  The value `0..4` displays the supported PD class.
  - The value `0` displays that the maximum power consumption of PD is up to `15.4W`.
  - The value `1` displays that the maximum power consumption of PD is up to `4W`.
  - The value `2` displays that the maximum power consumption of PD is up to `7W`.
  - The value `3` displays that the maximum power consumption of PD is up to `15.4W`.
  - The value `4` displays that the maximum power consumption of PD is up to `30W`.

Current state

Displays the current port status.

Possible values:

- *unknownState*
  PD state is unknown.
- *budgetExceeded*
  PoE is turned off due to power budget exceeded.
- *noPdDetected*
  No powered devices detected.
- *pdOn*
  PSE is supplying power to PD through PoE.
- *pdOverloaded*
  PD consumes more power than the maximum limit configured for the port.
- *unsupported*
  PoE is not supported.
- *disabled*
  PoE is disabled for the port.
- *shutdown*
  PD is inoperable due to port shutdown.
- *fault*
  PSE implementation specific fault detected.
- *pse-fault*
  PSE fault detected.

PSE type

Displays the PSE type.

PD structure

Displays the connection type of the powered devices.

Possible values:

- *notDetected*
  Test not yet performed.

- *open*
  No device found.
- *invalidSignature*
  No valid signature found.
- *ieee4PairSingleSig*
  4 pair single signature PD detected.
- *legacy4PairSingleSig*
  4 pair single signature Hirschmann legacy PD detected.
- *ieee4PairDualSig*
  4 pair dual signature PD detected.
- *p2p4CandidateFalse*
- *ieee2Pair*
  2 pair PD detected.
- *legacy2Pair*
  2 pair Hirschmann legacy PD detected.

PD type

Displays the power devices type.

Possible values:

- `0..2`

Operation mode

Displays the IEEE 802.3bt PoE standard operation mode.

Possible values:

- `0..3`
  The value `0..3` corresponds to IEEE 802.3bt PoE standard, other values display legacy modes.

Power management mode

Displays the PoE power management mode.

Power limit [W]

Displays the power limit of the port in watts.

Power reserved [W]

Displays the power reserved for the powered devices in watts.

Power consumption [W]

Displays the power consumption of the powered devices in watts.

Current consumption [mA]

Displays the current consumption of the powered devices in milliamperes.

Internal status

Displays the internal status value reported by the PoE controller.

Possible values:

▶ 0..77

Internal status text

Displays the text representation of the internal status value reported by the PoE controller.

Measured PD class A

Displays the measured PD class of the primary alternative. The measured classification result of each pair is set in a PSE logical port.

Measured PD class B

Displays the measured PD class of the secondary alternative. The measured classification result of each pair is set in a PSE logical port.

Requested PD Class A

Displays the requested PD class of the primary alternative. The requested port class value is determined by the measured class result and internal logic configuration of the port.

Requested PD Class B

Displays the requested PD class of the secondary alternative. The requested port class value is determined by the measured class result and internal logic configuration of the port.

Assigned power [W]

Displays the power limit of the port in watts, referring to a specific PD during the power delivery. If the port power exceeds the assigned power level, then the port is disconnected.

1.7 Restart

[Basic Settings > Restart]

This dialog lets you restart the device, reset port counters, reset MAC address table, and clear log files.

Buttons

Cold start

Restarts the device.

The device restarts and goes through the following phases:

- The device starts the device software that the *Running version* field displays in the *Basic Settings > Software* dialog.
- The device loads the settings from the startup-config configuration profile. See the *Basic Settings > Load/Save* dialog.

Note: During the restart, the device does not transfer any data. During this time, the device cannot be accessed by the Graphical User Interface or other management systems.

Clear access management statistics

Resets the counters of the *IP Access Restriction* statistics to the value `0`.

See the *Device Security > Management Access > IP Access Restriction* dialog, *Statistics* tab.

Clear ERPS statistics

Resets the counters of the *ERPS* statistics to the value `0`.

See the *Switching > L2-Redundancy > ERPS* dialog, *Statistics* tab.

Clear LLDP global statistics

Resets the counters of the *LLDP Topology Discovery* global statistics to the value `0`.

See the *Diagnostics > LLDP > Topology Discovery* dialog, *Statistics* tab.

Clear LLDP port statistics

Resets the counters of the *LLDP Topology Discovery* port statistics to the value `0`.

See the *Diagnostics > LLDP > Topology Discovery* dialog, *Statistics* tab.

Clear IGMP snooping statistics

Resets the counters of the *IGMP Snooping* statistics to the value `0`.

See the *Switching > IGMP Snooping > Status* dialog, *Statistics* tab.

Clear port control statistics

Resets the counters of the *Port* statistics to the value `0`.

See the *Basic Settings > Port* dialog, *Statistics* tab.

Clear MAC address table

Removes the dynamically learnt MAC addresses from the forwarding table.

See the *Switching > Filter for MAC Addresses* dialog.

Clear IPv4 statistics

Resets the counters of the IPv4 statistics available in the Command Line Interface to the value `0`.

Clear ACD table

Removes the set-up addresses from the ACD (Address Conflict Detection) table.

Clear ARP table

Removes the dynamically set-up addresses from the ARP (Address Resolution Protocol) table.

Clear all system logs

Removes the system logged events.

See the *Diagnostics > Report > System Log* dialog.

Clear MRP statistics

Resets the counters of the *MRP Client* statistics to the value `0`.

See the *Switching > L2-Redundancy > MRP Client* dialog, *Statistics* tab.

2 Time

The menu contains the following dialogs:
- Basic Settings
- NTPv4 Client

2.1 Basic Settings

[Time > Basic Settings]

To maintain the system time, the device is equipped with the daylight saving time feature, however, the device does not save the time and after a restart, the device initializes its clock to January 1, 00:00h of the year the firmware image was issued. Reset the time if you disconnect the device from the power supply or restart it.

In this dialog, you specify time-related settings independently of the time synchronization protocol specified.

The dialog contains the following tabs:
- [Global]
- [Daylight saving time]

[Global]

This tab displays the *System time*, and lets you specify the *System timezone offset [min]* in the device.

Configuration

System time

Displays the current date and time.

Set time from PC

The device uses the time on your PC as the system time.

System timezone offset [min]

Specifies system time zone with respect to UTC in minutes.

Possible values:

- `-1439..1439`

Timezone Acronym

Specifies the acronym name to identify the time zone.

Possible values:

- ASCII character string with 1..16 characters.
  The device accepts the following characters:
  - `<Space>`
  - `0..9`
  - `a..z`
  - `A..Z`
  - `!"#$%&'()*+,-./:;<=>?@[\]^_`{|}~`

[Daylight saving time]

This tab lets you switch among the 3 different modes: disable, recurring and non-recurring of the *Daylight saving time* function. Each mode lets you specify the individual settings. You specify the beginning and the end of summertime. During summertime, the device puts the local time forward by the value contained in the *Daylight saving time offset [min]* field.

Operation

Specifies the summertime mode.

Possible values:

- *Disable* (default setting)
  The daylight saving time feature is disabled, and no input validation is performed on the remaining set-up parameters.
- *Recurring*
  Summertime set-up repeats every year.
- *Non-recurring*
  Summertime set-up is specified once.

Configuration

Daylight saving time offset [min]

Specifies the time-offset in minutes to add or subtract during summertime.

Possible values:

- `-1439..1439`

Summertime begin

In the first 3 fields, you specify the day for the beginning of summertime, and in the last field the time.

When the time in the *System time* field reaches the value entered here, the device switches to summertime.

Week

Specifies the week in the current month.

Possible values:

- *none* (default setting)
- *first*
- *second*
- *third*
- *fourth*
- *last*

Day

Specifies the day of the week.

Possible values:

- *none* (default setting)
- *Sunday*
- *Monday*
- *Tuesday*
- *Wednesday*
- *Thursday*
- *Friday*
- *Saturday*

Month

Specifies the month.

Possible values:

- *none* (default setting)
- *January*

- *February*
- *March*
- *April*
- *May*
- *June*
- *July*
- *August*
- *September*
- *October*
- *November*
- *December*

Date

Specifies the non-recurring start date. This field lets you specify the values only when the radio button *Non-recurring* is selected in the *Operation* frame.

Possible values:

- a valid date in the format: <name of the day>, [<name of the month> <dd>], <YYYY>
  When you click this field, the device opens a calendar window. The calendar window displays the following details:
  - Calender
    Lets you select the value items for the year and month from the respective drop-down lists. The forward and backward arrows let you switch to the next and previous month, respectively. The month table lets you specify the date.
  - Clear
    Lets you clear the *Date* field.
  - Today
    Lets you specify the current system date.
  - Close
    Lets you close the clock window.

Time

Specifies the time.

Possible values:

- <HH:MM AM/PM>
  When you click this field, the device opens a clock window to specify the time in 12 hours format. The clock window displays the following details:
  - HH:MM AM/PM
    Displays the time in the digital format to let you select the hour, minute, and AM/PM components of the time.
  - Analog clock
    Displays the time in an analog clock to let you specify the values for the hour and minute components of the time.
  - Clear
    Lets you clear the *Time* field.
  - Now
    Lets you specify the current system time.
  - Close
    Lets you close the clock window.

Summertime end

In the first 3 fields you specify the day for the end of summertime, and in the last field the time.

When the time in the *System time* field reaches the value entered here, the device switches to wintertime.

Week

Specifies the week in the current month.

Possible values:

- *none* (default setting)
- *first*
- *second*
- *third*
- *fourth*
- *last*

Day

Specifies the day of the week.

Possible values:

- *none* (default setting)
- *Sunday*
- *Monday*
- *Tuesday*
- *Wednesday*
- *Thursday*
- *Friday*
- *Saturday*

Month

Specifies the month.

Possible values:

- *none* (default setting)
- *January*
- *February*
- *March*
- *April*
- *May*
- *June*
- *July*
- *August*
- *September*
- *October*
- *November*
- *December*

Date

Specifies the non-recurring start date. This field lets you specify the values only when the radio button *Non-recurring* is selected in the *Operation* frame.

Possible values:

- a valid date in the format: `<name of the day>, [<name of the month> <dd>], <YYYY>`
  When you click this field, the device opens a calendar window. The calendar window displays the following details:
  - `Calender`
    Lets you select the value items for the year and month from the respective drop-down lists. The forward and backward arrows let you switch to the next and previous month, respectively. The month table lets you specify the date.
  - `Clear`
    Lets you clear the *Date* field.
  - `Today`
    Lets you specify the current system date.
  - `Close`
    Lets you close the clock window.

Time

Specifies the time.

Possible values:

- `<HH:MM AM/PM>`
  When you click this field, the device opens a clock window to specify the time in 12 hours format. The clock window displays the following details:
  - `HH:MM AM/PM`
    Displays the time in the digital format to let you select the hour, minute, and AM/PM components of the time.
  - `Analog clock`
    Displays the time in an analog clock to let you specify the values for the hour and minute components of the time.
  - `Clear`
    Lets you clear the *Time* field.
  - `Now`
    Lets you specify the current system time.
  - `Close`
    Lets you close the clock window.

2.2 NTPv4 Client

[Time > NTPv4 Client]

The device lets you synchronize the system time in the device using the Network Time Protocol (NTP). The device supports time synchronization based on the IPv4 protocol.

An NTP server synchronizes to a reference clock directly traceable to Coordinated Universal Time (UTC) such as Global Positioning System (GPS) or Galileo.

As an NTP client, the device evaluates the time information received from an NTP server and synchronizes the network time with one of the specified NTP servers. The device does not provide synchronization to other NTP clients.

Operation

Enables/disables the *NTPv4 Client* function in the device.

Possible values:

- `On`
  The *NTPv4 Client* function is active.
  The device obtains the time information from one of the specified NTP servers in the network, if the servers are available.
- `Off` (default setting)
  The *NTPv4 Client* function is inactive.

Table

For information on how to customize the appearance of the table, see “Working with tables” on page 14.

Buttons

Clear IPv4 address

Clears the IPv4 address in the selected table rows.

Index

Displays the index number of the NTP server to which the table row relates. The device lets you set up the IPv4 address of up to 5 NTP servers.

Possible values:

- `1..5`

IPv4 address

Specifies the IPv4 address of an NTP server. This field lets you specify the DNS name server as well.

Possible values:

- Valid IPv4 address (default setting: `<no-address>`)

Note: Depending on your requirements, verify that you specify only trustworthy NTP server addresses.

- Valid DNS name server

3 Device Security

The menu contains the following dialogs:

- User Management
- Authentication List
- Management Access
- SNMP

3.1 User Management

[Device Security > User Management]

If a user with privilege level 15 (administrator) logs in to the device, then the device lets you access the device management. In this dialog, you manage the user accounts of the local user management.

Table

Every user requires an active user account to gain access to the device management. This table lets you set up and manage the user accounts.

Buttons

 Add

Opens the *Create* window to set up a new user account in the device.

- In the *Username* field, specify the login name for the user account.
  Possible values:
  - Alphanumeric ASCII character string with 1..31 characters.

- In the *Password* field, specify the login password for the user account.
  The field displays the entered password as ***** (asterisks). The device differentiates between upper case and lower case, and validates the minimum length of the entered password.
  Possible values:
  - Alphanumeric ASCII character string with 6..31 characters.
    The device accepts the following characters:
  - `a..z`
  - `A..Z`
  - `0..9`
  - `!#$%&'()*+,-./:;<=>?@[\]^_`{|}~`
- In the *Privilege* field, you select an item to assign the privilege level to the user account.
  Possible values:
  - `0` (Unauthorized)
    The device rejects the login. Assign this value to temporarily lock the user account.
  - `1` (CLI guest)
    The user with this privilege level accesses the device only using the Command Line Interface with the `enable` prompt access. The `enable` prompt in the Command Line Interface lets the user access the limited read-only commands.
  - `2..14` (Guest)
    The user with this privilege level gets read-only access to the device using the Graphical User Interface and the Command Line Interface to perform the monitoring steps.
  - `15` (Administrator)
    The user with this privilege level gets read and write access to the device. The device lets this user monitor and manage the other user accounts on the device.

Remove

Removes the selected user account from the device, except the default Administrator user account.

Username

Displays the name of the user account.

Privilege

Specifies the privilege level of the user account.

Password

Displays ***** (asterisks) instead of the password characters.

3.2 Authentication List

[Device Security > Authentication List]

This dialog lets you validate the user to access the device management through the following protocols:

- Telnet
- SSH
- HTTP

Configuration

Application

Displays the connection type to access the device.

Possible values:

- Telnet
- SSH
- HTTP

Policy

Specifies the method type to validate the login credentials of the relevant connection type.

Possible values:

- *reject*
  No login method available. The device disables the login.
- *local* (default setting)
  The device uses the local database stored within the device to validate the login credentials.

Note: The Telnet and HTTP connections make the device insecure. In the default settings, the Telnet and HTTP connections are disabled.

3.3 Management Access

[Device Security > Management Access]

The menu contains the following dialogs:

- Server
- Virtual Terminal
- IP Access Restriction

3.3.1 Server

[Device Security > Management Access > Server]

This dialog lets you set up the services which enable users or applications to access the management of the device.

The dialog contains the following tabs:
- [SNMP]
- [Telnet]
- [SSH]
- [HTTP/HTTPS]

[SNMP]

This tab lets you enable/disable the SNMP server in the device.

Operation

SNMP server

Enables/disables the SNMP server.

Possible values:
- *On*
  SNMP server is enabled.
- *Off* (default setting)
  SNMP server is disabled.

[Telnet]

This tab lets you enable/disable the Telnet server in the device.

The Telnet server enables access to the device management remotely through the Command Line Interface. Telnet connections are unencrypted.

Operation

Telnet server

Enables/disables the Telnet server.

Possible values:

- *On*
  The Telnet server is enabled.
  The access to the device management is possible through the Command Line Interface using an unencrypted Telnet connection.
- *Off* (default setting)
  The Telnet server is disabled.

[SSH]

This tab lets you enable/disable the SSH server in the device and specify its settings. The server works with SSH version 2.

The SSH server enables access to the device management remotely through the Command Line Interface. SSH connections are encrypted.

The SSH server identifies itself to the clients using its public RSA key. When first setting up the connection, the client program displays the user the fingerprint of this key. The fingerprint contains a Base64-coded character sequence that is easy to check. When you make this character sequence available to the users through an authentic channel, they have the option to compare both fingerprints. If the character sequences match, then the client is connected to the correct server.

Operation

SSH server

Enables/disables the SSH server.

Possible values:

- *On* (default setting)
  The SSH server is enabled.
  The access to the device management is possible through the Command Line Interface using an encrypted SSH connection.
  You can start the server only if there is an RSA signature in the device.
- *Off*
  The SSH server is disabled.

Global parameters

TCP port

Displays the TCP port on which the server receives the SSH request from client.

Possible values:

- `22`

Sessions (max.)

Displays the maximum number of SSH connections to the device that can be set up simultaneously.

Possible values:

- `4`

Protocol level

Displays the current version of the SSH server on the device.

Possible values:

- `SSHv2`
  Secure Shell version 2 is the default SSH protocol version for the SSH server and client communication.

Active session

Displays the number of SSH connections currently established with the device.

Possible values:

- `0..4`
  The value `0` means no SSH connection currently established with the device.

Signature

Key present

Displays that the RSA host key is present in the device.

Possible values:

- `marked`

Oper status

Displays if the device is currently generating an RSA host key.

It is possible that another user may have triggered this action.

Possible values:

- `rsa`
  The device is currently generating an RSA host key.
- `none`
  The device is currently not generating an RSA host key.

Fingerprint

The fingerprint is an easy to verify string that uniquely identifies the host key of the SSH server.

The fingerprint is a *Base64*-coded SHA256 hash that uniquely identifies the host key of the SSH server.

Fingerprint type

Displays the type of fingerprint present.

Possible values:

- `sha256`
  The *Fingerprint* field displays the fingerprint as a *Base64*-coded SHA256 hash.

Fingerprint

Displays the fingerprint present.

Possible values:

- *Base64*-coded SHA256 hash.

[HTTP/HTTPS]

This tab lets you enable/disable the HTTPS protocol for the web server and specify the settings required for HTTPS.

The web server provides the Graphical User Interface through an encrypted *HTTPS* connection.

A digital certificate is required for the encryption of the HTTP connection. The device lets you create this certificate yourself or to load an existing certificate onto the device.

The device supports up to 50 simultaneous connections using HTTP or HTTPS.

Note: If you change the settings in this tab and click the ✓ button, then the device ends the session and disconnects every opened connection. To continue working with the Graphical User Interface, log in again.

Operation

HTTPS

Enables/disables the *HTTPS* protocol for the web server.

Possible values:

- `On` (default setting)
  The *HTTPS* protocol is enabled.
  The access to the device management is possible through an encrypted *HTTPS* connection.
  When there is no digital certificate present, the device generates a digital certificate before it enables the *HTTPS* protocol.
- `Off`
  The *HTTPS* protocol is disabled.
  When the *HTTPS* protocol is disabled, the access to the device management is possible through an unencrypted HTTP connection.

Note: If the *HTTP/HTTPS* protocols are disabled, then you can enable the *HTTPS* protocol using the Command Line Interface command `ip http secure-server` to enable access to the Graphical User Interface.

Redirect HTTP to HTTPS

Enables/disables the automatic redirection from HTTP to HTTPS.

Possible values:

- `On` (default setting)
  The device redirects from HTTP to HTTPS. The prerequisite is that the *HTTPS* mode is enabled.
- `Off`
  The device does not redirect from HTTP to HTTPS.

Certificate

If the device uses an *HTTPS* certificate not signed by a certification authority (CA) known to the web browser, then the web browser may display a warning message before loading the Graphical User Interface.

To address the warning, you have the following possibilities:

- Install an *HTTPS* certificate on the device whose CA is known to your web browser. This may additionally require you to make the CA known to your web browser or operating system.
- As a workaround, you can also add an exception rule for the existing device certificate in your web browser.

Note: Disable the *HTTPS* mode before creating, deleting, or importing a certificate.

Present

Displays if the digital certificate is present in the device.

Possible values:

- `marked`
  The certificate is present.
- `unmarked`
  The certificate has been removed.

Create

Generates a digital certificate in the device.

Alternatively, you have the option of copying your own certificate to the device. See the *Certificate import* frame.

Delete

Deletes the digital certificate.

Certificate import

URL

Specifies the path and file name of the certificate.

The device accepts certificates with the following properties:

- `.PEM` file name extension

The device gives you the following options for copying the certificate to the device:

- Import from a TFTP server
  When the certificate is on a TFTP server, specify the URL for the file in the following form:
  `tftp://<IP address>/<path>/<file name>`
- Import from a HTTP server
  When the certificate is on a HTTP server, specify the URL for the file in the following form:
  `http://<IP address>/<path>/<file name>`

Start

Copies the certificate specified in the *URL* field to the device.

3.3.2 Virtual Terminal

[Device Security > Management Access > Virtual Terminal]

[Configuration]

Table

VTY ID

Displays the Virtual terminal (VTY) ID of the session.

Possible values:

- `0..15`

Session timeout [min]

Specifies the timeout in minutes. After the user logged in has been inactive for this time, the device ends the connection. Using the Command Line Interface, the user gets an option to configure this value in minutes and seconds as well.

A change in the value takes effect the next time a user logs in.

Possible values:

- `0`
  Deactivates the function. The connection remains established in the case of inactivity.
- `1..1500` (default setting: `10`)

[Status]

Table

VTY ID

Displays the Virtual terminal (VTY) ID of the session.

Possible values:

- `0..15`

IP address type

Displays the type of IP address of the client.

IP address

Displays the IP address of the client.

Possible values:

- Valid IPv4 address

Client port

Displays the TCP/IP port of the client that is used to establish a connection with the server.

Privilege

Displays the privilege level of the client user account.

Possible values:

- `1..15`

Elapsed time

Displays the time passed since the connection established in days, hours, minutes, seconds.

Idle time

Displays the inactivity time passed since the last activity performed by the client in days, hours, minutes, seconds.

Login type

Displays the login type of the connection.

3.3.3 IP Access Restriction

[Device Security > Management Access > IP Access Restriction]

This dialog lets you restrict the access to the device management to specific IPv4 address ranges and selected IP-based protocol.

- If the function is disabled, then the access to the device management is possible from any IPv4 address and using every supported IP-based protocol.
- If the function is enabled, then the access is restricted.

Operation

Before you enable the function, verify that at least one active table row in the table lets you access. Otherwise, if you change the settings, then the connection to the device terminates. You may get locked out of the device.

Mode

Enables/disables the *IP Access Restriction* function.

Possible values:

- `On`
  The *IP Access Restriction* function is enabled.
  The access to the device management is restricted.
- `Off` (default setting)
  The *IP Access Restriction* function is disabled.

[Configuration]

This tab lets you configure the entries for management access filtering.

Table

For information on how to customize the appearance of the table, see “Working with tables” on page 14.

Buttons

 Add

Opens the *Create* window to add a table row.

- In the *Index* field, specify the index number.
- In the *VLAN ID* field, specify the VLAN ID.
- In the *Start address* field, specify the start IPv4 address of the address range.
- In the *End address* field, specify the end IPv4 address of the address range.
- Mark the *HTTP/HTTPS* checkbox to activate the HTTP/HTTPS access.

- Mark the *SNMP* checkbox to activate the SNMP access.
- Mark the *Telnet/SSH* checkbox to activate the Telnet/SSH access.

 Remove

Removes the selected table row.

Index

Displays the index number to which the table row relates.

Possible values:

- `1..16`

VLAN ID

Specifies the VLAN ID to which the table row relates.

Possible values:

- `1..4093`

Start address

Specifies the start IPv4 address of the address range.

Possible values:

- Valid IPv4 address

End address

Specifies the end IPv4 address of the address range.

Possible values:

- Valid IPv4 address

HTTP/HTTPS

Activates/deactivates the HTTP/HTTPS access.

Possible values:

- `marked` (default setting)
  Access is activated for the specified IPv4 address range.
- `unmarked`
  Access is deactivated.

SNMP

Activates/deactivates the SNMP access.

Possible values:

- `marked` (default setting)
  Access is activated for the specified IPv4 address range.
- `unmarked`
  Access is deactivated.

Telnet/SSH

Activates/deactivates the Telnet/SSH access.

Possible values:

- `marked` (default setting)
  Access is activated for the specified IPv4 address range.
- `unmarked`
  Access is deactivated.

[Statistics]

This tab displays the following overview:

- Number of data packets received by the device
  - *HTTP received packets*
  - *HTTPS received packets*
  - *SNMP received packets*
  - *Telnet received packets*
  - *SSH received packets*
- Number of data packets allowed by the device
  - *HTTP allowed packets*
  - *HTTPS allowed packets*
  - *SNMP allowed packets*
  - *Telnet allowed packets*
  - *SSH allowed packets*
- Number of data packets discarded by the device
  - *HTTP discarded packets*
  - *HTTPS discarded packets*
  - *SNMP discarded packets*
  - *Telnet discarded packets*
  - *SSH discarded packets*

To reset the statistics counters in the table to `0`, click the button.

3.4 SNMP

[Device Security > SNMP]

Simple Network Management Protocol (SNMP) in the device lets you collect and organize information about the managed devices on IP networks. The device also lets you modify the collected information to change the device behavior. The devices that typically support SNMP include cable modems, routers, switches, servers, workstations, printers. You use the SNMP in network management for network monitoring. SNMP exposes management data in the form of variables on the managed systems organized in a management information base (MIB) which describes the system status and configuration. These variables can then be remotely queried (and, in some circumstances, customized) by managing applications.

3.4.1 Configuration

[Device Security > SNMP > Configuration]

Global

Mode

Enables/disables the *SNMP*.

Possible values:

- `On`
  The *SNMP* is enabled.
- `Off` (default setting)
  The *SNMP* is disabled.

Engine ID

Specifies the engine ID of the context. The engine ID indicates the context in which you access the management information.

Possible values:

- Alphanumeric ASCII character string with 10..64 characters (default setting: local engine ID with last 12 characters as the MAC address of the device)

The device lets you set up the respective SNMP settings in the following tabs:

- [Community v1/v2]
- [User]
- [Group]
- [View]
- [Access]

The device does not contain any default SNMP settings in the following tabs:

- [Community v1/v2]
- [User]
- [Group]
- [Access]

The device lets you set up the following:

- Add a community or user on the device with no prerequisites required, see [Community v1/v2] and [User] tabs.
- Add a group only when, at least 1 community or user is configured on the device, see [Group] tab.
- Add a view on the device with no prerequisites required. The configured view is needed while setting up an SNMP access, see [View] tab.
- Add an access only when, at least 1 group and 1 view are configured on the device, see [Access] tab.

[Community v1/v2]

In this dialog you specify the community name for the *SNMPv1/v2* protocol based applications. The applications send requests via *SNMPv1/v2* with a community name in the SNMP data packet header. Depending on the access settings, the community gets read only, or read and write access.

Table

For information on how to customize the appearance of the table, see “Working with tables” on page 14.

Buttons

 Add

Opens the *Create* window to add a new table row.

- In the *Community name* field, specify the *SNMP* community name.
  Possible values:
  - Alphanumeric ASCII character string with 1..32 characters
- In the *Source IP range* field, specify a valid IPv4 address or subnet.
- In the *Prefix* field, specify the prefix size for the *Source IP range*.
  Possible values:
  - `0..32`
- In the *Community secret* field, specify the password for the *SNMP* community.
  Possible values:
  - Alphanumeric ASCII character string with 1..32 characters (default setting: none)

 Remove

Removes the selected table row.

Community name

Specifies a name for this SNMP community.

Possible values:

- Alphanumeric ASCII character string with 1..32 characters

Source IP range

Specifies the IPv4 address or subnet of the Network Management System (NMS) which can perform the SNMP operation.

Possible values:

- Valid IPv4 address

Prefix

Specifies the prefix of the host IP.

Possible values:

- `0..32`

Community secret

Specifies the password for this SNMP community.

Possible values:

- Alphanumeric ASCII character string with 1..32 characters (default setting: none)

[User]

The SNMPv3 protocol provides authentication and encryption for SNMP messages. In this dialog, you specify the SNMP v3 user with a username associated with an engine-id, security level, authentication protocol, authentication password, privacy protocol, and privacy password. The security level defines the usage of authentication and encryption mechanism for the SNMPv3 messages.

Table

For information on how to customize the appearance of the table, see “Working with tables” on page 14.

Buttons

 Add

Opens the *Create* window to add a new table row.

- In the *Username* field, specify the name for the user entry.
  Possible values:
  - Alphanumeric ASCII character string with 1..32 characters
- In the *Engine ID* field, specify the engine ID of the SNMP instance.
  Possible values:
  - Alphanumeric ASCII character string with 10..64 characters except every character as zero (0) or (F) (default setting: local engine ID with the last 12 characters as the MAC address of the device)

 Remove

Removes the selected table row.

Username

Specifies the user name of this entry.

Possible values:

- Alphanumeric ASCII character string with 1..32 characters

Engine ID

Specifies the *SNMPv3* engine ID.

Possible values:

- Alphanumeric ASCII character string with 10..64 characters except every character as zero (0) or (F) (default setting: local engine ID with the last 12 characters as the MAC address of the device)

Security level

Specifies the security level of this entry.

Possible values:

- `no auth no priv` (default setting)
  Applies no authentication and no privacy settings.
- `auth no priv`
  Applies authentication settings only.
- `auth priv`
  Applies both authentication, and the privacy settings.

Auth protocol

Specifies the authentication protocol of this entry. This field is read-only if the *Security level* field contains the value *no auth no priv*.

Possible values:

- *no auth* (default setting)
  Applies no authentication protocol.
- *MD5*
  Applies the MD5 authentication protocol.
- *SHA*
  Applies the SHA authentication protocol.

Auth password

Specifies the authentication password of this entry. This field is read-only if the *Security level* field contains the value *no auth no priv*.

Possible values:

- Alphanumeric ASCII character string with 8..32 characters for the MD5.
- Alphanumeric ASCII character string with 8..40 characters for the SHA.

Priv protocol

Specifies the privacy protocol of this entry. This field is read-only if the *Security level* field contains the value *no auth no priv* or *auth no priv*.

Possible values:

- *no priv* (default setting)
  Applies no privacy protocol.
- *DES*
  Applies the DES privacy protocol.

Priv password

Specifies the privacy password of this entry. This field is read-only if the *Security level* field contains the value *no auth no priv* or *auth no priv*.

Possible values:

- Alphanumeric ASCII character string with 8..32 characters

[Group]

SNMP groups are used to associate existing community or user with security model.

Before creating an SNMP group, you need to ensure that at least 1 entry is available in the *Community v1/v2* or *User* tab.

Table

For information on how to customize the appearance of the table, see “Working with tables” on page 14.

Buttons


Add

Opens the *Create* window to add a new table row.

- In the *Group name* field, specify the name for this group entry.
  Possible values:
  - Alphanumeric ASCII character string with 1..32 characters
- In the *User/Community* field, select the value item to be associated with this group entry from the drop-down list.
  Possible values:
  - A list of the entries created in the *Community v1/v2* and *User* tabs.
- In the *Security model* field, select a value item from the drop-down list which matches with the user or community selection.
  Possible values:
  - *v1*
  - *v2c*
  - *v3*


Remove

Removes the selected table row.

Group name

Specifies the access group name of this group entry.

Possible values:

- Alphanumeric ASCII character string with 1..32 characters

User/Community

Displays the security name of this entry.

Security model

Displays the security model of this entry.

Possible values:

- *v1*
- *v2c* (default setting)
- *v3*

[View]

SNMP view lets you specify the settings to include or exclude specific Object Identifier (OID) of the MIB tree. The specified view lets the device control the level of detail that an SNMP community or user can retrieve or modify.

Table

For information on how to customize the appearance of the table, see “Working with tables” on page 14.

Buttons

 Add

Opens the *Create* window to add a new table row.

- In the *Name* field, specify the name for this view entry.
  Possible values:
  - Alphanumeric ASCII character string with 1..32 characters
- In the *Sub tree* field, specify the OID to be associated with the view entry.
  Possible values:
  - A valid Object Identifier (OID) value.

 Remove

Removes the selected table row.

Name

Displays the name of this view entry.

Possible values:

- Alphanumeric ASCII character string with 1..32 characters (default setting: `default_view`)

View type

Specifies the view type of this entry from the drop-down list.

Possible values:

- *`included`*
  The subtree is accessible.
- *`excluded`*
  The subtree is inaccessible.

Sub tree

Specifies the Object Identifier (OID) that defines the subtree to be associated with the named view.

Possible values:
- up to 32 OID length

[Access]

SNMP access defines the permissions granted to the SNMP group. The access settings specify the required view that controls the read/write operation of an SNMP group. Access control is imperative for security and ensures that only the authorized group can retrieve or modify specific information on the network devices.

To set up an SNMP access the prerequisite is to create the following set up first:
- Create at least 1 SNMP group in the *Group* tab.
- Ensure that the required view is available on the device, in the *View* tab.

Table

For information on how to customize the appearance of the table, see “Working with tables” on page 14.

Buttons

 Add

Opens the *Create* window to add a new table row.
- In the *Group name* field, select the group name to be associated from the drop-down list.
  Possible values:
  - A list of the group entries created in the *Group* tab.
- In the *Security model* field, select a value item from the drop-down list.
  Possible values:
  - *v1*
  - *v2c*
  - *v3*
- In the *Security level* field, select a value item from the drop-down list.
  Possible values:
  - *no auth no priv*
  - *auth no priv*
  - *auth priv*
- In the *Read view* field, select a value item from the drop-down list.
  Possible values:
  - Alphanumeric ASCII character string with 1..32 characters (default setting: `default_view`)

 Remove

Removes the selected table row.

Group name

Displays the name of the group entry selected for the access.

Possible values:

- Alphanumeric ASCII character string with 1..32 characters

Security model

Displays the security model of this entry.

Possible values:

- *v1*
- *v2c*
- *v3*

Security level

Displays the security level of this entry.

Possible values:

- *no auth no priv*
  Applies no authentication and no privacy protocol.
- *auth no priv*
  Applies authentication protocol only.
- *auth priv*
  Applies both authentication, and the privacy protocol.

Read view

Specifies the name of the MIB view that this access entry is allowed to read.

Possible values:

- Alphanumeric ASCII character string with 1..32 characters (default setting: `default_view`)

Write view

Specifies the name of the MIB view that this access entry is allowed to write.

Possible values:

- Alphanumeric ASCII character string with 1..32 characters (default setting: `none`)

3.4.2 Trap

[Device Security > SNMP > Trap]

[Source trap]

Table

For information on how to customize the appearance of the table, see “Working with tables” on page 14.

Buttons

Add

Opens the *Create* window to add a new table row.

- In the *Name* field, select a value item from the drop-down list.
  Possible values:
  - *Link up*
    When the connection is established to a port, this trap is sent.
  - *Link down*
    When the connection to a port is interrupted, this trap is sent.
  - *New root*
    In the *Switching > L2-Redundancy > Spanning Tree > Global* dialog, *Traps* frame, when a new bridge takes over the root bridge role, this trap is sent.
  - *Cold start*
    After the system startup is completed, this trap is sent.
  - *Warm start*
    When the SNMP entity is reinitializing itself in a way that the configuration remains unaltered, this trap is sent.
  - *Rising alarm*
    When the RMON input exceeds its upper threshold, this trap is sent.
  - *Falling alarm*
    When the RMON input goes below its lower threshold, this trap is sent.
  - *Topology change*
    When there is a transition in the port state that effectively changes the spanning tree topology, this trap is sent.
  - *Alarm trap status*
    When an alarm configuration is created, deleted, or there is a change in the status of the configured alarm expression, this trap is sent.
  - *Ent config change*
    When there is change in the entity MIB table entries, this trap is sent.
  - *PSec trap interfaces*
    In the *Network Security > Port Security* dialog, *Interface* tab, when an entry is created, deleted, or there is a change in the values associated with the configuration, this trap is sent.
  - *IP trap interfaces link*
    When an interface VLAN is created, modified or deleted, this trap is sent.
  - *Authentication failure*
    When the NMS is trying to execute the SNMP operation and the SNMP authentication is failed, this trap is sent.
  - *PSec trap global main*
    When the port security address table is full or becomes available to accommodate new entries, this trap is sent.

– *LLDP rem tables change*
When an entry is created, modified, or deleted in the tables associated with the LLDP remote systems data, this trap is sent.

Remove

Removes the selected table row.

Name

Displays the name of this source trap.

Index filter

Specifies the Object Identifier (OID) sub tree to use as an index filter.

Filter type

Specifies the type of filter for this source trap entry.

Possible values:

- *included*
  The subtree is accessible.
- *excluded*
  The subtree is inaccessible.

[Receiver trap]

Table

For information on how to customize the appearance of the table, see “Working with tables” on page 14.

Buttons

Add

Opens the *Create* window to add a new table row.

- In the *Name* field, specify a name for this receiver trap.
  Possible values:
  – Alphanumeric ASCII character string with 1..32 characters

Remove

Removes the selected table row.

Name

Displays the name of this receiver trap.

Enable

Activates/deactivates the receiver trap.

Possible values:

- `marked`
  The receiver trap is active.
- `unmarked`
  The receiver trap is inactive.

Address

Specifies the IPv4 address of the receiver trap.

Possible values:

- Valid IPv4 address

Port

Specifies the port number of the receiver trap.

Possible values:

- `162` (default setting)

Version

Specifies the SNMP version.

Possible values:

- *v1*
- *v2*
- *v3*

Community

Specifies the community secret to be used for the SNMP traps.

Possible values:

- Alphanumeric ASCII character string with 1..32 characters

Engine ID

Specifies the engine ID of the *SNMPv3* instance.

Possible values:

- Alphanumeric ASCII character string with 10..64 characters, each zero (0) and F are not accepted (default setting: local engine ID)

Username

Specifies the user name of the *SNMPv3* protocol.

Possible values:

- Alphanumeric ASCII character string with 1..32 characters

Notify type

Specifies the notification type.

Possible values:

- `trap`
  Does not notify when the data packet is received at the destination.
- `inform`
  Notifies when the data packet is received at the destination.

Timeout

Specifies the time in seconds that the device waits for an acknowledgement from the host, before resending the trap. This is applicable only when the *Notify type* contains the value `inform`.

Possible values:

- `0..2147` (default setting: `3`)

Retries

Specifies the maximum number of attempts that the device executes to resend the trap. This is applicable only when the *Notify type* contains the value `inform`.

Possible values:

- `0..255` (default setting: `5`)

4 Network Security

The menu contains the following dialogs:

- Port Security

4.1 Port Security

[Network Security > Port Security]

The device lets you limit the forwarding of data packets to those with specific source addresses. The device forwards only data packets from desired senders received on a port. When the *Port Security* function is active, the device checks the VLAN ID and MAC address of the sender before it forwards a data packet. The device discards data packets with an undesired source address and logs this event.

To simplify the setup process, the device lets you record the source address of the desired data packets automatically. The device “learns” the source addresses by evaluating the received data packets. In the device, these addresses are known as *dynamic entries*. When a user-defined upper limit for the learned addresses has been reached, the device stops the “learning” on the relevant port. The device forwards only the data packets of the senders already registered on the port. When you adapt the upper limit to the number of expected senders, you thus make *MAC Flooding* attacks more difficult.

Note: With the automatic recording of the *dynamic entries*, the device constantly discards the first data packet from an unknown sender. Using this first data packet, the device checks if the upper limit has been reached. The device records the addresses until the upper limit is reached. Afterward, the device forwards data packets that it receives on the relevant port from this sender.

The dialog contains the following tabs:

- [Interface]
- [MAC address]

Global

Enable aging

Activates/deactivates the deleting of allowed MAC addresses entries from the port security address table.

Possible values:

- `marked`
  The function is active.
- `unmarked` (default setting)
  The function is inactive.

Aging period [s]

Specifies the aging time in seconds, after which the device deletes MAC address entries from the port security address table.

Possible values:

- `10..10000000` (default setting: `3600`)

Hold time [s]

Specifies the hold time in seconds to determine how long a MAC address is held in the port security address table after violating the limit.

Possible values:

- `10..10000000` (default setting: `300`)

Traps

Port security global

Activates/deactivates the sending of traps if one or more objects are updated and the sending of traps for these objects is active.

Possible values:

- `marked`
  The function is active.
- `unmarked` (default setting)
  The function is inactive.

Port security interface

Activates/deactivates the sending of traps if a row is added, modified, or deleted. The index and value of the table row that has been added, modified, or deleted is sent in the trap.

Possible values:

- `marked`
  The function is active.
- `unmarked` (default setting)
  The function is inactive.

MAC status

Current unused MAC count

Displays the number of currently unused MAC addresses in the port security table.

Total MAC count

Displays the total number of MAC addresses in the port security table managed by the device.

[Interface]

Table

Port

Displays the port number.

Users

Displays the port security users that are enabled on the port.

Possible values:

- *administrative user*
  The software module *administrative user* controls the forwarding or blocking of a MAC address.
- *DHCP snooping*
  The software module *DHCP snooping* controls the forwarding or blocking of a MAC address.
- -
  No software module active on the port.

Active

Activates/deactivates the port security function on the port.

Possible values:

- marked
  The port security function is active.
- unmarked (default setting)
  The port security function is inactive.

MAC count

Displays the number of MAC addresses currently assigned to the port.

This includes the number of violating MAC addresses. The prerequisite is that you select the value *restrict* in the *Violation mode* column.

Violation mode

Specifies the violation mode of the device when the specified limit is reached.

Possible values:

- *protect* (default setting)
  Do not allow more than the specified limit of MAC addresses on the port, but take no further action.

- *restrict*
  If the learning limit is reached, subsequent MAC addresses on the port will be counted and marked as violating. Such MAC addresses are removed from the port security table when the hold time expires. The maximum number of MAC addresses that can be marked as violating depends on the violation limit set on the port.
- *shutdown*
  If the learning limit is reached, one additional undesired MAC address causes the port to be shut down. The device removes the previously learned MAC addresses on the port and stops learning new MAC addresses.

Sticky

Activates/deactivates the sticky learning of MAC addresses on the port. When the port is in sticky mode, every MAC address that would otherwise have been learned as dynamic is learned as sticky.

Sticky MAC addresses are part of the running-config and can therefore be saved to startup-config. Sticky MAC addresses survive link changes (in contrast to dynamic MAC addresses, which will have to be learned again). They also survive reboots if the running-config is saved to the startup-config.

Possible values:

- `marked`
  The sticky function is active.
- `unmarked` (default setting)
  The sticky function is inactive.

Limit reached

Displays if the source MAC address limit is reached on the port.

Possible values:

- `marked`
  Source MAC address limit is reached.
- `unmarked`
  Source MAC address limit not reached.

Static limit

Specifies the maximum number of MAC addresses that are allowed on the port.

Possible values:

- `1..1023` (default setting: `4`)

Violation limit

Specifies the maximum number of MAC addresses that can be marked as violating on the port.

Possible values:

- `1..1023` (default setting: `4`)

Latest violating VLAN

Displays the VLAN ID of the last violating host. The prerequisite is that you select the value *restrict* or *shutdown* in the *Violation mode* column.

Latest violating MAC

Displays the source MAC address of the last violating host. The prerequisite is that you select the value *restrict* or *shutdown* in the *Violation mode* column.

Current violate count

Displays the current number of violating MAC addresses. The prerequisite is that you select the value *restrict* in the *Violation mode* column.

Total violate count

Displays the total number of violating MAC addresses. The prerequisite is that you select the value *restrict* in the *Violation mode* column.

[MAC address]

Table

Buttons

Add

Opens the *Create* window to add a table row.

- In the *Port* field, you specify the port number.
- In the *VLAN ID* field, you specify the VLAN ID.
- In the *MAC address* field, you specify the MAC address to which the table row applies.
- In the *MAC type* drop-down list, select the type of the MAC address.
  - *static*
    The static MAC address is not affected by the aging period and remains added to the port security MAC address table.
  - *sticky*
    The sticky MAC address is part of the running-config, so survives the link state changes. It also survives reboots if saved to the startup-config.

Remove

Removes the selected table row.

Port

Displays the port number.

VLAN ID

Displays the VLAN ID to which the table row applies.

MAC address

Displays the MAC address to which the table row applies.

MAC type

Displays how the MAC address was learned on the port.

Possible values:

- *static*
- *sticky*

Creation time

Displays the creation time of the MAC address. This is synchronized with the system time of the device.

Changed time

Displays the last change time of the MAC address. This is synchronized with the system time of the device.

Age hold time

Displays the time (in seconds) left for the aging period or the hold time.

MAC violating

Displays if a MAC address is violating the limit and gets blocked.

Possible values:

- `marked`
  The device detected that the MAC address is violating the limit.
- `unmarked`
  The MAC address does not violate the limit.

MAC blocked

Displays if the MAC address is blocked from forwarding after hold-time expired.

Possible values:

- `marked`
  The device blocked the MAC address from forwarding. The MAC addresses in this state are subject to hold-time expiration.
- `unmarked`
  The MAC address is not blocked from forwarding.

MAC kept blocked

Displays if a MAC address is kept blocked from forwarding.

Possible values:

- `marked`
  The device kept blocked the MAC address from forwarding. The MAC addresses in this state are not subject to hold-time expiration.
- `unmarked`
  The MAC address is not kept blocked from forwarding.

CPU copying

Displays if the CPU copying is enabled for a MAC address due to aging. This is used for debugging.

Possible values:

- `marked`
  The CPU copying function is active.
- `unmarked`
  The CPU copying function is inactive.

Age frame seen

Displays if the device detected a frame during aging of a MAC address. This is used for debugging.

Possible values:

- `marked`
  The device detected a frame during aging of MAC address.
- `unmarked`
  The device did not detect a frame during aging of MAC address.

Forward administrative user

Displays if the source MAC address is marked as forwarding by an *administrative user*.

Possible values:

- `marked`
  The source MAC address is marked as forwarding by an *administrative user*.
- `unmarked`
  The source MAC address is not marked as forwarding by an *administrative user*.

Forward 802.1X

Displays if the source MAC address is marked as forwarding by *802.1X*.

Possible values:

- `marked`
  The source MAC address is marked as forwarding by *802.1X*.
- `unmarked`
  The source MAC address is not marked as forwarding by *802.1X*.

Forward DHCP snooping

Displays if the source MAC address is marked as forwarding by *DHCP snooping*.

Possible values:

- `marked`
  The source MAC address is marked as forwarding by *DHCP snooping*.
- `unmarked`
  The source MAC address is not marked as forwarding by *DHCP snooping*.

Forward voice VLAN

Displays if the source MAC address is marked as forwarding by *voice VLAN*.

Possible values:

- `marked`
  The source MAC address is marked as forwarding by *voice VLAN*.
- `unmarked`
  The source MAC address is not marked as forwarding by *voice VLAN*.

Block administrative user

Displays if the source MAC address is marked as blocked by an *administrative user*.

Possible values:

- `marked`
  The source MAC address is marked as blocked by an *administrative user*.
- `unmarked`
  The source MAC address is not marked as blocked by an *administrative user*.

Block forward 802.1X

Displays if the source MAC address is marked as blocked by *802.1X*.

Possible values:

- `marked`
  The source MAC address is marked as blocked by *802.1X*.
- `unmarked`
  The source MAC address is not marked as blocked by *802.1X*.

Block DHCP snooping

Displays if the source MAC address is marked as blocked by *DHCP snooping*.

Possible values:

- `marked`
  The source MAC address is marked as blocked by *DHCP snooping*.
- `unmarked`
  The source MAC address is not marked as blocked by *DHCP snooping*.

Block voice VLAN

Displays if the source MAC address is marked as blocked by *voice VLAN*.

Possible values:

- `marked`
  The source MAC address is marked as blocked by *voice VLAN*.
- `unmarked`
  The source MAC address is not marked as blocked by *voice VLAN*.

Keep blocked administrative user

Displays if the source MAC address is marked as keep blocked by an *administrative user*.

Possible values:

- `marked`
  The source MAC address is marked as keep blocked by an *administrative user*.
- `unmarked`
  The source MAC address is not marked as keep blocked by an *administrative user*.

Keep blocked 802.1X

Displays if the source MAC address is marked as keep blocked by *802.1X*.

Possible values:

- `marked`
  The source MAC address is marked as keep blocked by *802.1X*.
- `unmarked`
  The source MAC address is not marked as keep blocked by *802.1X*.

Keep blocked DHCP snooping

Displays if the source MAC address is marked as keep blocked by *DHCP snooping*.

Possible values:

- `marked`
  The source MAC address is marked as keep blocked by *DHCP snooping*.
- `unmarked`
  The source MAC address is not marked as keep blocked by *DHCP snooping*.

Keep blocked voice VLAN

Displays if the source MAC address is marked as keep blocked by *voice VLAN*.

Possible values:

- `marked`
  The source MAC address is marked as keep blocked by *voice VLAN*.
- `unmarked`
  The source MAC address is not marked as keep blocked by *voice VLAN*.

5 Switching

The menu contains the following dialogs:

- Switching Global
- Filter for MAC Addresses
- VLAN
- IPMC
- IGMP Snooping
- QoS
- L2-Redundancy

5.1 Switching Global

[Switching > Global]

[Aging]

Global parameters

MAC address aging

Enables/disables the *MAC address aging* function.

Possible values:

- *On* (default setting)
- *Off*

Age time [s]

Specifies the aging time in seconds.

Possible values:

- `10..1000000` (default setting: `300`)

The device monitors the age of the learned unicast MAC addresses. If the learned address entries exceed the specified age time, the device deletes them from the address table.

You find the address table in the *Switching > Filter for MAC Addresses* dialog.

MAC address

MAC address

Displays the *MAC address* of the device.

Total learned MAC addresses

Dynamic

Displays the number of dynamic MAC addresses learned.

Static

Displays the number of static MAC addresses configured.

[Port learning]

Table

Interface

Displays the physical port number.

Learning mode

Displays/specifies the learning mode of the port.

Possible values:

- *auto*
  When the port receives a frame with an unknown source MAC address, the device auto-learns that.
- *disable*
  Learning the unknown source MAC addresses is disabled.
- *secure*
  The device learns only the static MAC entries and discards the other frames.

Learned MAC address count

Displays the number of dynamically learned MAC addresses.

[VLAN learning]

Table

VLAN ID

Displays the VLAN ID.

Possible values:

- `1..4093`

MAC learning

Activates/deactivates the MAC learning for the VLAN ID.

Possible values:

- `marked`
  The MAC learning is active.
- `unmarked`
  The MAC learning is inactive.

5.2 Filter for MAC Addresses

[Switching > Filter for MAC Addresses]

This dialog displays and lets you edit the address filters in the MAC address table. Address filters specify the way the data packets are forwarded based on the destination MAC address entry in the table.

Each table row represents one filter. The device automatically sets up the filters based on the learned source MAC addresses. The device lets you set up additional filters manually.

The device transmits the data packets as follows:
- When the table contains an entry for the destination address of a data packet, the device transmits the data packet from the receiving port to the port specified in the table entry.
- When there is no table entry for the destination address, the device transmits the data packet from the receiving port to every other port.

VLAN 1 is the default VLAN ID that accepts the incoming frames.

Table

Buttons


Add

Opens the *Create* window to set up a new filter.
- In the *VLAN ID* field, specify the VLAN ID.
  Possible values:
  - `1..4093`
- In the *MAC address* field, specify a valid MAC address.
- In the *Port list* field, specify the physical port number.
  Possible values:
  - `Fa 1/1..Fa 1/7, Gi 1/1..Gi 1/3`
    `Fa` is the Fast Ethernet port and `Gi` is the Gigabit Ethernet port.


Remove

Removes the selected table row containing the static entry.


Clear MAC address table

Clears every dynamic entry from the table.

VLAN ID

Displays the VLAN ID.

Possible values:

- `1..4093`

MAC address

Displays the destination MAC address of the table entry.

Type

Displays the type of MAC entry.

Possible values:

- *Dynamic*
  The entry is dynamically learned.
- *Static*
  The entry is statically added.

CPU

Displays if the device copies the incoming frames to the CPU.

Possible values:

- `marked`
  The device copies the incoming frames to the CPU.
- `unmarked`
  The device does not copy the incoming frames to the CPU.

<Port numbers>

Activates/deactivates the port.

Possible values:

- `marked`
  Activates the port for transmitting the data packets.
- `unmarked`
  Deactivates the port from transmitting the data packets.

5.3 IPMC

[Switching > IPMC]

This dialog lets you specify the address range associated with an Internet Protocol Multicast Configuration (IPMC) profile. IPMC helps to provide access control for filtering group address registration. The device allows a maximum of 64 profiles with a maximum of 128 corresponding rules for each profile.

The dialog contains the following tabs:
- [Address range]
- [Profile settings]

[Address range]

Table

Buttons

In the following list, you find a description of buttons specific to this dialog. For a description of the non-listed buttons, see “Standard buttons” on page 13.

 Add

Opens the *Create* window to add an entry to the table.
- In the *Range name* field, you specify the name of the address range.
- In the *Start address* field, you specify the start address of the address range.
- In the *End address* field, you specify the end address of the address range.

 Remove

Removes the selected table row.

Range name

Specifies the range name of the IPv4 Multicast address range.

Each range has a unique name. This is limited to the alphanumeric ASCII character string with 1..16 characters.

Possible values:
- Alphanumeric ASCII character string with 1..16 characters.

Start address

Specifies the start IPv4 Multicast address of the address range.

End address

Specifies the end IPv4 Multicast address of the address range.

[Profile settings]

IPMC

Enables/disables the function of filtering profiles based on profile settings.

Possible values:

- `On`
  The *IPMC* is enabled. The device filters received IPv4 Multicast packets based on profile settings.
- `Off` (default setting)
  The *IPMC* is disabled.

Table

Buttons

In the following list, you find a description of buttons specific to this dialog. For a description of the non-listed buttons, see “Standard buttons” on page 13.


Add

Opens the *Create* window to add an entry to the table.

- In the *Profile name* field, you specify a profile name.
- In the *Profile description* field, you specify the additional information about the profile.


Remove

Removes the selected table row.


Wizard

Opens the *Wizard* window that helps you set up the profile. See “[Wizard: IPMC]” on page 102.

Profile name

Specifies the profile name used for indexing the profile table. Each entry has a unique profile name.

Possible values:
- Alphanumeric ASCII character string with 1..16 characters.

Profile description

Specifies the additional information about the profile.

Possible values:
- Alphanumeric ASCII character string with 0..64 characters.

Range name

Displays the range name assigned to a profile. Multiple range names (comma-separated) can be assigned to a profile.

Rules

Displays the number of rules applied to a profile.

[Wizard: IPMC]

The *Wizard* window helps you to set up the profile.

The *Wizard* window guides you through the following steps:
- Select profile
- Configuration

After closing the *Wizard* window, click the ✓ button to apply your settings.

Select profile

Profile name

Select the profile name.

Configuration

Profile name

Displays the profile name.

Range name

Select the range name.

Address range

Displays the address range.

Next rule range

Select the next rule range if more than one rule exists.

Action

Specifies how the device processes received data packets if the rule matches.

Possible values:

- *Permit* (default setting)
  The device forwards the data packets.
- *Deny*
  The device discards the data packets.

Log

Activates/deactivates the creating of a syslog entry if the rule matches.

Possible values:

- `marked`
  The device creates a syslog entry.
- `unmarked` (default setting)
  The device does not create a syslog entry.

Update address range

Creates an entry based on the values specified in the *Range name* and *Next rule range* fields. As a result, you find a new entry in the lower part of the *Wizard* window.

Entries in the lower part of the window

The lower part of the *Wizard* window displays the rule list.

When you click the icon, the device removes the entry from the rule list.

5.4 IGMP Snooping

[Switching > IGMP Snooping]

IGMP (Internet Group Management Protocol) is a protocol for dynamically managing Multicast groups. The protocol describes the distribution of Multicast data packets between routers and end devices on Layer 3.

The device lets you use the *IGMP Snooping* function and also use the IGMP mechanisms on Layer 2:
- Without *IGMP Snooping*, the device forwards the Multicast data packets to every port.
- With the *IGMP Snooping* function active, the device forwards the Multicast data packets only on ports to which Multicast receivers are connected. This reduces the network load. The device evaluates the IGMP data packets transmitted on Layer 3 and uses the information on Layer 2.

Activate the *IGMP Snooping* function when the following conditions are fulfilled:
- There is a Multicast router in the network that creates IGMP queries (periodic queries).
- The devices participating in IGMP Snooping forward the IGMP queries.

The device links the IGMP Report with the entries in its address table. When a Multicast receiver joins a Multicast group, the device creates a table entry for this port. When the Multicast receiver leaves the Multicast group, the device removes the table entry.

The menu contains the following dialogs:
- Global
- Configuration
- Querier
- Status

5.4.1 Global

[Switching > IGMP Snooping > Global]

This dialog lets you enable/disable the *IGMP Snooping* protocol in the device.

Configuration

Snooping function

Enables/disables the *IGMP Snooping* function in the device.

Possible values:

- `On`
  Enables the *IGMP Snooping* function.
- `Off` (default setting)
  Disables the *IGMP Snooping* function.
  The device forwards received *query*, *report*, and *leave* data packets without evaluating them.
  The device forwards received data packets with a Multicast destination address to every port.

Unregistered IPMCv4 flooding enabled

Activates/deactivates the unregistered IPv4 Multicast (IPMCv4) data packets flooding. The prerequisite for controlling the flooding is that the *IGMP Snooping* function is enabled globally.

Possible values:

- `marked` (default setting)
  The unregistered IPMCv4 data packets flooding is active.
- `unmarked`
  The unregistered IPMCv4 data packets flooding is inactive.

Proxy enabled

Activates/deactivates the function of forwarding unnecessary *join* and *leave messages* to the router.

Possible values:

- `marked` (default setting)
  The forwarding of unnecessary *join* and *leave message* to the router is active.
- `unmarked`
  The forwarding of unnecessary *join* and *leave message* to the router is inactive.

Leave proxy enabled

Activates/deactivates the function of forwarding unnecessary *leave messages* to the router.

Possible values:

- `marked`
  The forwarding of unnecessary *leave message* to the router is active.
- `unmarked` (default setting)
  The forwarding of unnecessary *leave message* to the router is inactive.

5.4.2 Configuration

[Switching > IGMP Snooping > Configuration]

This dialog lets you enable the *IGMP Snooping* function in the device and also set it up for each VLAN.

The dialog contains the following tabs:
- [VLAN]
- [Port]

[VLAN]

In this tab, you set up the *IGMP Snooping* function for each VLAN.

Table

For information on how to customize the appearance of the table, see “Working with tables” on page 14.

VLAN ID

Displays the ID of the VLAN to which the table entry applies.

Snooping function

Activates/deactivates the *IGMP Snooping* function in the VLAN.

Possible values:
- `marked`
  The *IGMP Snooping* function is active.
- `unmarked` (default setting)
  The *IGMP Snooping* function is inactive.

Compatibility

The hosts and routers in the network may support different versions of IGMP. To maintain compatibility, the device takes appropriate action depending on the respective supported version of IGMP.

Possible values:
- `auto` (default setting)
- `v1`
- `v2`
- `v3`

Priority

Specifies the *CoS (Class of Service)* value to the IGMP data packets on a specific interface. You can use these values to prioritize different classes of traffic.

Possible values:

- `0..7` (default setting: `0`)

Robustness variable

Specifies the value to tune the expected packet loss on a network.

The robustness variable specifies the number of repetitions for IGMP queries to account for possible loss of query packets. A higher value makes the IGMP queries more robust, but increases the timeout time for multicast groups.

Possible values:

- `2..255` (default setting: `2`)

Unsolicited report interval [s]

Specifies the period of time (in seconds) between sending repetitions of the initial report of membership in a group.

Possible values:

- `1..31744` (default setting: `1`)

Last member query interval [ds]

Specifies the maximum response time in deciseconds advertised in IGMP group-specific queries. This confirms the group deregistration that no more host requires the specific Multicast address.

Possible values:

- `0..31744` (default setting: `10`)

[Port]

Specifies the *IGMP Snooping* function for every port.

Table

For information on how to customize the appearance of the table, see “Working with tables” on page 14.

Port

Displays the port number.

Filtering profile

Specifies the IPMCv4 profile as the filtering condition for the specific port.

Immediate leave

Activates/deactivates the function on a port to delete the MAC forward entry immediately upon receiving message for group deregistration.

To optimize for minimum network load, you can activate the Immediate Leave function on the device.

Possible values:

- `marked`
  When the Immediate Leave function is active and the device receives a *leave message*, then the device immediately removes the group record and stops forwarding Multicast data packets. Activate this feature only when a single IGMPv2 host is connected to the specific port.
- `unmarked` (default setting)
  When the Immediate Leave function is inactive and the device receives a *leave message*, then the device first responds with sending out a corresponding *query message* and waits for the response timeout.

Router port

Activates/deactivates a port that leads towards the Multicast router or *IGMP Querier*.

Possible values:

- `marked`
  The *Router port* function is active.
- `unmarked` (default setting)
  The *Router port* function is inactive.

Max group throttling

Specifies the number of Multicast groups to which a device port can belong.

Possible values:

- `0..10` (default setting: `unlimited`)

5.4.3 Querier

[Switching > IGMP Snooping > Querier]

The device lets you forward a Multicast stream only to those ports to which a Multicast receiver is connected.

The device sends a *query message* to every IGMP enabled port at a defined interval to find out which ports are connected to Multicast receivers. Multicast receivers respond to the *query message* with a *report message* to join the Multicast stream if a Multicast receiver is connected.

This dialog lets you set up the *Querier* settings for the set-up VLANs.

Table

In the table, you specify the *Querier* settings for the set-up VLANs.

VLAN ID

Displays the ID of the VLAN to which the table entry applies.

Snooping function

Displays if the *IGMP Snooping* function is active in the VLAN.

Possible values:

- `marked`
  The *IGMP Snooping* function is active.
- `unmarked` (default setting)
  The *IGMP Snooping* function is inactive.

Election

Activates/deactivates if the device takes part in the election of the *Querier* role in the VLAN.

Possible values:

- `marked`
  The device takes part in the election of the *Querier* role in the VLAN.
- `unmarked` (default setting)
  The device does not take part in the election of the *Querier* role in the VLAN.

Querier address

Specifies the IPv4 address that the device adds as the source address in general *query messages* generated by the device. Enter the address of the Multicast router.

Possible values:

- Valid IPv4 unicast address of the IGMP router in the network (default setting: `0.0.0.0`)

Query interval [s]

Specifies the time interval (in seconds) between the general queries sent by the device.

Possible values:

- `1..31744` (default setting: `125`)

Max query response time [ds]

Specifies the maximum time in deciseconds in which the members of a Multicast group are expected to respond to a *query message*. The members of a Multicast group specify a random fraction of the response time. This random time helps prevent every Multicast group member to respond to the query at the same time.

Possible values:

- `0..31744` (default setting: `100`)

Robustness variable

Displays the value to tune the expected packet loss on a network.

Possible values:

- `2..255`

Last member query interval [ds]

Displays the maximum response time in deciseconds the device advertises in *IGMP group*-specific queries. This confirms the group deregistration that no more host requires the specific Multicast address.

Possible values:

- `0..31744`

Unsolicited report interval [s]

Displays the period of time in seconds between sending a repetition of the initial report of membership in a group.

Possible values:

- `1..31744`

Priority

Displays the *CoS (Class of Service)* value the device assigns to the IGMP data packets on a specific interface. You can use these values to prioritize different classes of traffic.

Possible values:

- `0..7`

Compatibility

Displays the IGMP version that the Multicast router used when sending the last IGMP*query message* received in this VLAN.

5.4.4 Status

[Switching > IGMP Snooping > Status]

This dialog displays the *IGMP Snooping* status for the set-up VLANs.

The dialog contains the following tabs:
- [Group address]
- [Status]
- [Statistics]

[Group address]

Table

For information on how to customize the appearance of the table, see “Working with tables” on page 14.

VLAN ID

Displays the VLAN ID to which the table row applies.

Group address

Displays the Multicast IPv4 address.

Source address

Displays the source IPv4 address.

Member ports

Displays the ports which are members of the Multicast address.

Mode

Displays the filter mode of the Multicast group IPv4 address on a port.

Possible values:
- *exclude*
  The traffic from the Multicast group IPv4 address associated with the source is not forwarded to the port, but the traffic from other sources is forwarded.
- *include*
  The traffic from the Multicast group IPv4 address associated with the source is forwarded to the port, but the traffic from other sources is not forwarded.

Source address forwarding

Displays if the source IPv4 address is forwarding on the Multicast group of the port.

Possible values:

- `marked`
  The source IPv4 address is forwarding on the Multicast group of the port.
- `unmarked`
  The source IPv4 address is blocked from forwarding on the Multicast group of the port.

Hardware switch forwarding

Displays if the device forwards group address information to another networking device.

[Status]

Table

For information on how to customize the appearance of the table, see “Working with tables” on page 14.

VLAN ID

Displays the VLAN ID to which the table row applies.

Querier status

Displays the *IGMP Querier* status of the VLAN.

Active querier address

Displays the active *IGMP Querier* address of the VLAN.

Querier uptime [s]

Displays the time in seconds this node acted as *IGMP Querier* on the VLAN.

Query interval [s]

Specifies the time interval in seconds between the general queries sent by the querier.

Querier expiry time [s]

Displays the time in seconds after a Multicast router decides that another Multicast router should not be the querier.

Querier version

Displays the current *IGMP Querier* version of a VLAN when a port which is a member of this VLAN acts as a router.

Querier present timeout [s]

Displays the time in seconds that the host takes to return to *IGMPv3* mode when it receives an older version query. If a host receives an older version query, then set its older version querier present timer to the older *querier version* interval.

Host version

Displays the current IGMP compatibility setting of the ports that are members of a certain VLAN.

Host present timeout [s]

Displays the time in seconds that the group takes to return to *IGMPv3* mode when an older version report is sent to that group. If a group receives an older version report, then the router sets the older host present timer to the older host present interval.

[Statistics]

Table

For information on how to customize the appearance of the table, see “Working with tables” on page 14.

Button

Clear statistics

Resets the statistics counters in the table to `0`.

VLAN ID

Displays the VLAN ID to which the table row applies.

Counter TX query

Displays the number of IGMP query data packets that the device transmitted in the VLAN.

Counter TX specific query

Displays the number of IGMP group query data packets that the device transmitted in the VLAN.

Counter RX query

Displays the number of IGMP query data packets that the device received in the VLAN.

Counter RX v1 join

Displays the number of *IGMPv1* join data packets that the device received in the VLAN.

Counter RX v2 join

Displays the number of *IGMPv2* join data packets that the device received in the VLAN.

Counter RX v2 leave

Displays the number of *IGMPv2* leave data packets that the device received in the VLAN.

Counter RX v3 join

Displays the number of *IGMPv3* join data packets that the device received in the VLAN.

Counter RX errors

Displays the number of invalid IGMP data packets that the device received in the VLAN.

5.5 VLAN

[Switching > VLAN]

The Virtual Local Area Network (VLAN) helps distribute the data packets in the physical network to logical subnetworks. This provides you with the following advantages:

- High flexibility
- Improved throughput
- Helps increase security

The device supports packet-based “tagged” VLANs according to the IEEE 802.1Q standard. The VLAN tag in the data packet indicates the related VLAN ID to which the data packet belongs.

The device transmits the received data packets of a VLAN only through the ports that are assigned to the same VLAN. This reduces the network load.

The device learns the MAC addresses for every VLAN separately (*independent VLAN learning*).

The menu contains the following dialogs:

- Global
- Configuration
- Port

5.5.1 Global

[Switching > VLAN > Global]

This dialog lets you see the general VLAN parameters on the device.

VLAN parameters

Max. VLAN ID

Displays the highest ID assignable to a VLAN.

Possible values:

- 4093

Note: VLANs 4094 and 4095 are reserved for internal functions.

VLANs (max.)

Displays the maximum number of VLANs possible.

Possible values:

- 64

VLANs

Displays the number of VLANs currently configured in the device.

VLAN ID 1 is the management VLAN constantly present in the device, the device neither lets you delete the VLAN 1 nor modify its name.

5.6 Configuration

This dialog lets you add/remove a new VLAN on the device.

Table

For information on how to customize the appearance of the table, see “Working with tables” on page 14.

Buttons


Add

Opens the *Create* window to add a table row.

- In the *VLAN ID* field, specify the VLAN ID.
  Possible values:
  - `2..4093`
- In the *VLAN name* field, specify a name for this VLAN. This is an optional field, if you leave this field blank, then the device assigns a default name that you can also change later in the *Configuration* table.


Remove

Removes the selected table row.

VLAN ID

Displays the VLAN ID.

Possible values:

- `2..4093`

VLAN name

Specifies the name of the VLAN.

Possible values:

- Alphanumeric ASCII character string with 1..32 characters

VLAN user

Displays the internal software module which uses the VLAN services.

Port list

Displays the port numbers that are members of the VLAN.

5.6.1 Port

[Switching > VLAN > Port]

[Configuration]

This tab lets you specify the VLAN configuration for each port in the table rows.

Table

For information on how to customize the appearance of the table, see “Working with tables” on page 14.

Port

Displays the physical port number on the device.

Mode

Specifies a VLAN mode.

Possible values:

- `access` (default setting)
  The port is a member of the VLAN you specified in the *VLAN ID* field. The port forwards the data packets without a VLAN tag. You use this setting if the connected device neither forwards the VLAN tagged data packets nor evaluates the VLAN tag of the received data packets, for example, on the end devices.
- `trunk`
  The port is a member of the VLAN and forwards the data packets with a VLAN tag.
  This mode lets you specify the values in the following fields:
  - *Trunk native VLAN*
  - *Trunk allowed VLAN*
  - *Trunk tag native VLAN*
- `hybrid`
  This mode lets you specify the values in the following fields:
  - *Hybrid native VLAN*
  - *Hybrid allowed VLAN*
  - *Hybrid ingress filtering*
  - *Hybrid ingress acceptance*
  - *Hybrid egress tagging*

VLAN ID

Displays the management VLAN ID configured in the device, if the *Mode* field contains the value *trunk* or *hybrid*. If the port *Mode* field contains the value *access*, then the device lets you specify the VLAN ID in this field.

Possible values:

- `1..4093` (default setting: `1`)

Trunk native VLAN

Specifies the native VLAN for the *trunk* mode.

Possible values:

- `1..4093` (default setting: `1`)

Trunk allowed VLAN

Specifies the VLAN that the port allows in *trunk* mode.

Possible values:

- `1..4093` (default setting: `1`)
  The device displays the default VLAN 1 and lets you specify the additional VLANs.

Trunk tag native VLAN

Displays if the device tags the data packets with the native VLAN in the *trunk* mode.

Possible values:

- `marked` (default setting)
  The device tags the data packets in *trunk* mode with the configured native VLAN ID.
- `unmarked`
  The device does not tag the data packets in *trunk* mode.

Hybrid port type

Specifies the type of port.

Possible values:

- *`c-port`* (default setting)
  On ingress, the device identifies the tagged data packets by the VLAN ID embedded in the tag. If a data packet is untagged or priority tagged, then according to priority, the device accepts the data packets.
  On egress, if the data packets require a tag, the device tags them with a C-tag. C-tag is an abbreviation of the customer VLAN tag.
- *`unaware`*
  On ingress, the device receives the data packets irrespective of the VLAN tag, and on egress, the port does not remove the possible tag from the data packets.

Hybrid native VLAN

Specifies the native VLAN, if the *Mode* field contains the value *hybrid*.

Possible values:

- `1..4093` (default setting: `1`)

Hybrid allowed VLAN

Specifies the VLAN, if the *Mode* field contains the value *hybrid*.

Possible values:

- `1..4093` (default setting: `1`)
  The device displays the default VLAN 1 and lets you specify the additional VLANs.

Hybrid ingress filtering

Activates/deactivates the setting of verifying the VLAN tag of the incoming data packets.

Possible values:

- `marked`
  The port discards the data packets that are classified to the VLAN, of which the port is not a member.
- `unmarked` (default setting)
  The port accepts and forwards the frames to the CPU, but does not transmit the frames that are classified to the VLAN, of which the port is not a member.

Hybrid ingress acceptance

Specifies the type of incoming data packets that the port accepts.

Possible values:

- *`tagged & untagged`*
  The port accepts both untagged and tagged data packets.
- *`tagged`*
  The port accepts only tagged data packets.
- *`untagged`*
  The port accepts only untagged data packets.

Hybrid egress tagging

Specifies a setting of VLAN tag of the outgoing data packets that the port allows to transmit.

Possible values:

- *`tag every except native`*
  The device tags every outgoing data packet except native.
- *`tag every`*
  The device tags every outgoing data packet.
- *`untag every`*
  The device untags every outgoing data packet.

[Status]

This tab displays the status of VLAN for each port.

Table

For information on how to customize the appearance of the table, see “Working with tables” on page 14.

Port

Displays the physical port number on the device.

VLAN user

Displays the internal software modules which uses the VLAN services.

Port VLAN ID

Displays the VLAN ID configured in the device and port is a member of the VLAN ID.

Untagged VLAN ID

Displays the VLAN ID that the device assigns to the untagged data packets received on the port.

Hybrid port type

Displays the type of port.

Possible values:

- `c-port` (default setting)
- `unaware`

Ingress filtering

Displays the active/inactive state of this setting.

Ingress acceptance

Displays the type of incoming data packets that the port accepts.

Egress tagging

Displays the VLAN tag setting that the port follows while transmitting the data packets.

5.7 QoS

[Switching > QoS]

Communication networks support several applications at the same time that have different requirements regarding availability, bandwidth, and latency periods.

Quality of Service (QoS) is a concept defined in IEEE 802.1D. It distributes the bandwidth among every resource to control the traffic congestion in the network. You therefore have the possibility of providing minimum bandwidth for necessary applications. The prerequisite is that the end devices and the devices in the network support prioritized data transmission. The device gives preference to data packets with high priority. The device transfers data packets with lower priority when there are no data packets with a higher priority to be transmitted. The data packets in queues 6 and 7 are high priority and queues 0 to 5 are weighted.

The device provides the following setting options:
- You specify how the device evaluates QoS/prioritization information for inbound data packets.
- For outbound packets, you specify which QoS/prioritization information the device writes in the data packet, for example priority for management packets, port priority.

Note: If you use the functions in this menu, then deactivate the flow control according to IEEE 802.3x. The default setting for IEEE 802.3x flow control is inactive. To deactivate the flow control, in the *Basic Settings > Port* dialog, *Configuration* tab unmark the checkbox in the *Flow control* column.

The menu contains the following dialogs:
- Global
- Port Configuration
- IP DSCP Mapping

5.7.1 Global

[Switching > QoS > Global]

The dialog lets you restrict the number of flooding data packets passing through the device. The flooding data packets are data packets where VLAN ID and destination MAC address are not present in the MAC Address table. You can apply storm policers individually to unknown unicast and multicast packets, as well as to broadcast packets.

Storm global parameter

Enable unicast

Activates/deactivates the function of flooding unknown unicast data packets.

Possible values:

- `marked`
  The function is active.
- `unmarked` (default setting)
  The function is inactive.

Unicast rate [fps]

Specifies the maximum allowed storm rate in frames per second (fps) for unknown unicast data packets.

Possible values:

- `1..1024000`
  The value is internally rounded to 2^n until the maximum value.

Enable multicast

Activates/deactivates the function of flooding unknown multicast data packets.

Possible values:

- `marked`
  The function is active.
- `unmarked` (default setting)
  The function is inactive.

Multicast rate [fps]

Specifies the maximum allowed storm rate in frames per second (fps) for unknown multicast data packets.

Possible values:

- `1..1024000`
  The value is internally rounded to 2^n until the maximum value.

Enable broadcast

Activates/deactivates the function of flooding broadcast data packets.

Possible values:

- `marked`
  The function is active.
- `unmarked` (default setting)
  The function is inactive.

Broadcast rate [fps]

Specifies the maximum allowed storm rate in frames per second (fps) for broadcast data packets.

Possible values:

- `1..1024000`
  The value is internally rounded to 2^n until the maximum value.

Storm detected

Displays if the device detects the flooding data packets.

Possible values:

- `marked`
  The device detects flooding data packets.
- `unmarked`
  The device detects no flooding data packets.

[Mapping - Tag to COS]

Table

For information on how to customize the appearance of the table, see “Working with tables” on page 14.

PCP

Displays the default *Priority Code Point* value which helps to prioritize different classes of traffic.

Possible values:

- `0..7`

DEI

Displays the default *Drop Eligible Indicator* value which indicates the eligibility of dropping the data packet in the presence of congestion. If congestion occurs, then the device discards data packets with *DEI* value of 1.

Possible values:

- `0..1`

COS

Specifies the default *Class of Service* value which helps in queuing, scheduling, and congestion control.

Possible values:

- `0..7` (default setting: `0`)

DPL

Specifies the default *Drop Precedence Level* value which helps to control congestion. If congestion occurs, then the device first discards data packets with the higher *DPL* value of 1.

Possible values:

- `0..1` (default setting: `0`)

5.7.2 Port Configuration

[Switching > QoS > Port Configuration]

In this dialog, you specify for every port how the device processes the data packets based on their QoS information.

The dialog contains the following tabs:
- [Port]
- [Egress port shaper]
- [Egress queue shaper]
- [Queue scheduler]

[Port]

Table

For information on how to customize the appearance of the table, see “Working with tables” on page 14.

Port

Displays the port number.

COS

Specifies the default *Class of Service* value which helps in queuing, scheduling, and congestion control.

The device applies the default *COS* value to each data packet. If the following conditions are met, then the device instead puts the data packet into a queue that depends on the *Priority Code Point (PCP)* and *Drop Eligible Indicator (DEI)* values in the VLAN tag.
- The received data packet contains a VLAN tag
- In the *Trust tag* column, the checkbox is marked

Possible values:
- `0..7` (default setting: `0`)

DPL

Specifies the default *Drop Precedence Level* value which helps to control congestion. If congestion occurs, then the device first discards data packets with the higher *DPL* value of 1.

The device applies the default *DPL* value to each data packet. If the following conditions are met, then the device instead puts the data packet into a queue that depends on the *Priority Code Point (PCP)* and *Drop Eligible Indicator (DEI)* values in the VLAN tag.
- The received data packet contains a VLAN tag
- In the *Trust tag* column, the checkbox is marked

Possible values:

- `0..1` (default setting: `0`)

PCP

Specifies the default *Priority Code Point* value which helps to prioritize different classes of traffic.

The device applies the default *COS* value to each data packet. If the following conditions are met, then the device instead puts the data packet into a queue that depends on the *Priority Code Point (PCP)* value in the VLAN tag.

- The received data packet contains a VLAN tag
- In the *Trust tag* column, the checkbox is marked

Possible values:

- `0..7` (default setting: `0`)

DEI

Specifies the default *Drop Eligible Indicator* value which indicates the eligibility of dropping a data packet in the presence of congestion. If congestion occurs, then the device drops data packets with *DEI* value of 1.

The device applies the default *DPL* value to each data packet. If the following conditions are met, then the device instead puts the data packet into a queue that depends on the *Drop Eligible Indicator (DEI)* value in the VLAN tag.

- The received data packet contains a VLAN tag
- In the *Trust tag* column, the checkbox is marked

Possible values:

- `0..1` (default setting: `0`)

Trust tag

Activates/deactivates the classification mode of VLAN-tagged data packets on the port.

Possible values:

- `marked`
  The device uses the mapped versions of *Priority Code Point (PCP)* and *Drop Eligible Indicator (DEI)* values for VLAN-tagged data packets.
- `unmarked` (default setting)
  The device uses the default *Class of Service (COS)* and *Drop Precedence Level (DPL)* values for VLAN-tagged data packets.

Note: If you have high security requirements and do not want to trust the values in the incoming VLAN-tagged data packets, then unmark the *Trust tag* checkbox.

Trust DSCP

Activates/deactivates the trusting of the DSCP value contained in the IP data packets on the port.

Possible values:

- `marked`
  The device trusts the DSCP value contained in the IP data packets.
- `unmarked` (default setting)
  The device does not trust the DSCP value contained in IP data packets.

[Egress port shaper]

Table

For information on how to customize the appearance of the table, see “Working with tables” on page 14.

Port

Displays the port number.

Active

Activates/deactivates the shaping of the bandwidth for the egress traffic on the port.

Possible values:

- `marked`
  Shaping the bandwidth on the port is active.
- `unmarked` (default setting)
  Shaping the bandwidth on the port is inactive.

Rate [kbps]

Specifies the port shaping rate in kbps. The device changes the value to the closest value that the device supports.

Possible values:

- `100..3281943` (default setting: `500`)

[Egress queue shaper]

Table

For information on how to customize the appearance of the table, see “Working with tables” on page 14.

Port

Displays the port number.

Queue

Displays the queue index number.

Active

Activates/deactivates the shaping of the bandwidth of a queue for the egress traffic on the port.

Possible values:

- `marked`
  Shaping the bandwidth of a queue on the port is active.
- `unmarked` (default setting)
  Shaping the bandwidth of a queue on the port is inactive.

Excess

Activates/deactivates the sharing of excess bandwidth. The device shares excess bandwidth if, in the *Egress port shaper* tab, the *Active* checkbox is unmarked for a port and no other queues with active shapers have data packets for transmission.

Possible values:

- `marked`
  Sharing of excess bandwidth on the port is active.
- `unmarked` (default setting)
  Sharing of excess bandwidth on the port is inactive.

Credit

Activates/deactivates the credit-based shaping support for the queue to create burst capacity when bandwidth is available.

Possible values:

- `marked`
  Credit-based shaping support for the queue is active.
- `unmarked` (default setting)
  Credit-based shaping support for the queue is inactive.

Rate [kbps]

Specifies the queue shaper rate in kbps. The device changes the value to the closest value that the device supports.

Possible values:

- `100..3281943` (default setting: `500`)

[Queue scheduler]

Table

For information on how to customize the appearance of the table, see “Working with tables” on page 14.

Port

Displays the port number.

Mode

Specifies the scheduling mode of the queues on the port.

Possible values:

- *Strict priority*
  The frames with the highest priority are transmitted before the frames with lower priority.
- 2 queues weighted
  Weightage is assigned to the queue numbers 0 and 1 to set their priorities on the port.
- 3 queues weighted
  Weightage is assigned to the queue numbers 0..2 to set their priorities on the port.
- 4 queues weighted
  Weightage is assigned to the queue numbers 0..3 to set their priorities on the port.
- 5 queues weighted
  Weightage is assigned to the queue numbers 0..4 to set their priorities on the port.
- 6 queues weighted
  Weightage is assigned to the queue numbers 0..5 to set their priorities on the port.
- 7 queues weighted
  Weightage is assigned to the queue numbers 0..6 to set their priorities on the port.
- 8 queues weighted
  Weightage is assigned to the queue numbers 0..7 to set their priorities on the port.

<Queue numbers>

Specifies the weightage of the queues on the port.

Possible values:

- 1..100 (default setting: 17)

5.7.3 IP DSCP Mapping

[Switching > QoS > IP DSCP Mapping]

The device transmits IP data packets according to the DSCP (Differentiated Service Code Point) value contained in the data packet with a higher or lower priority.

In this dialog, you map the trusted DSCP value contained in IP data packets to a specific *COS* and *DPL* value.

Table

For information on how to customize the appearance of the table, see “Working with tables” on page 14.

DSCP value

Displays the DSCP value.

Possible values:

- `0..63`

COS

Specify the *Class of Service* value which is mapped to the DSCP value.

Possible values:

- `0..7` (default setting: `0`)
  `0` assigned to the priority queue with the lowest priority.
  `7` assigned to the priority queue with the highest priority.

DPL

Specify the *Drop Precedence Level* value which is mapped to the DSCP value.

Possible values:

- `0..1` (default setting: `0`)
  If congestion occurs, then the device first discards data packets with the higher *DPL* value of 1.

5.8 L2-Redundancy

[Switching > L2-Redundancy]

The menu contains the following dialogs:

- ERPS
- CFM
- MRP Client
- Spanning Tree

5.8.1 ERPS

[Switching > L2-Redundancy > ERPS]

Ethernet Ring Protection Switching (ERPS) in the device provides fast protection and recovery switching for Ethernet traffic in a ring topology, while it also helps ensure that the Data Link Layer remains loop-free.

The *ERPS* dialog displays the following tabs:
- [Configuration]
- [Status]
- [Statistics]

[Configuration]

Table

For information on how to customize the appearance of the table, see “Working with tables” on page 14.

Buttons

 Add

Opens the *Create* window to add an *ERPS* instance.
- In the *ERPS instance* field, specify the value for this *ERPS* instance.
  Possible values:
  - `1..64`
- In the *Protected VLANs* field, specify the VLAN ID.
  Possible values:
  - `1..4093`
- In the *Port 0 interface* field, select a port from the drop-down list.
  Possible values:
  - `<port number>`
- In the *Port 1 interface* field, select a port from the drop-down list.
  Possible values:
  - `<port number>`

 Remove

Removes the selected *ERPS* instance.

ERPS instance

Displays the *ERPS* instance.

Possible values:

- `1..64`

Active

Activates/deactivates the *ERPS* instance.

Possible values:

- `marked`
  The *ERPS* instance is active.
- `unmarked` (default setting)
  The *ERPS* instance is inactive.

Version

Specifies the version for the *Ring-Automatic Protection Switching (R-APS)*.

Possible values:

- `v1`
  Version1
- `v2`
  Version2

Protected VLANs

Specifies the VLANs protected by the *ERPS* instance.

Possible values:

- `1..4093`

RPL mode

Specifies the mode for the *Ring Protection Link (RPL)*.

Loop avoidance in an Ethernet ring is achieved by assuring that, at any time, traffic may flow on one of the ring links. This particular link is called the ring protection link. When a *Signal Fail (SF)* condition occurs, the owner node and the neighbor node can block and unblock the port on the *RPL*.

Possible values:

- *`none`* (default setting)
  No RPL mode is active.
- *`owner`*
  This mode unblocks the port on RPL when a signal fail occurs and blocks the port in normal condition. This mode activates the reversion behavior.

- *`neighbor`*
  This mode unblocks the port on RPL when a signal fail occurs and blocks the port in normal condition. This mode does not activate the reversion behavior.

If a node has one of its ring ports set to owner or neighbor, then the other ring port of the RPL is automatically set to the none mode.

RPL port

Specifies the RPL ring port for this ERPS instance. The RPL ports are the ring ports of 2 different nodes, and the RPL is a link in between.

Possible values:

- *ring port 0*
  Ring port0 is selected.
- *ring port 1*
  Ring port1 is selected.

Control VLAN

Specifies the VLAN dedicated to carry the *R-APS*, which is called the control signal as well. The control VLAN is not considered as a protected VLAN.

Possible values:

- `1..4093` (default setting: none)

PCP

Specifies the *Priority Code Point (PCP)* for this ERPS instance. PCP is the means of classifying and managing traffic.

Possible values:

- `0..7` (default setting: `0`)

Ring type

Specifies the type of ring for the ERPS instance.

Possible values:

- *major* (default setting)
  Major ring always has 2 ports and supports the *R-APS v1*.
- *sub-ring*
  Sub is a non-interconnected sub ring that has 2 ring ports and supports the *R-APS v2*.
- *interconnected-sub-ring*
  It is an interconnected sub ring that has only one port (port0), however connects to a major ring. An interconnected sub-ring points to another ring with 2 ring ports (the other ring cannot itself be an interconnected sub-ring), which receives flush notifications and may carry *R-APS* PDUs for the sub-ring.

Virtual channel

Activates/deactivates the configuration of interconnected sub ring with the virtual *R-APS*.

Possible values:

- `marked`
  The configuration is active.
- `unmarked` (default setting)
  The configuration is inactive.

Connected ring instance

Specifies the *ERPS* instance of the connected ring to which the interconnected sub ring connects.

Possible values:

- `1..64` (default setting: none)

Interconnect propagate

Activates/deactivates the *Filtering database (FDB)* flushing of the connected ring.

If a topology change occurs on the interconnected sub ring, the nodes in the connected ring also flush their FDB for the connected ring instance. If this setting is active, the nodes in the connected ring will also send flush R-APS event PDUs onto their ring ports.

Possible values:

- `marked`
  Activates the FDB flushing of nodes in the connected ring.
- `unmarked` (default setting)
  Deactivates the FDB flushing of nodes in the connected ring.

Port 0 interface

Specifies the port number for the ring port0.

Possible values:

- `<port number>`
  Number of the physical port on the device.

Port 1 interface

Specifies the port number for the ring port1.

Possible values:

- `<port number>`
  Number of the physical port on the device.

Ring ID

Specifies the ring ID of the ERPS instance.

Possible values:

- `1..239` (default value: `1`)

Node ID

Specifies the valid unicast MAC address used in the R-APS specific PDUs to uniquely identify the node. If the address is not a unicast MAC address, the device does not accept the node ID.

Possible values:

- Valid unicast MAC address.

Level

Specifies the *Maintenance Domain/Maintenance Entity Group (MD/MEG)* level used in R-APS PDUs.

Possible values:

- `0..7` (default setting: `7`)

Hold off time [ms]

Specifies the hold off timer value in multiples of 100 milliseconds.

Possible values:

- `0..10000` in multiples of 100 milliseconds (default setting: `0`)

Revertive

Activates/deactivates the revertive setting of the instance.

When a detected failure ends and *Wait to Restore (WTR)* time has passed, then the ring instance attempts to revive the detected failure, and this operation is known as revertive.

Possible values:

- `marked` (default setting)
  The instance is revertive.
- `unmarked`
  The instance is non-revertive.

Guard time [ms]

Specifies the guard time in steps of 10 milliseconds.

The guard time is used to help prevent ring nodes from acting upon outdated R-APS PDUs for any topology changes.

Possible values:

- `10..2000` in steps of 10 milliseconds (default setting: `500`)

WTR [s]

Specifies the *Wait to Restore (WTR)* time in seconds. *WTR* is the timer started by the *RPL* owner node to delay the reversion of the *RPL* block after a detected defect has cleared. Only the revertive mode uses *WTR*.

Possible values:

- `5..720` (default setting: `300`)

Port 0 SMAC

Specifies the unicast source MAC address used in *R-APSPDUs* and sent on the ring port0.

Possible values:

- Valid unicast MAC address

Port 1 SMAC

Specifies the unicast source MAC address used in *R-APSPDUs* and sent on the ring port1.

Possible values:

- Valid unicast MAC address

Port 0 SF trigger

Displays the interface used as a *Signal Fail (SF)* trigger.

Possible values:

- *link* (default setting)
  The interface link state of the Port0 is used as an SF trigger.
- *MEP*
  A MEP installed on the Port0 is used as an SF trigger.

Port 0 domain

Specifies the domain name for the Port0 MEP, only when the *Port 0 SF trigger* column contains the value item `MEP`.

Possible values:

- Alphanumeric ASCII character string with 1..15 characters

Port 0 service

Specifies the service name that is within the MEP domain for the Port0 MEP, only when the *Port 0 SF trigger* column contains the value item `MEP`.

Possible values:

- Alphanumeric ASCII character string with 1..15 characters

Port 0 MEP ID

Specifies the ID of the Maintenance End Point (MEP) for the Port1 MEP.

Possible values:

- `1..8191`

Port 1 SF trigger

Displays the interface used as an *SF* trigger.

Possible values:

- `link` (default setting)
  The interface link state of the Port1 is used as an SF trigger.
- `MEP`
  A MEP installed on the Port1 is used as an SF trigger.

Port 1 domain

Specifies the domain name for the Port1 MEP, only when the *Port 1 SF trigger* column contains the value item `MEP`.

Possible values:

- Alphanumeric ASCII character string with 1..15 characters

Port 1 service

Specifies the service name that is within the MEP domain for the Port1 MEP, only when t he *Port 1 SF trigger* column contains the value item `MEP`.

Possible values:

- Alphanumeric ASCII character string with 1..15 characters

Port 1 MEP ID

Specifies the ID of the Maintenance End Point (MEP) for the Port1 MEP.

Possible values:

- `1..8191`

[Status]

Table

For information on how to customize the appearance of the table, see “Working with tables” on page 14.

ERPS instance

Displays the *ERPS* instance configured in the device.

Possible values:

- `1..64`

Control command

Specifies an *ERPS* command for this instance.

Possible values:

- `no request`
  There is no active local command. Issuing this command has no effect.
- *`force switch to port 0`*
  Causes a forced switchover. Blocks port1 and unblocks port0.
- *`force switch to port 1`*
  Causes a forced switchover. Blocks port0 and unblocks port1.
- *`manual switch to port 0`*
  Causes a switchover if the signal is good and no forced switch is in effect. Blocks port1 and unblocks port0.

- *manual switch to port 1*
  Causes a switchover if the signal is good and no forced switch is in effect. Blocks port0 and unblocks port1.
- *clear*
  Clears a switchover whether forced switch or manual switch request.

Oper state

Displays the operational state of the *ERPS* instance.

Possible values:

- *inactive*
  The instance is inactive.
- *active*
  The instance is active.

Oper warning

Displays the operational warning for the *ERPS* instance.

Possible values:

- *no warnings*
  No operational warning is present, everything is fine.
- *port 0 not member of control VLAN*
  Port0 ring port is not a member of the control VLAN.
- *port 1 not member of control VLAN*
  Port1 ring port is not a member of the control VLAN.
- *port 0 untags control VLAN*
  The VLAN configuration of the port0 causes the control VLAN to become untagged on egress.
- *port 1 untags control VLAN*
  The VLAN configuration of the port1 causes the control VLAN to become untagged on egress.
- *port 0 MEP not found*
  Port0 *MEP* is not found using the link-state for the *SF*.
- *port 1 MEP not found*
  Port1 *MEP* is not found using the link-state for the *SF*.
- *port 0 MEP admin disabled*
  Port0 *MEP* is administratively disabled using the link-state for the *SF*.
- *port 1 MEP admin disabled*
  Port1 *MEP* is administratively disabled using the link-state for the *SF*.
- *port 0 MEP Not down MEP*
  Port0 *MEP* is not a Down-*MEP* using the link-state for the *SF*.
- *port 1 MEP not down MEP*
  Port1 *MEP* is not a Down-*MEP* using the link-state for the *SF*.
- *port 0 and MEP ifIndex differ*
  Ring port of the Port0 *MEP* is not that of the Port0 using the link-state for the *SF*.
- *port 1 and MEP ifIndex differ*
  Ring port of the Port0 *MEP* is not that of the Port0 using the link-state for the *SF*.
- *port MEP shadows port 0 MIP*
  Port *MEP* of the port0 receives the *R-APS*.
- *port MEP shadows port 1 MIP*
  Port *MEP* of the port1 receives the *R-APS*.
- *MEP shadows port 0 MIP*
  A *MEP* on the port0 that matches the control VLAN which receives the *R-APS*.

- *MEP shadows port 1 MIP*
  A *MEP* on the port1 that matches the control VLAN which receives the *R-APS*.
- *connected ring does not exist*
  This is an interconnected sub-ring whose connected ring does not exist.
- *connected ring is an interconnected sub ring*
  This is an interconnected sub-ring whose connected ring is also an interconnected sub-ring.
- *connected ring is not operative*
  This is an interconnected sub-ring whose connected ring is not operative.
- *connected ring interface conflict*
  This is an interconnected sub-ring whose connected ring shares interfaces with this instance.
- *connected ring does not protect control VLAN*
  This is an interconnected sub-ring with a virtual channel whose connected ring does not protect the control VLAN.

Node state

Displays the protection/node state of the instance.

Possible values:

- *init*
  The node is defining the ring for the first time.
- *idle*
  No failures detected, no commands active.
- *protection*
  The ring protection is in protected state, the RPL is active.
- *MS*
  The ring protection is in manual switch mode.
- *FS*
  The ring protection is in forced switch mode.
- *pending*
  The state is changing from *Protection* to *Idle* until WTR expires.

TX R-APS active

Displays the status of transmitting (Tx) *R-APSPDUs* on the ring ports.

Possible values:

- `marked`
  Transmitting *R-APSPDUs* of the instance is active on the ring ports.
- `unmarked` (default setting)
  Transmitting *R-APSPDUs* of the instance is inactive on the ring ports.

FOP-TO

Displays the instance status of the *Failure of Protocol (FOP)R-APS* receiving (Rx) timeout.

Possible values:

- `marked`
  FOP-TO,R-APS Rx timeout is active.
- `unmarked`
  FOP-TO, *R-APS* Rx timeout is inactive.

TX info update time [s]

Displays the time in seconds since system startup, when the transmitted information parameters were last updated.

TX info request

Displays the request/state for the transmitted information.

Possible values:

- *no request*
  No local protection switching request.
- *manual switch*
  The request for manual switch.
- *signal failed*
  The state of signal fail condition.
- *force switch*
  The request for forced switch.
- *event*
  The event enables the transmission of a flush request.

TX info version

Displays the version of received/used *R-APS* protocol for the transmitted information.

Possible values:

- 0
  Version1
- 1
  Version2

TX info RB

Displays the *RB (RPL Blocked)* bit of *R-APS* information.

Possible values:

- marked
  RPL is blocked.
- unmarked (default setting)
  RPL is unblocked.

TX info DNF

Displays the *Do Not Flush (DNF)* status of the transmitted data packets.

Possible values:

- marked
  DNF is active.
- unmarked (default setting)
  DNF is inactive.

TX Info BPR

Displays the status of the transmitted *Blocked Port Reference (BPR)* data packets.

Possible values:

- *ring port 0*
  Ring port0 is blocked.
- *ring port 1*
  Ring port1 is blocked.

TX info node ID

Displays the unicast MAC address of the node for the transmitted data packets.

TX info SMAC

Displays the Source MAC Address (SMAC) used in the request/state.

Port 0 blocked

Displays the blocked status of the port0.

Possible values:

- `marked` (default setting)
  Ring port0 is blocked.
- `unmarked`
  Ring port0 is unblocked.

Port 0 SF

Displays the *signal fail* status of this request.

Possible values:

- `marked`
  Signal fail is active.
- `unmarked`
  Signal fail is inactive.

Port 0 FOP-PM

Displays the status of 2 RPL owners on the ring.

Possible values:

- `marked`
  Ring port0 has 2 RPL owners.
- `unmarked` (default setting)
  Ring port0 does not have 2 RPL owners.

Port 0 update time [s]

Displays the time in seconds since the system startup when this topology structure was last updated for the ring port0.

Port 0 request

Displays the request/state value for the port0.

Possible values:

- *no request*
  No local protection switching request.
- *manual switch*
  The request for manual switch.
- *signal failed*
  The state of signal fail condition.
- *force switch*
  The request for forced switch.
- *event*
  The event enables the transmission of a flush request.

Port 0 version

Displays the version number of the received/used R-APS protocol for the port0.

Possible values:

- 0
  Version1
- 1
  Version2

Port 0 RB

Displays the RPL blocked bit of *R-APS* information for the port0.

Possible values:

- marked
  RPL is blocked.
- unmarked
  RPL is unblocked.

Port 0 DNF

Displays the *Do Not Flush (DNF)* status of the port0.

Possible values:

- marked
  DNF is active.
- unmarked (default setting)
  DNF is inactive.

Port 0 BPR

Displays the status of blocked port reference for the port0.

Possible values:

- *ring-port 0*
  Ring port0 is blocked.
- *ring-port 1*
  Ring port1 is blocked.

Port 0 node ID

Displays the unicast MAC address of the node for the port0.

Port 0 SMAC

Displays the source MAC address used in the request/state for the port0.

Port 1 blocked

Displays the blocked status of the ring port1.

Possible values:

- `marked` (default setting)
  Ring port1 is blocked.
- `unmarked`
  Ring port1 is unblocked.

Port 1 SF

Displays the signal fail state of the port1 after the hold-off timer has expired.

Possible values:

- `marked`
  A signal fail has occurred.
- `unmarked`
  No signal fail has occurred.

Port 1 FOP-PM

Displays the status of 2 *Ring Protection Link (RPL)* owners on the ring.

Possible values:

- `marked`
  Ring port1 has 2 RPL owners.
- `unmarked` (default setting)
  Ring port1 does not have 2 RPL owners.

Port 1 update time [s]

Displays the time in seconds since the system startup when this topology structure was last updated for the ring port1.

Port 1 request

Displays the request/state for the port1.

Possible values:

- *no request*
  No local protection switching request.
- *manual switch*
  The request for manual switch.
- *signal failed*
  The state of signal fail condition.
- *force switch*
  The request for forced switch.
- *event*
  The event enables the transmission of flush request.

Port 1 version

Displays the version of received/used *R-APS* protocol for the port1.

Possible values:

- 0
  Version1
- 1
  Version2.

Port 1 RB

Displays the RPL blocked bit of *R-APS* information for the port1.

Possible values:

- marked
  RPL is blocked.
- unmarked
  RPL is unblocked.

Port 1 DNF

Displays the *Do Not Flush (DNF)* status of the port1.

Possible values:

- marked
  DNF is active.
- unmarked (default setting)
  DNF is inactive.

Port 1 BPR

Displays the status of *Blocked Port Reference (BPR)* for the port1.

Possible values:

- *ring port 0*
  Ring port0 is blocked.
- *ring port 1*
  Ring port1 is blocked.

Port 1 node ID

Displays the unicast MAC address of the node for the port1.

Port 1 SMAC

Displays the source MAC address used in the request/state.

[Statistics]

Button


Clear statistics

Clears the statistics of the selected *ERPS* instance.

Table

This table displays the following overview of the number of errors detected by the device, per *ERPS* instance:

For information on how to customize the appearance of the table, see “Working with tables” on page 14.

ERPS instance

Displays the *ERPS* instance configured in the device.

Possible values:

- 1..64

Port 0 RX error

Displays the number of wrong *R-APS PDUs* received.

Port 0 RX own

Displays the number of *R-APS PDUs* received with the own node ID.

Port 0 RX guard

Displays the number of *R-APS PDUs* received during the guard time.

Port 0 RX FOP-PM

Displays the number of *R-APS PDUs* received, causing *FOP-PM*.

Port 0 RX NR

Displays the number of *NR, R-APS PDUs* received.

Port 0 RX NR RB

Displays the number of *NR, RB, R-APS PDUs* received.

Port 0 RX SF

Displays the number of *SF, R-APS PDUs* received.

Port 0 RX FS

Displays the number of *FS, R-APS PDUs* received.

Port 0 RX MS

Displays the number of *MS, R-APS PDUs* received.

Port 0 RX event

Displays the number of event *R-APS PDUs* received.

Port 0 TX NR RB

Displays the number of *NR, RB, R-APS PDUs* transmitted.

Port 0 TX NR

Displays the number of *NR, R-APS PDUs* transmitted.

Port 0 TX SF

Displays the number of *SF, R-APS PDUs* transmitted.

Port 0 TX FS

Displays the number of *FS, R-APS PDUs* transmitted.

Port 0 TX MS

Displays the number of *MS, R-APS PDUs* transmitted.

Port 0 TX event

Displays the number of event *R-APS PDUs* transmitted.

Port 0 SF

Displays the number of local signal fails.

Port 0 flush

Displays the number of FDB flushes.

Port 1 RX error

Displays the number of wrong *R-APS PDUs* received.

Port 1 RX own

Displays the number of *R-APS PDUs* received with the own node ID.

Port 1 RX guard

Displays the number of *R-APS PDUs* received during the guard time.

Port 1 RX FOP-PM

Displays the number of *R-APS PDUs* received, causing *FOP-PM*.

Port 1 RX NR

Displays the number of *NR, R-APS PDUs* received.

Port 1 RX NR RB

Displays the number of *NR, RB, R-APS PDUs* received.

Port 1 RX SF

Displays the number of *SF, R-APS PDUs* received.

Port 1 RX FS

Displays the number of *FS, R-APS PDUs* received.

Port 1 RX MS

Displays the number of *MS, R-APS PDUs* received.

Port 1 RX event

Displays the number of event *R-APS PDUs* received.

Port 1 TX NR

Displays the number of *NR, R-APS PDUs* transmitted.

Port 1 TX NR RB

Displays the number of *NR, RB, R-APS PDUs* transmitted.

Collisions

Displays the number of *SF, R-APS PDUs* transmitted.

Port 1 TX FS

Displays the number of *FS, R-APS PDUs* transmitted.

Port 1 TX MS

Displays the number of *MS, R-APS PDUs* transmitted.

Port 1 TX event

Displays the number of event *R-APS PDUs* transmitted.

Port 1 SF

Displays the number of local signal fails.

Port 1 flush

Displays the number of FDB flushes.

5.8.2 CFM

[Switching > L2-Redundancy > CFM]

Connectivity Fault Management (CFM) is an *IEEE802.1ag* and *ITU Y.1731* standard that lets you manage connectivity at the Ethernet service level in the device. The *IEEE802.1ag* standard adds fault management capabilities to Ethernet, while the *ITU Y.1731* standard expands the capabilities to include performance.

The dialog contains the following tabs:
- CFM Global
- CFM Configuration
- CFM Status

5.8.2.1 CFM Global

[Switching > L2-Redundancy > CFM > Global]

[Capabilities]

This frame displays the following Ethernet fault management capabilities of the device:

Maintenance Domains count max

Displays the maximum number of the *Maintenance Domain (MD)* count.

Possible values:

- `50`

Maintenance Associations count max

Displays the maximum number of the *Maintenance Association (MA)* count.

Possible values:

- `10`

MEPs count port max

Displays the maximum number of the Port *Maintenance End Point (MEP)* count.

RMEPs count max

Displays the maximum number of the *Remote-MEP* count.

CCM Interval min

Displays the minimum duration of the *CCM* interval supported by the device.

CCM Interval max

Displays the maximum duration of the *CCM* interval supported by the device.

MEPs count service max

Displays the maximum number of the Service *Maintenance End Point (MEP)*.

Possible values:

- `32`

Has MIPs

Displays if the CFM contains the *Maintenance Intermediate Points (MIPs)*.

Possible values:

- `marked`
- `unmarked` (default setting)

Has up MEPs

Displays if the device supports the Up *Maintenance Intermediate Points (MEPs)*.

Possible values:

- `marked`
- `unmarked` (default setting)

Has VLAN MEPs

Displays if the CFM contains the VLAN *Maintenance End Points (MEPs)*.

Possible values:

- `marked` (default setting)
- `unmarked`

5.8.2.2 CFM Configuration

[Switching > L2-Redundancy > CFM > Configuration]

[Domain]

Table

For information on how to customize the appearance of the table, see “Working with tables” on page 14.

Buttons

 Add

Opens the *Create* window to add a new table row.

- In the *Domain* field, specify the domain name.
  Possible values:
  - Alphanumeric ASCII character string with 1..15 characters
- In the *Format* field, select a format from the drop-down list.
  Possible values:
  - `none`
    No format specified.
  - `string` (default setting)
    Lets you specify the format name in the *Name* column.
- In the *Name* field, specify a string name if the value item `string` is selected in the *Format* field.
  Possible values:
  - Alphanumeric ASCII character string with 1..43 characters
- In the *Level* field, select a priority level from the drop-down list.
  Possible values:
  - `0..7`
    The value `0` assigned to the priority queue with the lowest priority.
    The value `7` assigned to the priority queue with the highest priority.

 Remove

Removes the selected table row.

Domain

Displays the domain name.

Format

Specifies the type of format for the domain.

Name

Specifies the format name of the domain only if the *Format* column contains the value item `string`.

Level

Specifies the level for the domain.

[Service]

Table

For information on how to customize the appearance of the table, see “Working with tables” on page 14.

Buttons

 Add

Opens the *Create* window to add a new table row.

- In the *Domain* field, select a value item from the drop-down list.
- In the *Service* field, specify the name of the service provider.
  Possible values:
  - Alphanumeric ASCII character string with 1..15 characters
- In the *Format* field, select a value item from the drop-down list.
  Possible values:
  - `string`
    Lets you specify the name for the service format as an alphanumeric ASCII character string.
  - `two-octets`
    Lets you specify the name for the service format as a 2-byte hexadecimal string.
  - `primary-vid`
    The device uses the VLAN ID specified in the *MEP* tab, *VLAN* column.
- In the *Service name* field, specify the name for the service format. If the value `primary-vid` is selected from the *Format* drop-down list, then the *Service name* field becomes inactive.
  Possible values:
  - Alphanumeric ASCII character string with 1..15 characters
    When the *Format* field contains the value `string`.
  - Hexadecimal string.
    When the *Format* field contains the value `two-octets`.
- In the *CCM interval* field, select a value item from the drop-down list.
  Possible values:
  - *Invalid*
  - *3.3 ms*
  - *10 ms*
  - *100 ms*
  - *1 s*

 Remove

Removes the selected table row.

Domain

Displays the domain name selected for the service.

Service

Displays the service name specified.

Format

Specifies the format for the service.

Service name

Specifies the name for the service format.

CCM interval

Specifies the agreed upon interval that each *MEP* in the *MA* uses for sending the *CCMs*.

[MEP]

Table

For information on how to customize the appearance of the table, see “Working with tables” on page 14.

Buttons

 Add

Opens the *Create* window to add a new table row.

- In the *Domain* field, select a value item from the drop-down list.
- In the *Service* field, select a value item from the drop-down list.
- In the *MEP ID* field, specify a MEP ID.
  Possible values:
  - `1..8191, 2, 3`.
- In the *Port* field, select a value item from the drop-down list.
  Possible values:
  - `<port number>`
- In the *VLAN* field, specify the VLAN ID.
  Possible values:
  - `1..4093`
- In the *Remote MEP ID* field, specify the remote MEP ID that is expected to send the CCM PDUs to this MEP.
  Possible values:
  - `1..8191`
- Mark the *Admin active* checkbox to activate the MEP.
- Mark the *CCM enabled* checkbox to activate the generation of continuity-check messages.

 Remove

Removes the selected table row.

Domain

Displays the domain name selected for this service.

Service

Displays the service name specified.

MEP ID

Displays the MEP ID of this MEP.

Port

Specifies the physical port number for this MEP.

Possible values:

- `<port number>`

VLAN

Specifies the VLAN ID. Use this VLAN ID if the *Service* tab, *Format* column contains the value item `primary-vid`, then the MEP becomes a VLAN MEP using this VLAN ID.

Possible values:

- `1..4093`

Remote MEP ID

Specifies the remote MEP ID other than the ID specified in the *MEP ID* column.

Possible values:

- `1..8191` (other than the value specified in the *MEP ID* field)

Admin active

Activates/deactivates the MEP.

Possible values:

- `marked` (default setting)
  The MEP is active.
- `unmarked`
  The MEP is inactive.

CCM enabled

Activates/deactivates the generation of continuity check messages (CCM).

Possible values:

- `marked`
  The device generates continuity-check messages.
- `unmarked` (default setting)
  The device does not generate continuity-check messages.

5.8.2.3 CFM Status

[Switching > L2-Redundancy > CFM > Status]

Table

For information on how to customize the appearance of the table, see “Working with tables” on page 14.

Domain

Displays the domain name.

Service

Displays the service name.

MEP ID

Displays the MEP ID.

Possible values:

- `1..8191, 2, 3`

Port

Displays the physical port number.

State

Displays the status of the MEP.

Possible values:

- `marked`
  The MEP is active.
- `unmarked`
  The MEP is inactive.

RMEP defect state

Displays the status of the RMEP defect.

Possible values:

- `marked`
  The RMEP defect exist.
- `unmarked`
  The RMEP defect does not exist.

RMEP defect description

Displays the detail about the RMEP defect.

Fng state

Displays the message of the Fault Notification Generation (FNG) alarm. FNG alarm provides real-time notifications of faults or connectivity issues detected within the network.

Possible values:

- *reset*
  No defect has been present since reset timer expired or the State Machine (SM) was last reset.
- *defect*
  A defect is present, but not for a long enough time to be reported.
- *defect-report*
  A transient state during which the defect is reported.
- *defect-reported*
  A defect is present, and some defects have been reported.
- *defect-clearing*
  No defect is present, but the reset timer has not yet expired.

Defects

Displays the detected defect.

Possible values:

- *some-RDI-defect*
  One or more network components receive a Remote Defect Indication (RDI) signal, indicating a defect on the remote side of the network.
- *some-MAC-status-defect*
  A defect is detected in the Media Access Control (MAC) functions.
- *some-RMEP-CCM-defect*
  A valid Continuity Check Message (CCM) is not received within 3.5 times *CCM* interval from at least one remote *MEP*.
- *error-CCM-defect*
  Received Continuity Check Message (CCM) from an unknown remote *MEP*-ID or *CCM* interval mismatch.
- *xcon-CCM-defect*
  Received Continuity Check Message (CCM) with an *MD/MEG* level smaller than configured or wrong *MAID/MEGID* (cross-connection or misconfiguration).

Highest defect

Displays the detected defect that has occurred maximum times.

Possible values:

- *none*
  No defect detected.
- *some-RDI-defect*
  def-RDI-CFM is maximum.
- *some-MAC-status-defect*
  def-MAC-status is maximum.
- *some-RMEP-CCM-defect*
  some-RMEP-CCM-defect is maximum.
- *error-CCM-defect*
  error-CCM-defect is maximum.
- *xcon-CCM-defect*
  xcon-CCM-defect is maximum.

SMAC

Displays the source MAC address.

Possible values:

- A valid source MAC address.

CCM RX valid

Displays the number of the *CCM Rx valid* PDUs.

CCM RX invalid

Displays the number of the *CCM Rx invalid* PDUs.

CCM RX error

Displays the number of the *CCM Rx error* PDUs.

CM TX

Displays the number of the *CM Tx* PDUs.

5.8.3 MRP Client

[Switching > L2-Redundancy > MRP Client]

The device lets you set up a Media Redundancy Client (MRC) node. The MRC node in the MRP ring topology is responsible for forwarding of every MRP PDUs from its one ring port to the other ring port. In normal configuration, both the ring ports of the MRC remain unblocked to forward the MRP test PDUs received from the Media Redundancy Manager (MRM). Upon a link failure, the PDUs do not pass through the MRC node, which helps the MRM to detect a failure and unblock its blocked ring port. On a link change on a ring port, the MRC transmits an *MRP_LinkChange* PDU, which takes a form of the *MRP_LinkUp* or the *MRP_LinkDown* PDU.

The *MRP Client* dialog displays the following tabs:

- [Configuration]
- [Status]
- [Statistics]

[Configuration]

Instance

Instance

Displays the MRP instance currently added on the device.

Possible values:

- `No MRP instance found` (default setting)
  No MRP instance is currently added on the device.
- `1` (default setting)
  MRP instance 1 is currently added on the device.

Create

Lets you specify the MRP instance 1 on the device.

Delete

Lets you delete the MRP instance 1 from the device.

Operation

Operation

Enables/disables the *MRP Client* function. After you configured the parameters for the MRP Ring, enable the function here.

Possible values:

- `On`
  The *MRP Client* function is enabled.
  After you configured the device in the MRP Ring, the redundancy is active.
- `Off` (default setting)
  The *MRP Client* function is disabled.

Ring role

Displays the ring role of this media-redundancy instance.

Possible values:

- `mrc` (default setting)
  MRC is the Media Redundancy Client.

Ring port 1

Port

Specifies the port number operating as the ring port1.

Possible values:

- `<port number>`
  Physical port number on the device.

Link

Displays the operating status of the ring port1.

Possible values:

- `marked`
  The ring port1 uses the link as an SF trigger.

Ring port 2

Port

Specifies the port number operating as the ring port2.

Possible values:

- `<port number>`
  Physical port number on the device.

Link

Displays the operating status of the ring port2.

Possible values:

- `marked`
  The ring port2 uses the link as an SF trigger.

Configuration

Recovery profile

Specifies the maximum recovery time in milliseconds for reconfiguration of the ring.

Possible values:

- `500 ms` (default setting)
  The maximum recovery time for this profile is 500 milliseconds.
- `200 ms`
  The maximum recovery time for this profile is 200 milliseconds.

Shorter switching times make greater demands on the response time of every individual device in the ring. Use values lower than `500 ms` only if the other devices in the ring also support this shorter recovery time.

Domain name

Specifies the domain name for the media-redundancy instance.

Possible values:

- Alphanumeric ASCII character string with 1..240 characters (default setting: `<empty>`)

Domain ID

Specifies the UUID for this media-redundancy instance, which is also used in PDUs.

Possible values:

- Valid Universally Unique Identifier (UUID) enclosed within double-quotes (default setting: `"ffffffff-ffff-ffff-ffff-ffffffffffff"`)

OUI type

Specifies the Organizationally Unique Identifier (OUI) type that the device uses in the MRP option Type Length Values (TLVs).

Possible values:

- `default` (default setting)
- `siemens`
- `custom`
  Enables the *Custom OUI* field to specify the OUI value.

Custom OUI

Specifies the custom OUI when the value `custom` is specified in the *Custom OUI* column.

Possible values:

- Valid 3-octet OUI representing hexadecimal notation separated by dashes, for example, `08-00-06`.

Control VLAN

Specifies the ID of the VLAN on which the device forwards the MRP PDUs and receives on the ring ports.

Possible values:

- `0`
  No VLAN assigned.
- `1..4093`
  VLAN assigned.
  While assigning the VLAN ID, you ensure that both the ring ports are members of this VLAN. If you assign a non-existing VLAN to the ring ports, then the device creates this VLAN. In the *Diagnostics > LLDP > Configuration* dialog, the device creates a table row.

[Status]

Table

This table displays the status of a media-redundancy instance in a table row.

For information on how to customize the appearance of the table, see “Working with tables” on page 14.

MRP instance

Displays the media-redundancy instance number.

Possible values:

- `1`

Oper state

Displays the operational state of the media-redundancy instance.

Possible values:

- *disabled*
  The media-redundancy instance is inactive.
- *active*
  The media-redundancy instance is active.
- *internal-error*
  The media-redundancy instance has an internal error detected.

Oper warnings

Displays the number of operational warnings of the media-redundancy instance.

Transitions

Displays the number of transitions that happened between the interconnection topology open and closed state.

Flush count

Displays the number of FDB flushes since the MRP configuration.

[Statistics]

Table

This table displays the following overview of the number of errors detected by the device for the ring port1 and port2 of the media-redundancy instance:

For information on how to customize the appearance of the table, see “Working with tables” on page 14.

Button

Clear statistics

Clears the statistics of the media-redundancy instance.

MRP instance

Displays the media-redundancy instance configured in the device.

Possible values:

- 1

Port 1 TX test

Displays the number of transmitted MRP *test* PDUs for the ring port1.

Port 1 TX topology change

Displays the number of transmitted MRP *topology* PDUs for the ring port1.

Port 1 TX link down

Displays the number of transmitted MRP *link down* PDUs for the ring port1.

Port 1 TX link up

Displays the number of transmitted MRP *link up* PDUs for the ring port1.

Port 1 TX test manager NAck

Displays the number of transmitted test *TestMgrNAck* PDUs for the ring port1.

Port 1 TX test propagate

Displays the number of transmitted MRP *test propogate* PDUs for the ring port1.

Port 1 TX option

Displays the number of transmitted MRP *option* PDUs for the ring port1.

Port 1 TX In test

Displays the number of transmitted MRP *InTest* PDUs for the ring port1.

Port 1 TX In topology change

Displays the number of transmitted MRP *InTopologyChange* PDUs for the ring port1.

Port 1 TX In link down

Displays the number of transmitted MRP *InLinkDown* PDUs for the ring port1.

Port 1 TX In link up

Displays the number of transmitted MRP *InLinkUp* PDUs for the ring port1.

Port 1 TX In link status poll

Displays the number of transmitted MRP *InLinkStatusPoll* PDUs for the ring port1.

Port 1 RX test

Displays the number of received MRP *test* PDUs for the ring port1.

Port 1 RX topology change

Displays the number of received MRP *topology* PDUs for the ring port1.

Port 1 RX link down

Displays the number of received MRP *LinkDown* PDUs for the ring port1.

Port 1 RX link up

Displays the number of received MRP *LinkUp* PDUs for the ring port1.

Port 1 RX test manager NAck

Displays the number of received MRP *TestMgrNAck* PDUs for the ring port1.

Port 1 RX test propagate

Displays the number of received MRP *TestPropogate* PDUs for the ring port1.

Port 1 RX option

Displays the number of received MRP *option* PDUs for the ring port1.

Port 1 RX In test

Displays the number of received MRP *InTest* PDUs for the ring port1.

Port 1 RX In topology change

Displays the number of received MRP *InTopologyChange* PDUs for the ring port1.

Port 1 RX In link down

Displays the number of received MRP *InLinkDown* PDUs for the ring port1.

Port 1 RX In link up

Displays the number of received MRP *InLinkUp* PDUs for the ring port1.

Port 1 RX In link status poll

Displays the number of received MRP *InLinkStatuPoll* PDUs for the ring port1.

Port 1 RX unknown

Displays the number of received MRP *unknown* PDUs for the ring port1.

Port 1 RX error

Displays the number of received MRP *error* PDUs for the ring port1.

Port 1 RX unhandled

Displays the number of received MRP *unhandled* PDUs for the ring port1.

Port 1 RX own

Displays the number of received MRP PDUs with the own Source MAC address (SMAC) for the ring port1.

Port 1 SF

Displays the number of local signal fails for the ring port1.

Port 2 TX test

Displays the number of transmitted MRP *test* PDUs for the ring port2.

Port 2 TX topology change

Displays the number of transmitted MRP *topology* PDUs for the ring port2.

Port 2 TX link down

Displays the number of transmitted MRP *link down* PDUs for the ring port2.

Port 2 TX link up

Displays the number of transmitted MRP *link up* PDUs for the ring port2.

Port 2 TX test manager NAck

Displays the number of transmitted test *TestMgrNAck* PDUs for the ring port2.

Port 2 TX test propagate

Displays the number of transmitted MRP *test propogate* PDUs for the ring port2.

Port 2 TX option

Displays the number of transmitted MRP *option* PDUs for the ring port2.

Port 2 TX In test

Displays the number of transmitted MRP *InTest* PDUs for the ring port2.

Port 2 TX In topology change

Displays the number of transmitted MRP *InTopologyChange* PDUs for the ring port2.

Port 2 TX In link down

Displays the number of transmitted MRP *InLinkDown* PDUs for the ring port2.

Port 2 TX In link up

Displays the number of transmitted MRP *InLinkUp* PDUs for the ring port2.

Port 2 TX In link status poll

Displays the number of transmitted MRP *InLinkStatusPoll* PDUs for the ring port2.

Port 2 RX test

Displays the number of received MRP *test* PDUs for the ring port2.

Port 2 RX topology change

Displays the number of received MRP *topology* PDUs for the ring port2.

Port 2 RX link down

Displays the number of received MRP *LinkDown* PDUs for the ring port2.

Port 2 RX In link up

Displays the number of received MRP *LinkUp* PDUs for the ring port2.

Port 2 RX test manager NAck

Displays the number of received MRP *TestMgrNAck* PDUs for the ring port2.

Port 2 RX test propagate

Displays the number of received MRP *TestPropogate* PDUs for the ring port2.

Port 2 RX option

Displays the number of received MRP *option* PDUs for the ring port2.

Port 2 RX In test

Displays the number of received MRP *InTest* PDUs for the ring port2.

Port 2 RX In topology change

Displays the number of received MRP *InTopologyChange* PDUs for the ring port2.

Port 2 RX In link down

Displays the number of received MRP *InLinkDown* PDUs for the ring port2.

Port 2 RX In link up

Displays the number of received MRP *InLinkUp* PDUs for the ring port2.

Port 2 RX In link status poll

Displays the number of received MRP *InLinkStatusPoll* PDUs for the ring port2.

Port 2 RX unknown

Displays the number of received MRP *unknown* PDUs for the ring port2.

Port 2 RX error

Displays the number of received MRP *error* PDUs for the ring port2.

Port 2 RX unhandled

Displays the number of received MRP *unhandled* PDUs for the ring port2.

Port 2 RX own

Displays the number of received MRP PDUs with the own SMAC for the ring port2.

Port 2 SF

Displays the number of local signal fails for the ring port2.

5.8.4 Spanning Tree

[Switching > L2-Redundancy > Spanning Tree]

The *Spanning Tree Protocol (STP)* is a protocol that deactivates redundant paths of a network to help avoid loops. If a network component becomes inoperable on the path, then the device calculates the new topology and reactivates these paths.

The *Rapid Spanning Tree Protocol (RSTP)* enables fast switching to a newly calculated topology without interrupting existing connections. *RSTP* gets average reconfiguration times of less than a second. When you use *RSTP* in a ring with 10 to 20 devices, you can get reconfiguration times in the order of milliseconds.

The menu contains the following dialogs:

- Spanning Tree Global
- Spanning Tree Port

5.8.4.1 Spanning Tree Global

[Switching > L2-Redundancy > Spanning Tree > Global]

In this dialog, you enable/disable the *Spanning Tree* function and specify the bridge settings.

Variant

Force version

Specifies the protocol used for the *Spanning Tree* function.

Possible values:

- `stp`
  The protocol *stp* is active.
  The *Spanning Tree protocol (STP)* is a layer 2 link management protocol that provides path redundancy which helps prevent loops in the network.
- `rstp` (default setting)
  The protocol *rstp* is active.
  The *Rapid Spanning Tree protocol (RSTP)* provides rapid convergence of spanning tree instances by immediately changing root and designated ports to the forwarding state.

Traps

New root

Activates/deactivates the sending of SNMP traps when another bridge takes over the root bridge role.

Possible values:

- `marked`
  The function is active.
- `unmarked` (default setting)
  The function is inactive.

Topology change

Activates/deactivates the sending of SNMP traps when topology changes. A port changes its *Port state* from *forwarding* to *discarding*, or from *discarding* to *forwarding*.

Possible values:

- `marked`
  The function is active.
- `unmarked` (default setting)
  The function is inactive.

Bridge configuration

Bridge ID

Displays the bridge ID of the device.

The device with the lowest bridge ID numerical value takes over the role of the root bridge in the network.

Possible values:

- `<Bridge priority> <MAC address>`
  Value in the *Priority* field followed by MAC address of the device

Priority

Specifies the bridge priority of the device.

Possible values:

- `0..61440` in steps of 4096 (default setting: `32768`)

To make this device the root bridge, assign the lowest numeric priority value in the network to the device.

Hello time [s]

Specifies the time in seconds between the sending of two configuration messages (Hello data packets).

Possible values:

- `1..2` (default setting: `2`)

If the device takes over the role of the root bridge, then the other devices in the network use the value specified here.

Otherwise, the device uses the value specified by the root bridge. See the *Root information* frame.

Due to the interaction with the *TX holds* parameter, we recommend that you do not change the default setting.

Forward delay [s]

Specifies the delay time for the status change in seconds.

Possible values:

- `4..30` (default setting: `15`)

If the device takes over the role of the root bridge, then the other devices in the network use the value specified here.

Otherwise, the device uses the value specified by the root bridge. See the *Root information* frame.

In the *RSTP* protocol, the bridges negotiate a status change without a specified delay.

The *Spanning Tree* protocol uses the parameter to delay the status change between the statuses *disabled*, *discarding*, *learning*, and *forwarding*.

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.

Max age

Specifies the maximum permitted branch length, namely, the number of devices to the root bridge.

Possible values:

- `6..40` (default setting: `20`)

If the device takes over the role of the root bridge, then the other devices in the network use the value specified here.

Otherwise, the device uses the value specified by the root bridge. See the *Root information* frame.

The *Spanning Tree* protocol uses the parameter to specify the validity of STP-BPDUs in seconds.

TX holds

Specifies the limits of maximum transmission rate for sending BPDUs. When the device sends a BPDU, the device increments a counter on this port.

Possible values:

- `1..10` (default setting: `6`)
  If the counter reaches the value specified here, then the port stops sending BPDUs. On the one hand, this reduces the load generated by *RSTP*, and on the other when the device does not receive BPDUs, a communication interruption can be caused.
  The device decrements the counter by `1` every second. In the following second, the device sends a maximum of `1` new BPDUs.

Max hops

Specifies the number of times that a root bridge can distribute its BPDU information.

Possible values:

- `6..40` (default setting: `20`)

Root topology information

Designated root

Displays the designated root.

Root port

Displays the port number from which the current path leads to the root bridge.

A hyphen (`-`) is displayed when the device takes over the role of the root bridge.

Root path cost

Displays the path cost for the path that leads from the root port of the device to the root bridge of the layer 2 network.

Possible values:

- `0..200000000`
  The value `0` is displayed when the device takes over the role of the root bridge.

Root forward delay [s]

Displays the delay time in seconds set up by the root bridge for status changes.

Possible values:

- `4..30`

The device uses this specified value. See the *Bridge configuration* frame.

In the *RSTP* protocol, the bridges negotiate a status change without a specified delay.

The *Spanning Tree* protocol uses the parameter to delay the status change between the statuses *disabled*, *discarding*, *learning*, and *forwarding*.

Root max age

Displays the maximum age of the information transmitted by a Bridge in the layer 2 network.

Possible values:

- `6..40`

The *Spanning Tree* protocol uses the parameter to specify the validity of STP-BPDUs in seconds.

Topology change count

Displays the number of times the Topology has changed for the Bridge since the *Spanning Tree* instance was started.

Time since topology change

Displays the time since the last topology change.

Possible values:

- `<days, hours:minutes:seconds>`

5.8.4.2 Spanning Tree Port

[Switching > L2-Redundancy > Spanning Tree > Port]

In this dialog, you activate the *Spanning Tree* function on the ports, specify edge ports, specify path cost, and port priority.

The dialog contains the following tabs:
- [Configuration]
- [Status]
- [Statistics]

[Configuration]

Port

Displays the port number.

Active

Activates/deactivates the *Spanning Tree* function on the port.

Possible values:

- `marked`
  The *Spanning Tree* function is active on the port.
- `unmarked` (default setting)
  The *Spanning Tree* function is inactive on the port.

Edge port

Activates/deactivates the *Edge port* mode. If the port is connected to an end device, then use the *Edge port* mode. This setting lets the edge port change faster to the forwarding state after linkup and thus a faster accessibility of the end device.

Possible values:

- `marked`
  The *Edge port* mode is active.
  The port is connected to an end device
  After the connection is set up, the port changes to the *`forwarding`* status without changing to the *`learning`* status beforehand.
- `unmarked` (default setting)
  The *Edge port* mode is inactive.
  The port is connected to another *STP* bridge.
  After the connection is set up, the port changes to the *`learning`* status before changing to the *`forwarding`* status, if applicable.

Auto-edge port

Activates/deactivates the automatic detection of whether you connect an end device to the port. The prerequisite is that the checkbox in the *Edge port* column is `unmarked`.

Possible values:

- `marked` (default setting)
  The automatic detection is active.
  After the installation of the connection, and after 1.5 × *Hello time [s]*, the device sets the port to the *`forwarding`* status (default setting: 1.5 × 2 s) if the port did not receive any STP-BPDUs during this time.
- `unmarked`
  The automatic detection is inactive.
  After the installation of the connection, and after *Max age* the device sets the port to the *`forwarding`* status.
  (default setting: 20 s)

Point-to-point MAC

Specifies whether the port connects to a point-to-point LAN rather than to a shared medium. This can be automatically determined, or forced, either true or false. Transition to the forwarding state is faster for point-to-point LANs than for shared media.

Possible values:

- *`force true`*
- *`force false`*
- *`auto`* (default setting)

Path cost

Specifies the path costs of the port.

Possible values:

- `1..200000000` (default setting: `0`)
  When the value is `0`, the device automatically calculates the path costs depending on the data rate of the port.

Port priority

Specifies the priority of the port.

Possible values:

- `0..240` in steps of 16 (default setting: `128`)

Restricted role

Activates/deactivates the port to take over the role of root port.

Possible values:

- `marked`
  The port cannot take over the role of root port.
- `unmarked` (default setting)
  The port can take over the role of root port.

Restricted TCN

Activates/deactivates the sending of topology change notifications to other ports.

Possible values:

- `marked`
  The port does not send topology change notifications to other ports.
- `unmarked` (default setting)
  The port sends topology change notifications to other ports.

[Status]

Port

Displays the port number.

Instance

Displays the bridge instance number.

Spanning tree member

Displays if a port is a member of *Spanning Tree* protocol.

Possible values:

- `marked` (default setting)
  The port is a member of *Spanning Tree* protocol.
- `unmarked`
  The port is not a member of *Spanning Tree* protocol.

Active

Displays if the *Spanning Tree* function is active on the port.

Possible values:

- `marked`
  The *Spanning Tree* function is active.
- `unmarked`
  The *Spanning Tree* function is inactive.

Parent port

Displays the parent port if the physical port is aggregated.

Uptime

Displays the time in days, hours, minutes, and seconds since the port was reset.

Port state

Displays the current state of the port.

Port ID

Displays the unique port identifier number. Port identifier number consist of port number and port priority field.

Path cost

Displays the path cost of the port.

Designated root

Displays the designated root.

Designated cost

Displays the designated cost.

Port priority

Displays the priority of the port.

Designated bridge

Displays the designated bridge.

Designated port

Displays the designated port.

TC ack

Displays the topology change acknowledgment.

Possible values:

- `marked`
  The topology is changed.
- `unmarked`
  No change in the topology.

Hello time

Displays the hello time in seconds.

Edge port

Displays if the edge port mode is active on the port.

Possible values:

- `marked`
  The edge port mode is active.
- `unmarked`
  The edge port mode is inactive.

Operation edge port

Displays if an end device or an STP bridge is connected to the port.

Possible values:

- `marked`
  The operation edge port is active.
- `unmarked`
  The operation edge port is inactive.

Auto-edge port

Displays if the automatic detection of edge port is active on the port.

Possible values:

- `marked`
  The automatic detection of edge port is active.
- `unmarked`
  The automatic detection of edge port is inactive.

MAC operational

Displays if MAC service is provided by the port.

Possible values:

- `marked`
  The MAC service is provided.
- `unmarked`
  The MAC service is not provided.

Admin point-to-point MAC

Displays the current state of the *Admin point-to-point MAC* configuration.

Possible values:

- *`force true`*
  The device assigns the MAC address.
- *`force false`*
  The device does not assign the MAC address.
- *`auto`*
  The device assigns the MAC address automatically.

Operation point-to-point MAC

Displays the current state of the *Operation point-to-point MAC* configuration.

Possible values:

- `marked`
  The specified setting is active.
- `unmarked`
  The specified setting is inactive.

Port role

Displays the current port role.

Restricted role

Displays if the port can take over the role of root port.

Possible values:

- `marked`
  The port cannot take over the role of root port.
- `unmarked`
  The port can take over the role of root port.

Restricted TCN

Displays if the port sends the topology change notifications to other ports.

Possible values:

- `marked`
  The port does not send topology change notifications to other ports.
- `unmarked`
  The port sends topology change notifications to other ports.

[Statistics]

The tab displays the following statistics per port:

- Number of frames sent
  - *STP frame transmitted*
  - *RSTP frame transmitted*
  - *TCN frame transmitted*
- Number of frames received
  - *STP frame received*
  - *RSTP frame received*
  - *TCN frame received*
- Number of frames discarded
  - *Unknown frame discarded*
  - *Illegal frame discarded*

6 Diagnostics

The menu contains the following dialogs:

- RMON
- Alarm
- Syslog
- Port Mirroring
- DDMI
- LLDP
- Report
- System

6.1 RMON

[Diagnostics > RMON]

Remote Monitoring (RMON) is an Internet Engineering Task Force (IETF) standard that allows various network agents and console systems to exchange network monitoring data.

The menu contains the following dialogs:

- Configuration
- Statistics

6.1.1 Configuration

[Diagnostics > RMON > Configuration]

This dialog lets you configure the RMON parameters.

The dialog contains the following tabs:
- [Alarm]
- [Event]
- [Ether stats]
- [History]

Traps

Rising alarm

Activates/deactivates the sending of an SNMP trap when an alarm exceeds the rising threshold value and generates an event.

Possible values:

- `marked`
  The sending of SNMP traps is active.
- `unmarked` (default settings)
  The sending of SNMP traps is inactive.

Falling alarm

Activates/deactivates the sending of an SNMP trap when an alarm value is lower than the falling threshold value and generates an event.

Possible values:

- `marked`
  The sending of SNMP traps is active.
- `unmarked` (default settings)
  The sending of SNMP traps is inactive.

[Alarm]

Table

For information on how to customize the appearance of the table, see “Working with tables” on page 14.

Buttons

 Add

Opens the *Create* window to add a new entry to the table.

- In the *Alarm ID* field, specify the alarm ID.
  Possible values:
  - `1..65535`
- In the *Port* drop-down list, select the port number.
- In the *Var name* drop-down list, select the variable name to be sampled.
- In the *Sample type* drop-down list, select the sampling method of the selected variable.
- In the *Interval [s]* field, specify the time in seconds for sampling and comparing the rising and falling threshold.
  Possible values:
  - `1..2147483647`
- In the *Rising threshold* field, specify the rising threshold value.
  Possible values:
  - `-2147483648..2147483647`
- In the *Falling threshold* field, specify the falling threshold value.
  Possible values:
  - `-2147483648..2147483647`
- In the *Rising event index* field, specify the index value from the event table to trigger the corresponding event when the rising threshold value is reached.
  Possible values:
  - `0..65535`
    If the value is `0`, then no associated event generated as `0` is not a valid event index.
- In the *Falling event index* field, specify the index value from the event table to trigger the corresponding event when the falling threshold value is reached.
  Possible values:
  - `0..65535`
    If the value is `0`, then no associated event generated as `0` is not a valid event index.
- In the *Startup type* drop-down list, select the sampling method for the variable.

 Remove

Removes the selected table row.

Alarm ID

Displays the alarm entry ID.

Possible values:

- `1..65535`

Port

Displays the port number.

Var name

Specifies the variable name for sampling.

Possible values:

- *ifInOctets*
  The total number of octets received on the port.
- *ifInUcastPkts*
  The number of unicast packets delivered to a higher-layer protocol.
- *ifInNUcastPkts*
  The number of broadcast and multicast packets delivered to a higher-layer protocol.
- *ifInDiscards*
  The number of incoming packets that were discarded even though the packets are normal.
- *ifInErrors*
  The number of incoming packets that contained errors and that preventing them from being delivered to a higher-layer protocol.
- *ifInUnknownProtos*
  The number of the incoming packets that were discarded because of an unknown or unsupported protocol.
- *ifOutOctets*
  The number of octets sent out of the port.
- *ifOutUcastPkts*
  The number of unicast packets that were requested to send.
- *ifOutNUcastPkts*
  The number of broadcast and multicast packets that were requested to send.
- *ifOutDiscards*
  The number of outgoing packets that were discarded even though the packets were normal.
- *ifOutErrors*
  The number of outgoing packets that were not sent due to errors.
- *ifOutQLen*
  The length of the output packet queue (in packets).

Sample type

Specifies the sampling method of the selected variable.

Possible values:

- *absolute*
  The device checks each sample.
- *delta* (default setting)
  The device checks the differences between samples.

Interval [s]

Specifies the time in seconds for sampling and comparing the rising and falling threshold.

Possible values:

- `1..2147483647`

Rising threshold

Specifies the rising threshold value.

Possible values:

- `-2147483648..2147483647`

Falling threshold

Specifies the falling threshold value.

Possible values:

- `-2147483648..2147483647`

Rising event index

Specifies the rising event index value.

Possible values:

- `0..65535`
  If the value is `0`, then no associated event generated as `0` is not a valid event index.

Falling event index

Specifies the falling event index value.

Possible values:

- `0..65535`
  If the value is `0`, then no associated event generated as `0` is not a valid event index.

Startup type

Specifies the method of sampling the selected variable and calculating the value to be compared against the thresholds.

Possible values:

- *none*
  The device does not generates any alarm.
- *rising*
  The device generates an alarm when the value of the first received sample is higher than the rising threshold.
- *falling*
  The device generates an alarm when the value of the first received sample is less than the falling threshold.
- *both*
  The device generates an alarm when the value of the first received sample is higher than the rising threshold or less than the falling threshold.

Trigger count

Displays the number of rising and falling alarm counts.

[Event]

Table

For information on how to customize the appearance of the table, see “Working with tables” on page 14.

Buttons

Add

Opens the *Create* window to add a new table row.

- In the *Event ID* field, specify the event ID.
  Possible values:
  - `1..65535`
- In the *Event description* field, specify the event description.
- In the *Event type* drop-down list, select the event type.

Remove

Removes the selected table row.

Event ID

Displays the event ID.

Possible values:

- `1..65535`

Event description

Specifies the event description.

Possible values:

- Alphanumeric ASCII character string with 0..127 characters

Event type

Specifies the notification type when an event is triggered.

Possible values:

- *none*
  The device does not generate an event log entry and does not send an SNMP trap.
- *log*
  The device generates an event log entry when an event is triggered.

- *trap*
  The device sends an SNMP trap when an event is triggered.
- *both*
  The device generates an event log entry and sends an SNMP trap.

[Ether stats]

Table

For information on how to customize the appearance of the table, see “Working with tables” on page 14.

Buttons

Add

Opens the *Create* window to add a new entry to the table.

- In the *Ether stats ID* field, specify the ether stats ID.
  Possible values:
  – 1..65535
- In the *Port* drop-down list, select the port number.

Remove

Removes the selected table row.

Ether stats ID

Displays the ether statistics ID.

Possible values:

- 1..65535

Port

Displays the port number.

[History]

Table

For information on how to customize the appearance of the table, see “Working with tables” on page 14.

Buttons


Add

Opens the *Create* window to add a new entry to the table.

- In the *History ID* field, specify the history ID.
  Possible values:
  - `1..65535`
- In the *Port* drop-down list, select the port number.


Remove

Removes the selected table row.

History ID

Displays the history ID to which the table entry relates.

Possible values:

- `1..65535`

Port

Displays the port number.

Interval

Specifies the time in seconds for sampling the history statistics data.

Possible values:

- `1..3600` (default setting: `1800`)

Bucket size

Specifies the maximum data entries associated with the history control entry stored in RMON.

Possible values:

- `1..65535` (default setting: `50`)

Data granted

Displays the number of data entries saved in the RMON.

6.1.2 Statistics

[Diagnostics > RMON > Statistics]

This dialog lets you display the Ether statistics, history, and port statistics of RMON parameters.

The dialog contains the following tabs:
- [Event]
- [Ether stats]
- [History]
- [Port RMON statistics]

[Event]

Table

For information on how to customize the appearance of the table, see “Working with tables” on page 14.

Event ID

Displays the event ID.

Possible values:
- `1..65535`

Log index

Displays the log index number to which the table entry relates.

Log time

Displays the event log time.

Log description

Displays the log description.

Possible values:

- Alphanumeric ASCII character string with 0..127 characters

[Ether stats]

Table

For information on how to customize the appearance of the table, see “Working with tables” on page 14.

Ether stats ID

Displays the ether statistics ID.

Drop events

Displays the total number of events in which data packets were dropped.

Octets

Displays the total number of octets (including invalid data packets) received.

Packets

Displays the total number of packets (including invalid data packets, broadcast data packets, and multicast data packets) received.

Broadcast packets

Displays the total number of data packets directed to the broadcast address.

Multicast packets

Displays the total number of data packets directed to the multicast address.

CRC align errors

Displays the total number of data packets received which had an invalid *Frame Check Sequence (FCS)*, did not have an integral number of octets (multiple of 8), or both.

Undersize packets

Displays the total number of data packets received that were less than 64 octets.

Oversize packets

Displays the total number of data packets received that were longer than 1518 octets.

Fragments

Displays the number of data packets shorter than 64 octets received with an invalid CRC.

Jabbers

Displays the number of data packets longer than 1518 octets received with an invalid CRC.

Collisions

Displays the total number of collisions.

Packets 64 octets

Displays the total number of data packets of 64 octets received.

Packets 65 to 127 octets

Displays the total number of data packets between 65 and 127 octets received.

Packets 128 to 255 octets

Displays the total number of data packets between 128 and 255 octets received.

Packets 256 to 511 octets

Displays the total number of data packets between 256 and 511 octets received.

Packets 512 to 1023 octets

Displays the total number of data packets between 512 and 1023 octets received.

Packets 1024 to 1518 octets

Displays the total number of data packets between 1024 and 1518 octets received.

[History]

Table

For information on how to customize the appearance of the table, see “Working with tables” on page 14.

History ID

Displays the index of the history ID.

Log index

Displays the log index.

Interval start

Displays the value of the system uptime at the start of the interval over which this sample was measured.

Drop events

Displays the total number of events in which packets were dropped.

Octets

Displays the total number of octets (including invalid packets) received.

Packets

Displays the total number of packets (including invalid data packets, broadcast data packets, and multicast data packets) received.

Broadcast packets

Displays the total number of data packets directed to the broadcast address.

Multicast packets

Displays the total number of data packets directed to the multicast address.

CRC align errors

Displays the total number of data packets received which had an invalid *Frame Check Sequence (FCS)*, did not have an integral number of octets (multiple of 8), or both.

Undersize packets

Displays the total number of data packets received that were shorter than 64 octets.

Oversize packets

Displays the total number of data packets received that were more than 1518 octets.

Fragments

Displays the number of data packets shorter than 64 octets received with an invalid CRC.

Jabbers

Displays the number of data packets longer than 1518 octets received with an invalid CRC.

Collisions

Displays the total number of collisions.

Utilization

Displays the utilization in percentage of the network physical layer during the sampling interval.

[Port RMON statistics]

Table

For information on how to customize the appearance of the table, see “Working with tables” on page 14.

Buttons

Clear port statistics

Clears the port RMON statistics in the table to 0.

Port

Displays the port number.

Received frames discarded

Displays the number of frames discarded.

Received drop events

Displays the number of data packets discarded due to ingress congestion.

Received octets

Displays the number of octets (including invalid packets) received.

Received packets

Displays the total number of data packets (including invalid packets) received.

Received broadcast packets

Displays the total number of broadcast packets (including invalid packets) received.

Received multicast packets

Displays the total number of multicast packets (including invalid packets) received.

Received CRC align error packets

Displays the number of data packets received with CRC or alignment errors.

Received undersize packets

Displays the number of data packets shorter than 64 octets received with valid CRC.

Received oversize packets

Displays the total number of data packets longer than 1518 octets received with valid CRC.

Received fragments packets

Displays the number of data packets shorter than 64 octets received with an invalid CRC.

Received jabbers packets

Displays the number of data packets longer than 1518 octets received with an invalid CRC.

Received packets with payload size 0 to 64 bytes

Displays the total number of data packets between 0 and 64 bytes received.

Received packets with payload size 65 to 127 bytes

Displays the total number of data packets between 65 and 127 bytes received.

Received packets with payload size 128 to 255 bytes

Displays the total number of data packets between 128 and 255 bytes received.

Received packets with payload size 256 to 511 bytes

Displays the total number of data packets between 256 and 511 bytes received.

Received packets with payload size 512 to 1023 bytes

Displays the total number of data packets between 512 and 1023 bytes received.

Received packets with payload size 1024 to 1518 bytes

Displays the total number of data packets between 1024 and 1518 bytes received.

Transmitted packets with payload size 1519 or more bytes

Displays the total number of data packets with 1519 or more bytes received.

Transmit drop events

Displays the number of data packets discarded due to egress congestion.

Transmitted octets

Displays the number of octets (including invalid packets) transmitted.

Transmit packets

Displays the total number of packets (including invalid packets) transmitted.

Transmit broadcast packets

Displays the total number of broadcast packets (including invalid packets) transmitted.

Transmit multicast packets

Displays the total number of multicast packets (including invalid packets) transmitted.

Transmitted packets with payload size 0 to 64 bytes

Displays the total number of data packets between 0 and 64 bytes transmitted.

Transmitted packets with payload size 65 to 127 bytes

Displays the total number of data packets between 65 and 127 bytes transmitted.

Transmitted packets with payload size 128 to 255 bytes

Displays the total number of data packets between 128 and 255 bytes transmitted.

Transmitted packets with payload size 256 to 511 bytes

Displays the total number of data packets between 255 and 511 bytes transmitted.

Transmitted packets with payload size 512 to 1023 bytes

Displays the total number of data packets between 512 and 1023 bytes transmitted.

Transmitted packets with payload size 1024 to 1518 bytes

Displays the total number of data packets between 1024 and 1518 bytes transmitted.

Transmitted packets with payload size 1519 or more bytes

Displays the total number of data packets with 1519 or more bytes transmitted.

6.2 Alarm

[Diagnostics > Alarm]

This dialog lets you enable or disable the sending of alarm traps and configure the alarm parameters.

Operation

Alarm status trap

Enables/disables the sending of alarm traps if a row is added/modified/deleted.

Possible values:

- *On*
  The device sends alarm traps.
- *Off* (default setting)
  The device does not send any alarm traps.

Table

For information on how to customize the appearance of the table, see “Working with tables” on page 14.

Buttons

 Add

Opens the *Create* window to add a new table row.

- In the *Name* field, specify the alarm name.
  Possible values:
  - Alphanumeric ASCII character string with 6..99 characters.
- In the *Alarm parameter* drop-down list, select the port number for the alarm.
  Possible values:
  - `Gi 1/1..Gi 1/11`
- In the *Parameter type* drop-down list, select the parameter type of the alarm.
  Possible values:
  - *link*
    The device generates an alarm if a change in the link status is detected.
  - *fdx*
    The device generates an alarm if an interface is operating at full-duplex.
  - *fiber*
    The device generates an alarm if an interface is a fiber link.
  - *speed*
    The device generates an alarm depending upon the selected link speed in the *Value type* drop-down list.
- In the *Value type* drop-down list, select the value for the assigned *Parameter type*.
  Possible values:
  - *true*
    The function of the selected value in the *Parameter type* drop-down list is active.
  - *false*
    The function of the selected value in the *Parameter type* drop-down list is inactive.
  - *undefined*
    The port link speed is not defined.
  - *10 Mbit/s*
    The device generates alarm at *10 Mbit/s* link speed.
  - *100 Mbit/s*
    The device generates alarm at *100 Mbit/s* link speed.
  - *1 Gbit/s*
    The device generates alarm at *1 Gbit/s* link speed.

 Remove

Removes the selected table row.

Name

Displays the alarm name.

Feature name

Displays the feature name of the alarm.

Possible values:

- `port`
  The alarm is related to the port.

Alarm type

Displays the type of alarm.

Possible values:

- `status`
  The device displays the port status alarm.

Alarm parameter

Displays the port number for the alarm.

Parameter type

Displays the parameter to which the alarm relates.

Value type

Displays the value type for the assigned parameter in the *Parameter type* column.

Suppressed

Activates/deactivates the suppression of an active alarm.

Possible values:

- `marked`
  The alarm is suppressed.
- `unmarked` (default setting)
  The alarm is not suppressed.

Active

Displays if the alarm is active.

Possible values:

- `marked`
  The alarm is active.
- `unmarked`
  The alarm is inactive.

Exposed active

Displays if the active alarm is not yet suppressed.

Possible values:

- `marked`
  The active alarm is suppressed.
- `unmarked`
  The active alarm is not yet suppressed.

6.3 Syslog

[Diagnostics > Syslog]

This dialog lets you specify the settings for the syslog server.

Operation

Mode

Enables/disables the reporting of logs to the syslog server.

Possible values:

- `On`
  The reporting of logs is enabled.
- `Off` (default setting)
  The reporting of logs is disabled.

Server configuration

This frame lets you specify the server settings. The prerequisite is that the user privilege level `15` is assigned to your user account.

IPv4 address

Specifies the IPv4 address of the syslog server.

Possible values:

- Valid IPv4 address (default setting: `<no-address>`)

Severity level

Specifies the severity level for the logs that the device reports to the syslog server.

Possible values:

- *error*
- *warning*
- *notice*
- *informational*

6.4 Port Mirroring

[Diagnostics > Port Mirroring]

The *Port Mirroring* function lets you copy received and sent data packets from selected source ports or VLANs to a destination port. You can monitor the data packets on the source ports in the sending and receiving directions with a management tool connected to the destination port. The function has no effect on the data packets of the source ports.

Note: A user with a privilege level 10 or higher can configure the *Port Mirroring* function for troubleshooting purposes. This may expose sensitive data which may be considered a security risk.

Global parameters

Max session count

Displays the maximum number of available mirroring sessions in the device.

Max session source count

Displays the maximum number of mirror source sessions.

CPU mirror support

Displays the current status of the *CPU mirror support*, separately for the received (Rx) and the transmitted (Tx) direction.

The CPU port is the port that allows capture of data packets originating and terminating at the internal CPU.

Possible values:

- `marked`
  The *CPU mirror support* is active. The device copies data packets from the selected CPU port (Rx and/or Tx direction) to the configured destination port.
- `unmarked`
  The *CPU mirror support* is inactive. The device can not copy data packets from the CPU port to the destination port.

Table

Session ID

Displays the number of the session.

Mode

Activates/deactivates the mirror session.

Possible values:

- `marked`
  The session is active.
- `unmarked` (default setting)
  The session is inactive.

Type

Displays which type of the mirror function is active on the session.

Possible values:

- *mirror*
  There is only one type of the mirror function available.

Source VLANs

Specifies a list of the source VLANs. The data packets in the VLANs specified in this list get mirrored to the destination port.

For configuring a mirror source, you can specify the value either in the *Source VLANs* column or in the *Source port list RX* and *Source port list TX* columns.

If you specify a value in the *Source port list RX* or *Source port list TX* columns, then the GUI disables the *Source VLANs* column. Conversely if you specify a value in the *Source VLANs* column, then the GUI disables the *Source port list RX* and the *Source port list TX* columns.

If you want to change the source type, perform the following steps:

- ☐ Clear any values you may have already specified for the current source type column.
- ☐ Apply the changes.
- ☐ Specify value in the other source type column.
- ☐ Apply the changes.

Possible values:

- `1..4093` (default setting: `1`)
  The possible values can be a single VLAN ID, multiple VLAN IDs, or a VLAN range. Refer to the examples below:
  - Single value, such as: `7`
  - Multiple values, separated by comma (`,`) such as: `11,77`
  - Range value, separated by hyphen (`-`), such as: `10-20`

Note: 4094 and 4095 are reserved for management purposes.

Source port list RX

Specifies a list of source ports that are enabled for mirroring of the received (Rx) data packets on that port.

If you want to change the source type, first clear any values you may have already specified for the current source type.

Possible values:

- `Fa 1/1..Fa 1/7, Gi 1/1..Gi 1/3`
  `Fa` is a Fast Ethernet port and `Gi` is a Gigabit Ethernet port.

Source port list TX

Specifies a list of source ports that are enabled for mirroring of the transmitted (Tx) data packets on that port.

If you want to change the source type, first clear any values you may have already specified for the current source type.

Possible values:

- `Fa 1/1..Fa 1/7, Gi 1/1..Gi 1/3`

CPU RX

Activates/deactivates mirroring of data packets received by the internal CPU.

Possible values:

- `marked`
  Active
- `unmarked` (default setting)
  Inactive

CPU TX

Activates/deactivates mirroring of data packets transmitted by the internal CPU.

Possible values:

- `marked`
  Active
- `unmarked` (default setting)
  Inactivate

Destination port

Specifies the port that receives the mirrored data packets.

If you already use a port as a source port (any direction), then you cannot use that port as a destination port.

Possible values:

- `Fa 1/1..Fa 1/7, Gi 1/1..Gi 1/3`
  Select any one value from the range.

Note: Select a destination port with a data rate high enough to accommodate the expected combined data packets of all source ports or VLANs. This helps you avoid losing mirrored data packets. For example, if you mirror two Fast Ethernet (Fa) ports with a port speed of 100 Mbit/s and heavy traffic in both directions, you will need a Gigabit Ethernet (Gi) port as the mirror destination.

6.5 DDMI

[Diagnostics > DDMI]

The DDMI (Digital Diagnostics Monitoring Interface) provides an enhanced digital diagnostic monitoring interface for SFP (Small Form-factor Pluggable) transceivers. This helps ensure real-time access to SFP operating parameters.

The dialog contains the following tabs:
- [Overview]
- [Temperature [C]]
- [Voltage [V]]
- [Bias [mA]]
- [Transmitted power [mW]]
- [Received power [mW]]

DDMI mode

DDMI mode

Enables/disables the *DDMI mode* function.

Possible values:

- `On`
  The *DDMI mode* function is enabled.
- `Off` (default settings)
  The *DDMI mode* function is disabled.

[Overview]

Table

For information on how to customize the appearance of the table, see “Working with tables” on page 14.

Port

Displays the port number.

Transceiver status

Displays the SFP transceiver status support information.

Possible values:

- `marked`
  The function is active on the port.
- `unmarked`
  The function is inactive on the port.

DDMI status

Displays the DDMI status support information.

Possible values:

- `marked`
  The function is active on the port.
- `unmarked`
  The function is inactive on the port.

SFP detected

Displays the detected SFP transceiver.

Possible values:

- `marked`
  The device detects an SFP transceiver.
- `unmarked`
  No SFP transceiver is detected.

SFP type

Displays the type of the SFP transceiver.

Vendor

Displays the vendor name of the SFP transceiver.

Part number

Displays the vendor-specific part number of the SFP transceiver.

Serial number

Displays the vendor-specific serial number of the SFP transceiver.

Revision

Displays the vendor-specific revision level of the part number of the SFP transceiver.

Date code

Displays the vendor-specific manufacturing date code of the SFP transceiver.

[Temperature [C]]

Table

For information on how to customize the appearance of the table, see “Working with tables” on page 14.

Port

Displays the port number.

State

Displays the current temperature monitoring state of the SFP transceiver.

Possible values:

- *none*
- *low-warn*
- *high-warn*
- *low-alarm*
- *high-alarm*

Current

Displays the current temperature of the SFP transceiver in °Celsius.

Low alarm threshold

Displays the temperature low alarm threshold value of the SFP transceiver in °Celsius.

High alarm threshold

Displays the temperature high alarm threshold value of the SFP transceiver in °Celsius.

Low warn threshold

Displays the temperature low warning threshold value of the SFP transceiver in °Celsius.

High warn threshold

Displays the temperature high warning threshold value of the SFP transceiver in °Celsius.

[Voltage [V]]

Table

For information on how to customize the appearance of the table, see “Working with tables” on page 14.

Port

Displays the port number.

State

Displays the current voltage monitoring state of the SFP transceiver.

Possible values:

- *none*
- *low-warn*
- *high-warn*
- *low-alarm*
- *high-alarm*

Current

Displays the current voltage of the SFP transceiver.

Low alarm threshold

Displays the voltage low alarm threshold value of the SFP transceiver.

High alarm threshold

Displays the voltage high alarm threshold value of the SFP transceiver.

Low warn threshold

Displays the voltage low warning threshold value of the SFP transceiver.

High warn threshold

Displays the voltage high warning threshold value of the SFP transceiver.

[Bias [mA]]

Table

For information on how to customize the appearance of the table, see “Working with tables” on page 14.

Port

Displays the port number.

State

Displays the current transmit bias monitoring state of the SFP transceiver.

Possible values:

- *none*
- *low-warn*
- *high-warn*
- *low-alarm*
- *high-alarm*

Current

Displays the current transmit bias of the SFP transceiver in milliamperes.

Low alarm threshold

Displays the transmit bias low alarm threshold value of the SFP transceiver in milliamperes.

High alarm threshold

Displays the transmit bias high alarm threshold value of the SFP transceiver in milliamperes.

Low warn threshold

Displays the transmit bias low warning threshold value of the SFP transceiver in milliamperes.

High warn threshold

Displays the transmit bias high warning threshold value of the SFP transceiver in milliamperes.

[Transmitted power [mW]]

Table

For information on how to customize the appearance of the table, see “Working with tables” on page 14.

Port

Displays the port number.

State

Displays the current transmitted power monitoring state of the SFP transceiver.

Possible values:

- *none*
- *low-warn*
- *high-warn*
- *low-alarm*
- *high-alarm*

Current

Displays the current transmitted power of the SFP transceiver in milliwatts.

Low alarm threshold

Displays the transmitted power low alarm threshold value of the SFP transceiver in milliwatts.

High alarm threshold

Displays the transmitted power high alarm threshold value of the SFP transceiver in milliwatts.

Low warn threshold

Displays the transmitted power low warning threshold value of the SFP transceiver in milliwatts.

High warn threshold

Displays the transmitted power high warning threshold value of the SFP transceiver in milliwatts.

[Received power [mW]]

Table

For information on how to customize the appearance of the table, see “Working with tables” on page 14.

Port

Displays the port number.

State

Displays the current received power monitoring state of the SFP transceiver.

Possible values:

- *none*
- *low-warn*
- *high-warn*
- *low-alarm*
- *high-alarm*

Current

Displays the current received power of the SFP transceiver in milliwatts.

Low alarm threshold

Displays the received power low alarm threshold value of the SFP transceiver in milliwatts.

High alarm threshold

Displays the received power high alarm threshold value of the SFP transceiver in milliwatts.

Low warn threshold

Displays the received power low warning threshold value of the SFP transceiver in milliwatts.

High warn threshold

Displays the received power high warning threshold value of the SFP transceiver in milliwatts.

6.6 LLDP

[Diagnostics > LLDP]

The device lets you gather information about neighboring devices. For this, the device is equipped with the Link Layer Discovery Protocol (LLDP). The gathered information enables your network management station to map the structure of your network.

The menu contains the following dialogs:

- LLDP Configuration
- Topology Discovery

6.6.1 LLDP Configuration

[Diagnostics > LLDP > Configuration]

This dialog lets you set up the global parameters in the *Global* frame and parameters for every port in the port configuration table below the *Global* frame.

Global

Re-initialization delay [s]

Specifies the LLDP transmit delay in seconds. This is the time between the shutdown data packet and a new LLDP initialization.

Possible values:

- `1..10` (default setting: `2`)

Message transmit hold

Specifies a multiplier value for the *Message transmit interval [s]*.

Each LLDP data packet contains a time value during which the information in LLDP data packet is considered valid. The device calculates the valid time value by multiplying the value in the current field with the value in the *Message transmit interval [s]* field.

Possible values:

- `2..10` (default setting: `4`)

Message transmit interval [s]

Specifies the interval in seconds. When this time passes since the previous LLDP data packet was sent, the device transmits the next periodic LLDP data packet.

Possible values:

- `5..32768` (default setting: `30`)

Transmit delay [s]

Specifies the delay in seconds. Whenever you change the LLDP configuration, the device delays the transmission of LLDP data packets for this time.

Possible values:

- `1..8192` (default setting: `2`)
  The recommended value is a quarter of the *Message transmit interval [s]*.

Table

For information on how to customize the appearance of the table, see “Working with tables” on page 14.

Port

Displays the port number.

Operation

Specifies the type of operation that the device allows on the port for the LLDP data packets.

Possible values:

- *transmit*
  The device transmits the LLDP data packets but discards the received information from neighboring devices.
- *receive*
  The device stores received LLDP data packets but does not transmit any information to neighboring devices.
- *receive and transmit* (default setting)
  The device transmits the LLDP data packets and also saves information received from neighboring devices.
- *disabled*
  The device neither transmits the LLDP data packets nor saves information received from neighboring devices.

Trap notification

Activates/deactivates the trap notifications on the port. The device generates the trap notification only when the *LLDP rem tables change* is configured in the *Trap* dialog, *Source trap* tab.

Possible values:

- marked
  Trap notification is active on the port. When the value of the *Last change time [s]* changes, the device generates a notification.
- unmarked (default setting)
  Trap notifications are inactive on the port.

Transmit port description

Activates/deactivates the transmitting of the port description.

Possible values:

- marked (default setting)
  The device transmits the port description.
- unmarked
  The device does not transmit the port description.

Transmit system name

Activates/deactivates the transmitting of the *Type Length Value* packets with the device name.

Possible values:

- `marked` (default setting)
  The device transmits the *Type Length Value* packets with the device name.
- `unmarked`
  The device does not transmit the *Type Length Value* packets with the device name.

Transmit system description

Activates/deactivates the transmitting of the *Type Length Value* packets with the system description.

Possible values:

- `marked` (default setting)
  The device transmits the *Type Length Value* packets with the system description.
- `unmarked`
  The device does not transmit the *Type Length Value* packets with the system description.

Transmit system capabilities

Activates/deactivates the transmitting of the *Type Length Value* packets with the system capabilities.

Possible values:

- `marked` (default setting)
  The device transmits the *Type Length Value* packets with the system capabilities.
- `unmarked`
  The device does not transmit the *Type Length Value* packets with the system capabilities.

Transmit management address

Activates/deactivates the transmitting of the management IP address with the system capabilities.

Possible values:

- `marked` (default setting)
  The device transmits the management IP address with the system capabilities.
- `unmarked`
  The device does not transmit the management IP address with the system capabilities.

Transmit PoE

Activates/deactivates the transmitting of Power over Ethernet information.

Possible values:

- `marked`
  The device transmits the information about Power over Ethernet.
- `unmarked` (default setting)
  The device does not transmit the information about Power over Ethernet.

6.6.2 Topology Discovery

[Diagnostics > LLDP > Topology Discovery]

Devices in the network send notification in the form of data packets, which are also known as LLDP Data Units (LLDPDU). The data sent and received through LLDPDU is useful for many reasons. Thus, the device detects which devices in the network are neighbors and through which ports they are connected.

The dialog contains the following tabs:
- [Neighbor]
- [Neighbor management]
- [Statistics]

[Neighbor]

Table

For information on how to customize the appearance of the table, see “Working with tables” on page 14.

Port

Displays the port number of your device.

Chassis ID

Displays the chassis ID of the neighbor device.

Port ID

Displays the port number of the neighbor device.

Port description

Displays the port description of the neighbor device.

System name

Displays the system name of the neighbor device.

System description

Displays the system description of the neighbor device.

Repeater supported

Displays if the repeater function is supported on the neighbor device.

Repeater enabled

Displays if the repeater function of the neighbor device is active or not.

Bridge supported

Displays if the bridge function is supported on the neighbor device.

Bridge enabled

Displays if the bridge function of the neighbor device is active or not.

WLAN access point supported

Displays if the WLAN access point function is supported on the neighbor device.

WLAN access point enabled

Displays if the WLAN access point function of the neighbor device is active or not.

Router supported

Displays if the router function is supported on the neighbor device.

Router enabled

Displays if the router function of the neighbor device is active or not.

Telephone supported

Displays if the telephone function is supported on the neighbor device.

Telephone enabled

Displays if the telephone function of the neighbor device is active or not.

DOCSIS cable device supported

Displays if the DOCSIS cable function is supported on the neighbor device.

DOCSIS cable device enabled

Displays if the DOCSIS cable function of the neighbor device is active or not.

Station only supported

Displays if the station function is supported on the neighbor device.

Station only enabled

Displays if the station function of the neighbor device is active or not.

Reserved supported

Displays if the reserved function is supported on the neighbor device.

Reserved enabled

Displays if the reserved function of the neighbor device is active or not.

Other supported

Displays if the other function is supported on the neighbor device.

Other enabled

Displays if the other function of the neighbor device is active or not.

[Neighbor management]

Table

For information on how to customize the appearance of the table, see “Working with tables” on page 14.

Port

Displays the port number.

System management address subtype

Displays the subtype of the management address associated with the neighbor device.

System management address

Displays the management address associated with the neighbor device.

System management interface subtype

Displays the value that identifies the interface numbering method used to define the interface number associated with the neighbor device.

Possible values:

- `unknown(1)`
- `if Index(2)`
- `system port number(3)`

System management interface

Displays the interface of the neighbor device. The value displayed in the current field depends on the value of the *System management interface subtype* field.

System management OID

Displays the system management object identifier (OID).

[Statistics]

Global

Buttons

Clear global statistics

Clears the text fields of the *Global* frame.

Entries added

Displays the number of new entries that were added to the table in the *Neighbor* tab since the system startup of the device.

Entries deleted

Displays the number of entries that were deleted from the table in the *Neighbor* tab since the startup of the device.

Table drops

Displays the number of LLDP data packets that the device dropped because the table in the *Neighbor* tab was full.

Table age outs

Displays the number of entries that the device deleted due to expiry of the LLDP information.

Last change time [s]

Displays the time in seconds since the device deleted or added the last entry.

Table

The *Statistics* table displays the following information about each port on the device:

For information on how to customize the appearance of the table, see “Working with tables” on page 14.

Buttons

Clear port statistics

Clears the port statistics for the table row you select in the *Statistics* table.

Port

Displays the port number.

TX total

Displays the number of LLDP data packets transmitted by the device.

RX total

Displays the number of LLDP data packets received by the device.

RX error

Displays the number of LLDP data packets received with an error by the device.

RX discarded

Displays the number of LLDP data packets counted and discarded by the device because the table was full.

TLVs discarded

Displays the number of corrupt *Type Length Value* packets counted and discarded by the device.

TLVs unrecognized

Displays the number of well-formed *Type Length Value* packets with an unknown value.

TLVs org discarded

Displays the number of well-formed *Type Length Value* packets with an unknown organizational *Type Length Value* that are unsupported by the device.

Age outs

Displays the number of age outs.

When the age out time of a received LLDP data packet has passed and the port has not received a newer data packet of the same type from the same neighbor, then the device removes that information and increments the *Age outs* counter.

6.7 Report

[Diagnostics > Report]

The menu contains the following dialog:

- System Log

6.7.1 System Log

[Diagnostics > Report > System Log]

The device generates the logs of the device-internal events. This dialog displays the system logs as per their severity level. The device also lets you clear the generated logs of a specific severity level or of every severity level together. To search the log file for search terms, use the search function of your web browser. The generated system logs are kept until a restart is performed on the device. After a restart, the device starts keeping the generated logs again.

System information

System name

Displays the name of the device.

System uptime

Displays the total duration passed since the previous system startup.

System time

Displays the current time on your device.

IPv4 address

Displays the IPv4 address of the device.

MAC address

Displays the MAC address of the device.

Release version

Displays the version number of the release software.

Running version

Displays the version number, creation date and time of the device software that the device loaded during the last system startup and is currently running.

Backup version

Displays the version number, creation date and time of the device software saved as a backup in the non-volatile memory (NVM). The device copied the running version into the backup partition during the last software update, or after you clicked the Restore button. See “Software” on page 27.

Boot code

Displays the version number, creation date and time of the boot code.

Hardware version

Displays the current version of the device hardware.

Power supply 1

Displays the current status of the main power supply.

Power supply 2

Displays the current status of the redundant power supply.

Serial number

Displays the serial number of the device hardware.

Product

Displays the product code of the device.

Table

For information on how to customize the appearance of the table, see “Working with tables” on page 14.

Buttons

Lets you clear the log entries.

Possible values:

- *Clear error*
  Removes every error log generated by the device.
- *Clear warning*
  Removes every warning log generated by the device.
- *Clear notice*
  Removes every notice log generated by the device.
- *Clear informational*
  Removes every informational log generated by the device.
- *Clear all*
  Removes every system log entries generated by the device.

ID

Displays the sequential number for the generated system logs.

Level

Displays the severity level of the generated system logs.

Possible values:

- *error*
- *warning*
- *notice*
- *informational*

Timestamp

Displays the date and time of when the system log was generated.

Possible values:

- Date and time in the format: `<YYYY-MM-DD, HH:MM:SS>`

Message

Displays the information about the generated log.

Possible values:

- Alphanumeric ASCII character string.

6.8 System

[Diagnostics > System]

The menu contains the following dialogs:

- File System

6.8.1 File System

[Diagnostics > System > File System]

This dialog displays the file system information.

Information

Number of files

Displays the number of files stored in the non-volatile memory (NVM).

Total size [bytes]

Displays the total memory occupation size in bytes stored in the non-volatile memory (NVM).

Flash size [bytes]

Displays the total size of the non-volatile memory (NVM) in bytes.

Flash free size [bytes]

Displays the available size of the non-volatile memory (NVM) in bytes.

Table

For information on how to customize the appearance of the table, see “Working with tables” on page 14.

Buttons

Remove

Removes the selected table row.

Index

Displays the index number to which the table row relates.

File name

Displays the file name.

Modification date

Displays the last modified date of the file.

Bytes

Displays the file size in bytes.

Access

Displays the access permission of the file.

Possible values:

- *read-write*
  The file has *read-write* access.
- *read-only*
  The file has *read-only* access.

7 Advanced

The menu contains the following dialogs:
- Command Line Interface
- DNS Client

7.1 Command Line Interface

[Advanced > CLI]

This dialog lets you access the device using the Command Line Interface.

Prerequisites:
- In the *Device Security > Management Access > Server* dialog, *SSH* tab the SSH server is enabled.
- On your workstation, install a SSH-capable client application which registers a handler for URLs starting with `ssh://` in your operating system.

Buttons

Open SSH connection

Opens the SSH-capable client application.

When you click the button, the web application passes the URL of the device starting with `ssh://` and the user name of the currently logged in user.

If the web browser finds a SSH-capable client application, then the SSH-capable client establishes a connection to the device using the SSH protocol.

7.2 DNS Client

[Advanced > DNS Client]

This dialog lets you set up the Domain Name System (DNS) Client settings on the device.

Operation

DNS-proxy

Enables/disables the *DNS-proxy* function.

Possible values:

- `On`
  The *DNS-proxy* is active.
- `Off` (default setting)
  The *DNS-proxy* is inactive.

Default domain name source

Specifies the administrative type for the default domain name. The device uses a default domain name as a suffix of the given name in DNS lookup.

Possible values:

- `none` (default setting)
  No default domain name is used, so the domain name suffix is not added for the DNS lookup.
- `static`
  The device lets you specify the default domain name manually.
- `dhcpv4`
  DHCPv4 discovery determines the default domain name.
- `dhcpv4-vlan`
  DHCPv4 discovery on a specific VLAN interface determines the default domain name.
- The prerequisite for the values `dhcpv4` and `dhcpv4-vlan` is that the VLAN interface has an IPv4 address assigned using the DHCP client in the *Basic Settings > Network > IPv4* dialog, *DHCP client enable* column.

VLAN ID

Specifies the VLAN interface that the device uses when retrieving the default domain name by means of DHCP. The prerequisite is that the item *dhcpv4-vlan* is selected in the *Operation* frame, *Default domain name source* field.

Possible values:

- 1..4093

Domain name

Specifies the static default domain name. You can specify a valid IPv4 address as well in this field. The prerequisite is that the *static* item is selected in the *Operation* frame, *Default domain name source* field.

Possible values:

- ASCII character string with 1..254 characters.
  The device accepts the following characters:
  - a..z
  - A..Z
  - 0..9
  - .
  - -

  The possible values can be a valid DNS or IPv4 address.

[Name server]

Table

For information on how to customize the appearance of the table, see “Working with tables” on page 14.

Index

Displays the sequential number of the name server entries on the device.

Possible values:

- 0..2

Default domain name source

Specifies the administrative type of the name server.

Possible values:

- *none* (default setting)
  The device does not use the name server settings in a DNS lookup, so the domain name lookup is unsuccessful.
- *static*
  The device lets you specify the IPv4 address.
- *dhcpv4*
  The device uses the IPv4 address of the name server that was received in the *DHCPOFFER* message, when the interface IP address got assigned.

- *dhcpv4-vlan*
  The device uses the IPv4 address of the name server that was received in the *DHCPOFFER* message, when the IP address of the associated VLAN interface got assigned.
- The prerequisite for the *dhcpv4* and *dhcpv4-vlan* values is that the VLAN interface has an IPv4 address assigned using the DHCP client in the *Basic Settings > Network > IPv4* dialog, *DHCP client enable* column.

IPv4 address

Specifies the static IPv4 address for the name server. The prerequisite is that the *static* item is selected in the *Name server* table, *Default domain name source* field.

Possible values:

- Valid IPv4 address

VLAN ID

Specifies the VLAN interface, when the item *dhcpv4-vlan* is selected in the *Name server* table, *Default domain name source* field.

The device uses this VLAN interface to retrieve the IPv4 address of the name server via DHCP client.

Possible values:

- 1..4093

A Index

B Further support

Technical questions

For technical questions, please contact any Hirschmann dealer in your area or Hirschmann directly. You find the addresses of our partners on the Internet at www.belden.com.

For technical support, visit hirschmann-support.belden.com. This site also includes a free of charge knowledge base and a software download section.

Technical Documents

The current manuals and operating instructions for Hirschmann products are available at doc.hirschmann.com.

Customer Innovation Center

The Customer Innovation Center is ahead of its competitors on three counts with its complete range of innovative services:

- Consulting incorporates comprehensive technical advice, from system evaluation through network planning to project planning.
- Training offers you an introduction to the basics, product briefing and user training with certification.
  You find the training courses on technology and products currently available at www.belden.com/solutions/customer-innovation-center.
- Support ranges from the first installation through the standby service to maintenance concepts.

With the Customer Innovation Center, you decide against any compromise in any case. Our client-customized package leaves you free to choose the service components you want to use.

C Readers' Comments

What is your opinion of this manual? We are constantly striving to provide as comprehensive a description of our product as possible, as well as important information to assist you in the operation of this product. Your comments and suggestions help us to further improve the quality of our documentation.

Your assessment of this manual:

	Very Good	Good	Satisfactory	Mediocre	Poor
Precise description	O	O	O	O	O
Readability	O	O	O	O	O
Understandability	O	O	O	O	O
Examples	O	O	O	O	O
Structure	O	O	O	O	O
Comprehensive	O	O	O	O	O
Graphics	O	O	O	O	O
Drawings	O	O	O	O	O
Tables	O	O	O	O	O

Did you discover any errors in this manual?
If so, on what page?

Suggestions for improvement and additional information:

General comments:

Sender:

Company / Department:

Name / Telephone number:

Street:

Zip code / City:

E-mail:

Date / Signature:

Dear User,

Please fill out and return this page
- as a fax to the number +49 (0)7127/14-1600 or
- per mail to
  Hirschmann Automation and Control GmbH
  Department IRD-NT
  Stuttgarter Str. 45-51
  72654 Neckartenzlingen
  Germany

HIRSCHMANN

A BELDEN BRAND

HIRSCHMANN
A BELDEN BRAND

User Manual

Configuration
Lemur Rail Switch
HiEOS

Technical support
https://hirschmann-support.belden.com

You find the latest user documentation for your device at: doc.hirschmann.com

Hirschmann Automation and Control GmbH
Stuttgarter Str. 45-51
72654 Neckartenzlingen
Germany

Contents

Safety instructions

⚠ WARNING

UNCONTROLLED MACHINE ACTIONS

To avoid uncontrolled machine actions caused by data loss, configure all the data transmission devices individually.

Before you start any machine which is controlled via data transmission, be sure to complete the configuration of all data transmission devices.

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

About this Manual

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 Industrial HiVision 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 a server.
  See “Importing a configuration profile” on page 57.

With this 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 certificate to the device.
  See “HTTPS certificate management” on page 151.

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 (GUI)	*Secure Hypertext Transfer Protocol (HTTPS)*	Web browser
Command Line Interface (CLI)	*Secure Shell (SSH)* *Telnet*	Terminal emulation software *SSH* client *Telnet* client

1.1 Command Line Interface (CLI) using Secure Shell (SSH) or Telnet

The Command Line Interface lets you use the functions of the device through a 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 Hirschmann devices.

1.1.1 Preparing the data connection

Information for installing 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 port and network parameters.

If you are using a Windows version which is released after Windows Vista then you need a terminal emulator such as PuTTY, MobaXterm, and so on. You can access the user interface of the Command Line Interface for example, with the freeware program *PuTTY*. You can download the software from www.chiark.greenend.org.uk/~sgtatham/putty/.

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

1.1.2 Accessing the CLI using Telnet

Telnet is an unencrypted protocol and therefore potentially insecure. For this reason, the *Telnet* function in the device is disabled by default. We recommend you to use *SSH*.

Note: During setting up the device the first time, after a factory reset, and after you run the command `clear config`, the device has limited availability on the network. The default user name is `admin`, and the default password is `private`. After you have changed the default password, login with the new password and enable the protocol, if necessary.

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>`.

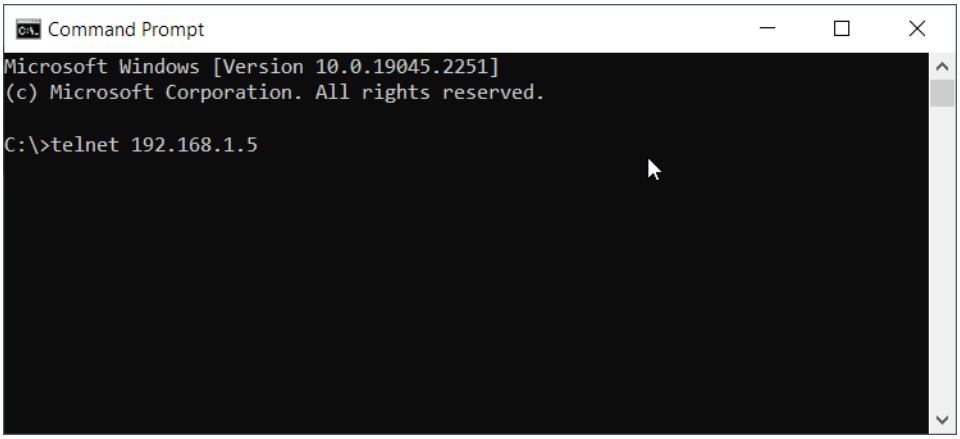


Figure 1: Command prompt: Setting up the Telnet connection to the device

Telnet connection using PuTTY

Perform the following steps:
- ☐ Start the *PuTTY* program on your computer.

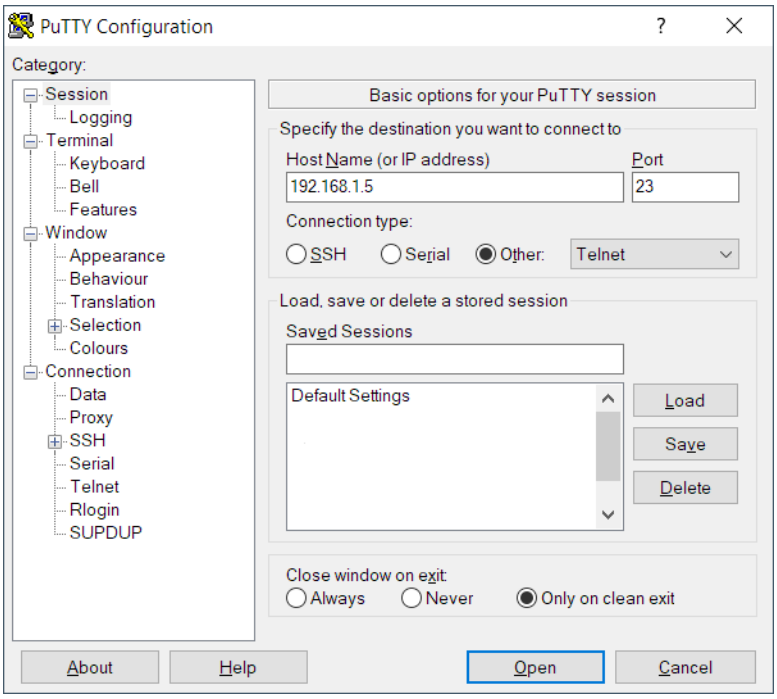


Figure 2:PuTTY input screen

- ☐ In the *Host Name (or IPv4 address)* field you enter the IPv4 address of your device. The IPv4 address consists of 4 decimal numbers with values from 0 to 255. The 4 decimal numbers are separated by dots.

- ☐ 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 4 users to have access to the Command Line Interface at the same time.

Perform the following steps:

- ☐ Enter the user name.
  The default user name is `admin`.
- ☐ Press the <Enter> key.
- ☐ Enter the new password.
  The new password is the password you configured while changing the default password to set up the device.
- ☐ Press the <Enter> key.

```
                Copyright (c) 2011-2024 Hirschmann Automation and Control GmbH
                                        All rights reserved
                                LRS40-0803 Release HiEOS-01.1.00
                                  (Build date 2024-04-09 11:34)

                    System Name    :  LRS40-ECE555d6e234
                    Management IP  :  192.168.1.5
                    Subnet Mask    :  255.255.255.0
                    Base MAC       :  EC:E5:55:01:02:03
                    System Time    :  2024-04-11 14:46:10
Username: admin
Password:*******

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.

LRS>
```

Figure 3: Start screen of the Command Line Interface

Logging out from the Telnet connection

During your active *Telnet* session, when you have performed the required steps and need to logout.
Perform the following steps:

- ☐ To return to the User Exec mode, enter the command `end`.
- ☐ To logout, enter the command `logout`. Alternatively you can also enter the command `exit`.

2 Specifying the IP parameters

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

- Entry using the Industrial HiVision 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 *Dynamic Host Configuration Protocol (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.
- 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.
- Configuration using the Graphical User Interface.
  When the device already has an IPv4 address and is reachable using the network, the Graphical User Interface provides you with another option for configuring the IP parameters.

This chapter contains the following topics:

2.1 IP parameter basics

2.1.1 IPv4

IPv4 address

The IPv4 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 2: IPv4 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 IPv4 address is the network address. The worldwide leading regulatory board for assigning network addresses is the Internet Assigned Numbers Authority (IANA). When you require an IPv4 address block, contact your Internet Service Provider (ISP). Your ISP contacts their local higher-level organization to reserve an IPv4 address block:

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

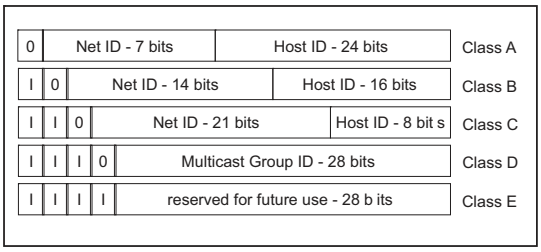


Figure 4: Bit representation of the IPv4 address

When the first bit of an IPv4 address is a zero, it belongs to class A for example, the first octet is less than 128.

When the first bit of an IPv4 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 IPv4 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 IPv4 addresses.

Netmask

Routers and Gateways subdivide large networks into subnetworks. The netmask assigns the IPv4 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 IPv4 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?

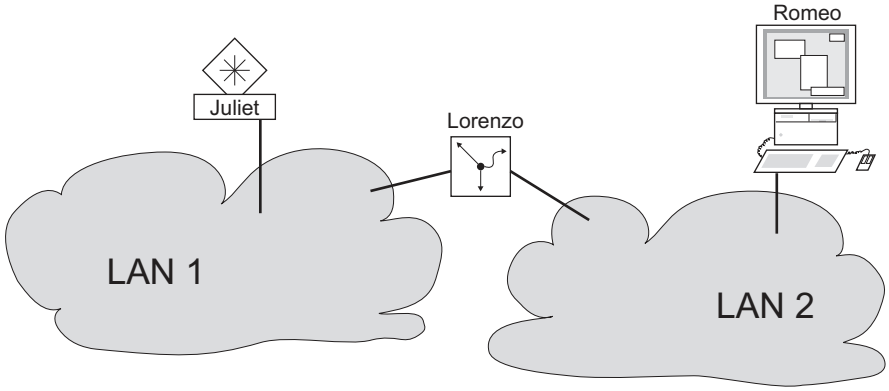


Figure 5: The management agent is separated from its network management station by a router

The network management station “Romeo” wants to send data to the management agent “Juliet”. Romeo knows Juliet's IPv4 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 IPv4 address as the destination address; for the source address he writes his own IPv4 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 IPv4 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 IPv4 address as destination and her own IPv4 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 `hmabbNetGatewayIPAddr` as a means of communicating with Romeo. She therefore puts the envelope with the IPv4 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 specify the number of bits that designate the IPv4 address range. You represent the IPv4 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 IPv4 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 combining a number of class C address ranges. Supernetting lets you subdivide class B address ranges to a fine degree.

2.2 Specifying the IP parameters using the Command Line Interface

2.2.1 IPv4

There are following methods to enter the IP parameters:
- HiDiscovery protocol
- *Dynamic Host Configuration Protocol (DHCP)*

The device lets you specify the IP parameters using the HiDiscovery protocol.

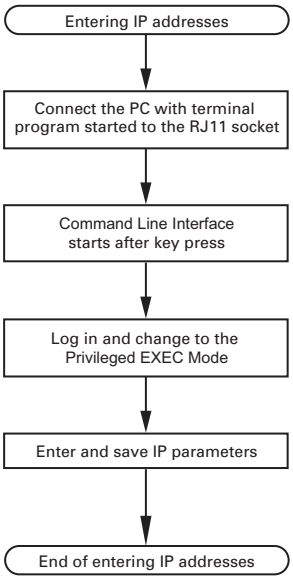
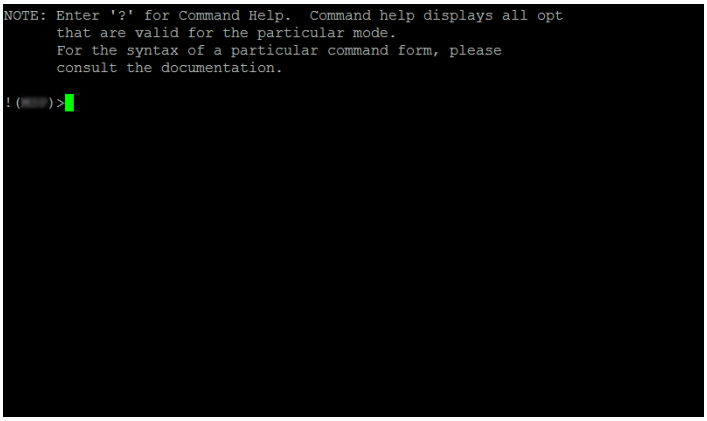


Figure 6: Flow chart for entering IPv4 addresses

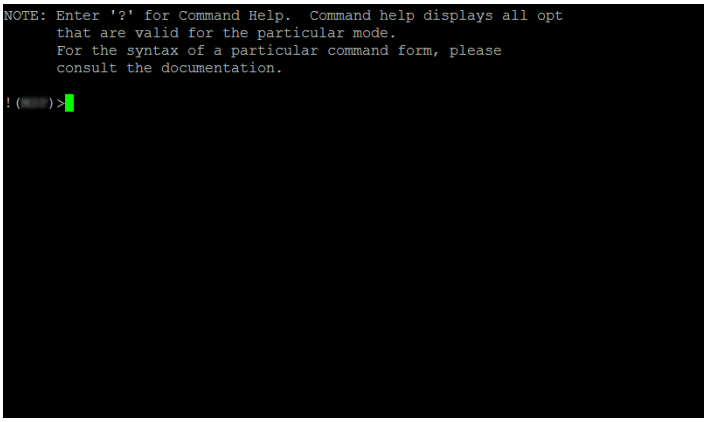
Note: If a terminal or PC with terminal emulation is unavailable in the vicinity of the installation location, you can configure the device at your own workstation, then take it to its final installation location.

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



☐ Enter the IP parameters.
- ▶ Local IPv4 address
  In the default setting, for the interface VLAN 1 the IPv4 address is configured using DHCP, and for the other interface VLANs, no IPv4 address is specified.
- ▶ Netmask
  When you divided your network into subnetworks, and these are identified with a netmask, enter the netmask here.
- ▶ IPv4 address of the Gateway.
  This entry is only required, in cases where the device and the network management station or *Trivial File Transfer Protocol (TFTP)* server are located in different subnetworks (see on page 21 “Example of how the netmask is used”).
  This entry is only required, in cases where the device and the network management station are located in different subnetworks (see on page 21 “Example of how the netmask is used”).
  Specify the IPv4 address of the Gateway between the subnetwork with the device and the path to the network management station.
  In the default setting, no IPv4 address is specified.

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



`configure terminal`	To change to the Configuration mode from the Privileged Exec mode.
`interface vlan 1`	To enter the management VLAN interface mode.
`ip address 10.0.1.23 255.255.255.0`	To assign the device the IPv4 address `10.0.1.23` and the netmask `255.255.255.0`.
`do copy running-config startup-config`	To save the configuration specified.
`end`	To return to the Privileged Exec mode.

☐ Specifying a Gateway address

`configure terminal`	To change to the Configuration mode from the Privileged Exec mode.
`ip route default 10.0.1.23`	To specify the Gateway address `10.0.1.23`.
`do copy running-config startup-config`	To save the configuration specified.
`end`	To return to the Privileged Exec mode.

After entering the IP parameters, you easily configure the device using the Graphical User Interface, see “Specifying the IP parameters using the Graphical User Interface” on page 26.

2.3 Specifying the IP parameters using Provize Explorer

The Provize Explorer application lets you assign IP parameters to the device using the Ethernet.

You easily configure other parameters using the Graphical User Interface.

Perform the following steps:
- ☐ Install the Provize Explorer application on your computer.
  You can download the application from https://www.belden.com/get-ProvizeExplorer.
- ☐ Start the Provize Explorer application.

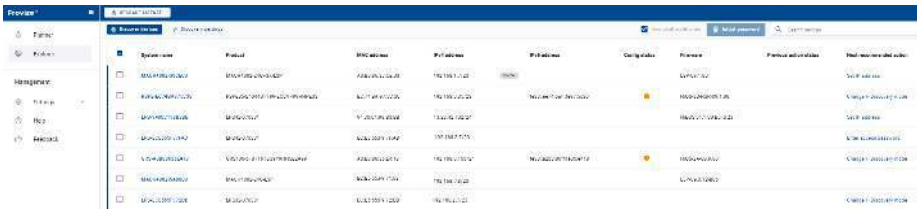


Figure 7: Provize Explorer

After you started the Provize Explorer application, click the *Discover devices* button to search the network for those devices which support the HiDiscovery protocol.

The Provize Explorer application uses the first network interface found on the PC. When your computer has multiple network interfaces, click the *Discovery settings* button and select the desired network interface.

The Provize Explorer application displays a line for every device that responds to a HiDiscovery protocol inquiry.

The Provize Explorer application lets you identify the devices displayed.
- ☐ Select a device line.
- ☐ To set the LEDs to flashing for the selected device, click the *Start signal* button on the side pane.
  To stop the flashing, click the *Stop signal* button.
- ☐ Specify the device IP parameters in the *IP address* field on the side pane.

Figure 8: Assigning IP parameters using the Provize Explorer application

Note: Disable the HiDiscovery 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

In the following example, you specify the IPv4 parameters on the device.

Perform the following steps:

- ☐ Open the *Basic Settings > Network > Global* dialog.
- ☐ In the *Management interface* frame, *IPv4 address assignment* field, select the `DHCP` radio button.
  When you change the IPv4 address assignment, the device activates the new setting immediately after you click the ✓ button.
- ☐ If you have selected the `Local` radio button, then specify the values in the required fields of the *Management IP parameter* frame using the further example steps.
- ☐ In the *IPv4 address* field, specify the value `10.192.113.73`
- ☐ In the *Prefix size* field, specify the value `24`.
- ☐ In the *Gateway address* field, specify the value `10.192.113.1`
- ☐ Apply the settings temporarily. To do this, click the ✓ button.

2.5 Specifying the IP parameters using DHCP

2.5.1 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 in the *Basic Settings > System* dialog under *Transmit system name* 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 IPv4 address as an alternative to the MAC address.

In addition to the IPv4 address, the DHCP server sends
- the netmask
- the default Gateway (if available)
- the TFTP URL of the configuration file (if available).

Table 3: 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*

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 IPv4 address based on a unique hardware ID (known as static address allocation).

In the default setting, DHCP is activated. As long as DHCP is active, the device attempts to obtain an IPv4 address. When the device cannot find a DHCP server after restarting, it will not have an IPv4 address. The dialog lets you activate or deactivate DHCP.

Note: When using Industrial HiVision network management, verify that DHCP allocates the original IPv4 address to every device.

The appendix contains an example configuration of the 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 IPv4 address to the device.

It is the responsibility of the network administrator to set up the required settings on the DHCP server to get the desired IPv4 address assigned to the device.

2.6 Adding a VLAN interface

The prerequisite is that the VLAN 11 is also created. See “Adding a VLAN” on page 105.

In the following example you set up a new VLAN interface 11.

Perform the following steps:

- ☐ Open the *IPv4* dialog.
  The dialog displays the table below the *Management IP parameter* frame.
- ☐ Click the button.
  The dialog displays the *Create* window.
- ☐ In the *VLAN ID* field, enter the value `11`.
- ☐ Click the *Ok* button.
  The table displays the VLAN 11 in a table row.
- ☐ To activate the VLAN, in the table row for the VLAN 11, mark the checkbox in the *Active* column.
  The device enables the *MTU*, *IPv4 address*, *Prefix size*, and the *DHCP client enable* columns.
- ☐ In the *IPv4 address* field, enter the value `222.2.2.20`
- ☐ In the *Prefix size* field, enter the value `26`
- ☐ To activate the *DHCP* client function, in the *DHCP client enable* column, mark the checkbox.
  The device enables the *DHCP fallback timeout [s]*, *DHCP host name*, and the *DHCP ID type* columns.
- ☐ In the *DHCP fallback timeout [s]* column, enter the value `100`.
- ☐ In the *DHCP host name* column, enter the value `test.com`.
- ☐ In the *DHCP ID type* column, select the value item *`If MAC`* from the drop-down list.
  When the *DHCP ID type* column contains the value item *`auto`*, then the device does not allow specifying the values in the *DHCP ID if MAC*, *DHCP ID ASCII*, and *DHCP ID hex* columns.
- ☐ In the *DHCP ID if MAC* column, select the value item `Gi 1/1` from the drop-down list.
  or
  if you select the value item *`ASCII`*, then in the *DHCP ID ASCII* column, enter the value `trial`.
  or
  if you select the value item *`hex`*, then in the *DHCP ID hex* column, enter the value`1d`.
- ☐ Apply the settings temporarily. To do this, click the ✓ button.

```
configure terminal
```

To change to the Configuration mode from the Privileged Exec mode.

```
interface vlan 11
```

To specify the VLAN `11`.

```
ip address dhcp client-id
GigabitEthernet 1/1 fallback 222.2.2.20
255.255.255.192 timeout 100 hostname
test.com
```

To activate the VLAN 11, enable the *DHCP* client function, with the following settings:

- *DHCP* fallback timeout `100`
- *DHCP* host name `test.com`
- *DHCP* ID type value `if MAC`
- *DHCP* ID If MAC value `GigabitEthernet 1/1`
- IPv4 address value `222.2.2.20`
- Net mask value `255.255.255.192`

`ip address dhcp client-id ascii trial fallback 222.2.2.20 255.255.255.192 timeout 100 hostname test.com`	To activate the VLAN 11, enable the *DHCP* client function, and specify the *DHCP* parameters with the following settings: • *DHCP* ID type value `ascii` • *DHCP* ID ASCII value `trial` • *DHCP* fallback timeout `100` • *DHCP* host name `test.com` • IPv4 address value `222.2.2.20` • Net mask value `255.255.255.192`
`ip address dhcp client-id hex 1d fallback 222.2.2.20 255.255.255.192 timeout 100 hostname test.com`	To activate the VLAN 11, enable the *DHCP* client function, and specify the *DHCP* parameters with the following settings: • *DHCP* ID type value `hex` • *DHCP* ID ASCII value `1d` • *DHCP* fallback timeout `100` • *DHCP* host name `test.com` • IPv4 address value `222.2.2.20` • Net mask value `255.255.255.192`
`no ip address`	To disable the *DHCP* client function.
`no interface vlan 11`	To deactivate the interface VLAN `11`.
`end`	To return to the Privileged Exec mode.

2.7 Restarting the DHCP client function

The device allows you to restart the *DHCP* client function for a selected interface VLAN. In the following example you restart the *DHCP* client function for the interface VLAN 11.

Perform the following steps:

- ☐ Open the *IPv4* dialog, *IPv4 address* tab.
  The tab displays the interface VLAN 11 in a table row.
- ☐ In the table row for the VLAN 11, mark the checkbox in the first column.
- ☐ Click the *Client restart* button.

`configure terminal`	To change to the Configuration mode from the Privileged Exec mode.
`interface vlan 11`	To switch to the interface VLAN `11`.
`ip address dhcp`	To restart the *DHCP* client function.
`end`	To return to the Privileged Exec mode.

2.8 Clearing the system logs

The device lets you clear the system logs as per their severity level or every generated log together. In the following example, you clear the system logs which were generated with the severity level *error*.

Perform the following steps:

- ☐ Open the *System Log* dialog.
  The dialog displays the system logs in the table below the *System information* frame.
- ☐ Click the ☰ menu button.
  The menu button displays the value items to clear the system logs.
- ☐ Select the value item *Clear error*.
  The device clears only the error logs.

`show logging`	To display every system log generated by the device.
`clear logging error`	To clear only the error logs from the device.
`clear logging`	To clear every log from the device.

3 Access to the device

The device lets you set up the following configurations to access the device:

- Force password change (FPC)
- User management
- Authentication List
- SNMP access

3.1 Force password change (FPC)

During the first login to the new device, after a factory reset, and after you run the command `clear config`, you bring the device to an operational state. To do this, you need to change the default password of the default administrator account. Until then, the device only has limited availability to the network:

- The protocols *Telnet*, *Hypertext Transfer Protocol (HTTP)*, and *Simple Network Management Protocol (SNMP)* are disabled on the device, by default. After you have changed the default password, enable the needed protocols.
- The Provize Explorer application lets you change the default password using the protocols *Secure Shell (SSH)* or *Hypertext Transfer Protocol Secure (HTTPS)*.

Hirschmann recommends to set a password that is different from the default password.

Perform the following steps:

- ☐ Open the Graphical User Interface (GUI), the application Provize Explorer or the Command Line Interface (CLI) of the device.
- ☐ Log in with the default user name and the default password.
  On successful login, the device prompts you to type in a new password.
- ☐ Type in your new password.
  The device displays an error when the new password you entered is not in the range of 6..31 characters.
- ☐ Confirm the new password.
  The device displays an error when the new password and the confirm new password do not match.
- ☐ On successful password change, log in again with your new password.
  On successful login with your new password, you get access to the device.

Note: The password change requirement is to comply with the California Senate Bill 327.

For further information, see hirschmann-support.belden.com.

3.2 User management

When a user with privilege level 15 logs in to the device, then the device lets the user have access to the device management. The device authenticates the users using the configured authentication method.

In the local user management, a user with the privilege level 15 manages the user accounts. One user account is allocated to each user.

3.2.1 Privilege levels

The device lets you use a privilege-level based authorization model to specifically control the access to the device management. Users to whom a specific privilege level is assigned are allowed to use commands and functions from the same privilege level or a lower one.

The device uses the privilege level when a user accesses the device management using the Graphical User Interface or Command Line Interface.

Every user account is assigned a privilege level that controls the access to the individual functions of the device. Depending on the planned activity for the respective user account, you assign a privilege level to the user account. The device differentiates between the following privilege levels:

Table 4: Privilege levels for user accounts

Privilege level	Description	Authorizes the user for the following activities
15 (Administrator)	The user is authorized to monitor and administer the device.	Every activity 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. ▶ Set up password management. ▶ Set or change system time. ▶ Load files to the device, for example device configurations, certificates, or software images. ▶ Reset the device settings and counters. ▶ Enable/disable the services for the access to the device management (for example *HTTP, SSH, and Telnet*). ▶ Set up access restrictions to the Graphical User Interface or the Command Line Interface based on the IPv4 addresses.

Table 4: Privilege levels for user accounts (cont.)

Privilege level	Description	Authorizes the user for the following activities
2..14 (Guest)	The user is authorized to monitor the device except for security-related settings.	Monitoring activities with read access.
1 (CLI guest)	The user is authorized to access the device only using the Command Line Interface in the Enable mode. The Enable mode lets the CLI Guest access the limited read-only commands.	Activities are limited to read access. Upgrade to higher privilege level using the *Enable Secret*. See Modifying the privilege level during an active login session.
0 (Unauthorized)	No access to the device possible. ▶ As an administrator, you assign this privilege level to temporarily lock a user account.	No activities allowed.

3.2.2 Managing user accounts

With an assigned privilege level 15, you manage the user accounts using the Graphical User Interface or Command Line Interface.

Perform the following steps:

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

The dialog displays the user accounts that are set up in the device.

`show user-privilege` — To display the user accounts that are set up in the device.

Default setting

In the state of delivery, the device displays the `admin` user account.

Table 5: Default settings for the factory setting user accounts

Parameter	Default setting
Username	`admin`
Password	`private`

To change the default password, see “Force password change (FPC)” on page 33.

Setting up a new user account

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

The user with privilege level 15 sets up a new user account in the device.

In the following example, we set up a user account Test1 with the privilege level 10 so that the user gets read-only access to perform the monitoring activities.

Perform the following steps:

- ☐ Open the *Device Security > User Management* dialog.
- ☐ Click the button.
  The dialog displays the *Create* window.
- ☐ In the *Username* field, enter the user name `Test1`.
- ☐ In the *Password* field, enter the password `Safety1`.
  - ▶ The device differentiates between an upper case and a lower case character.
  - ▶ The device validates the minimum length of the entered password.
- ☐ In the *Privilege* field, specify `10`.
- ☐ Click the *Ok* button.
- ☐ Apply the settings temporarily. To do this, click the ✓ button.
  The dialog displays the user account in the table row.

`configure terminal`	To change to the Configuration mode from the Privileged Exec mode.
`username Test1 privilege 10 password unencrypted Safety1`	To set up the user Test1 with the privilege level 10 and the password Safety1.
`do copy running-config startup-config`	To save the settings on the device.
`end`	To return to the Privileged Exec mode.

Removing an existing user account

When you remove a user account, the device denies the related user access to the device management.

The user with privilege level 15 can remove a user account from the device except the default `admin` account.

In the following example, we delete the user account Test1.

Perform the following steps:

- ☐ Open the *Device Security > User Management* dialog.
  The dialog displays the user accounts that are set up in the device.

- ☐ In the first column of the table row for the user account `Test1`, mark the checkbox.
- ☐ Click the button.
- ☐ Apply the settings temporarily. To do this, click the ✓ button.

`configure terminal`	To change to the Configuration mode from the Privileged Exec mode.
`no username Test1`	To delete the user account Test1.
`do copy running-config startup-config`	To save the setting on the device.
`end`	To return to the Privileged Exec mode.

Setting up the Enable secret for a specific privilege level

The Enable secret of a specific privilege level lets the user with the privilege level 1..14 get the authorization access of a higher privilege level.

The user with the privilege level 15 sets up the Enable secret for a specific privilege level between 1..15, only using the Command Line Interface.

In the following example, we set up the Enable secret for the privilege level 15.

Perform the following steps:

`configure terminal`	To change to the Configuration mode from the Privileged Exec mode.
`enable secret 0 level 15 covert1`	To set up the unencrypted Enable secret `covert1` for the privilege level 15. You use the number `0` after the command `secret` to set up the password using an unencrypted input method.
`enable secret 5 level 10 DEA6EB2A236CC41C64AA562B8CC44A07`	To set up the encrypted Enable secret `DEA6EB2A236CC41C64AA562B8CC44A07` (`covert5`) for the privilege level 10. You use the number `5` after the command `secret` to set up the password using an encrypted input method.
`do copy running-config startup-config`	To save the setting on the device.
`end`	To return to the Privileged Exec mode.

Modifying the privilege level during an active login session

The users with the privilege level 1..14 can upgrade their user accounts to a higher privilege level using the Enable secret during an active login session. For the Enable secret, see “Setting up the Enable secret for a specific privilege level” on page 37.

On successful login to the device using the Command Line Interface, the CLI guest users get access to the Enable mode and the Guest users get access to the Privileged Exec mode.

In the following example, we upgrade the privilege level of the user Test2 from 1 to 15.

Perform the following steps:

```
enable 15
```

To upgrade the user account Test2 from the privilege level 1 to the privilege level 15.

The device prompts to enter the Enable secret `covert1` of the privilege level 15. On entering the correct Enable secret, the user Test2 gets authorization access of the privilege level 15.

The device does not prompt to enter the Enable secret when you downgrade the privilege level. Because the user is already at a higher privilege level. In the following example, we downgrade the privilege level of the user Test2 from 15 to 2.

Perform the following steps:

```
disable 2
```

To downgrade the user account Test2 from the privilege level 15 to 2.

Now, when the user Test2 again wants to upgrade to the privilege level 10 from the existing privilege level 2, then the user needs to enter the Enable secret of the privilege level 10. See the following example configuration.

Perform the following steps:

```
enable 10
```

To upgrade the user account Test2 from the privilege level 2 to 10.

The device prompts to enter the Enable secret `covert5` of the privilege level 10. On entering the correct Enable secret, the user Test2 gets authorization access of the privilege level 10.

3.3 Authentication List

[Device Security > Authentication List]

When a user accesses the device using a specific connection, the device verifies the login credentials to validate the user. If a user logs in with valid login credentials, then the device lets the user have access to its device management.

[Applications]

The device provides an application for each type of connection through which someone accesses the device:

- Access to the Command Line Interface using SSH: `SSH`
- Access to the Command Line Interface using Telnet: `Telnet`
- Access to the Graphical User Interface: `HTTP`

[Configuring the authentication]

Perform the following steps:

- ☐ Open the *Device Security > Authentication List* dialog.
- ☐ In the *Configuration* frame, select the desired login method type from the *Policy* drop-down list for the relevant connection type.
  - If the item *local* is selected, then the device verifies the login credentials stored within the device to validate the user.
  - If the item *reject* is selected, then the device disables the login.
- ☐ Apply the settings temporarily. To do this, click the ✓ button.

`configure terminal`	To change to the Configuration mode from the Privileged Exec mode.
`aaa authentication login telnet local`	To verify the `telnet` connection login credentials using the local database.
`aaa authentication login ssh local`	To verify the `ssh` connection login credentials using the local database.
`aaa authentication login http local`	To verify the `http` connection login credentials using the local database.
`exit`	To return to the Privileged Exec mode.

Note: The `Telnet` and `HTTP` connections make the device unsecure. In the default setting, the `Telnet` and `HTTP` connections are disabled.

3.4 SNMP access

Simple Network Management Protocol (SNMP) is the protocol that lets you collect and organize information about the managed devices on IP networks and modify that information to change the device behavior.

This dialog contains the following example configuration:

- Enabling the SNMP
- Configuring the Engine ID
- Adding/removing an SNMP community v1/v2
- Adding/removing an SNMP v3 User
- Adding/removing an SNMP Group
- Adding/removing an SNMP view
- Adding/removing an SNMP access
- Adding/removing an SNMP source trap
- Adding/removing an SNMP v1/v2 receiver trap
- Adding/removing an SNMP v3 Receiver trap

3.4.1 Enabling the SNMP

Perform the following steps:

- ☐ Open the *Device Security > SNMP > Configuration* dialog.
  The dialog displays the *Global* frame.
- ☐ Enable the SNMP. To do this, in the *Global* frame, *Mode* field, select the *On* radio button.
- ☐ Apply the settings temporarily. To do this, click the ✓ button.

`configure terminal`	To change to the Configuration mode from the Privileged Exec mode.
`snmp-server`	To enable the SNMP.
`no snmp-server`	To disable the SNMP.
`end`	To return to the Privileged Exec mode.

3.4.2 Configuring the Engine ID

Perform the following steps:

- ☐ Open the *Device Security > SNMP > Configuration* dialog.
  The dialog displays the *Global* frame.
- ☐ In the *Engine ID* field, specify the local engine ID `800000f8030200c1f6ddda`.
- ☐ Apply the settings temporarily. To do this, click the ✓ button.

`configure terminal`	To change to the Configuration mode from the Privileged Exec mode.
`snmp-server engine-id local 800000f8030200c1f6ddda`	To specify the local engine ID 800000f8030200c1f6ddda.
`end`	To return to the Privileged Exec mode.

3.4.3 Adding/removing an SNMP community v1/v2

In the following example, you create a new community `Test1` on the device.
☐ Perform the following steps:

- ☐ Open the *Device Security > SNMP > Configuration* dialog, *Community v1/v2* tab.
- ☐ Click the  button.
  The dialog displays the *Create* window.
- ☐ In the *Community name* field, enter the name `Test1`.
- ☐ In the *Source IP range* field, enter the IPv4 address `192.168.1.10`.
- ☐ In the *Prefix* field, enter the value `32`.
- ☐ In the *Community secret* field, enter the password `Test123`.
- ☐ Click the *Ok* button.
- ☐ Apply the settings temporarily. To do this, click the ✓ button.

`configure terminal`	To change to the Configuration mode from the Privileged Exec mode.
`snmp-server community Test1 ip-range 192.168.1.10 255.255.255.255 Test123`	To add the community `Test1` with the IP range 192.168.1.10, netmask 255.255.255.255, and the community secret Test123.
`no snmp-server community Test1 ip-range 192.168.1.10 255.255.255.255`	To remove the community `Test1`, which was added with the IPv4 address 192.168.1.10 and the netmask 255.255.255.255.
`snmp-server community Test1 ip-range 192.168.1.10 255.255.255.255 encrypted 5513b57e8619b4bfc275a514c2d036c98fb1b46c2d5cedbea4c937c9b16795e0dfb0e6f3234dc724b5e60ffa8af89fe48610f567f68729253d06b142e298d6f7`	To add the community `Test1` with the IPv4 address 192.168.1.10, netmask 255.255.255.255, and the encrypted community secret for the Test123.
`end`	To return to the Privileged Exec mode.
`show snmp community`	To display the SNMP community v1/v2 currently added on the device.

3.4.4 Adding/removing an SNMP v3 User

In the following example, you add a new SNMP v3 user `Test2` on the device.
☐ Perform the following steps:

- ☐ Open the *Device Security > SNMP > Configuration* dialog, *User* tab.
- ☐ Click the button.
  The dialog displays the *Create* window.
- ☐ In the *Username* field, enter the name `Test2`.
- ☐ In the *Engine ID* field, specify the value `800000f8030200c14d3039`.
- ☐ Click the *On* button.
  The table displays the added user `Test2` in a table row.
- ☐ In the *Security level* column, select the value item *`auth priv`* from the drop-down list.
- ☐ In the *Auth protocol* column, select the value item *`MD5`* from the drop-down list.
- ☐ In the *Auth password* column, specify the value `safety123`.
- ☐ In the *Priv protocol* column, select the value item *`DES`* from the drop-down list.
- ☐ In the *Priv password* column, specify the value `safety123`.
- ☐ Apply the settings temporarily. To do this, click the ✓ button.

`configure terminal`	To change to the Configuration mode from the Privileged Exec mode.
`snmp-server user Test2 engine-id 800000f8030200c14d3039 md5 safety123 priv des safety123`	To add the new SNMP v3 user `Test2` with the engine ID 800000f8030200c14d3039, auth protocol md5 with the password `safety123`, priv protocol DES with the password `safety123`.
`no snmp-server user Test2 engine-id 800000f8030200c14d3039`	To remove the SNMP v3 user `Test2`, which was added using the engine ID 800000f8030200c14d3039.
`end`	To return to the Privileged Exec mode.
`show snmp user`	To display the SNMP v3 users currently added on the device.

3.4.5 Adding/removing an SNMP Group

In the following example, you add a new SNMP v1 group `Test1_group` on the device.
☐ Perform the following steps:

- ☐ Open the *Device Security > SNMP > Configuration* dialog, *Group* tab.
- ☐ Click the button.
  The dialog displays the *Create* window.
- ☐ In the *Group name* field, enter the name `Test1_group`.
- ☐ In the *VLAN ID* field, select the value item `Test1` from the drop-down list.

- ☐ In the *Security model* field, select the value item `v1` from the drop-down list.
- ☐ Click the *Ok* button.
- ☐ Apply the settings temporarily. To do this, click the ✓ button.

`configure terminal`	To change to the Configuration mode from the Privileged Exec mode.
`snmp-server security-to-group model v1 name Test1 group Test1_group`	To add the new group `Test1_group` with the community `Test1` and the security model v1.
`no snmp-server security-to-group model v1 name Test1 group Test1_group`	To remove the group `Test1_group` that was added with the community Test1 and the security model v1.
`end`	To return to the Privileged Exec mode.
`show snmp security-to-group`	To display the SNMP groups currently added on the device.

3.4.6 Adding/removing an SNMP view

In the following example you add a new SNMP view `Test4_view` on the device.
☐ Perform the following steps:

- ☐ Open the *Device Security > SNMP > Configuration* dialog, *View* tab.
- ☐ Click the ⊞ button.
  The dialog displays the *Create* window.
- ☐ In the *Name* field, enter the name `Test4_view`.
- ☐ In the *Sub tree* field, enter the object identifier (OID) value `.1`.
- ☐ Click the *Ok* button.
  The device displays the created view Test4_view in a table row.
- ☐ In the table row of the view `Test4_view`, in the *View type* field, select the value item `excluded` from the drop-down list.
- ☐ Apply the settings temporarily. To do this, click the ✓ button.

`configure terminal`	To change to the Configuration mode from the Privileged Exec mode.
`snmp-server view Test4_view .1 exclude`	To add the new SNMP view `Test4_view` with the sub tree `.1` and the view type as `exclude`.
`no snmp-server view test4_view .1`	To remove the SNMP view `Test4_view` which was added with the sub tree `.1`.
`end`	To return to the Privileged Exec mode.
`show snmp view`	To display the SNMP views currently added on the device.

3.4.7 Adding/removing an SNMP access

The prerequisite is to create the following set up first:
- Create at least 1 SNMP group, see Adding/removing an SNMP Group.
- The required view is configured on the device, see *Device Security > SNMP > Configuration* dialog, *View* tab.

In the following example you add the SNMP access for the SNMP v1 group `Test1_group` using the read view `Test4_view` and the write view `Test4_view`.
☐ Perform the following steps:

- ☐ Open the *Device Security > SNMP > Configuration* dialog, *Access* tab.
- ☐ Click the button.
  The dialog displays the *Create* window.
- ☐ In the *Group name* field, select the value item `Test1_group` from the drop-down list.
- ☐ In the *Security model* field, select the value item *v1* from the drop-down list.
- ☐ In the *Security level* field, select the value item *no auth no priv* from the drop-down list.
- ☐ In the *Read view* field, select the value item `Test4_view` from the drop-down list.
- ☐ Click the *Ok* button.
  The tab displays the created group `Test1_group` in a table row.
- ☐ In the *Write view* column, select the value item `Test4_view` from the drop-down list.
- ☐ Apply the settings temporarily. To do this, click the ✓ button.

`configure terminal`	To change to the Configuration mode from the Privileged Exec mode.
`snmp-server access Test1_group model v1 read Test4_view write Test4_view`	To add the SNMP access for the group `Test1_group` with the security model v1, the read view `Test4_view` and the write view Test4_view.
`no snmp-server access Test1_group model v1`	To remove the access added for the group `Test1_group`.
`end`	To return to the Privileged Exec mode.
`show snmp access`	To display the SNMP access currently granted to the SNMP groups on the device.

3.4.8 Adding/removing an SNMP source trap

In the following example you add the source trap *Rising alarm* on the device.
☐ Perform the following steps:

- ☐ Open the *Device Security > SNMP > Trap* dialog, *Source trap* tab.
- ☐ Click the button.
  The dialog displays the *Create* window.
- ☐ In the *Name* field, select the value item *Rising alarm* from the drop-down list.
- ☐ Click the *Ok* button.
  The tab displays the created source trap *Rising alarm* in a table row.

- ☐ In the *Index filter* field, enter the value `.1000001` to select the trap updates for the interface GigabitEthernet 1/1.
- ☐ In the *Filter type* column, select the value item `excluded` from the drop-down list.
- ☐ Apply the settings temporarily. To do this, click the ✓ button.

`configure terminal`	To change to the Configuration mode from the Privileged Exec mode.
`snmp-server trap risingAlarm .1000001 exclude`	To add the SNMP source trap Rising alarm with the index filter OID `.1000001` to select the trap updates for the `interface GigabitEthernet 1/1`, and the filter type `exclude`.
`no snmp-server trap risingAlarm`	To remove the SNMP source trap Rising alarm.
`end`	To return to the Privileged Exec mode.
`show snmp trap`	To display the SNMP source traps added on the device.

3.4.9 Adding/removing an SNMP v1/v2 receiver trap

In the following example you add an SNMPv1 receiver trap `Receiver1` on the device. Following steps are applicable for adding/removing an SNMP v2 receiver trap as well.

☐ Perform the following steps:

- ☐ Open the *Device Security > SNMP > Trap* dialog, *Receiver trap* tab.
- ☐ Click the button.
  The dialog displays the *Create* window.
- ☐ In the *Name* field, enter the name `Receiver1`.
- ☐ Click the *Ok* button.
  The tab displays the created trap `Receiver1` in a table row.
- ☐ Enable the trap. To do this, in the *Enable* column, mark the checkbox.
- ☐ In the *Address* field, enter the value `192.168.1.10`.
- ☐ In the *Port* field, enter the value `3162`.
- ☐ In the *Version* field, select the value item `v1` from the drop-down list.
- ☐ In the *Community* field, enter the value `com1`.
- ☐ In the *Notify type* field, select the value item `trap` from the drop-down list.
- ☐ Apply the settings temporarily. To do this, click the ✓ button.

`configure terminal`	To change to the Configuration mode from the Privileged Exec mode.
`snmp-server host Receiver1`	To add the SNMP receiver trap `Receiver1`.
`no snmp-server host Receiver1`	To remove the SNMP receiver trap `Receiver1`.
`host 192.168.1.10 3162 traps`	To specify the host IPv4 address 192.168.1.10, host port number 3162, and the notify type `trap`.

`version v1 com1`	To specify the SNMP version v1, and the community name `com1`.
`end`	To return to the Privileged Exec mode.
`show snmp host`	To display the SNMP receiver traps added on the device.

3.4.10 Adding/removing an SNMP v3 Receiver trap

In the following example you add an SNMP v3 receiver trap `Receive3` on the device.
☐ Perform the following steps:

- ☐ Open the *Device Security > SNMP > Trap* dialog, *Receiver trap* tab.
- ☐ Click the button.
  The dialog displays the *Create* window.
- ☐ In the *Name* field, enter the name `Receiver3`.
- ☐ Click the *Ok* button.
  The tab displays the created trap `Receiver3` in a table row.
- ☐ Enable the trap. To do this, in the *Enable* column, mark the checkbox.
- ☐ In the *Address* field, enter the value `10.192.113.53`.
- ☐ In the *Port* field, enter the value `163`.
- ☐ In the *Version* field, select the value item *v3* from the drop-down list.
- ☐ In the *Engine ID* field, enter the value `800000f8030200c14d3039`.
- ☐ In the *Username* field, enter the value `abc`.
- ☐ In the *Notify type* field, select the value item *inform* from the drop-down list.
- ☐ In the *Timeout* field, specify the value `7`.
- ☐ In the *Retries* field, specify the value `7`.
- ☐ Apply the settings temporarily. To do this, click the ✓ button.

`configure terminal`	To change to the Configuration mode from the Privileged Exec mode.
`snmp-server host receiver3`	To add the SNMP receiver trap `receiver3`.
`no snmp-server host receiver3`	To remove the SNMP receiver trap `receiver3`.
`no shutdown`	To enable this trap set up.
`host 10.192.113.53 163 informs`	To specify the IPv4 address 10.192.113.53, host port number 163, and the notify type `informs`.
`informs retries 7 timeout 7`	To specify the retries value 7 and the timeout value 7.
`version v3 engineID 800000f8030200c14d3039 abc`	To specify the SNMP version v3, engine ID 800000f8030200c14d3039 and the user name `abc`.
`end`	To return to the Privileged Exec mode.

4 Synchronizing the system time in the network

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

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

The device synchronizes the time using the Network Time Protocol version 4.

This chapter describes the working steps to set up the following features:
- Basic Settings
- NTPv4 Client

4.1 Basic Settings

4.1.1 Setting the time

When there is no reference time source available to you, you can manually apply your computer time to the *System time*, and set the *System timezone offset [min]* in the device. As an alternative, you specify the *System time* using the command line interface.

After a restart, the device initializes the clock with January 1 2024, 00:00.

Perform the following steps:

- ☐ Open the *Time > Basic Settings* dialog, *Global* tab.
  The *System time* field displays the current date and time.
- ☐ To make the device apply the time of your computer to the *System time* field, click the *Set time from PC* button.
- ☐ To specify the *System timezone offset [min]*, in the *System timezone offset [min]* field, specify the value `50`.
- ☐ Apply the settings temporarily. To do this, click the ✓ button.

`configure terminal`	To change to the Configuration mode from the Privileged EXEC mode.
`clock timezone test 00 50 0`	To specify the *System timezone offset [min]* value `50`.
`clock set 2023/03/31 17:50:23`	To specify the *System time* value `2023/03/31 17:50:23`.
`end`	To return to the Privileged Exec mode.

4.1.2 Automatic daylight saving time changeover

When you operate the device in a time zone with a summertime change, the device lets you set up the automatic daylight saving time changeover.

If the *Daylight saving time* mode is enabled, the device advances the standard time by the value contained in the *Daylight saving time offset [min]* field at the start of the summertime. At the end of summertime, the device restores the standard time.

Setting the recurring mode

Enabling this mode requires that the Month, Week, and Day parameters of the *Summertime begin* and *Summertime end* frames contain the valid values (`<apart from none>`). The parameters Year and Date are not used in this mode.

The network administrator wants to specify the following daylight saving time settings:

Configuration
- *Timezone Acronym* = `TestStart`
- *Daylight saving time offset [min]* = `60`

Summertime begin
- *Week* = `last`
- *Day* = `Sunday`
- *Month* = `March`
- *Time* = `02:00`

Summertime end
- *Week* = `last`
- *Day* = `Sunday`
- *Month* = `October`
- *Time* = `03:00`

For the purpose described above, perform the following steps:

- ☐ Open the *Time > Basic Settings* dialog, *Daylight saving time* tab.
- ☐ Enable the *Recurring* mode. To do this, in the *Operation* frame, select the *`Recurring`* radio button.
- ☐ Specify the *Timezone Acronym*. To do this, in the *Configuration* frame, *Timezone Acronym* field, enter the value `TestStart`.
- ☐ Specify the *Daylight saving time offset [min]*. To do this, in the *Configuration* frame, *Daylight saving time offset [min]* field, enter the value `60`.
- ☐ In the *Summertime begin* frame, specify the following settings:
  - *Week* = *`first`*
  - *Day* = *`Sunday`*
  - *Month* = *`March`*
  - *Time* = `02:00`
- ☐ In the *Summertime end* frame, specify the following settings:
  - *Week* = *`first`*
  - *Day* = *`Sunday`*
  - *Month* = *`October`*
  - *Time* = `03:00`
- ☐ Apply the settings temporarily. To do this, click the ✓ button.

`configure terminal`	To change to the Configuration mode from the Privileged EXEC mode.
`clock summer-time TestStart recurring 1 7 3 02:00 1 7 10 03:00 60`	To specify the *Timezone Acronym* value `TestStart`. To specify the time at which the device sets the clock forward from standard to summertime. • `1` To specify the *first* week of the month. • `7` To specify the day *Sunday*. • `3` To specify the month *March*. • `02:00` To specify the time `02:00 AM`. To specify the time at which the device resets the clock from summertime to standard time. • `1` To specify the *first* week of the month. • `7` To specify the day *Sunday*. • `10` To specify the month *October*. • `03:00` To specify the time `03:00 AM`. To specify the *Daylight saving time offset [min]* value `60`.
`do show clock detail`	To display the *Daylight saving time* settings.
`end`	To return to the Privileged EXEC mode.

Setting the non-recurring mode

Enabling this mode requires that the Year, Month, and Date parameters of the *Summertime begin* and *Summertime end* frames contain the valid values (`<apart from none>`). The parameters Week and Day are not used in this mode.

The network administrator wants to specify the following daylight saving time settings:

Configuration
- *Timezone Acronym* = `NonRe`
- *Daylight saving time offset [min]* = `50`

Summertime begin
- *Date* = `Saturday, April 1, 2023`
- *Time* = `04:00 AM`

Summertime end
- *Date* = `Saturday, September 30, 2023`
- *Time* = `05:00 AM`

For the purpose described above, perform the following steps:

- ☐ Open the *Time > Basic Settings* dialog, *Daylight saving time* tab.
- ☐ Enable the *Non-recurring* mode. To do this, in the *Operation* frame, select the *Non-recurring* radio button.
- ☐ Specify the *Timezone Acronym*. To do this, in the *Configuration* frame, *Timezone Acronym* field, enter the value `NonRe`.
- ☐ Specify the *Daylight saving time offset [min]*. To do this, in the *Configuration* frame, *Daylight saving time offset [min]* field, enter the value `50`.
- ☐ In the *Summertime begin* frame, specify the following settings:
  - *Date* = `Saturday, April 1, 2023`
  - *Time* = `04:00 AM`
- ☐ In the *Summertime end* frame, specify the following settings:
  - *Date* = `Saturday, September 30, 2023`
  - *Time* = `05:00 AM`
- ☐ Apply the settings temporarily. To do this, click the ✓ button.

`configure terminal`	To change to the Configuration mode from the Privileged EXEC mode.
`clock summer-time NonRe date 4 1 2023 04:00 09 30 2023 05:00 50`	To specify the *Timezone Acronym* value `NonRe`. To specify the time at which the device sets the clock forward from standard to summertime. • `4` To specify the month, *`April`*. • `1` To specify the date `1`. • `2023` To specify the year, `2023`. • `04:00` To specify the time `04:00 AM`. To specify the time at which the device resets the clock from summertime to standard time. • `9` To specify the month *`September`*. • `30` To specify the date, `30`. • `2023` To specify the year, `2023`. • `05:00` To specify the time `05:00 AM`. To specify the *Daylight saving time offset [min]* value `50`.
`do show clock detail`	To display the *Daylight saving time* settings.
`end`	To return to the Privileged EXEC mode.

4.2 NTPv4 Client

The device lets you synchronize the system time in the device and in the network using the Network Time Protocol (NTP). The device supports time synchronization based on the IPv4 protocol.

4.2.1 Enabling the NTPv4 Client function

Enable the *NTPv4 Client* function. To do this, perform the following steps:

- ☐ Open the dialog.
- ☐ Select the *On* radio button in the *Operation* frame.
- ☐ Apply the settings temporarily. To do this, click the ✓ button.

`configure terminal`	To change to the Configuration mode.
`ntp`	To enable the *NTPv4 Client* function.
`no ntp`	To disable the *NTPv4 Client* function.
`exit`	To quit the Configuration mode.

4.2.2 Adding an NTP Server Address

Perform the following steps:

Note: Depending on your security requirements, make sure you configure only trustworthy NTP server addresses.

- ☐ Open the *Time > NTPv4 Client* dialog.
- ☐ In the *IPv4 address* column of any table row, enter a valid IPv4 address pointing to an NTP server.
  When adding or changing an NTP server address, make sure the IPv4 addresses are unique.
- ☐ Apply the settings temporarily. To do this, click the ✓ button.

`configure terminal`	To change to the Configuration mode.
`ntp server <index no> ip <ipv4 address>`	To specify a valid IPv4 address for an NTP server.
`do show ntp status`	To display a list of the NTP servers that the device uses to synchronize the system time.
`do copy running-config startup-config`	To save the settings.
`exit`	To quit the Configuration mode.

4.2.3 Removing an NTP Server Address

Perform the following steps:

- ☐ Open the dialog.
- ☐ Mark the checkbox to select the table row that contains the IPv4 address to be removed.
- ☐ Click the 🗑 button.
  The field in the *IPv4 address* column displays the value `<no-address>`.
- ☐ Apply the settings temporarily. To do this, click the ✓ button.

`configure terminal`	To change to the Configuration mode.
`no ntp server <index no>`	To remove the *IPv4 address* of a specific table row.
`do show ntp status`	To display a list of the NTP servers that the device uses to synchronize the system time.
`do copy running-config startup-config`	To save the settings.
`exit`	To quit the Configuration mode.

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.

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

5.1 Saving the settings

5.1.1 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). 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 non-volatile memory (NVM).

Perform the following steps:

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

`show running-config`	To display the current configuration.
`copy running-config startup-config`	To save the configuration profile in the non-volatile memory (NVM).

Copying settings to a configuration profile

The device lets you store the settings saved in the memory (RAM) in a 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 *File name* field, click the + button to save the configuration profile under a new name. If you keep the proposed name, the device will overwrite an existing configuration profile of the same name.
- ☐ Click the *Ok* button.

`show running-config`	To display the current configuration.
`copy running-config flash:<file-name>`	To save the current settings of configuration profile in the non-volatile memory (NVM). If present, the device overwrites a configuration profile of the same name.

5.1.2 Exporting a configuration profile

The device lets you save a configuration profile to a server as a text file.

Prerequisites:
▶ To save the file on a server, you need a configured server on the network.

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

- ☐ Open the *Basic Settings > Load/Save* dialog.
- ☐ Select the table row of the desired configuration profile.
- ☐ 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 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 HTTP server, specify the URL for the file in the following form:
    `http://<IP address>/<path>/<file name>`
- ☐ Click the *Ok* button.
  The configuration profile is now saved as a text file in the specified location.

`show running-config`	To display the current configuration.
`copy running-config tftp://<IP_address>/<path>/<file name>`	To export a running configuration profile on a TFTP server.
`copy flash:<file-name> tftp://<IP_address>/<path>/<file name>`	To export the selected configuration profile on a TFTP server from the flash file system.
`copy running-config http://<IP_address>/<path>/<file name>`	To export a running configuration profile on an HTTP server.
`copy flash:<file-name> http://<IP_address>/<path>/<file name>`	To export the selected configuration profile on an HTTP server from the flash file system.

5.2 Loading settings

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

5.2.1 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.
- ☐ Select the table row of the desired 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.

`show running-config`	To display the current configuration.
`copy flash:<file-name> running-config`	To activate the settings of the selected configuration profile 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 selected configuration profile.

5.2.2 Importing a configuration profile

The device lets you import the configuration profile saved as a text file from a server.

Prerequisites:
▶ To load the file from a server, you need a configured server on the network.

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.
- ☐ Import the configuration profile:
  - ☐ 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 HTTP server, specify the URL for the file in the following form:
    `http://<IP address>/<path>/<file name>`
- ☐ In the *File name* drop-down list, select the desired file to be imported. The imported file can be saved to either non-volatile memory (NVM) or running-config.
- ☐ Mark the *Merge* checkbox to merge the configuration from the imported file into running-config. The prerequisite is that running-config profile is selected in the *File name* drop-down list.
- ☐ Click the *Ok* button.

`copy tftp://<IP_address>/<path>/<file name> running-config`	To import a configuration profile from a TFTP server to running configuration.
`copy tftp://<IP_address>/<path>/<file name> flash:<file-name>`	To import a configuration profile from a TFTP server to the flash file system.
`copy http://<IP_address>/ <path>/<file name> running-config`	To import a configuration profile from an HTTP server to running configuration.
`copy http://<IP_address>/<path>/<file name> flash:<file-name>`	To import a configuration profile from an HTTP server to the flash file system.

5.2.3 Loading the running-config from script

The device lets you load the running configuration profile from a script, which is saved as a text file on a server.

Prerequisites:
▶ To load the file from a server, you need a configured server on the network.

Perform the following steps:

- ☐ Open the *Basic Settings > Load/Save* dialog.
- ☐ Click the ☰ button and then the *Load running-config from script* item.
  The dialog displays the *Load running-config from script* window.
- ☐ Load the running configuration profile from script:
  - ☐ 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 HTTP server, specify the URL for the file in the following form:
    `http://<IP address>/<path>/<file name>`
- ☐ Mark the *Merge* checkbox to merge the configuration profile into running-config.
- ☐ Click the *Ok* button.

`copy tftp://<IP_address>/<path>/<file name> running-config`	To import a running configuration profile from a TFTP server to running configuration.
`copy http://<IP_address>/ <path>/<file name> running-config`	To import a running configuration profile from an HTTP server to running configuration.

5.3 Reset the device to default settings

To reset the device to default settings, perform the following steps:

- ☐ Open the *Basic Settings > Load/Save* dialog.
- ☐ Click the ☰ button, then *Back to default* item.
  The dialog displays a message.
- ☐ Click the *Ok* button.
  The device deletes the current operating settings from the volatile memory (RAM) and loads the default-config settings from the non-volatile memory (NVM).
  The device also triggers force password change (FPC) to change the default password of the device.

`clear config`	To reset the device to the default settings.

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 from the volatile memory and non-volatile 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 from the volatile memory (RAM) and non-volatile memory (NVM).

After a brief period, the device restarts and loads the delivery settings. The device also triggers force password change (FPC) to change the default password of the device.

`clear factory`	To delete the configuration profiles from the non-volatile memory. After a brief period, the device restarts and loads the delivery settings.

6 Loading software updates

Hirschmann 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 Hirschmann product pages on the Internet at www.hirschmann.com.

The device displays the version information of the installed software in the *Software* dialog of the Graphical User Interface (GUI).

You see the version information when you are already logged in to the device. To do this, perform the following step:

- ☐ Open the *Basic Settings > Software* frame.
  The *Running version* field displays the version number, creation date, and time of the device software that the device loaded during the last system startup and is currently running.

You can also see the version of the installed device software along with the other system information using the Command line interface (CLI). To do this, perform the following step:

`show version`	To display the system information such as the version number, creation date, time, and so on. The system information displayed is for the software that the device loaded during the last reboot and is currently running.

Note: The device settings are kept after updating the device software. However, the new version gets active when you reboot the device. Rebooting of the device removes the unsaved device settings, therefore, make sure you save the device settings before rebooting the device.

The device gives you the following options for updating the device software:
- Loading a previous software version
- Software update from the PC
- Software update from a server
- Firmware recovery

6.1 Loading a previous software version

The device lets you replace the device software with a previous version. To do this, perform the following step:

- ☐ Open the *Basic Settings > Software* frame.
  Click the *Restore* button which is next to the *Backup version* field to load the previous software version saved in the backup partition of the non-volatile memory.

`firmware swap`	The device replaces the current device software with the previous version saved in the backup partition of the non-volatile memory.

Note: Basic settings in the device are kept after replacing the device software, only the settings for the functions which are available in the newer device software version are lost. However, the previous version gets active only when you reboot the device and rebooting of the device removes the unsaved device settings. Therefore, make sure you save the device settings before rebooting the device.

6.2 Software update from the PC

The prerequisite is that the image file of the device software is saved on your local PC which is accessible through the device.

Perform the following steps:

- ☐ Navigate to the folder where the image file of the device software is saved.
- ☐ Open the *Basic Settings > Software* frame.
- ☐ Drag and drop the software file in the  area. As an alternative, click the  area to select the file by navigating to the folder where the image file of the device software is saved.
- ☐ To start the update procedure, click the *URL* 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.
  During the next system startup, the device loads the installed device software.

6.3 Software update from a server

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

Perform the following steps:

- ☐ Open the *Basic Settings > Software* frame.
- ☐ In the *URL* field, enter the URL for the image file in the following form:
  - ▶ When the image file is saved on the *TFTP* server:
    `tftp://<IP_address>/<path>/<firmware_file_name>.bin`
    or
    `tftp://<IP_address>/<path>/<bootloader_file_name>.bin`
  - ▶ When the image file is saved on the *HTTP* server:
    `http://<IP_address>/<path>/<firmware_file_name>.bin`
    or
    `http://<IP_address>/<path>/<bootloader_file_name>.bin`
  - ▶ When the image file is saved on the *HTTPs* server:
    `https://<IP_address>/<path>/<firmware_file_name>.bin`
    or
    `https://<IP_address>/<path>/<bootloader_file_name>.bin`
- ☐ Select the type of software to be uploaded. To do this, in the *Image type* field, select a desired value item between the `bootloader` and the `firmware` from the drop-down list.
- ☐ To start the update procedure, click the *URL* 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.
  During the next system startup, the device loads the installed device software.

`firmware upgrade tftp://10.0.1.159/product.bin`	To transfer the `product.bin` file from the TFTP server with the IPv4 address `10.0.1.159` to the device.
`firmware bootloader tftp://10.0.1.159/bootloader.bin`	To upgrade the boot loader image.

6.4 Firmware recovery

A firmware recovery might be necessary, for example if the device does not respond to your commands due to a detected failure in the current software. In this case, you can activate the backup software by restarting the device manually 4 times. After the 4 manual restarts are completed, the device starts up normally using the backup software to let you set up the device again and be able to use the features.

Perform the following work steps:

- ☐ Disconnect or disable the power supply of the device.
  When the device status LED stops glowing, the POWER OFF is completed.
- ☐ After you have POWERED OFF the device, begin the consecutive restart cycle.
- ☐ Connect or enable the power supply to the device. Wait until each of the device LEDs have been glowing for about 3..5 seconds, indicating that the device is POWERED ON and booted. 1 cycle of the system restart is now completed.
- ☐ Repeat the steps described above 3 more times. The prerequisite is that the consecutive restart cycle is started within a time interval of less than 2 minutes after the device LEDs have been glowing for about 3..5 seconds then, stopped.

When the manual recovery is successful, the device starts up during the fourth restart by loading the version of the device software stored in the backup partition to help provide you the device access.

After successful manual recovery, before setting up the device, it is advised to upload the latest version of the device software. To upload the new device software, see section “Software update from the PC” on page 63 or “Software update from a server” on page 64.

If the device has detected a failure during boot up with the new software version, then the device tries to recover automatically. If 3 automatic restart attempts do not help recover the current software version, then the device aborts the current software upload. Finally, the device starts up with the previous device software stored in the backup partition.

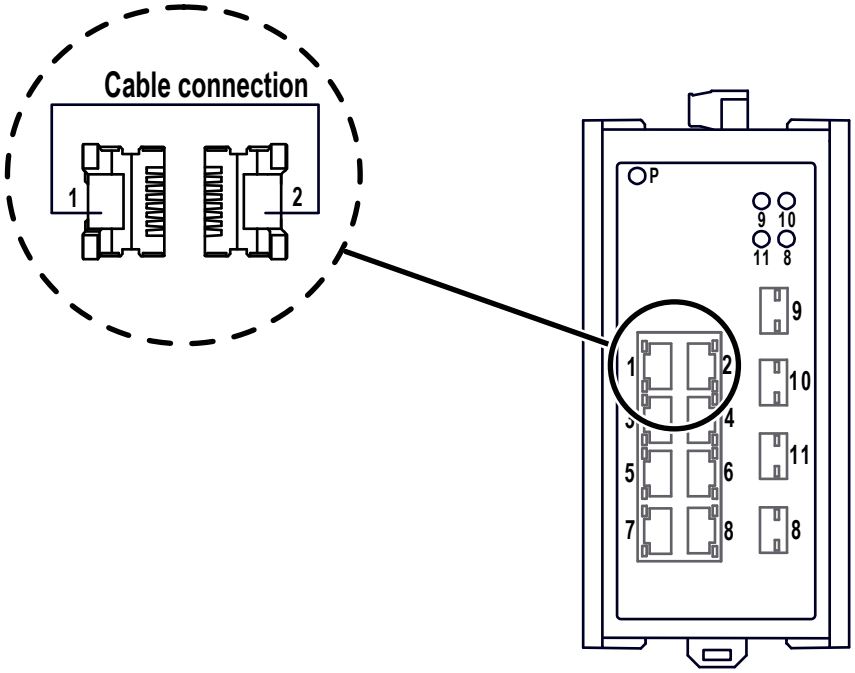
6.5 Device Recovery

The device recovery mechanism lets you recover the device when the device is inaccessible or has an unstable configuration due to one of the following reasons:

- The default Administrator password is lost and the password recovery is needed.
- The device is locked out using the management access filtering.
- The device is locked out using the AAA feature.
- The VLAN 1 gets deleted or is inaccessible.

When the device is neither accessible nor the configuration is stable, perform the following work steps:

☐ Create a physical loopback by connecting a cable between the port 1 and port 2.



☐ Reboot the device.

Note: A successful reboot is required for a successful execution of the manual recovery.

When the reboot is completed, the device software boots up normally with the startup configuration stored in the non-volatile memory that takes up to 70 seconds.
The completion of the device software boot up is identified by the following:

- The power LED is on.
- Flashing of the connected port LEDs.

After the boot up is completed, the device detects the physical loopback connected between the port 1 and port 2, and transmits a loopback packet from the port 2. When the port 1 receives and validates the loopback packet, the device performs the `clear config` operation.
As a result, the following happens on the device:

- Clears active configuration from the running configuration including the IPv4 address configured on the management VLAN.
- The device loads the default configuration, which uses DHCP client to set the management IPv4 address. Alternatively, you can use the Provize Explorer application to find and administrate the device.
- The password of the default administrator user is restored to default.
- Existing user configurations are removed.
- When the `clear config` operation is completed, the device triggers the Force Password Change (FPC) to let you change the default password of the device.

- ☐ After the device has triggered the Force Password Change (FPC), you remove the loopback cable from the device.
- ☐ Change the default password of the device. See “Force password change (FPC)” on page 33

Note: If required, you take the back-up of the startup configuration and overwrite the startup configuration using the command `copy running-config startup-config` else, on the next reboot the device will boot up with the older settings stored in startup configuration.

When you complete the device recovery steps, you get access to the device.

7 Configuring the ports

The following port configuration functions are available:
- Activating/deactivating the port
- Setting the port speed and duplex mode
- Gigabit Ethernet mode
- Configuring the Power over Ethernet

7.1 Activating/deactivating a port

In the default setting, every port is active. For a higher level of access security, deactivate the unused ports.

7.1.1 Deactivating a port

To deactivate a port, perform the following steps:

- ☐ Open the *Basic Settings > Port* dialog, *Configuration* tab.
- ☐ Deactivate the port. To do this, in the *Enable* column, unmark the checkbox for the relevant port.
- ☐ Apply the settings temporarily. To do this, click the ✓ button.

`configure terminal`	To change to the configuration mode.
`interface FastEthernet 1/1`	To change to the interface configuration mode of the Fast Ethernet port `1/1`.
`interface GigabitEthernet 1/1`	To change to the interface configuration mode of the Gigabit Ethernet port `1/1`.
`shutdown`	To deactivate the admin status of the interface. The port is now disabled.
`exit`	To quit the configuration mode.

7.1.2 Activating a port

To activate a port, perform the following steps:

- ☐ Open the *Basic Settings > Port* dialog, *Configuration* tab.
- ☐ Activate the port. To do this, in the *Enable* column mark the checkbox for the relevant port.
- ☐ Apply the settings temporarily. To do this, click the ✓ button.

`configure terminal`	To change to the configuration mode.
`interface FastEthernet 1/1`	To change to the interface configuration mode of the Fast Ethernet port `1/1`.
`interface GigabitEthernet 1/1`	To change to the interface configuration mode of the Gigabit Ethernet port `1/1`.
`no shutdown`	To activate the admin status of the interface. The port is now enabled.
`exit`	To quit the configuration mode.

7.2 Setting the port speed and duplex mode

The Gigabit Ethernet ports only support 1 Gbit/s and full duplex.

For Fast Ethernet ports you can set the port speed and duplex mode. In the default setting, the Fast Ethernet ports are set to *Autonegotiation* mode.

To set the desired port speed and duplex mode manually, perform the following steps:

- ☐ Open the *Basic Settings > Port* dialog, *Configuration* tab.
- ☐ Set the desired port speed and duplex mode for Fast Ethernet ports. To do this, in the *Speed/Duplex mode* column select the desired port speed and duplex mode.
- ☐ Apply the settings temporarily. To do this, click the ✓ button.

`configure terminal`	To change to the configuration mode.
`interface FastEthernet 1/1`	To change to the interface configuration mode of the Fast Ethernet port `1/1`.
`speed auto`	To enable the automatic configuration mode.
`no speed auto`	To disable the automatic configuration mode.
`speed 10`	To set port speed `10` Mbit/s.
`speed 100`	To set port speed `100` Mbit/s.
`duplex full`	To set full duplex mode.
`duplex half`	To set half duplex mode.
`exit`	To quit the configuration mode.

7.3 Gigabit Ethernet mode

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

To check the status of the inserted SFP, perform the following steps:

- ☐ Open the *Basic Settings > Port* dialog, *Configuration* tab.
  The column *Speed/Duplex mode* displays the value `1 Gbit/s Full Duplex` for the ports that have a 1 Gbit/s SFP transceiver inserted.

`show interface GigabitEthernet 1/1 status`	Displays the value `1 Gbit/s Full Duplex` for the ports that have a `1 Gbit/s` SFP transceiver inserted.

7.4 Configuring the Power over Ethernet

In Power over Ethernet (PoE), the *Power Source Equipment (PSE)* supplies current to powered devices (PD) such as IP phones through the twisted pair cable.

7.4.1 Setting the Global PSE power supply

Perform the following steps:

- ☐ Open the *Basic Settings > Power over Ethernet > Global* dialog.
- ☐ In the *Configuration* frame, specify the `20` watts power supply in the *Max. power [W]* field.
- ☐ Apply the settings temporarily. To do this, click the ✓ button.

`configure terminal`	To change to the configuration mode from the Privileged Exec mode.
`poe power-supply-limit 20`	To set the `20` watts power supply.
`end`	To return to the Privileged Exec mode.

7.4.2 Deactivating the Power over Ethernet on a port

In the default setting, Power over Ethernet is active for every port. To deactivate the Power over Ethernet, perform the following steps:

- ☐ Open the *Basic Settings > Power over Ethernet > Port* dialog, *Configuration* tab.
- ☐ Deactivate the Power over Ethernet function. To do this, unmark the checkbox in the *PoE* column for the relevant port.
- ☐ Apply the settings temporarily. To do this, click the ✓ button.

`configure terminal`	To change to the configuration mode from the Privileged Exec mode.
`interface GigabitEthernet 1/1`	To change to the interface configuration mode of the `GigabitEthernet 1/1`.
`no poe mode standard`	To deactivate the Power over Ethernet function on a port.
`end`	To return to the Privileged Exec mode.

7.4.3 Setting the Power over Ethernet priority on a port

Perform the following steps:

- ☐ Open the *Basic Settings > Power over Ethernet > Port* dialog, *Configuration* tab.
- ☐ In the *Priority* column, select the desired priority level from the drop-down list for the relevant port.

Note: When multiple ports have the same priority, the device first deactivates the Power over Ethernet function on the ports with the higher port number.

- ☐ Apply the settings temporarily. To do this, click the ✓ button.

`configure terminal`	To change to the configuration mode from the Privileged Exec mode.
`interface GigabitEthernet 1/1`	To change to the interface configuration mode of interface `GigabitEthernet 1/1`.
`poe priority low`	To set the `low` priority level of PoE on a port.
`poe priority high`	To set the `high` priority level of PoE on a port.
`poe priority critical`	To set the `critical` priority level of PoE on a port.
`end`	To return to the Privileged Exec mode.

7.4.4 Deactivating the LLDP awareness on a port

In the default setting, LLDP awareness is active for every port. To deactivate the LLDP awareness, perform the following steps:

- ☐ Open the *Basic Settings > Power over Ethernet > Port* dialog, *Configuration* tab.
- ☐ Deactivate the LLDP awareness on the port. To do this, unmark the checkbox in the *LLDP aware* column for the relevant port. The port determines the reserve power as per the class of the connected powered devices.
- ☐ Apply the settings temporarily. To do this, click the ✓ button.

`configure terminal`	To change to the configuration mode from the Privileged Exec mode.
`interface GigabitEthernet 1/1`	To change to the interface configuration mode of interface `GigabitEthernet 1/1`.
`no poe lldp`	To deactivate the LLDP awareness on a port. The port determines the reserve power as per the class of the connected powered devices.
`end`	To return to the Privileged Exec mode.

7.4.5 Setting the PoE power management

Perform the following steps:

- ☐ Open the *Basic Settings > Power over Ethernet > Port* dialog, *Configuration* tab.
- ☐ In the *Power management* column, select the value *dynamic* from the drop-down list for the relevant port.
- ☐ Apply the settings temporarily. To do this, click the ✓ button.

`configure terminal`	To change to the configuration mode from the Privileged Exec mode.
`interface GigabitEthernet 1/1`	To change to the interface configuration mode of interface `GigabitEthernet 1/1`.
`poe power-management dynamic`	To set the PoE power-management mode to `dynamic`. The device determines the actual PD power consumption and withdraws the free available power from the PD, ignoring the PD class.
`poe power-management static`	To set the PoE power-management mode to `static`. The device ignores the actual PD power consumption and uses the PD class to withdraw the free available power from the PD.
`poe power-management hybrid`	To set the PoE power-management mode to `hybrid`. The device uses both `dynamic` and `static` power management mode. If a port is configured with `hybrid` power management mode, then it acts like in `dynamic` power management mode unless it has negotiated a maximum power consumption over LLDP. A port that negotiated a maximum PoE over LLDP is switched automatically to `static` power management mode.
`end`	To return to the Privileged Exec mode.

7.4.6 Displaying the Power over Ethernet status

Perform the following steps:

- ☐ Open the *Basic Settings > Power over Ethernet > Port* dialog, *Status* tab.

`show poe`	To display the Power over Ethernet status of every interface.
`show poe interface GigabitEthernet 1/1`	To display the Power over Ethernet status of a specific interface `GigabitEthernet 1/1`.

8 Assistance in the protection from unauthorized access

To protect your network against unauthorized access, the device offers you the following functions:

- Enabling SNMP
- Enabling Telnet
- Disabling SSH
- Disabling HTTPS
- Displaying management servers status
- Adjusting session timeouts
- Displaying login session status
- Port Security
- Enabling IP access restriction

8.1 Enabling SNMP

The SNMP server is disabled in the device by default. In the following steps, you enable the SNMP server.

Perform the following steps:

- ☐ Open the *Device Security > Management Access > Server* dialog, *SNMP* tab.
  The tab displays the *Operation* frame of the SNMP server.
- ☐ In the *Operation* frame, select the `On` radio button.
- ☐ Apply the settings temporarily. To do this, click the ✓ button.

`configure terminal`	To change to the Configuration mode.
`snmp-server`	To enable the SNMP server.
`no snmp-server`	To disable the SNMP server.
`end`	To exit the Configuration mode.

8.2 Enabling Telnet

The Telnet server is disabled in the device by default. If you enable the Telnet server, then unencrypted remote access to the Command Line Interface becomes possible. In the following steps, you enable the Telnet server.

Perform the following steps:

- ☐ Open the *Device Security > Management Access > Server* dialog, *Telnet* tab. The tab displays the *Operation* frame of the Telnet server.
- ☐ In the *Operation* frame, select the `On` radio button.
- ☐ Apply the settings temporarily. To do this, click the ✓ button.

`configure terminal`	To change to the Configuration mode.
`aaa authentication login telnet local`	To enable the Telnet server.
`no aaa authentication login telnet`	To disable the Telnet server.
`end`	To exit the Configuration mode.

8.3 Disabling SSH

The SSH connections are encrypted and SSH server is enabled in the device by default. In the following steps, you disable the SSH server.

Perform the following steps:

- ☐ Open the *Device Security > Management Access > Server* dialog, *SSH* tab.
  The tab displays the *Operation* frame of the SSH server.
- ☐ In the *Operation* frame, select the `Off` radio button.
- ☐ Apply the settings temporarily. To do this, click the ✓ button.

`configure terminal`	To change to the Configuration mode.
`no ip ssh`	To disable the SSH server.
`ip ssh`	To enable the SSH server.
`end`	To exit the Configuration mode.

8.4 Disabling HTTPS

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

The HTTPS protocol is enabled by default. If you disable HTTPS, then secure access to the Graphical User Interface is not possible. To disable the HTTPS protocol, perform the following steps:

- ☐ Open the *Device Security > Management Access > Server* dialog, *HTTP/HTTPS* tab.
- ☐ In the *Operation* frame, select the `Off` radio button in the *HTTPS* mode option.
- ☐ Apply the settings temporarily. To do this, click the ✓ button.

`configure terminal`	To change to the Configuration mode.
`no ip http secure-server`	To disable the HTTPS protocol.
`exit`	To quit the Configuration mode.

If the HTTPS protocol is disabled, 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:

`configure terminal`	To change to the Configuration mode.
`ip http secure-server`	To enable the HTTPS protocol.
`exit`	To quit the Configuration mode.

If the HTTPS protocol is enabled and redirection from HTTP to HTTPS is also enabled, 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 `http://` before the IPv4 address of the device. In the default setting, the redirection from HTTP to HTTPS is enabled. To disable the redirection, perform the following steps:

- ☐ Open the *Device Security > Management Access > Server* dialog, *HTTP/HTTPS* tab.
- ☐ In the *Operation* frame, select the `Off` radio button in the *Redirect HTTP to HTTPS* option.
- ☐ Apply the settings temporarily. To do this, click the ✓ button.

`configure terminal`	To change to the Configuration mode.
`no ip http secure-redirect`	To disable the redirection from HTTP to HTTPS.
`exit`	To quit the Configuration mode.

8.5 Displaying management servers status

When you access the device using the Graphical User Interface, the device displays the servers operational state in the *Server* dialog.

When you access the device using the Command Line Interface, the device lets you display the servers status using their commands.

Perform the following steps:

- ☐ Open the *Device Security > Management Access > Server* dialog.
  The dialog displays the different tabs of the *Device Security > Management Access > Server* dialog.
- ☐ Open the *Device Security > Management Access > Server* dialog, *SNMP* tab.
  The *Operation* frame displays the current state of the SNMP server.
- ☐ Open the *Device Security > Management Access > Server* dialog, *Telnet* tab.
  The *Operation* frame displays the current state of the Telnet server.
- ☐ Open the *Device Security > Management Access > Server* dialog, *SSH* tab.
  The *Operation* frame displays the current state of the SSH server.
- ☐ Open the *Device Security > Management Access > Server* dialog, *HTTP/HTTPS* tab.
  The *Operation* frame displays the current state of the HTTPS server.

`show snmp`	To display the current status of the SNMP server.
`show aaa`	To display the current authentication status of the different connections to the device.
`show ip ssh`	To display the current state of the SSH server.
`show ip http`	To display the current state of the HTTPS server.

8.6 Adjusting session timeouts

The device automatically terminates the session upon inactivity of the logged-on user for the specified time. The device lets you specify the session timeout. In the following example, you specify a session timeout of 2 minutes for the VTY ID=1 session.

Perform the following steps:

- ☐ Open the *Device Security > Management Access > Virtual Terminal* dialog, *Configuration* tab. The dialog displays the configuration table.
- ☐ In the table row with *VTY ID* = `1`, *Session timeout [min]* column, specify the timeout value `2`.
- ☐ Apply the settings temporarily. To do this, click the ✓ button.

`configure terminal`	To change to the Configuration mode.
`line vty 1`	To select the VTY `1` session.
`exec-timeout 2`	To specify the timeout value `2`.
`end`	To exit the Configuration mode.

8.7 Displaying login session status

When you access the device using the Graphical User Interface, the device lets you display the status of active login sessions to the device.

When you access the device using the Command Line Interface, the device lets you display the session status at each VTY ID together.

Perform the following steps:

- ☐ Open the *Device Security > Management Access > Virtual Terminal* dialog, *Status* tab. The dialog displays the status table.

`show line`	To display the session status at each VTY ID.

8.8 Disabling the HiDiscovery function

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

After commissioning the device, we recommend granting read-only access to the device or disable the HiDiscovery function entirely. Disabling the HiDiscovery function after initial use helps secure the device against possible attacks that use the HiDiscovery protocol. To do this, perform the following steps:

- ☐ Open the *Basic Settings > Network > Global* dialog.
- ☐ To grant read-only access to the device using the HiDiscovery function, in the *HiDiscovery protocol v2* frame, from the *Access* drop-down list select the `read-only` item.
- ☐ To disable the HiDiscovery function, select the *Off* radio button in the *HiDiscovery protocol v2* frame.
- ☐ Apply the settings temporarily. To do this, click the ✓ button.

`configure terminal`	To change to the Configuration mode.
`network hidiscovery mode read-only`	To grant read-only access to the device using the HiDiscovery function.
`no network hidiscovery operation`	To disable the HiDiscovery function.
`exit`	To quit the Configuration mode.

8.9 Port Security

The *Port Security* function helps to restrict the forwarding of data packets with a specific source MAC address on a particular port. *Port Security* differentiates frames by their MAC source address. This restriction helps decide which source device the network device accepts on a particular port. This helps in hardening your network.

To configure the *Port Security* function, create a list of allowed MAC source addresses. If the device receives a frame with a MAC source address that is not allowed then the device takes a configurable action like sending a trap to the network management station and/or disabling the port.

8.9.1 Activating the Port Security

Activate the *Port Security* function globally on the device. To do this, perform the following steps:

- ☐ Open the *Network Security > Port Security* dialog.
- ☐ In the *Global* frame, mark the *Enable aging* checkbox.
- ☐ In the *Global* frame, set the desired values in the *Aging period [s]* and *Hold time [s]* fields.
- ☐ Apply the settings temporarily. To do this, click the ✓ button.

`configure terminal`	To change to the Configuration mode.
`port-security aging`	To activate the port security.
`port-security aging time <10-10000000>`	To set the aging time.
`port-security hold time <10-10000000>`	To set the hold time.
`exit`	To quit the Configuration mode.

8.9.2 Activating the Port Security for a port

Activate the *Port Security* function for a port. To do this, perform the following steps:

- ☐ Open the *Network Security > Port Security* dialog, *Interface* tab.
- ☐ Activate the *Port Security* function for a port. To do this, in the *Active* column mark the checkbox for the relevant port.
- ☐ Apply the settings temporarily. To do this, click the ✓ button.

`configure terminal`	To change to the Configuration mode.
`port-security interface FastEthernet 1/1`	To activate the *Port Security* for an interface Fast Ethernet `1/1`.
`exit`	To quit the Configuration mode.

8.9.3 Creating a MAC address entry

To create a *MAC address* entry, perform the following steps:

- ☐ Open the *Network Security > Port Security* dialog, *MAC address* tab.
- ☐ Add a MAC address entry:
  - ▶ Click the button.
    The dialog displays the *Create* window.
  - ▶ In the *Port* list, select the port number on which the source MAC address shall be allowed.
  - ▶ In the *VLAN ID* field, specify the ID of the VLAN from which the source MAC address shall be allowed.
  - ▶ In the *MAC address* field, specify the source *MAC address* which shall be allowed on the selected port number.
  - ▶ In the *MAC type* drop-down list, select the type of the MAC address.
  - ▶ Click the *Ok* button.
- ☐ Apply the settings temporarily. To do this, click the ✓ button.

`configure terminal`	To change to the Configuration mode from the Privileged Exec mode.
`interface GigabitEthernet 1/1`	To change to the interface configuration mode of Gigabit Ethernet `1/1`.
`port-security mac-address sticky 00-e0-4c-84-a9-f9 vlan 2`	To create a sticky MAC address `00-e0-4c-84-a9-f9` entry in the port security table with an optional VLAN ID `2` from which the mentioned MAC address shall be allowed.
`end`	To return to the Privileged Exec mode.

8.10 Enabling IP access restriction

In the default setting, you access the device management from any IPv4 address with the supported protocols.

The IP access restriction lets you restrict access to the device management to selected IPv4 address ranges and selected IP-based protocols.

Perform the following steps:

- ☐ Open the *Device Security > Management Access > IP Access Restriction* dialog.
- ☐ To add a table row, click the button.
  - In the *Index* field, specify the index number.
  - In the *VLAN ID* field, specify the VLAN ID.
  - In the *Start address* field, specify the start IPv4 address of the address range.
  - In the *End address* field, specify the end IPv4 address of the address range.
  - Mark the *HTTP/HTTPS* checkbox to activate the *HTTP/HTTPS* access for the specified address range.
  - Mark the *SNMP* checkbox to activate the *SNMP* access for the specified address range.
  - Mark the *Telnet/SSH* checkbox to activate the *Telnet/SSH* access for the specified address range.

Before you enable the function, verify that at least one active table row lets you have access. Otherwise, if you change the settings, then the connection to the device terminates. You may get locked out of the device.

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

`configure terminal`	To change to the Configuration mode.
`no access management`	To disable the IP access restriction.
`access management`	To enable the IP access restriction.
`access management 2`	To create the index number `2` for the address range.
`access management 2 3`	To create a VLAN ID `3` for the access management entry.
`access management 2 3 192.168.13.75 to 192.168.13.80`	To specify the IPv4 address range.
`access management 2 3 192.168.13.75 to 192.168.13.80 telnet`	To activate the *Telnet* access for the specified address range. Repeat the operation for other protocols.

9 Network load control

The device features a number of functions that can help you reduce the network load:
- Direct packet distribution
- QoS
- Controlling Multicasts with IGMP Snooping
- IPMC

9.1 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 of source port and MAC address in its MAC address table Forwarding Database (FDB).

9.1.1 Specifying the global configurations

Perform the following steps:
☐ Configure the *Global parameters*.

- ☐ Open the *Switching > Global* dialog, *Aging* tab.
- ☐ To disable the *MAC address aging* function, in the *MAC address aging* field of the *Global parameters* frame, select the *Off* radio button.
- ☐ In the *Age time [s]* text field, specify the age time `300`.
- ☐ Apply the settings temporarily. To do this, click the ✓ button.

`configure terminal`	To change to the Configuration mode.
`no mac address-table aging-time`	To disable the MAC address aging function on the device.
`mac address-table aging-time 300`	To enable the MAC address aging and specify the age time `300` in seconds.
`do copy running-config startup-config`	To save the settings.
`exit`	To quit the Configuration mode.

☐ Specify the *Learning mode*.

- ☐ Open the *Switching > Global* dialog, *Port learning* tab.
- ☐ In the table row for the Gigabit Ethernet 1/1 port, in the *Learning mode* column, select the value *secure*.
- ☐ Apply the settings temporarily. To do this, click the ✓ button.

`configure terminal`	To change to the Configuration mode.
`interface GigabitEthernet 1/1`	To select the port `GigabitEthernet 1/1`.
`mac address-table learning secure`	To specify the learning mode `secure`.
`do copy running-config startup-config`	To save the settings.
`end`	To return to the Configuration mode.
`exit`	To quit the Configuration mode.

You can activate/deactivate the *MAC learning* setting for a selected *VLAN ID* in the *VLAN learning* tab. The MAC learning is active by default on the device.

☐ Deactivate the *MAC learning*.

- ☐ Open the tab.
- ☐ In the table row for the VLAN ID `7`, mark the checkbox in the *MAC learning* column.
- ☐ Apply the settings temporarily. To do this, click the ✓ button.

`configure terminal`	To change to the Configuration mode.
`no mac address-table learning vlan 7`	To deactivate MAC learning for the VLAN ID `7`.
`do copy running-config startup-config`	To save the settings.
`exit`	To quit the Configuration mode.

9.1.2 Adding a filter for a MAC address

You can add a table row in the filter for a MAC address table. To do this, perform the following steps:

☐ Add a table row.

- ☐ Open the *Switching > Filter for MAC Addresses* dialog.
- ☐ In the *VLAN ID* field, specify `7`.
- ☐ In *MAC address* field, specify the MAC address `ff-ff-ff-ff-ff-ff`.
- ☐ In the *Port list* field, select the value item `Gi 1/1`.
- ☐ Apply the settings temporarily. To do this, click the ✓ button.

`configure terminal`	To change to the Configuration mode.
`mac address-table static ff-ff-ff-ff-ff-ff vlan 7 interface GigabitEthernet 1/1`	To add a row for the MAC address `ff-ff-ff-ff-ff-ff` with the VLAN ID `7` on the port GigabitEthernet 1/1.
`do copy running-config startup-config`	To save the settings.
`exit`	To quit the Configuration mode.

9.2 QoS

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.

9.2.1 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*:
  - Active *Trust tag* function
    The device uses the priority of the data packet contained in the VLAN tag.
  - Inactive *Trust tag* function
    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 *Trust tag* function is active on the port, 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 *Trust tag* function is inactive on the port, 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 Priority*
  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 Priority* method, then under high network load the device can permanently block the data of lower *traffic classes*.
- *Deficit weighted round robin (DWRR)*
  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*.

9.2.2 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)

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

- Active *Trust tag* function
  The device assigns data packets with a VLAN tag 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.
- Inactive *Trust tag* function
  The device ignores the priority information in the data packets and assigns the priority of the receiving port to them.

9.2.3 VLAN tagging

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

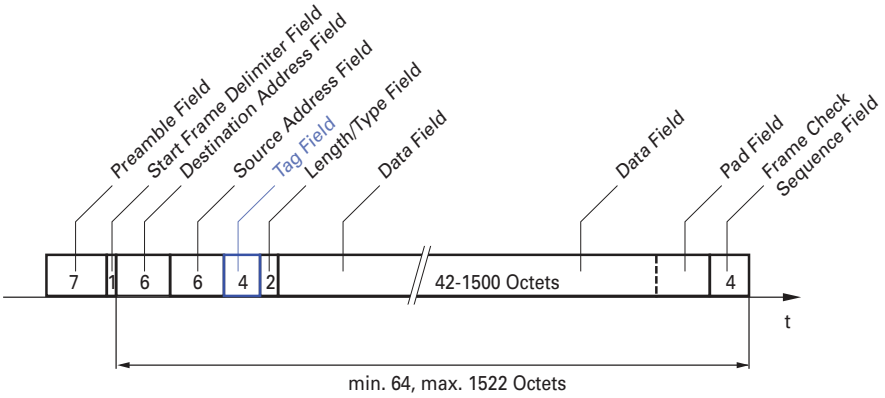


Figure 9: Ethernet data packet with tag

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

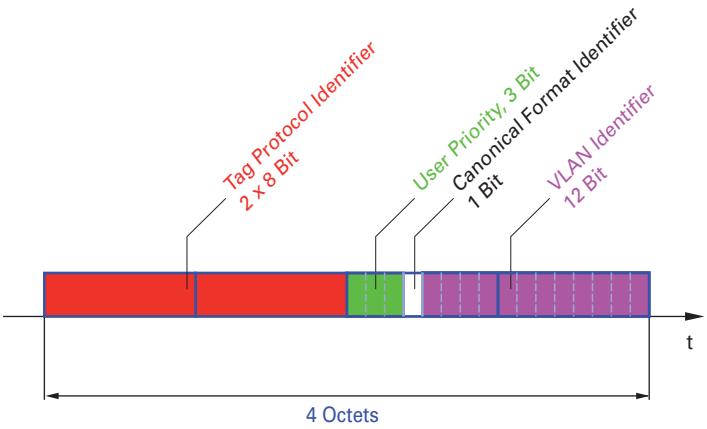


Figure 10: Structure of the VLAN tagging

Data packets with a VLAN tag 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.

9.2.4 Handling of traffic classes

The device provides the following options for handling *traffic classes*:
- *Strict Priority*
- *Deficit weighted round robin (DWRR)*
- *Strict Priority* combined with *Deficit weighted round robin (DWRR)*
- 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.

Deficit Weighted Round Robin description

With *Deficit Weighted Round Robin (DWRR)*, 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 *Deficit Weighted Round Robin* to every *traffic class*, the entire bandwidth of the corresponding port is available to you.

Combining Strict Priority and Deficit Weighted Round Robin

When combining *Weighted Round Robin* with *Strict Priority*, verify that the highest *traffic class* of *Deficit Weighted Round Robin* is lower than the lowest *traffic class* of *Strict Priority*.

If you combine *Deficit Weighted Round Robin* with *Strict Priority*, then a high *Strict Priority* network load can significantly reduce the bandwidth available for *Deficit Weighted Round Robin*.

9.2.5 Queue management

Queue Shaping

Queue Shaping throttles the rate at which a queue transmits packets. For example, using *Queue Shaping*, you rate-limit a higher priority queue so that it lets a lower 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.

Shaping the bandwidth of a queue

Perform the following steps:

- ☐ Open the *Switching > QoS > Port Configuration* dialog, *Egress queue shaper* tab.
- ☐ In the *Rate [kbps]* column, specify the desired bandwidth for the relevant queue on a port to shape the bandwidth of a queue.
- ☐ Activate the sharing of excess bandwidth. To do this, in the *Excess* column, mark the checkbox for the relevant queue on the required ports.
- ☐ Activate the credit-based shaping support. To do this, in the *Credit* column, mark the checkbox for the relevant queue on the required ports.
- ☐ Activate the shaping of bandwidth function for a priority queue. To do this, in the *Active* column, mark the checkbox for the relevant queue on the required ports.
- ☐ Apply the settings temporarily. To do this, click the ✓ button.

`configure terminal`	To change to the Configuration mode.
`interface FastEthernet 1/1`	To change to the interface configuration mode of `FastEthernet 1/1`.
`qos queue-shaper queue <queue_id> <100-1024000> [excess|credit] {kbps|mbps}`	To specify the desired bandwidth of a queue on a port where excess or credit option is active.
`exit`	To quit the Configuration mode.

Scheduling a queue priority

Perform the following steps:

- ☐ Open the *Switching > QoS > Port Configuration* dialog, *Queue scheduler* tab.
- ☐ In the *Mode* column, select the scheduling mode of the queues on the port.
- ☐ In the `<Queue numbers>` column, specify the desired weight to the relevant queue on a port. The assigned weight decides the priority of a queue.
- ☐ Apply the settings temporarily. To do this, click the ✓ button.

`configure terminal`	To change to the Configuration mode.
`interface FastEthernet 1/1`	To change to the interface configuration mode of `FastEthernet 1/1`.
`qos wrr <1-100>`	To specify the desired weight to the relevant queue on a port.
`exit`	To quit the configuration mode.

9.2.6 Setting prioritization

Assigning the port priority

Perform the following steps:

- ☐ Open the *Switching > QoS > Port Configuration* dialog, *Port* tab.
- ☐ In the *COS* and *DPL* columns, specify the priority with which the device forwards the data packets received on this port without a VLAN tag.
- ☐ In the *PCP* and *DEI* columns, specify the priority with which the device forwards the data packets received on this port with a VLAN tag.
- ☐ Apply the settings temporarily. To do this, click the ✓ button.

`configure terminal`	To change to the Configuration mode.
`interface GigabitEthernet 1/1`	To change to the interface configuration mode of `GigabitEthernet 1/1`.
`qos cos <0-7>`	To specify the default *COS* value.

`qos dpl <0-1>`	To specify the default *DPL* value.
`qos pcp <0-7>`	To specify the default *PCP* value.
`qos dei <0-1>`	To specify the default *DEI* value.
`exit`	To quit the Configuration mode.

Shaping the bandwidth on a port

Perform the following steps:

- ☐ Open the *Switching > QoS > Port Configuration* dialog, *Egress port shaper* tab.
- ☐ In the *Rate [kbps]* column, specify the desired bandwidth for the relevant port.
- ☐ Activate the port shaping function. To do this, in the *Active* column, mark the checkbox for the relevant port.
- ☐ Apply the settings temporarily. To do this, click the ✓ button.

`configure terminal`	To change to the Configuration mode.
`interface GigabitEthernet 1/1`	To change to the interface configuration mode of `GigabitEthernet 1/1`.
`qos shaper <100-1024000>`	To specify the desired traffic shaping rate.
`exit`	To quit the Configuration mode.

Mapping DSCP value to a specific COS and DPL value

Perform the following steps:

- ☐ Open the *Switching > QoS > IP DSCP Mapping* dialog.
- ☐ In the *COS* and *DPL* columns, specify the priority with which the device forwards the data packets containing the trusted DSCP value.
- ☐ Trust the data packets containing DSCP value. To do this, in the *Trust* column, mark the checkbox for the relevant DSCP value.
- ☐ Apply the settings temporarily. To do this, click the ✓ button.

`configure terminal`	To change to the Configuration mode.
`interface GigabitEthernet 1/1`	To change to the interface configuration mode of `GigabitEthernet 1/1`.
`qos trust dscp`	To activate the trusting of DSCP value contained in the IP data packets.
`exit`	To quit the Configuration mode.

`configure terminal`	To change to the Configuration mode.
`qos map dscp-classify 10`	To activate the classification of DSCP value `10`.
`qos map dscp-cos 10 cos 6 dpl 1`	To map the trusted DSCP value `10` with *COS* value `6` and *DPL* value `1`.
`exit`	To quit the Configuration mode.

9.3 Controlling Multicasts with IGMP Snooping

In the default setting, the device floods data packets with a Multicast destination address. This means that the device forwards these data packets to every port. This can lead to an unnecessary 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 where the connected devices explicitly want to receive packets from specific Multicast addresses.

9.3.1 Example of a Multicast application

A surveillance camera transmit video images to a monitor in the machine room as well as to a monitor in the surveillance room. With an IPv4 Multicast transmission, the camera forwards its data over the network as Multicast packets.

The protocol IGMP helps control the Multicast data traffic between Multicast data sources and receivers. For this, IGMP-aware devices in the network path between the camera and the monitors observe the IGMP transactions.

IGMP-capable Multicast receivers register subscriptions for a Multicast stream by sending an IGMP Report. An IGMP-capable switching device then creates an entry in its MAC address table and forwards the respective Multicast packets only to the ports on which it has previously received IGMP Reports.

9.3.2 IGMP Snooping

The protocol IGMP helps the controlled distribution of Multicast data between Multicast routers and connected receivers on Layer 3. *IGMP Snooping* describes the function of a switch that continuously monitors IGMP transactions and optimizes its own forwarding settings for the related Multicast data traffic.

The *IGMP Snooping* function in the device operates according to RFC 2236 for IGMPv2 and RFC 3376 for IGMPv3.

Multicast routers with an active IGMP function periodically query registration of Multicast streams to determine the associated IPv4 Multicast group members. IPv4 Multicast group members reply with a *report message*. This *report message* contains the parameters required by IGMP. The Multicast router enters the IPv4 Multicast address from the *report message* in its routing table. This causes the Multicast router to forward data packets with this IPv4 Multicast destination address only to the registered Multicast group members.

If the Multicast router does not receive any *report messages* for a specific multicast group on a port within a certain time (max query response time), then the Multicast router removes the routing table entry for this port. For IGMP version 2 and higher, receivers actively unsubscribe with a *leave message* when leaving a Multicast group and do not send further *report messages*.

When several IGMP Multicast routers are in the same network, the device with the smallest IPv4 address takes over the query function. When there are no Multicast routers in the network, you have the option to enable the query function in the device.

A device that connects a Multicast receiver with a Multicast router analyzes the IGMP transactions with the *IGMP Snooping* function.

The *IGMP Snooping* function also makes it possible to provide the IGMP function to the network on Layer 2. The device stores the MAC addresses derived from IPv4 addresses of the Multicast receivers as recognized Multicast receiver addresses in its MAC address table. In addition, the device identifies the ports on which it has received IGMP Reports for a specific Multicast address. In this way, the device forwards Multicast packets only to ports to which known Multicast receivers are connected. The other ports of the device do not forward these Multicast packets.

A special feature of the device is the possibility to determine the processing of data packets with unknown Multicast addresses. Depending on the setting, the device either discards these packets or forwards them to every port.

Enabling the IGMP Snooping function

Perform the following steps:

- ☐ Open the *Switching > IGMP Snooping > Global* dialog.
- ☐ Enable the *IGMP Snooping* function. To do this, in the *Configuration* frame select the `On` radio button.
- ☐ Apply the settings temporarily. To do this, click the ✓ button.

`configure terminal`	To change to the Configuration mode from the Privileged Exec mode.
`ip igmp snooping`	To enable the IGMP Snooping function.
`end`	To return to the Privileged Exec mode.

Activating the IGMP Snooping for a VLAN

Perform the following steps:

- ☐ Open the *Switching > IGMP Snooping > Configuration* dialog, *VLAN* tab.
- ☐ Activate the *IGMP Snooping* function for a specific VLAN. To do this, in the *Snooping function* column mark the checkbox for the relevant VLAN.
- ☐ Apply the settings temporarily. To do this, click the ✓ button.

`configure terminal`	To change to the Configuration mode from the Privileged Exec mode.
`interface vlan 2`	To change to interface configuration mode of the VLAN `2`.
`ip igmp snooping`	To activate the IGMP Snooping function for the VLAN `2`.
`end`	To return to the Privileged Exec mode.

Activating the Querier function for a VLAN

The device optionally sends *query messages* itself. Alternatively, it responds to *query messages* or detects other Multicast queriers in the network (*Querier* function).

The prerequisite is that the *IGMP Snooping* function is enabled globally.

Perform the following steps:

- ☐ Open the *Switching > IGMP Snooping > Querier* dialog.
- ☐ Activate the *Querier* function for a specific VLAN. To do this, in the *Snooping function* column mark the checkbox for the relevant VLAN.
- ☐ In the *Querier address* column, you specify the IPv4 address that the device adds as the source address in general query messages generated by the device. You use the address of the Multicast router.
- ☐ Apply the settings temporarily. To do this, click the ✓ button.

Note: The device carries out a selection process: When the IPv4 source address of another Multicast querier is lower than its own management IP address, the device transitions to a passive state, in which it does not send out any more query requests.

`configure terminal`	To change to the Configuration mode from the Privileged Exec mode.
`interface vlan 2`	To change to the interface configuration mode of the VLAN `2`.
`ip igmp snooping querier address 192.168.0.5`	To specify the IGMP querier address.
`end`	To return to the Privileged Exec mode.

9.4 IPMC

Internet Protocol Multicast Configuration (IPMC) helps to provide access control for filtering group address registration.

9.4.1 Enabling the IPMC profile

In the default setting, IPMC profile is disabled. To enable the IPMC profile, perform the following steps:

- ☐ Open the *Switching > IPMC* dialog, *Profile settings* tab.
- ☐ To enable the IPMC profile, select the `On` radio button in the *IPMC* frame.
- ☐ Apply the settings temporarily. To do this, click the ✓ button.

`configure terminal`	To change to the Configuration mode from the Privileged Exec mode.
`ipmc profile`	To enable the IPMC profile to start filtering.
`end`	To return to the Privileged Exec mode.

9.4.2 Disabling the IPMC profile

To disable the IPMC profile, perform the following steps:

- ☐ Open the *Switching > IPMC* dialog, *Profile settings* tab.
- ☐ To disable the IPMC profile, select the `Off` radio button in the *IPMC* frame.
- ☐ Apply the settings temporarily. To do this, click the ✓ button.

`configure terminal`	To change to the Configuration mode from the Privileged Exec mode.
`no ipmc profile`	To disable the IPMC profile.
`end`	To return to the Privileged Exec mode.

9.4.3 Creating an IPv4 Multicast Address range

To create an address range, perform the following steps:

- ☐ Open the *Switching > IPMC* dialog, *Address range* tab.
- ☐ Add an address range:
  - ▶ Click the button.
    The dialog displays the *Create* window.
  - ▶ In the *Range name* field, you specify the name of the address range.
  - ▶ In the *Start address* field, you specify the start address of the address range.
  - ▶ In the *End address* field, you specify the end address of the address range.
  - ▶ Click the *Ok* button.
- ☐ Apply the settings temporarily. To do this, click the ✓ button.

`configure terminal`	To change to the Configuration mode from the Privileged Exec mode.
`ipmc range <range-name> <start-ipmc-address> <end-ipmc-address>`	To create an IPv4 multicast address range name, consisting of start and end address.
`end`	To return to the Privileged Exec mode.

9.4.4 Creating an IPMC Profile

To create an IPMC profile, perform the following steps:

- ☐ Open the *Switching > IPMC* dialog, *Profile settings* tab.
- ☐ Click the button.
  The dialog displays the *Create* window.
- ☐ In the *Profile name* field, you specify the name of an IPMC profile.
- ☐ In the *Profile description* field, you specify the additional information about an IPMC profile.

- ☐ Click the *Ok* button.
  The device creates an IPMC profile.
- ☐ Apply a rule to an IPMC profile. To do this, perform the following steps:
  - ☐ Open the *Wizard* dialog. To do this, Click the  button.
    The dialog displays the *IPMCWizard* window.
  - ☐ In the *Profile name* drop-down list, select the name of an IPMC profile.
  - ☐ Click the *Next* button.
  - ☐ In the *Range name* drop-down list, select a range name.
  - ☐ In the *Next rule range* drop-down list, select a next range name if more than one rule exists.
  - ☐ In the *Action* options, select the *Permit* radio button to transmit the data packet if the rule matches.
  - ☐ In the *Action* options, select the *Deny* radio button to drop the data packet if the rule matches.
  - ☐ Mark the *Log* checkbox to create a log entry if the rule matches.
  - ☐ Apply the changes. To do this, click the *Update address range* button.
  - ☐ Click the *Finish* button to close the *IPMCWizard* window.
- ☐ Apply the settings temporarily. To do this, click the ✓ button.

`configure terminal`	To change to the Configuration mode from the Privileged Exec mode.
`ipmc profile <profile_name>`	To create an IPMC profile name and change to config-ipmc-profile sub mode.
`description`	To add detail information of a profile.
`range <entry_name> { permit | deny } [ log ] [next <next_range_name]`	To select IPv4 Multicast range name, consisting of permit or deny option along with optional log events and next rule. The next rule would succeed the current rule.
`end`	To return to the Privileged Exec mode.

10 VLANs

In the simplest case, a Virtual Local Area Network (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 Local Area Network (LAN).

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

10.1 VLAN configuration

The device lets you perform the following VLAN settings:

- Adding a VLAN
- Configuring VLAN ports

10.1.1 Adding a VLAN

In the following example you create a new VLAN 77.

Perform the following steps:

- ☐ Open the *Configuration* dialog.
  The dialog displays a VLAN table.
- ☐ Click the button.
  The dialog displays the *Create* window.
- ☐ In the *VLAN ID* field, enter the value `77`.
- ☐ In the *VLAN name* field, enter the value `abc`.
- ☐ Click the *Ok* button.
  The table displays the VLAN 77 in a table row.
- ☐ Apply the settings temporarily. To do this, click the ✓ button.

`configure terminal`	To change to the Configuration mode from the Privileged Exec mode.
`vlan 77`	To add the VLAN `77`.
`name abc`	To specify the VLAN name `abc`.
`end`	To return to the Privileged Exec mode.

10.1.2 Configuring VLAN ports

The following practical examples provide a quick introduction to the 3 port modes of the VLAN.

VLAN port mode: access

You use access mode when you connect an end node to a switch in a network. This mode lets the following behavior happen on the assigned port:
- While receiving, the port accepts both tagged and untagged data packets with a port VLAN.
- While sending, sends every data packet through the port without any tag.
- Discards the data packets not assigned with the Access VLAN.

In the following example you set up the *access* mode in the table row for the `Gi 1/1` port.

Perform the following steps:

- ☐ Open the *Diagnostics > LLDP > Configuration* tab.
- ☐ In the *Mode* column, select the value item *access* from the drop-down list.
- ☐ In the *VLAN ID* column, enter the value `4`.
- ☐ Apply the settings temporarily. To do this, click the ✓ button.

`configure terminal`	To change to the Configuration mode from the Privileged Exec mode.
`interface GigabitEthernet 1/1`	To select the port `interface GigabitEthernet 1/1`.
`switchport mode access`	To switch to the `access` mode.
`vlan 4`	To specify the VLAN `4`.
`end`	To return to the Privileged Exec mode.

VLAN port mode: trunk

You use trunk mode when you connect a switch to another switch in a network. This mode lets the following behavior happen on the assigned port:
- Default native and allowed VLAN is 1 and lets you specify the additional allowed VLANs.
- Receives and sends data packets of the multiple VLANs.
- While receiving, accepts both tagged and untagged data packets with a port VLAN.
- While sending, except the data packets assigned with a port VLAN, sends every data packet with a VLAN tag.
- Except the data packet assigned with an allowed VLAN, discards every other data packet.

In the following example you set up the *trunk* mode in the table row for the port `Gi 1/2`.

Perform the following steps:

- ☐ Open the *Diagnostics > LLDP > Configuration* tab.
- ☐ In the *Mode* column, select the value *trunk*.
- ☐ In the *Trunk native VLAN* column, enter the value `15`.
- ☐ In the *Trunk allowed VLAN* column, enter the value `20-40`.
- ☐ Apply the settings temporarily. To do this, click the ✓ button.

`configure terminal`	To change to the Configuration mode from the Privileged Exec mode.
`interface GigabitEthernet 1/2`	To select the port `GigabitEthernet 1/2`.
`switchport mode trunk`	To switch to the `trunk` mode.
`switchport trunk native vlan 15`	To specify the native VLAN `15`.
`switchport trunk allowed vlan 20-40`	To specify the allowed VLAN range `20-40`.
`end`	To return to the Privileged Exec mode.

VLAN Port Mode: hybrid

The hybrid mode is similar to the trunk mode in many ways and also lets you specify some additional settings on the assigned port. This mode lets the following behavior happen on the assigned port:

- Default native and allowed VLAN is 1 and lets you specify the additional allowed VLANs.
- Receives and sends data packets of the multiple VLANs.
- While receiving, accepts both tagged and untagged data packets with a port VLAN and lets you control the filtering of the data packets received.
- While sending, lets you specify the tagging for the data packets on the port.
- Except the data packet assigned with an allowed VLAN, discards every other data packet.

In the following example you set up the *hybrid* mode in the table row for the port `Gi 1/3`.

Perform the following steps:

- ☐ Open the *Diagnostics > LLDP > Configuration* tab.
- ☐ In the *Mode* column, select the value item *hybrid* from the drop-down list.
- ☐ In the *Hybrid native VLAN* column, enter the value `11`.
- ☐ In the *Hybrid allowed VLAN* column, enter the value `42-50`.
- ☐ In the *Hybrid egress tagging* column, select the value item *tag every* from the drop-down list.
- ☐ In the *Hybrid ingress acceptance* column, select the value item *tagged & untagged* from the drop-down list.
- ☐ In the *Hybrid ingress filtering* column, mark the checkbox.
- ☐ Apply the settings temporarily. To do this, click the ✓ button.

`configure terminal`	To change to the Configuration mode from the Privileged Exec mode.
`interface GigabitEthernet 1/3`	To select the port `GigabitEthernet 1/3`.
`switchport mode hybrid`	To switch to the `hybrid` mode.
`switchport hybrid native vlan 11`	To specify the native VLAN `11`.
`switchport hybrid allowed vlan 42-50`	To specify the allowed VLAN range `42-50`.
`switchport hybrid egress-tag all`	To specify the egress tagging type `tag all`.
`switchport hybrid acceptable-frame-type all`	To specify the ingress acceptance tag type `tagged & untagged`.
`switchport hybrid ingress-filtering`	To activate the Ingress filtering setting.
`end`	To return to the Privileged Exec mode.

11 Redundancy

11.1 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.

11.1.1 Adding/removing an MRP instance

In the following example, you add and remove the MRP instance 1 on the device.

Perform the following steps:

- ☐ Open the *Switching > L2-Redundancy > MRP Client* dialog, *Configuration* tab.
  The tab displays the *Instance* frame.
- ☐ In the *Instance* frame, click the *Create* button.
  The device adds the MRP instance 1 and displays:
  - The MRP instance 1 in the *Instance* field.
  - The *Configuration* tab displays the MRP instance 1 details in the frames below the *Instance* frame.
- ☐ In the *Instance* frame, click the *Delete* button.
  The device removes the MRP instance 1:
  - The *Instance* field displays the value `No MRP instance found.`
  - The *Configuration* tab does not display the MRP instance 1 details below the *Instance* frame.
- ☐ Apply the settings temporarily. To do this, click the ✓ button.

`configure terminal`	To change to the Configuration mode from the Privileged Exec mode.
`media-redundancy 1`	To add the media-redundancy instance 1.
`no media-redundancy 1`	To remove the media-redundancy instance 1.
`end`	To return to the Privileged Exec mode.

11.1.2 Prerequisites for MRP client

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 through the ring ports. Apart from its neighbors, no other ring participants are connected to the respective device.
- *Spanning Tree*, *LLDP* (transmit and receive function) and Ring Redundancy have an effect on each other. Deactivate the *Spanning Tree* and the *LLDP* (transmit and receive function) protocols for the ports connected to the MRP ring, see the *Spanning Tree Port* and the *LLDP* dialogs.
  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 is deactivated on every port.)

11.1.3 Configuring an MRP client

In the following example configuration, you set up the media-redundancy instance 1. The device lets you set up only 1 media-redundancy instance.

Perform the following steps:

- ☐ Open the *Switching > L2-Redundancy > MRP Client* dialog, *Configuration* tab.
- ☐ In the *Ring port 1* frame, select the value item `Gi 1/1` from the drop-down list.
- ☐ In the *Ring port 2* frame, select the value item `Gi 1/3` from the drop-down list.
- ☐ In the *Recovery profile* field, select the value item *200 ms* from the drop-down list.
  If selecting the value *200 ms* for the ring recovery does not help provide the ring stability necessary to meet the requirements of your network, then select the value item *500 ms* from the drop-down list.
- ☐ In the *Domain name* field, enter the value `instance1`.
- ☐ In the *Domain ID* field, enter the value `"ffffffff-ffff-ffff-ffff-ffffffffffff"`.
- ☐ In the *OUI type* field, select the value item *custom* from the drop-down list.
- ☐ In the *Custom OUI* field, enter the value `08-00-06`.
- ☐ In the *Control VLAN* field, enter the value `1`.
  You ensure that the *Ring port 1* and the *Ring port 2* are the members of this VLAN ID, while specifying the control VLAN.
- ☐ To enable the MRP client, in the *Operation* frame, select the *On* radio button.
- ☐ Apply the settings temporarily. To do this, click the ✓ button.

`configure terminal`	To change to the Configuration mode from the Privileged Exec mode.
`media-redundancy 1`	To create/modify the media-redundancy instance 1 and enter the media redundancy configuration mode.
`port1 interface GigabitEthernet 1/1`	To assign the GigabitEthernet 1/1 to the ring port1.
`no port1 interface`	To unassign the GigabitEthernet 1/1 from the ring port1.
`port2 interface GigabitEthernet 1/3`	To assign the GigabitEthernet 1/3 to the ring port2.
`no port2 interface`	To unassign the GigabitEthernet 1/3 from the ring port2.

`name instance1`	To specify the domain name instance1.
`no name`	To delete the specified domain name.
`uuid "ffffffff-ffff-ffff-ffff-ffffffffffff"`	To specify the UUID "ffffffff-ffff-ffff-ffff-ffffffffffff".
`no uuid`	To delete the specified UUID.
`oui custom 08-00-06`	To specify the custom OUI 08-00-06.
`no oui`	To delete the specified OUI.
`control-vlan 1`	To specify the control VLAN `1`.
`no control-vlan`	To delete the specified control VLAN.
`admin-state enable`	To enable the media-redundancy instance 1. You first set up every parameter of the media-redundancy instance, then only enable the instance as a last step of the set-up procedure.
`recovery-profile 200ms`	To specify recovery profile 200ms.
`do show media-redundancy status`	To display the status of the media-redundancy instance.
`do show media-redundancy statistics`	To display the statistics of the media-redundancy instance.
`end`	To return to the Privileged Exec mode.

11.1.4 Clearing the MRP Client statistics and displaying the details

In the following example, you clear the statistics of the media-redundancy instance.

Perform the following steps:

- ☐ Open the *Switching > L2-Redundancy > MRP Client* dialog, *Statistics* tab.
  The *Statistics* tab displays the statistics of the media-redundancy instance.
- ☐ In the table row for the media-redundancy 1, in the first column, mark the checkbox.
- ☐ Click the 🗑 *Clear Statistics* button.
- ☐ Apply the settings temporarily. To do this, click the ✓ button.

`clear media-redundancy statistics`	To clear the statistics of the media-redundancy instance.
`show media-redundancy status`	To display the status of the media-redundancy instance.
`show media-redundancy statistics`	To display the statistics of the media-redundancy instance.

11.2 ERPS

Ethernet Ring Protection Switching (ERPS) provides fast protection and recovery switching for Ethernet traffic in a ring topology, while it also helps ensure that the Ethernet layer remains loop-free.

ERPS is defined by the ITU G.8032 standard. The implementation conforms to the *ITUT-G.8032(V1)* and the *ITUT-G.8032(V2)*.

The *ITU G.8032* standard defines the Automatic Protection Switching (APS) protocol and protection switching mechanisms for Ethernet layer network (ETH) ring topologies. The protection protocol defined in ITU G.8032 enables protected point to point, point to multipoint and multipoint to multipoint connectivity within a ring or interconnected rings, called Multi-Ring/Ladder Network topology. The ETH ring maps to the physical layer ring structure.

The device lets you perform the following work steps:
- Setting up an ERPS instance
- Switching the Control command
- Clearing/displaying the ERPS statistics

11.2.1 Setting up an ERPS instance

In the following example, you create a new *ERPS* instance 2 and specify its settings.

Perform the following steps:

- ☐ Open the *Diagnostics > LLDP > Configuration* tab.
- ☐ Click the button.
  The dialog displays the *Create* window.
- ☐ In the *ERPS instance* field, enter the value `2`.
- ☐ In the *Protected VLANs* field, enter the value `5`.
- ☐ In the *Port 0 interface* field, select the value item `Gi 1/1` from the drop-down list.
- ☐ In the *Port 1 interface* field, select the value item `Gi 1/2` from the drop-down list.
- ☐ Click the *Ok* button.
  The configuration tab displays the *ERPS* instance `2` in a table row.
  In the table row for the *ERPS* instance 2 follow the further steps:
- ☐ Activate the instance. To do this, mark the checkbox in the *Active* column.
- ☐ In the *Version* column, select the value item `v2` from the drop-down list.
- ☐ In the *RPL mode* column, select the value item `owner` from the drop-down list.
- ☐ In the *RPL port* column, select the value item `ring port 1` from the drop-down list.
- ☐ In the *Control VLAN* column, enter the value `7`.
- ☐ In the *PCP* column, enter the value `1`.
- ☐ In the *Ring ID* column, select the value item `sub-ring` from the drop-down list.
- ☐ To restrict the transmission of R-APS PDUs on a sub ring to a major ring, in the *Virtual channel* column, unmark the checkbox.
- ☐ In the *Connected ring instance* column, enter the value `1`.

- ☐ To activate the FDB flushing of the connected ring, in the *Interconnect propagate* column, mark the checkbox.
- ☐ In the *Ring ID* column, enter the value `2`.
- ☐ In the *Node ID* column, enter the value `00:11:22:33:44:55`.
- ☐ In the *Level* column, enter the value `5`.
- ☐ In the *Hold off time [ms]* column, enter the value `10000`.
- ☐ To deactivate the revertive setting of the instance, in the *Revertive* column, unmark the checkbox.
- ☐ In the *Guard time [ms]* column, enter the value `10`.
- ☐ In the *WTR [s]* column, enter the value `100` seconds.
- ☐ In the *Port 0 SMAC* column, enter the value `00:12:23:34:45:56`.
- ☐ In the *Port 1 SMAC* column, enter the value `00:13:24:35:46:57`.
- ☐ In the *Port 0 SF trigger* column, select the value item *MEP* from the drop-down list.
- ☐ In the *Port 0 domain* column, enter the value `test0.com`.
- ☐ In the *Port 0 service* column, enter the value `test0A`.
- ☐ In the *Port 0 MEP ID* column, enter the value `1`.
- ☐ In the *Port 1 SF trigger* column, select the value item *MEP* from the drop-down list.
- ☐ In the *Port 1 domain* column, enter the value `test1.com`.
- ☐ In the *Port 1 service* column, enter the value `test1A`.
- ☐ In the *Port 1 MEP ID* column, enter the value `2`.
- ☐ Apply the settings temporarily. To do this, click the ✓ button.

`configure terminal`	To change to the Configuration mode from the Privileged Exec mode.
`erps 2`	To create the new *ERPS* instance `2` and change to the ERPS configuration sub mode.
`no erps 2`	To delete the created *ERPS* instance `2`.
`admin-state enable`	To activate the *ERPS* instance `2`.
`version v2`	To specify the version `v2`.
`ring-type sub-ring`	To specify the ring type `sub-ring` with the virtual channel inactive.
`ring-type sub-ring virtual-channel`	To specify the ring type `sub-ring` with the virtual channel active.
`ring-type interconnected-sub-ring connected-ring 2`	To specify the ring type `interconnected-sub-ring` and the `connected-ring 2`.
`ring-type interconnected-sub-ring connected-ring 2 propagate-topology-change`	To specify the ring type `interconnected-sub-ring` and the `connected-ring 2` with the interconnect propagate active.
`ring-type interconnected-sub-ring connected-ring 2 propagate-topology-change virtual-channel`	To specify the ring type `interconnected-sub-ring` and the connected-ring 2 with the interconnect propagate and the virtual channel active.
`protected vlans 5`	To specify the protected *VLAN* `5`.
`rpl neighbor port0`	To specify the RPL mode `neighbor` and the RPL port as `ring port0`.
`control vlan 7 pcp 1`	To specify the control *VLAN* `7` and the PCP `1`.
`port0 interface GigabitEthernet 1/1`	To specify the port0 interface `GigabitEthernet 1/1`.

`port1 interface GigabitEthernet 1/2`	To specify the port1 interface `GigabitEthernet 1/2`.
`ring-id 2`	To specify the ring ID `2`.
`node-id 00:11:22:33:44:55`	To specify the unicast MAC address `00:11:22:33:44:55` as the node ID.
`level 5`	To specify the level `5`.
`hold-off-time 10000`	To specify the hold off time as `10000` milliseconds.
`no revertive`	To deactivate the revertive state of the instance.
`guard-time 10`	To specify the guard time as `10` milliseconds.
`wait-to-restore 100`	To specify the WTR as `100` milliseconds.
`port0 smac 00:12:23:34:45:56`	To specify the Port0 SMAC value `00:12:23:34:45:56`.
`port1 smac 00:13:24:35:46:57`	To specify the Port1 SMAC value `00:13:24:35:46:57`.
`port0 sf-trigger mep`	To specify the value `MEP` for the Port0 SF trigger.
`port0 sf-trigger mep domain test0.com service test0A mep-id 1`	To specify the domain name `test0.com`, service name `test0A`, and the MEP ID `1` for the Port0SF trigger.
`port1 sf-trigger mep domain test1.com service test1A mep-id 2`	To specify the domain name `test1.com`, service name `test1A`, and the MEP ID `2` for the Port1 SF trigger.
`end`	To return to the Privileged Exec mode.

11.2.2 Switching the Control command

In the following example, you switch to the control command *`force switch to port 0`* for the *ERPS* instance 2.

Perform the following steps:

- ☐ Open the *Switching > L2-Redundancy > ERPS* tab.
  The tab displays the *ERPS* instance 2 in a table row.
- ☐ In the *Control command* column, select the value item *`force switch to port 0`* from the drop-down list.
- ☐ Apply the settings temporarily. To do this, click the ✓ button.

`erps 2 switch force port1-to-port0`	To block the port1 and unblock the port0 by causing the forced switchover.
`erps 2 switch force port0-to-port1`	To block the port0 and unblock the port1 by causing the forced switchover.
`erps 2 switch manual port1-to-port0`	If the signal is good and no forced switch is in effect, blocks the port1 and unblocks the port0 by causing the switchover.
`erps 2 switch manual port0-to-port1`	If the signal is good and no forced switch is in effect, blocks the port0 and unblocks the port1 by causing the switchover.
`erps 2 clear`	To clear the forced/manual switchover request, WTR condition and the forced reversion.

11.2.3 Clearing/displaying the ERPS statistics

In the following example, you clear the statistics for the *ERPS* instance 2.

Perform the following steps:

- ☐ Open the tab.
  The tab displays the statistics for the *ERPS* instance 2 in a table row.
- ☐ In the row for the *ERPS* instance 2, in the first column, mark the checkbox.
- ☐ Click the *Clear ERPS statistics* button.

`clear erps 2 statictics`	To clear the statistics for the *ERPS* instance 2.
`clear erps statictics`	To clear the statistics for every *ERPS* instance added in the device.
`show erps details 2`	To display the detailed status for the ERPS instance 2.
`show erps details`	To display the detailed status for every ERPS instance currently added on the device.
`show erps statistics`	To display the detailed statistics for every ERPS instance currently added on the device.

11.3 Spanning Tree

Note: The Spanning Tree Protocol is a protocol for MAC bridges. For this reason, the following description uses the term bridge for the device.

Local networks are getting bigger and bigger. This applies to both the geographical expansion and the number of network participants. Therefore, it is advantageous to use multiple bridges, for example:

- to reduce the network load in sub-areas,
- to set up redundant connections and
- to overcome distance limitations.

However, using multiple bridges with multiple redundant connections between the subnetworks can lead to loops and thus interruption of communication across the network. To help avoid this, you can use Spanning Tree. Spanning Tree helps avoid loops 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.

11.3.1 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 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 bridge with the smallest number for the Bridge Identifier has the highest bridge priority.

According to the original standard IEEE 802.1D-1998, the 2 highest-value bytes are the Bridge Priority. When configuring the bridge, the bridge administrator can change the default setting for the Bridge Priority, which is `32768 (8000H)`.

In the newer standard IEEE 802.1Q-2014, the Bridge Priority is interpreted differently. The highest 4 bits represent the Bridge Priority. The lower 12 bits are reserved for the VLAN ID and are each zero. As a result, the bridge administrator can set the Bridge Priority in steps of 4096. The default value is `32768 (8000H)`, and the max. value is `61440 (F000H)`.

The 6 lowest-value bytes of the Bridge Identifier are the bridge's MAC address. The MAC address lets each bridge have a unique Bridge Identifier.

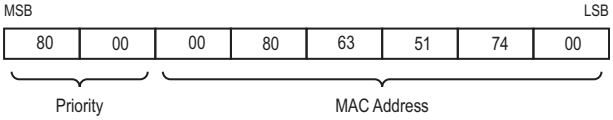


Figure 11: Bridge Identifier, Example (interpretation according to IEEE 802.1D-1998, values in hexadecimal notation)

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 6 on page 118). 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.

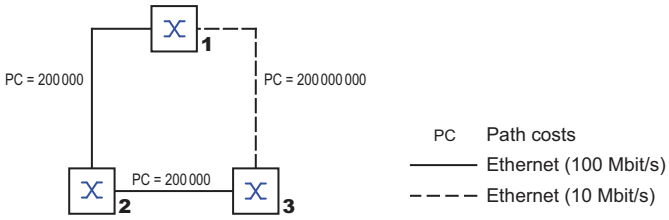


Figure 12: Path costs

Table 6: Recommended path costs for RSTP based on the data rate.

Data rate	Recommended value	Recommended range	Possible range
10 Mbit/s	2000000 [1]	200000-20000000	1..200000000
100 Mbit/s	200000 [a]	20000..2000000	1..200000000
1 Gbit/s	20000	2000..200000	1..200000000

1. Bridges that conform with IEEE 802.1D 1998 and only support 16-bit values for the path costs should 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

According to the original standard, IEEE 802.1D-1998, the Port Identifier consists of 2 bytes. The lower-value byte contains the physical port number. This provides a unique identifier for the port of this bridge. The higher-value byte is the Port Priority, which is specified by the Administrator (default value: `128 (80H)`.

In the newer standard IEEE 802.1Q-2014, the Port Priority is interpreted differently. The highest 4 bits represent the Port Priority. The lower 12 bits are the port number. This allows for bridges with up to 4095 ports. As a result, the bridge administrator can set the Port Priority in steps of 4096, when viewed as a 16-bit number. The default value is `32768 (8000H)`, and the max. value is `61440 (F000H)`. When viewed as a 4-bit number, the default value is `8 (8H)`, the min. value is `0 (0H)`, and the max. value is `15 (FH)`.

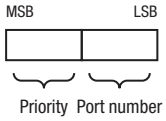


Figure 13: Port Identifier (interpretation according to IEEE 802.1D-1998)

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.

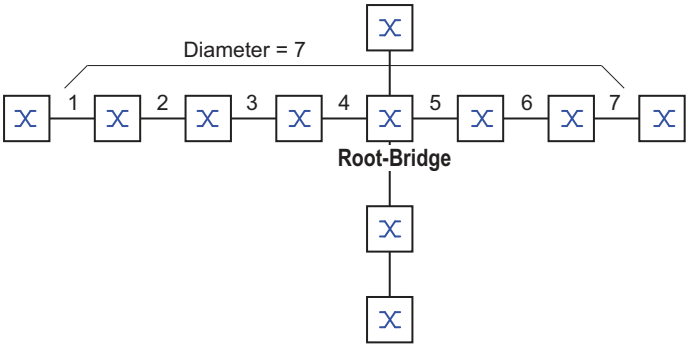


Figure 14: Definition of diameter

The network diameter that can be achieved in the network is MaxAge 1.

In the state of delivery, MaxAge=20 and the maximum diameter that can be achieved is 19. When you set the maximum value of 40 for MaxAge, the maximum diameter that can be achieved is 39.

MaxAge

Every STP-BPDU contains a “MessageAge” counter. When a bridge is passed through, the counter increases by 1.

Before forwarding an 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.

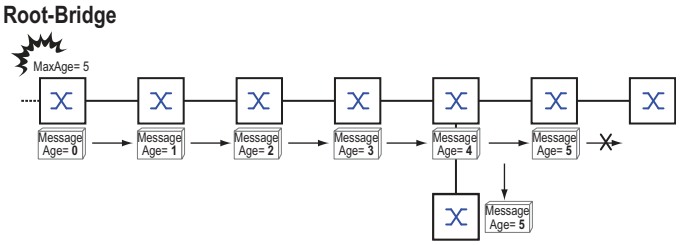


Figure 15: Transmission of an STP-BPDU depending on MaxAge

11.3.2 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 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 13 on page 118). 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.

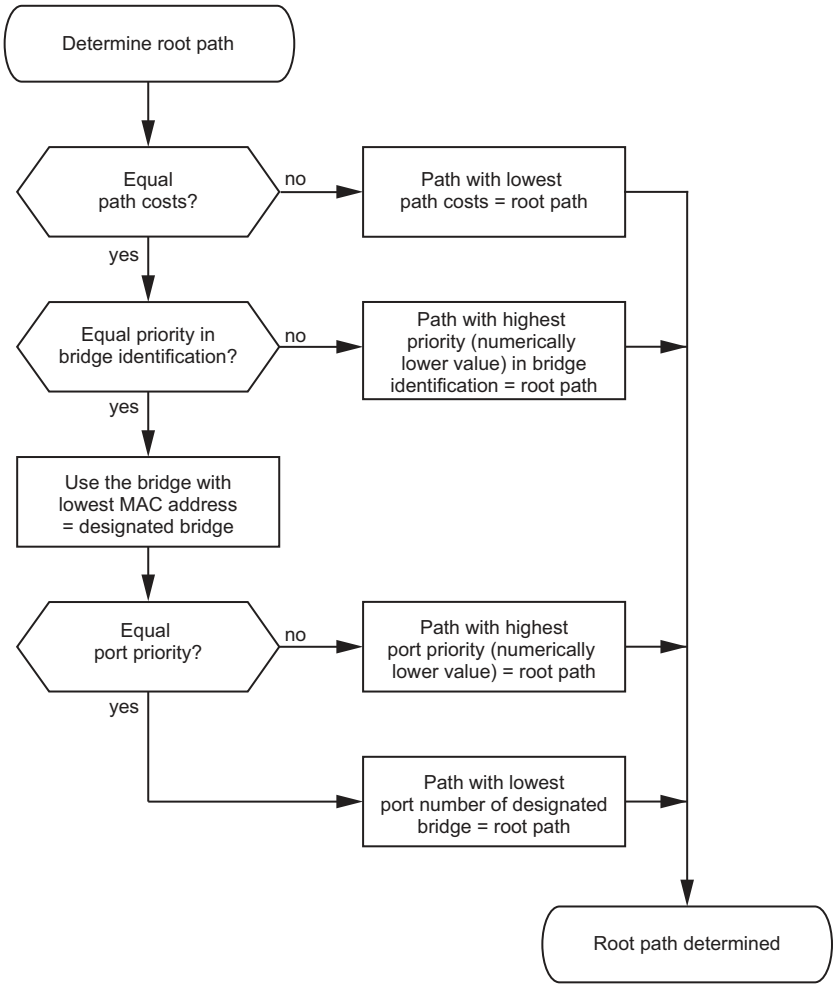


Figure 16: Flow diagram for specifying the root path

11.3.3 Examples

Example of determining the root path

You can use the network plan to follow the flow chart (see figure 16 on page 121) 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 through bridge 2 to the root bridge would result in higher path costs.

- The path through bridge 5 and bridge 3 creates the same root path costs as the path through 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).

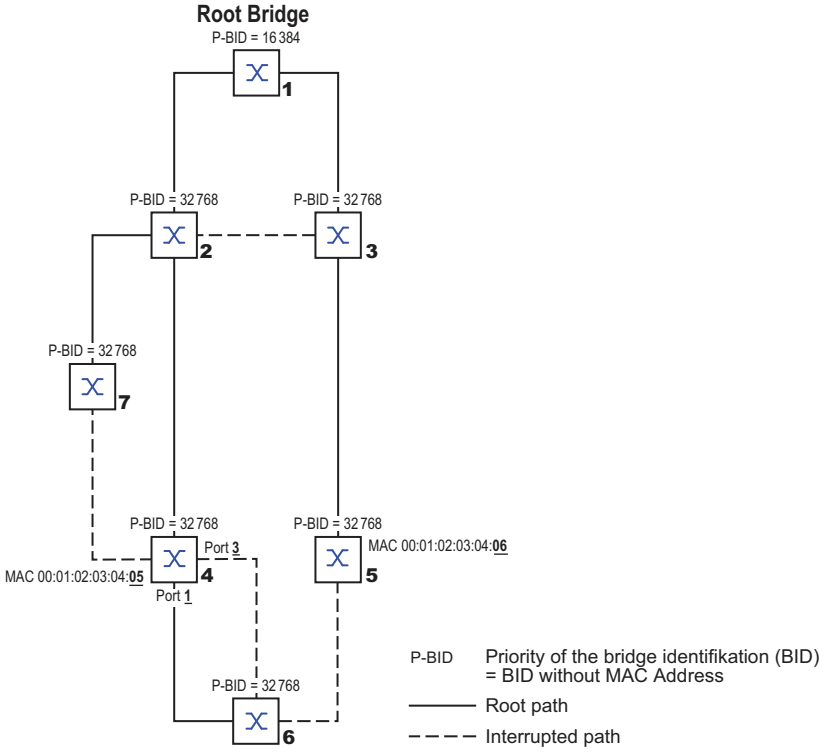


Figure 17: Example of a network plan for determining the root path

Note: When the current root bridge goes inoperable, 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 to follow the flow chart (see figure 16 on page 121) 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 through bridge 2 to the root bridge would result in higher path costs.

The path from bridge 6 to the root bridge is interesting:

▶ The bridges select the path through bridge 5 because the value 28672 for the priority in the bridge identifier is smaller than value 32768.

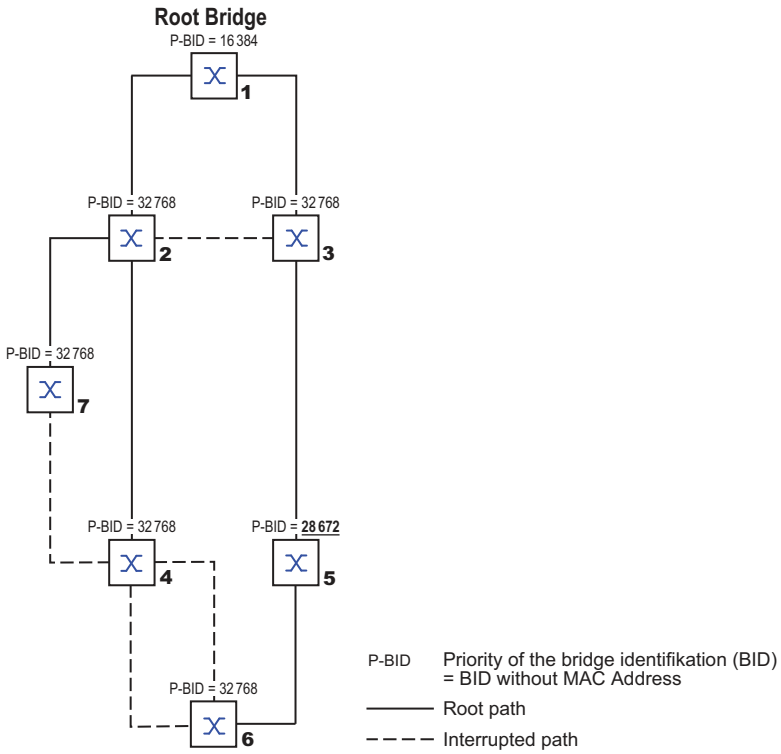


Figure 18: Example of a network plan for manipulating the root path

11.4 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 parameters and mechanisms that speed up the reconfiguration.

The ports play a significant role in this context.

11.4.1 Port roles

RSTP assigns each bridge port one of the following roles:

- Root Port:
  This is the port at which a bridge receives data packets with the lowest path costs from the root bridge.
  When there are multiple ports with equally low path costs, the bridge ID of the bridge that leads to the root (designated bridge) 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 16 on page 121).
  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 (through 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.

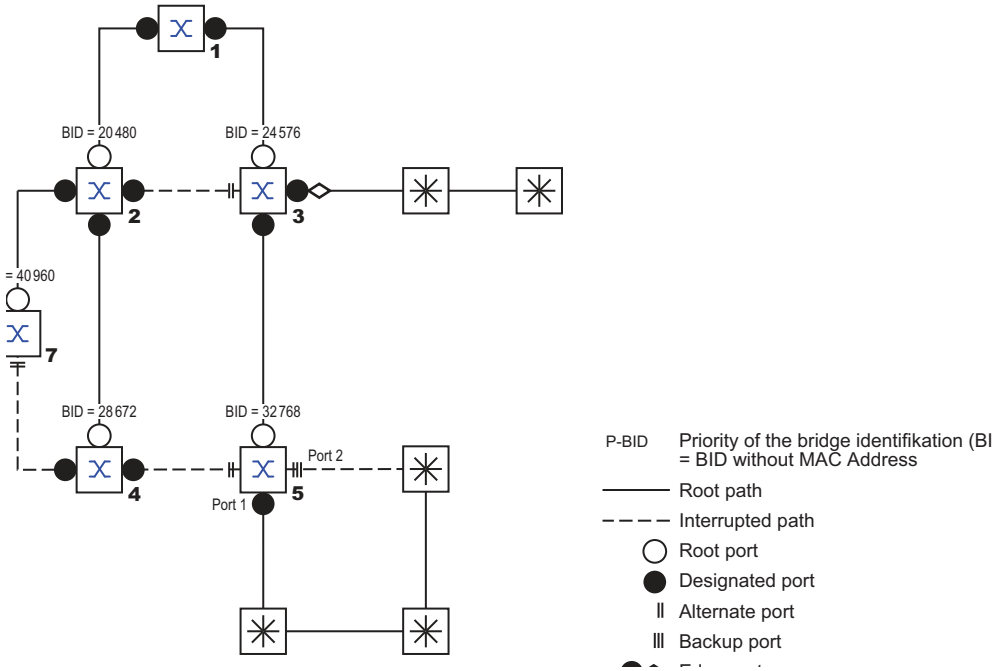


Figure 19: Port role assignment

11.4.2 Port states

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

Table 7: 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”.

The 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)

11.4.3 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 can determine port roles themselves and define the port states of their ports.

11.4.4 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 match 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.

11.4.5 Configuring the device

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.
- ☐ In the *Variant* frame, you select the protocol used for the spanning tree function.
- ☐ Apply the settings temporarily. To do this, click the ✓ button.

`configure terminal`	To change to the Configuration mode.
`spanning-tree mode <rstp | stp>`	To select the protocol used for the spanning tree function.
`exit`	To quit the Configuration mode.

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 *Bridge configuration* frame, you specify a numerically lower value in the *Priority* field. The bridge with the numerically lowest bridge ID has the highest priority and becomes the root bridge of the network.
- ☐ Apply the settings temporarily. To do this, click the ✓ button.

`spanning-tree mst 0 priority <0..61440>`	To specify the bridge priority of the device. **Note:** Specify the bridge priority in the range `0..61440` in steps of `4096`.

After saving, the *Root topology information* frame displays the following information:

- The value – (hyphen) in the *Root port* field.
- The value `0` in the *Root path cost* field.

`show spanning-tree`	To display the parameters for checking.

- ☐ If applicable, in the *Bridge configuration* frame, change the values in the *Forward delay [s]* and *Max age* fields.
  - The root bridge transmits the changed values to the other devices.
- ☐ Apply the settings temporarily. To do this, click the ✓ button.

`configure terminal`	To change to the Configuration mode.
`spanning-tree mst forward-time <4..30>`	To specify the delay time for the status change in seconds.
`spanning-tree mst max-age <6..40>`	To specify the maximum permissible branch length, for example the number of devices to the root bridge.
`exit`	To quit the Configuration mode.
`show spanning-tree`	To display 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`	To display the parameters for checking.

11.5 Connectivity Fault Management (CFM)

This feature lets you specify the following CFM settings:

- Adding/removing a domain
- Adding/removing a service
- Adding/removing a MEP

11.5.1 Adding/removing a domain

In the following example, you add the domain test on the device.

Note: If you remove a domain added on the device, then the device automatically removes the service and MEP set-ups as well that you added using the same domain that you want to remove.

Perform the following steps:

- ☐ Open the *Switching > L2-Redundancy > CFM > Configuration* dialog, *Domain* tab.
- ☐ Click the button.
  The dialog displays the *Create* window.
- ☐ In the *Domain* field, enter the value `test`.
- ☐ In the *Format* field, select the value item `string` from the drop-down list.
- ☐ In the *Name* field, enter the value `"abc"`.
- ☐ In the *Level* field, select the value item `1` from the drop-down list.
- ☐ Click the *Ok* button.
  The tab displays the domain `test` in a table row.
- ☐ Apply the settings temporarily. To do this, click the ✓ button.

`configure terminal`	To change to the Configuration mode from the Privileged Exec mode.
`cfm domain test`	To add the domain `test`.
`no cfm domain test`	To remove the domain `test`. If you have added the Service and MEP set-ups using the Domain test, then the device automatically removes that Service and MEP as well from the device.
`no cfm domain all`	To remove every Domain added on the device. If you use this command, then the device automatically removes every Service and MEP set-up as well from the device.
`format string "abc"`	To specify the format `string` and the service name `abc`. You specify the value of the format name between the quotation marks ("<abc>") only.
`level 1`	To specify the Level `1`.

`do show cfm domains`	To display the details of the CFM domains currently added on the device.
`do show cfm errors`	To display the details of the CFM errors detected by the device.
`end`	To return to the Privileged Exec mode.

11.5.2 Adding/removing a service

In the following example, you add the Service trial using the Domain test on the device. The prerequisite is that the Domain test is already added to the device.

Note: If you remove a service added on the device, then the device automatically removes the MEP set-up as well that you added using the same service that you want to remove.

Perform the following steps:

- ☐ Open the *Switching > L2-Redundancy > CFM > Configuration* dialog, *Service* tab.
- ☐ Click the button.
  The dialog displays the *Create* window.
- ☐ In the *Domain* field, select the value item `test` from the drop-down list.
- ☐ In the *Service* field, enter the value `xyz`.
- ☐ In the *Format* field, select the value item `string` from the drop-down list.
- ☐ In the *Service name* field, enter the value `sample`.
- ☐ In the *CCM interval* field, select the value item *10 ms* from the drop-down list.
- ☐ Click the *Ok* button.
  The tab displays the Service `xyz` in a table row.
- ☐ Apply the settings temporarily. To do this, click the ✓ button.

`configure terminal`	To change to the Configuration mode from the Privileged Exec mode.
`cfm domain test`	To specify the domain `test`.
`service xyz`	To add the Service `xyz`.
`no service xyz`	To remove the Service `xyz`. If you have added a MEP set-up using the Service xyz, then the device automatically removes that MEP as well from the device.
`format string "sample"`	To specify the format `string` and the service name `"sample"`. You specify the value of the service name between the quotation marks ("<sample>") only.
`continuity-check interval 10ms`	To specify the CCM interval `10ms`.
`do show cfm services`	To display the details of the CFM Services currently added on the device.
`end`	To return to the Privileged Exec mode.

11.5.3 Adding/removing a MEP

In the following example, you add the MEP 3 using the Domain test and service xyz on the device. The prerequisite is that the Domain test and Service xyz are already added on the device.

Perform the following steps:

- ☐ Open the *Switching > L2-Redundancy > CFM > Configuration* dialog, *MEP* tab.
- ☐ Click the ⊞ button.
  The dialog displays the *Create* window.
- ☐ In the *Domain* field, select the value item `test` from the drop-down list.
- ☐ In the *Service* field, select the value item `xyz` from the drop-down list.
- ☐ In the *MEP ID* field, enter the value `3`.
- ☐ In the *Port* field, select the value item `Gi1/1` from the drop-down list.
- ☐ In the *VLAN* field, enter the value `13`.
- ☐ In the *Remote MEP ID* field, enter the value `15`.
  You need to enter only the value that is different from the value specified in the *MEP ID* field.
- ☐ Mark the *Admin active* checkbox to activate the MEP.
- ☐ Mark the *CCM enabled* checkbox to activate the generation of continuity check messages (CCM).
- ☐ Click the *Ok* button.
  The tab displays the Service `xyz` in a table row.
- ☐ Apply the settings temporarily. To do this, click the ✓ button.

`configure terminal`	To change to the Configuration mode from the Privileged Exec mode.
`cfm domain test`	To specify the domain `test`.
`service xyz`	To specify the Service `xyz`.
`mep 3`	To specify the MEP `3`.
`interface GigabitEthernet 1/1`	To specify the port number `GigabitEthernet 1/1`.
`vlan 13`	To specify the VLAN `13`.
`remote mep 15`	To specify the remote MEP `15`.
`admin-state enable`	To activate the MEP.
`admin-state disable`	To deactivate the MEP.
`continuity-check`	To activate the generation of the continuity-check messages.
`no continuity-check`	To deactivate the generation of the continuity-check messages.
`do show cfm meps`	To display the details of the MEPs currently added on the device.
`end`	To return to the Privileged Exec mode.

12 Operation diagnosis

The device provides you with the following diagnostic tools:

- Syslog server
- Port Mirroring
- DDMI
- LLDP
- RMON
- Alarm

12.1 Syslog server

The device lets you specify the settings for the syslog server.

12.1.1 Enabling the syslog server mode

Perform the following steps:

- ☐ Open the frame.
- ☐ To enable the syslog server mode, select the *On* radio button.
- ☐ Apply the settings temporarily. To do this, click the ✓ button.

`configure terminal`	To change to the Configuration mode.
`logging on`	To enable the syslog server mode.
`no logging on`	To disable the syslog server mode.
`do copy running-config startup-config`	To save the change.
`end`	To exit the Configuration mode.

12.1.2 Specifying the syslog server configuration

In the following example configuration, we specify the IPv4 address for the syslog server and assign the severity level of the log that the device sends to the server.

Perform the following steps:

- ☐ Open the frame.
- ☐ In the *URL* field, specify `192.168.2.1`.
- ☐ In the *Start* field, select the item *warning*.
- ☐ Apply the settings temporarily. To do this, click the ✓ button.

`configure terminal`	To change to the Configuration mode.
`logging host 192.168.2.1`	To specify the IPv4 address `192.168.2.1`.
`logging host www.localsyslogserver.com`	To specify the host name `www.localsyslogserver.com` for the *DNS* server.
`logging level warning`	To specify the severity level `warning`.
`do copy running-config startup-config`	To save the configuration you specified.
`end`	To exit the Configuration mode.

12.2 Port Mirroring

The *Port Mirroring* function lets you copy received and sent data packets from selected source ports or VLANs to a destination port.

You can monitor the data packets on the source ports in the sending and receiving directions with a management tool connected on the destination port. The function has no effect on the data packets of the source ports.

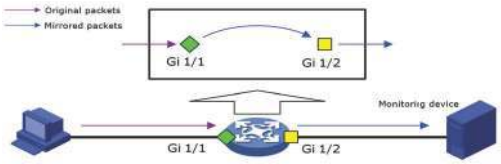


Figure 20: Example for Gigabit Ethernet (Gi) ports

To the destination port, the device only forwards the data packets copied from the source ports.

Note: A user with a privilege level 10 or higher can configure the *Port Mirroring* function for troubleshooting purposes. This may expose sensitive data which may be considered a security risk.

12.2.1 Configuring the Port Mirroring function

Perform the following steps:

- ☐ Open the *Diagnostics > Port Mirroring* dialog.
  The dialog displays the port mirroring table below the *Global parameters* frame.
- ☐ In the *Mode* column mark the checkbox to activate the mirroring session.
- ☐ In the *Source VLANs* column specify the value in the range `1..4093`.
  For configuring a mirror source, you can specify the value either in the *Source VLANs* column or in the *Source port list RX* and *Source port list TX* columns.
  If you specify a value in the *Source port list RX* or *Source port list TX* columns, then the GUI disables the *Source VLANs* column. Conversely if you specify a value in the *Source VLANs* column, then the GUI disables the *Source port list RX* and the *Source port list TX* columns.
  If you want to change the source type, first clear any values you may have already specified for the current source type.
- ☐ In the *Source port list RX* column select the `<port number>` from the drop-down list.
- ☐ In the *Source port list TX* column select the `<port number>` from the drop-down list.
- ☐ In the *CPU RX* column mark the checkbox to activate mirroring of the data packets received by the internal CPU.
- ☐ In the *CPU TX* column mark the checkbox to activate mirroring of the data packets transmitted by the internal CPU.
- ☐ In the *Destination port* column select the `<port number>` from the drop-down list.
- ☐ Apply the settings temporarily. To do this, click the ✓ button.

`configure terminal`	To change to the configuration mode.
`monitor session 1`	To enable the mirroring function.
`monitor session 1 source interface vlan 10,20`	To specify the session ID `1`, source VLAN IDs `10, 20`. **Note:** The user can only set up either source VLAN or the source interface mentioned in the below command at a time.
`monitor session 1 source interface GigabitEthernet 1/1`	To specify the source interface GigabitEthernet 1/1.
`monitor session 1 source cpu rx`	To specify the source interface `cpu rx`.
`monitor session 1 source cpu tx`	To specify the source interface `cpu tx`.
`monitor session 1 destination interface GigabitEthernet 1/2`	To specify the destination port GigabitEthernet 1/2.

12.3 DDMI

DDMI (Digital Diagnostic Monitoring Interface) helps to monitor the SFP (Small Form-factor Pluggable) transceiver status and diagnose the port parameters.

12.3.1 Enabling the DDMI function

Perform the following steps:

- ☐ Open the *Diagnostics > DDMI* dialog.
- ☐ In the *DDMI mode* frame, select the *On* radio button.
- ☐ Apply the settings temporarily. To do this, click the ✓ button.

`configure terminal`	To change to the configuration mode.
`ddmi`	To enable the *DDMI* function.
`exit`	To quit the configuration mode.

12.3.2 Disabling the DDMI function

Perform the following steps:

- ☐ Open the *Diagnostics > DDMI* dialog.
- ☐ In the *DDMI mode* frame, select the *Off* radio button.
- ☐ Apply the settings temporarily. To do this, click the ✓ button.

`configure terminal`	To change to the configuration mode.
`no ddmi`	To disable the *DDMI* function.
`exit`	To quit the configuration mode.

12.3.3 Displaying the SFP transceiver status

Perform the following steps:

- ☐ Open the *Diagnostics > DDMI* dialog.
  The following tabs display the SFP transceiver status:
  - *Overview*
  - *Temperature [C]*
  - *Voltage [V]*
  - *Bias [mA]*
  - *Transmitted power [mW]*
  - *Received power [mW]*

```
show interface GigabitEthernet 1/1
transceiver

Transceiver Information
Vendor.....................-
Part Number................-
Serial Number..............-
Revision...................-
Date Code..................-
Transceiver................-
DDMI Information
Temperature(C).............-
Voltage(V).................-
Tx Bias(mA)................-
Tx Power(mW)...............-
Rx Power(mW)...............-
```

Displays the SFP transceiver status for the port that has a 1 Gbit/s SFP transceiver inserted.

12.4 LLDP

The Link Layer Discovery Protocol (LLDP) in the device lets the network devices advertise information about themselves to the other devices on the network. The LLDP supports a set of attributes referred to as the *Type Length Value (TLV)*. The LLDP uses the *TLV* packets to receive and send information to their neighboring devices.

12.4.1 Specifying the global parameters

In the following example, you specify the values for the global parameters.

Perform the following steps:

- ☐ Open the *Diagnostics > LLDP > Configuration* dialog, *Configuration* frame.
- ☐ In the *Re-initialization delay [s]* field, specify the value `3`.
- ☐ In the *Message transmit hold* field, specify the value `5`.
- ☐ In the *Message transmit interval [s]* field, specify the value `40`.
- ☐ In the *Transmit delay [s]* field, specify the value `3`.
- ☐ Apply the settings temporarily. To do this, click the ✓ button.

`configure terminal`	To change to the Configuration mode.
`lldp reinit 3`	To specify the reinitialization delay value `3`.
`lldp holdtime 5`	To specify the message transmit hold value `5`.
`lldp timer 40`	To specify the message transmit interval value `40`.
`lldp transmission-delay 3`	To specify the transmit delay value `3`.
`end`	To quit the Configuration mode.

12.4.2 Specifying the port configuration

Each physical port in the device has a set of control parameters. The device lets you specify the settings for each port. In the following example, you specify the settings for the port Gi 1/1.

Perform the following steps:

- ☐ Open the *Diagnostics > LLDP > Configuration* dialog.
  The dialog displays the configuration table below the *Global* frame.
- ☐ In the *Operation* column, select the value item *`receive and transmit`* from the drop-down list.
- ☐ Activate the trap notification. To do this, in the *Trap notification* column, mark the checkbox.
- ☐ Deactivate the transmitting of the port description. To do this, in the *Transmit port description* column, unmark the checkbox.
- ☐ Deactivate the transmitting of the system name. To do this, in the *Transmit system name* column, unmark the checkbox.

- ☐ Deactivate the transmitting of the system description. To do this, in the *Transmit system description* column, unmark the checkbox.
- ☐ Deactivate the transmitting of the system capabilities. To do this, in the *Transmit system capabilities* column, unmark the checkbox.
- ☐ Deactivate the transmitting of the management address. To do this, in the *Transmit management address* column, unmark the checkbox.
- ☐ Activate the transmitting of the Power over Ethernet information. To do this, in the *Transmit management address* column, mark the checkbox.
- ☐ Apply the settings temporarily. To do this, click the ✓ button.

`configure terminal`	To change to the Configuration mode.
`interface gigabitethernet 1/1`	To select the port interface `gigabitethernet 1/1`.
`lldp receive`	To specify the `receive` operation.
`no lldp receive`	To disable the `receive` operation.
`lldp transmit`	To specify the `transmit` operation.
`no lldp transmit`	To disable the `transmit` operation.
`lldp trap`	To activate the `trap` notification.
`no lldp trap`	To deactivate the `trap` notification.
`no lldp tlv-select port-description`	To deactivate the transmitting of the port description.
`lldp tlv-select port-description`	To activate the transmitting of the port description.
`no lldp tlv-select system-name`	To deactivate the transmitting of the system name.
`lldp tlv-select system-name`	To activate the transmitting of the system name.
`no lldp tlv-select system-description`	To deactivate the transmitting of the system description.
`lldp tlv-select system-description`	To activate the transmitting of the system description.
`no lldp tlv-select system-capabilities`	To deactivate the transmitting of the system capabilities.
`lldp tlv-select system-capabilities`	To activate the transmitting of the system capabilities.
`lldp med transmit-tlv poe`	To activate the transmitting of the Power over Ethernet information.
`no lldp med transmit-tlv poe`	To deactivate the transmitting of the Power over Ethernet information.
`end`	To quit the Configuration mode.

12.4.3 Displaying the discovery results

The device lets you display the topology discovery results.

Perform the following steps:

- ☐ Open the *Diagnostics > LLDP > Topology Discovery* dialog, *Neighbor* tab.
  The *Neighbor* tab displays the discovery results in the table.
- ☐ Open the *Diagnostics > LLDP > Topology Discovery* dialog, *Neighbor management* tab.
  The *Neighbor management* tab displays the discovery results in the table.
- ☐ Open the *Diagnostics > LLDP > Topology Discovery* dialog, *Statistics* tab.
  The *Statistics* tab displays the discovery results in the table.

`show lldp neighbors`	To display the status of the *LLDP* neighbors.
`show lldp statistics`	To display the *LLDP* Global and Port statistics.

12.4.4 Clearing the global statistics

Perform the following steps:

- ☐ Open the *Diagnostics > LLDP > Topology Discovery* dialog, *Statistics* tab.
  The *Statistics* tab displays the *Global* frame.
- ☐ In the *Global* frame, click the 🗑 *Clear global statistics* button.

`clear lldp statistics global`	To clear the *LLDP* Global statistics.

12.4.5 Clearing the port statistics

In the following example, you clear the port statistics for the port Gi 1/1.

Perform the following steps:

- ☐ Open the *Diagnostics > LLDP > Topology Discovery* dialog, *Statistics* tab.
  The *Statistics* tab displays the port statistics table below the *Global* frame.
- ☐ Select the port. To do this, in the table row for the port Gi 1/1, in the *Port* column, mark the checkbox.
- ☐ In the table below the *Global* frame, click the 🗑 *Clear global statistics* button.

`clear lldp statistics interface gigabitethernet 1/1`	To clear the *LLDP* Port statistics for the `interface gigabitethernet 1/1`.

12.5 RMON

Remote monitoring (RMON) allows various network agents and console systems to exchange network monitoring data.

The following RMON groups are supported:
- Event
- Alarm
- Statistics
- History

12.5.1 Configuring an RMON event

To configure an RMON event entry, perform the following steps:

- ☐ Open the *Diagnostics > RMON > Configuration* dialog, *Event* tab.
- ☐ Click the button.
  The dialog displays the *Create* window.
  - ☐ In the *Event ID* field, specify the event ID.
    Possible values:
    `1..65535`
  - ☐ In the *Event description* field, specify the description of the event.
  - ☐ In the *Event type* drop-down list, select the notification type when an event is triggered.
  - ☐ Click the *Ok* button.
- ☐ Apply the settings temporarily. To do this, click the ✓ button.

`configure terminal`	To change to the Configuration mode from the Privileged Exec mode.
`rmon event 5`	To specify the entry ID `5` for the event.
`rmon event 5 log trap`	To generate an event log entry and send an SNMP trap when an event is triggered.
`rmon event 5 log trap description <Event description>`	To specify the description of the event.
`no rmon event 5`	To remove the event entry ID `5`.
`end`	To return to the Privileged Exec mode.

12.5.2 Configuring an RMON alarm

To configure an RMON alarm entry, perform the following steps:

- ☐ Open the *Diagnostics > RMON > Configuration* dialog, *Alarm* tab.
- ☐ Click the button.
  The dialog displays the *Create* window.
  - ☐ In the *Alarm ID* field, specify the alarm ID.
    Possible values:
    `1..65535`
  - ☐ In the *Port* drop-down list, select the port number.
  - ☐ In the *Var name* drop-down list, select the variable name to be sampled.
  - ☐ In the *Sample type* drop-down list, select the sampling method of the selected variable.
  - ☐ In the *Interval [s]* field, specify the time in seconds for sampling and comparing the rising and falling threshold.
    Possible values:
    `1..2147483647`
  - ☐ In the *Rising threshold* field, specify the rising threshold value.
    Possible values:
    `-2147483648..2147483647`
  - ☐ In the *Falling threshold* field, specify the falling threshold value.
    Possible values:
    `-2147483648..2147483647`
  - ☐ In the *Rising event index* field, specify the index value from the event table to trigger the corresponding event when the rising threshold value is reached.
    Possible values:
    `0..65535`
    If the value is `0`, then no associated event generated as `0` is not a valid event index.
  - ☐ In the *Falling event index* field, specify the index value from the event table to trigger the corresponding event when the falling threshold value is reached.
    Possible values:
    `0..65535`
    If the value is `0`, then no associated event generated as `0` is not a valid event index.
  - ☐ In the *Startup type* drop-down list, select the condition to trigger an alarm.
  - ☐ Click the *Ok* button.
- ☐ Apply the settings temporarily. To do this, click the ✓ button.

`configure terminal`	To change to the Configuration mode from the Privileged Exec mode.
`rmon alarm 5 ifInOctets 1000002 10 delta rising-threshold 200000 5 falling-threshold 10000 4 both`	To configure the alarm entry ID `5` which samples a variable `ifInOctets` of interface index `1000002` using the `delta` sampling method. A sampling interval of `10` seconds for comparing the rising and falling threshold values along with event index value to trigger the event when the threshold value is reached.
`no rmon alarm 5`	To remove the alarm entry ID `5`.
`end`	To return to the Privileged Exec mode.

12.5.3 Configuring an RMON statistics entry

To configure an RMON statistics entry, perform the following steps:

- ☐ Open the *Diagnostics > RMON > Configuration* dialog, *Ether stats* tab.
- ☐ Click the ⊞ button.
  The dialog displays the *Create* window.
  - ☐ In the *Ether stats ID* field, specify the ether stats ID.
    Possible values:
    `1..65535`
  - ☐ In the *Port* drop-down list, select the port number.
  - ☐ Click the *Ok* button.
- ☐ Apply the settings temporarily. To do this, click the ✓ button.

`configure terminal`	To change to the Configuration mode from the Privileged Exec mode.
`interface GigabitEthernet 1/1`	To change to the interface configuration mode of interface `GigabitEthernet 1/1`.
`rmon collection stats 5`	To configure the RMON statistics entry ID `5`.
`no rmon collection stats 5`	To remove the statistics entry ID `5`.
`end`	To return to the Privileged Exec mode.

12.5.4 Configuring an RMON history

To configure an RMON history entry, perform the following steps:

- ☐ Open the *Diagnostics > RMON > Configuration* dialog, *History* tab.
- ☐ Click the ⊞ button.
  The dialog displays the *Create* window.
  - ☐ In the *History ID* field, specify the history ID.
    Possible values:
    `1..65535`
  - ☐ In the *Port* drop-down list, select the port number.
  - ☐ Click the *Ok* button.
- ☐ In the *Interval* field, specify the sampling interval time (seconds) of the history statistics data.
- ☐ In the *Bucket size* field, specify the maximum data entries stored in RMON.
- ☐ Apply the settings temporarily. To do this, click the ✓ button.

`configure terminal`	To change to the Configuration mode from the Privileged Exec mode.
`interface GigabitEthernet 1/1`	To change to the interface configuration mode of interface `GigabitEthernet 1/1`.
`rmon collection history 5`	To configure the RMON history entry ID `5`.

`rmon collection history 5 bucket 10`	To specify the maximum data entries stored in RMON.
`rmon collection history 5 bucket 10 interval 10`	To specify the sampling interval time (seconds) of the history statistics data.
`no rmon collection history 5`	To remove the history entry ID 5.
`end`	To return to the Privileged Exec mode.

12.5.5 Activating an SNMP trap

To activate an SNMP trap, perform the following steps:

- ☐ Open the *Diagnostics > RMON > Configuration* dialog.
- ☐ In the *Traps* frame, mark the *Rising alarm* checkbox to activate the sending of an SNMP trap when an alarm exceeds the rising threshold value.
- ☐ In the *Traps* frame, mark the *Falling alarm* checkbox to activate the sending of an SNMP trap when an alarm value is lower than the falling threshold value.
- ☐ Apply the settings temporarily. To do this, click the ✓ button.

`configure terminal`	To change to the Configuration mode from the Privileged Exec mode.
`snmp trap risingAlarm`	To activate the sending of an SNMP trap when an alarm exceeds the rising threshold value.
`snmp trap fallingAlarm`	To activate the sending of an SNMP trap when an alarm value is lower than the falling threshold value.
`end`	To return to the Privileged Exec mode.

12.6 Alarm

12.6.1 Configuring an Alarm entry

To create an alarm entry, perform the following steps:

- ☐ Open the *Diagnostics > Alarm* dialog.
- ☐ Click the ⊞ button.
  The dialog displays the *Create* window.
- ☐ In the *Name* field, specify the alarm name.
  Possible values:
  – Alphanumeric ASCII character string with 6..99 characters
- ☐ In the *Alarm parameter* drop-down list, select the port number for the alarm.
- ☐ In the *Parameter type* drop-down list, select the parameter to which the alarm relates.
- ☐ In the *Value type* drop-down list, select the value for the assigned *Parameter type*.
- ☐ Click the *Ok* button.
- ☐ Apply the settings temporarily. To do this, click the ✓ button.

`configure terminal`	To change to the Configuration mode from the Privileged Exec mode.
`alarm alarm.test1 port.status["GigabitEthernet 1/2"]@Speed=="speed1G"`	To specify the alarm name `alarm.test1` and expression `port.status["GigabitEthernet 1/2"]@Speed=="speed1G"` that defines the alarm. **Note:** An alarm name starts with `alarm.` followed by the name.
`no alarm alarm.test1`	To remove an alarm `alarm.test1`.
`end`	To return to the Privileged Exec mode.

12.6.2 Suppressing an Alarm using the Command Line Interface

To suppress an alarm, perform the following steps:

`configure terminal`	To change to the Configuration mode from the Privileged Exec mode.
`alarm suppress alarm.test1`	To suppress an alarm `alarm.test1`.
`exit`	To return to the Privileged Exec mode.

12.6.3 Enabling the Alarm status trap

To enable the alarm status trap, perform the following steps:

- ☐ Open the *Diagnostics > Alarm* dialog.
- ☐ In the *Operation* frame, select the *On* radio button to enable the sending of alarm trap if an alarm table row is added/modified/deleted.
- ☐ Apply the settings temporarily. To do this, click the ✓ button.

`configure terminal`	To change to the Configuration mode from the Privileged Exec mode.
`snmp trap alarmTrapStatus`	To enable the sending of alarm trap if an alarm table row is added/modified/deleted.
`end`	To return to the Privileged Exec mode.

12.6.4 Displaying the Alarm status

To display the alarm status, perform the following steps:

- ☐ Open the *Diagnostics > Alarm* dialog.
  The dialog displays the table containing the list of alarms and their status.

`show alarm status`	To display the list of alarms and their status.

13 Advanced functions of the device

This menu contains the following functions:

13.1 Using DNS on the device

The Domain Name System (DNS) function in the device queries the name servers to resolve host names and IPv4 addresses of the network devices. Much like a telephone book, the DNS converts the names of the devices into IPv4 addresses.

The device lets you set up the DNS from the DHCP server using the VLAN. The DNS provides the name server list, with space for 3 domain name server IPv4 addresses.

13.1.1 Configuring the DNS client

Perform the following steps:

- ☐ Open the *Advanced > DNS Client* dialog.
- ☐ To enable the *DNS-proxy*, in the *Operation* frame, *DNS-proxy* field, select the `On` radio button.
- ☐ To specify the administrative type `static`, in the *Operation* frame, *Default domain name source* field, select the value item `static`.
  The device enables the *Domain name* field.
  - ☐ To specify the static default domain name manually. In the *Domain name* field, specify the value `testdomain`.
  - ☐ Apply the settings temporarily. To do this, click the ✓ button.
- ☐ To specify the administrative type `dhcpv4-vlan`, in the *Operation* frame, *Default domain name source* field, select the value item `dhcpv4-vlan`.
  The device enables the *VLAN ID* field.
  - ☐ To specify the VLAN interface. In the *VLAN ID* field, enter the value `11`.
  - ☐ Apply the settings temporarily. To do this, click the ✓ button.

`configure terminal`	To change to the Configuration mode from the Privileged Exec mode.
`ip dns proxy`	To enable the DNS-proxy function on the device.
`no ip dns proxy`	To disable the DNS-proxy function on the device.
`ip domain name testdomain`	To specify the administrative type `static` with the static default domain name `testdomain`.
`ip domain name dhcp ipv4 interface vlan 11`	To specify the administrative type `dhcpv4 - vlan` using the interface VLAN `11`.
`end`	To return to the Privileged Exec mode.

Configure the name server. To do this, perform the following steps:

- ☐ Open the *Advanced > DNS Client* dialog.
  The dialog displays the name server table below the *Operation* frame.
- ☐ In the table row of the *Index* value `0`: To specify the administrative type *`static`*, in the *Default domain name source* field, select the value item *`static`*.
  The device enables the *IPv4 address* field.
  - ☐ To specify the static IPv4 address. In the *IPv4 address* field, enter the value `10.0.0.1`.
  - ☐ Apply the settings temporarily. To do this, click the ✓ button.
- ☐ In the table row of the *Index* value `1`: To specify the administrative type *`dhcpv4-vlan`*, in the *Default domain name source* field, select the value item *`dhcpv4-vlan`*.
  The device enables the *VLAN ID* field.
  - ☐ To specify the VLAN interface. In the *VLAN ID* field, enter the value `22`.
  - ☐ Apply the settings temporarily. To do this, click the ✓ button.

`configure terminal`	To change to the Configuration mode from the Privileged Exec mode.
`ip name-server 0 10.0.0.1`	To specify the administrative type `static` with the IPv4 address `10.0.0.1`, for the name server index value `0`.
`ip name-server 1 dhcp ipv4 interface vlan 22`	To specify the administrative type `dhcpv4 - vlan` with the interface VLAN `22`, for the name server index value `1`.
`end`	To return to the Privileged Exec mode.

A Setting up the configuration environment

A.1 HTTPS certificate

Your web browser establishes the connection to the device using the HTTPS protocol. The prerequisite is that you enable the *HTTPS* function in the *Device Security > Management Access > Server* dialog, *HTTP/HTTPS* tab. The default setting for HTTPS data connection is TCP port `443`.

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, like 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.1.1 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 create a new self-signed certificate on the device, perform the following steps:

- ☐ Open the *Device Security > Management Access > Server* dialog, *HTTP/HTTPS* tab.
- ☐ To create a self-signed X509/PEM certificate, in the *Certificate* frame, click the *Create* button.
- ☐ Apply the settings temporarily. To do this, click the ✓ button.

`configure terminal`	To change to the Configuration mode.
`no ip http secure-server`	To disable the HTTPS function.
`ip http secure-certificate generate`	To generate a self-signed X.509/PEM certificate.
`ip http secure-server`	To enable the HTTPS function.
`exit`	To quit the Configuration mode.

☐ The device also lets you transfer an externally generated X.509/PEM certificate onto the device:

- ☐ Open the *Device Security > Management Access > Server* dialog, *HTTP/HTTPS* tab.
- ☐ In the *Certificate import* frame, specify the TFTP or HTTP server path in the *URL* field.
- ☐ Click on the *Start* button to copy the certificate to the device.
- ☐ Apply the settings temporarily. To do this, click the ✓ button.

`configure terminal`	To change to the Configuration mode.
`no ip http secure-server`	To disable the HTTPS function.
`ip http secure-certificate upload <url_file>`	To upload a HTTPS certificate from the TFTP or HTTP server.
`ip http secure-server`	To enable the HTTPS function.
`exit`	To quit the Configuration mode.

B Appendix

B.1 Literature references

A small selection of books on network topics, ordered by publication date (newest first):

- *TCP/IP Illustrated, Volume 1: The Protocols (2nd Edition)* (in English)
  W. R. Stevens, Kevin R. Fall
  Addison Wesley, 2011
  ISBN 978-0-321-33631-6
- *Measurement, Control and Communication Using IEEE 1588* (in English)
  John C. Eidson
  Springer, 2006
  ISBN 978-1-84628-250-8 (Print), ISBN 978-1-84628-251-5 (eBook)
- *TCP/IP: Der Klassiker. Protokollanalyse. Aufgaben und Lösungen* (in German)
  W. R. Stevens
  Hüthig-Verlag, 2008
  ISBN 978-3-7785-4036-7
- *Optische Übertragungstechnik in der Praxis* (in German)
  Christoph Wrobel
  Hüthig-Verlag, 3rd edition, 2004
  ISBN 978-3-8266-5040-6

B.2 Maintenance

Hirschmann 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 Hirschmann product pages on the Internet at www.hirschmann.com.

B.3 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 `hm2PSState` (`OID` = `1.3.6.1.4.1.248.11.11.1.1.1.1.2`) 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 1.3.6.1.4.1.248.11.11.1.1.1.1.2.1` returns the response `0`, 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
IPv4 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 1.3.6.1.1.4.1.248...)
Octet String	ASCII character string
PSID	Power supply identifier (number of the power supply unit)
TimeTicks	Stopwatch, Elapsed time = numerical value / 10 ms numerical value = integer in the range 0..2^{32}-1
Timeout	Time value in 10 ms 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`.

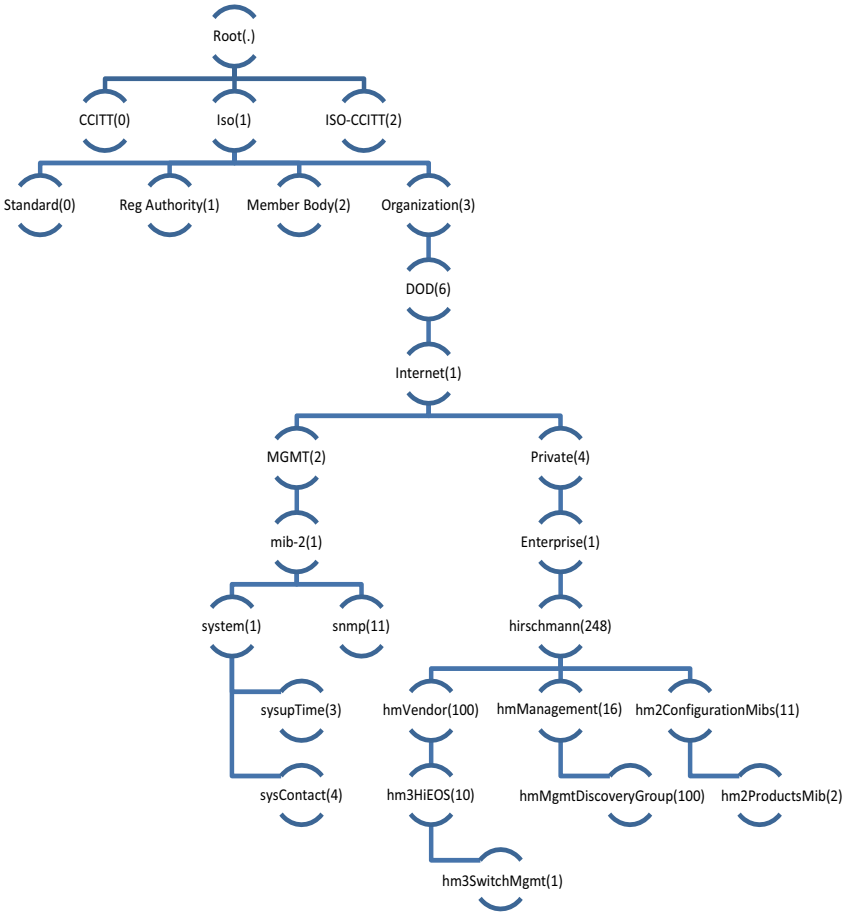


Figure 21: Tree structure of the Hirschmann private MIB

B.4 List of RFCs

RFC 1213	Management Information Base for Network Management of TCP/IP-based internets: MIB-II
RFC 1215	A Convention for Defining Traps for use with the SNMP
RFC 2131	Dynamic Host Configuration Protocol (Section 4.4)
RFC 2236	Internet Group Management Protocol, Version 2
RFC 2613	Remote Network Monitoring MIB Extensions for Switched Networks Version 1.0
RFC 2674	Definitions of Managed Objects for Bridges with Traffic Classes, Multicast Filtering and Virtual LAN Extensions
RFC 2819	Remote Network Monitoring Management Information Base (Group 1, 2, 3 and 9)
RFC 2863	The Interfaces Group MIB
RFC 3376	Internet Group Management Protocol, Version 3
RFC 3411	An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks
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 3621	Power Ethernet MIB
RFC 3635	Definitions of Managed Objects for the Ethernet-like Interface Types
RFC 3636	Definitions of Managed Objects for IEEE 802.3 Medium Attachment Units (MAUs)
RFC 4133	Entity MIB (Version 3)
RFC 4188	Definitions of Managed Objects for Bridges
RFC 4293	Management Information Base for the Internet Protocol (IP)
RFC 5519	Multicast Group Membership Discovery MIB

B.5 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 802.3	Ethernet
IEEE 802.3x	Flow Control
IEEE 802.3ad	Link Aggregation

B.6 Underlying IEC Norms

IEC 62443	Requirements including: ▶ The scope and boundaries of the system, in general terms in both a physical and logical way. ▶ The required capability security level (SL-C) of the product. ▶ Security privileges required to install, configure, operate, and maintain the product. ▶ Security considerations/actions associated with decommissioning the product (for example, wiping sensitive data).

B.7 Underlying ANSI Norms

ANSI/TIA-1057	Link Layer Discovery Protocol for Media Endpoint Devices, April 2006

B.8 Technical Data

13.1.2 Switching

Size of the MAC address table (incl. static filters)	8000
Max. number of statically configured MAC address filters	8000
Max. number of MAC address filters learnable through IGMP Snooping	8000
Number of priority queues	8
Port priorities that can be set	0..7
MTU (Max. allowed length of packets a port can receive or transmit)	10240 Bytes

13.1.3 VLAN

VLAN ID range	1..4095
Number of VLANs	max. 4095 simultaneously per device max. 4095 simultaneously per trunk port max. 1 per access port

B.9 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 dialog.

B.10 Abbreviations used

BOOTP	Bootstrap Protocol
CLI	Command Line Interface
DHCP	Dynamic Host Configuration Protocol
EUI	Extended Unique Identifier
FDB	Forwarding Database
GUI	Graphical User Interface
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
ICMP	Internet Control Message Protocol
IEEE	Institute of Electrical and Electronics Engineers
IGMP	Internet Group Management Protocol
IPv4	Internet Protocol Version 4
LED	Light Emitting Diode
LLDP	Link Layer Discovery Protocol
MAC	Media Access Control
MIB	Management Information Base
NMS	Network Management System
NTP	Network Time Protocol
OID	Object Identifier
PC	Personal Computer
QoS	Quality of Service
RFC	Request For Comment
RSTP	Rapid Spanning Tree Protocol
SFP	Small Form-factor Pluggable
SSH	Secure Shell
SNMP	Simple Network Management Protocol
STP	Spanning Tree Protocol
TCP	Transmission Control Protocol
TP	Twisted Pair
UDP	User Datagram Protocol
URL	Uniform Resource Locator
UTC	Coordinated Universal Time
VLAN	Virtual Local Area Network

C Index

D Further support

Technical questions

For technical questions, please contact any Hirschmann dealer in your area or Hirschmann directly. You find the addresses of our partners on the Internet at www.belden.com.

For technical support, visit hirschmann-support.belden.com. This site also includes a free of charge knowledge base and a software download section.

Technical Documents

The current manuals and operating instructions for Hirschmann products are available at doc.hirschmann.com.

Customer Innovation Center

The Customer Innovation Center is ahead of its competitors on three counts with its complete range of innovative services:

- Consulting incorporates comprehensive technical advice, from system evaluation through network planning to project planning.
- Training offers you an introduction to the basics, product briefing and user training with certification.
  You find the training courses on technology and products currently available at www.belden.com/solutions/customer-innovation-center.
- Support ranges from the first installation through the standby service to maintenance concepts.

With the Customer Innovation Center, you decide against any compromise in any case. Our client-customized package leaves you free to choose the service components you want to use.

E Readers' Comments

What is your opinion of this manual? We are constantly striving to provide as comprehensive a description of our product as possible, as well as important information to assist you in the operation of this product. Your comments and suggestions help us to further improve the quality of our documentation.

Your assessment of this manual:

	Very Good	Good	Satisfactory	Mediocre	Poor
Precise description	O	O	O	O	O
Readability	O	O	O	O	O
Understandability	O	O	O	O	O
Examples	O	O	O	O	O
Structure	O	O	O	O	O
Comprehensive	O	O	O	O	O
Graphics	O	O	O	O	O
Drawings	O	O	O	O	O
Tables	O	O	O	O	O

Did you discover any errors in this manual?
If so, on what page?

Suggestions for improvement and additional information:

General comments:

Sender:

Company / Department:

Name / Telephone number:

Street:

Zip code / City:

E-mail:

Date / Signature:

Dear User,

Please fill out and return this page
- as a fax to the number +49 (0)7127/14-1600 or
- per mail to
  Hirschmann Automation and Control GmbH
  Department IRD-NT
  Stuttgarter Str. 45-51
  72654 Neckartenzlingen
  Germany

HIRSCHMANN

A BELDEN BRAND