HIRSCHMANN

A **BELDEN** BRAND

Hirschmann Automation and Control GmbH

EESX   HiOS-2E   Rel. 07100

Reference Manuals

Graphical User Interface

Command Line Interface

User Manual

Configuration

Reference Manual

Graphical User Interface
Embedded Ethernet Switch eXtend
HiOS-2E

Contents

Contents

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 "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 "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 "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 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 an important fact or draws your attention to a dependency.
Courier	Representation of a CLI command or field contents in the graphical user interface

Key

Notes on the graphical user interface

The graphical user interface of the device is divided as follows:
- ▶ Navigation area
- ▶ Dialog area
- ▶ Buttons

Navigation area

The Navigation area is located on the left side of the graphical user interface.

The Navigation area contains the following elements:
- ▶ Toolbar
- ▶ Filter
- ▶ Menu

You have the option of collapsing the entire Navigation area, for example when displaying the graphical user interface on small screens. To collapse or expand, you click the small arrow at the top of the navigation area.

■ Toolbar

The toolbar at the top of the navigation area contains several buttons.
- – When you position the mouse pointer over a button, a tooltip displays further information.
- – If the connection to the device is lost, the toolbar is grayed out.

Button	Meaning
	The device automatically refreshes the toolbar information every 5 seconds. Clicking the button refreshes the toolbar manually.
	When you position the mouse pointer over the button, a tooltip displays the following information: ▶ *User:* Name of the logged in user ▶ *Device name:* Name of the device Clicking the button opens the *Device Security > User Management* dialog.
	When you position the mouse pointer over the button, a tooltip displays the summary of the *Diagnostics > System > Configuration Check* dialog. Clicking the button opens the *Diagnostics > System > Configuration Check* dialog.
	Clicking the button logs out the current user and displays the login page.
	Displays the remaining time in seconds until the device automatically logs out an inactive user. Clicking the button opens the *Device Security > Management Access > Web* dialog. There you can specify the timeout.
	This button is visible if the configuration profile in the volatile memory (RAM) differs from the "Selected" configuration profile in the non-volatile memory (NVM). Otherwise, the button is hidden. Clicking the button opens the *Basic Settings > Load/Save* dialog. By right-clicking the button you can save the current settings in the non-volatile memory (NVM).

Button	Meaning
ⓘ	When you position the mouse pointer over the button, a tooltip displays the following information: ▶ *Device Status:* This section displays a compressed view of the *Device status* frame in the *Basic Settings > System* dialog. The section displays the alarm that is currently active and whose occurrence was recorded first. ▶ *Security Status:* This section displays a compressed view of the *Security status* frame in the *Basic Settings > System* dialog. The section displays the alarm that is currently active and whose occurrence was recorded first. ▶ *Boot Parameter:* If you permanently save changes to the settings and at least one boot parameter differs from the configuration profile used during the last restart, then this section displays a note. The following settings cause the boot parameters to change: – *Basic Settings > Network* dialog, *MAC configuration* tab, *Local admin MAC address* parameter – *Basic Settings > External Memory* dialog, *Software auto update* parameter – *Basic Settings > External Memory* dialog, *Config priority* parameter – *Device Security > Management Access > Server* dialog, *SNMP* tab, *UDP port* parameter – *Diagnostics > System > Selftest* dialog, *RAM test* parameter – *Diagnostics > System > Selftest* dialog, *SysMon1 is available* parameter – *Diagnostics > System > Selftest* dialog, *Load default config on error* parameter Clicking the button opens the *Diagnostics > Status Configuration > Device Status* dialog.

■ Filter

The filter enables you to reduce the number of menu items in the menu. When filtering, the menu displays only menu items matching the search string entered in the filter field.

■ Menu

The menu displays the menu items.
You have the option of filtering the menu items. See section "Filter".

To display the corresponding dialog in the dialog area, you click the desired menu item. If the selected menu item is a node containing sub-items, then the node expands or collapses while clicking. The dialog area keeps the previously displayed dialog.

You have the option of expanding or collapsing every node in the menu at the same time. When you right-click anywhere in the menu, a context menu displays the following entries:
▶ *Expand*
Expands every node in the menu at the same time. The menu displays the menu items for every level.
▶ *Collapse*
Collapses every node in the menu at the same time. The menu displays the top level menu items.

Dialog area

The Dialog area is located on the rigth side of the graphical user interface. When you click a menu item in the Navigation area, the Dialog area displays the corresponding dialog.

■ Updating the display

If a dialog remains opened 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.

■ Saving the settings

☐ To transfer the changed settings to the volatile memory (RAM) of the device, click the ✓ button.
☐ To keep the changed settings, even after restarting the device, proceed as follows:
 ☐ Open the *Basic Settings > Load/Save* dialog.
 ☐ In the table, highlight the desired configuration profile.
 ☐ If in the *Selected* column the checkbox is `unmarked`, click the ☰ button and then the *Select* item.
 ☐ Click the ☰ button and then the *Save* item.

Note: Unintentional changes to the settings may terminate the connection between your PC and the device. To keep the device accessible, enable the *Undo configuration modifications* function in the *Basic Settings > Load/Save* dialog, before changing any settings. Using the function, the device continuously checks whether it can still be reached from the IP address of the user's PC. If the connection is lost, the device loads the configuration profile saved in the non-volatile memory (NVM) after the specified time. Afterwards, the device can be accessed again.

■ Working with tables

The dialogs display numerous settings in table form.

When you modify a table cell, the table cell displays a red mark in its top-left corner. The red mark indicates that your modifications are not yet transfered to the volatile memory (RAM) of the device.

You have the option of customizing the look of the tables to fit your needs. When you position the mouse pointer over a column header, the column header displays a drop-down list button. When you click this button, the drop-down list displays the following entries:

▶ Sort ascending
 Sorts the table entries in ascending order based on the entries of the selected column.
 You recognize sorted table entries by an arrow in the column header.

▶ Sort descending
 Sorts the table entries in descending order based on the entries of the selected column.
 You recognize sorted table entries by an arrow in the column header.

▶ Columns
 Displays or hides columns.
 You recognize hidden columns by an unmarked checkbox in the drop-down list.

▶ Filters
 The table only displays the entries whose content matches the specified filter criteria of the selected column.
 You recognize filtered table entries by an emphasized column header.

You have the option of selecting multiple table entries simultaneously and subsequently applying an action to them. This is useful when you are going to remove multiple table entries at the same time.

▶ Select several consecutive table entries:
  ☐ Click the first desired table entry to highlight it.
  ☐ Press and hold the <SHIFT> key.
  ☐ Click the last desired table entry to highlight every desired table entry.

▶ Select multiple individual table entries:
  ☐ Click the first desired table entry to highlight it.
  ☐ Press and hold the <CTRL> key.
  ☐ Click the next desired table entry to highlight it.
     Repeat until every desired table entry is highlighted.

Buttons

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

Button	Meaning
✔	Transfers the changes to the volatile memory (`RAM`) of the device and applies them to the device. To save the changes in the non-volatile memory, proceed as follows: ☐ Open the *Basic Settings > Load/Save* dialog. ☐ In the table, highlight the desired configuration profile. ☐ If in the *Selected* column the checkbox is `unmarked`, click the ☰ button and then the *Select* item. ☐ Click the 🖫 button to save your current changes.
🔄	Updates the fields with the values that are saved in the volatile memory (`RAM`) of the device.
🖫	Transfers the settings from the volatile memory (`RAM`) into the configuration profile designated as "Selected" in the non-volatile memory (`NVM`). If in the *Basic Settings > External Memory* dialog the checkbox in the *Backup config when saving* column is marked, then the device generates a copy of the configuration profile on the external memory.
☰	Displays a submenu with menu items corresponding to the respective dialog.
🪄	Opens the *Wizard* dialog.
🗏	Adds a new table entry.
🗏	Removes the highlighted table entry.
⑦	Opens the online help.

1 Basic Settings

The menu contains the following dialogs:
- ▶ System
- ▶ Network
- ▶ Software
- ▶ Load/Save
- ▶ External Memory
- ▶ Port
- ▶ Restart

1.1　System

In this dialog, you monitor individual operating statuses.

■ Device status

The fields in this frame display the device status and inform you about alarms that have occurred. When an alarm currently exists, the frame is highlighted.

You specify the parameters that the device monitors in the *Diagnostics > Status Configuration > Device Status* dialog.

Parameters	Meaning
Alarm counter	Displays the number of currently existing alarms.
ⓘ	The icon is visible if there is at least one currently existing alarm.
	When you position the mouse pointer over the icon, a tooltip displays the cause of the currently existing alarms and the time at which the device triggered the alarm.
	The device triggers an alarm if a monitored parameter differs from the desired status. The *Diagnostics > Status Configuration > Device Status* dialog, *Status* tab displays an overview of the alarms.

■ Security status

The fields in this frame display the security status and inform you about alarms that have occurred. When an alarm currently exists, the frame is highlighted.

You specify the parameters that the device monitors in the *Diagnostics > Status Configuration > Security Status* dialog.

Parameters	Meaning
Alarm counter	Displays the number of currently existing alarms.
ⓘ	The icon is visible if there is at least one currently existing alarm.
	When you position the mouse pointer over the icon, a tooltip displays the cause of the currently existing alarms and the time at which the device triggered the alarm.
	The device triggers an alarm if a monitored parameter differs from the desired status. The *Diagnostics > Status Configuration > Security Status* dialog, *Status* tab displays an overview of the alarms.

■ Signal contact status

The fields in this frame display the signal contact status and inform you about alarms that have occurred. When an alarm currently exists, the frame is highlighted.

You specify the parameters that the device monitors in the *Diagnostics > Status Configuration > Signal Contact > Signal Contact 1/Signal Contact 2* dialog.

Parameters	Meaning
Alarm counter	Displays the number of currently existing alarms.
ⓘ	The icon is visible if there is at least one currently existing alarm.
	When you position the mouse pointer over the icon, a tooltip displays the cause of the currently existing alarms and the time at which the device triggered the alarm.
	The device triggers an alarm if a monitored parameter differs from the desired status. The *Diagnostics > Status Configuration > Signal Contact > Signal Contact 1/Signal Contact 2* dialog, *Status* tab displays an overview of the alarms.

■ System data

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

Parameters	Meaning
System name	Specifies the name for which the device is known in the network.
	Possible values: ▶ Alphanumeric ASCII character string with 0..255 characters The following characters are allowed: – `0..9` – `a..z` – `A..Z` – `!#$%&'()*+,-./:;<=>?@[\\]^_`{}~` – `<device name>-<MAC address>` (default setting)
	When creating HTTPS X.509 certificates, the application generating the certificate uses the specified value as the domain name and common name.
	The following functions use the specified value as a host name or FQDN (Fully Qualified Domain Name). For compatibility, it is recommended to use only small letters, since not every system compares the case in the FQDN. Verify that this name is unique in the whole network. ▶ DHCP client ▶ *Syslog* ▶ *IEC61850-MMS*
Location	Specifies the location of the device.
	Possible values: ▶ Alphanumeric ASCII character string with 0..255 characters
Contact person	Specifies the contact person for this device.
	Possible values: ▶ Alphanumeric ASCII character string with 0..255 characters
Device type	Displays the product name of the device.
Power supply 1 Power supply 2	Displays the status of the power supply unit on the relevant voltage supply connection.
	Possible values: ▶ `present` ▶ `defective` ▶ `notInstalled` ▶ `unknown`
Uptime	Displays the time that has elapsed since this device was last restarted.
	Possible values: ▶ Time in the format `day(s), ...h ...m ...s`
Temperature [°C]	Displays the current temperature in the device in °C.
	You activate the monitoring of the temperature thresholds in the *Diagnostics > Status Configuration > Device Status* dialog.
Upper temp. limit [°C]	Specifies the upper temperature threshold in °C.
	The "Installation" user manual contains detailed information about setting the temperature thresholds.
	Possible values: ▶ `-99..99` (integer) If the temperature in the device exceeds this value, the device generates an alarm.
Lower temp. limit [°C]	Specifies the lower temperature threshold in °C.
	The "Installation" user manual contains detailed information about setting the temperature thresholds.
	Possible values: ▶ `-99..99` (integer) If the temperature in the device falls below this value, the device generates an alarm.

■ Port status

This frame displays a simplified view of the ports of the device at the time of the last update.

The icons represent the status of the individual ports. In some situations, the following icons interfere with one another. When you position the mouse pointer over the appropriate port icon, a tooltip displays a detailed information about the port state.

Parameters	Status	Meaning
`<Port number>`		The port is inactive. The port does not send or receive any data.
		The port is inactive. The cable is connected. Active link.
		The port is active. No cable connected or no active link.
		The port is active. The cable is connected. Connection okay. Active link. Full-duplex mode
		The half-duplex mode is enabled. Verify the settings in the *Basic Settings > Ports* dialog, *Configuration* tab.
		The port is in a blocking state due to a redundancy function.
		The port operates as a router interface.

■ Buttons

You find the description of the standard buttons in section "Buttons" on page 16.

1.2   Network

This dialog allows you to specify the IP, VLAN and HiDiscovery settings required for the access to the device management through the network.

The dialog contains the following tabs:
▶ [Global]
▶ [MAC configuration]

[Global]

This dialog allows you to specify the IP, VLAN and HiDiscovery settings.

■ Management interface

This frame allows you to specify the following settings:
▶ The source from which the device management receives its IP parameters
▶ VLAN in which the management can be accessed

Parameters	Meaning
IP address assignment	Specifies the source from which the device receives its IP parameters after starting: Possible values: ▶ `Local` (default setting) The device uses the IP parameters from the internal memory. You specify the settings for this in the *IP parameter* frame. ▶ `BOOTP` The device receives its IP parameters from a BOOTP or DHCP server. The server evaluates the MAC address of the device, then assigns the IP parameters. ▶ `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. **Note:** If there is no response from the BOOTP or DHCP server, the device sets the IP address to `0.0.0.0` and makes another attempt to obtain a valid IP address.
VLAN ID	Specifies the VLAN in which the device management is accessible through the network. The device management is accessible through ports that are members of this VLAN. Possible values: ▶ `1..4042` (default setting: `1`) The prerequisite is that the VLAN is already configured. See the *Switching > VLAN > Configuration* dialog. When you click the ✓ button after changing the value, the *Information* window opens. Select the port, over which you connect to the device in the future. After clicking the *Ok* button, the new management VLAN settings are assigned to the port. – After that the port is a member of the VLAN and transmits the data packets without a VLAN tag (untagged). See the *Switching > VLAN > Configuration* dialog. – The device assigns the port VLAN ID of the management VLAN to the port. See the *Switching > VLAN > Port* dialog. After a short time the device is reachable over the new port in the new management VLAN.
MAC address	Displays the MAC address of the device. The device management is accessible via the network using the MAC address.

■ BOOTP/DHCP

Parameters	Meaning
Client ID	Displays the DHCP client ID that the device sends to the BOOTP or DHCP server. If the server is configured accordingly, it reserves an IP address for this DHCP client ID. Therefore, the device receives the same IP from the server every time it requests it. The DHCP client ID that the device sends is the device name specified in the *System name* field in the *Basic Settings > System* dialog.

■ **HiDiscovery protocol v1/v2**

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

On a PC, the HiDiscovery software displays the Hirschmann devices that can be accessed in 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 HiDiscovery software allows you to assign or change the IP parameters in the device.

Parameters	Meaning

Operation	Enables/disables the HiDiscovery function on the device.
	
	Possible values:
	▶ `On` (default setting)
	  HiDiscovery is enabled.
	  You can use the HiDiscovery software to access the device from your PC.
	▶ `Off`
	  HiDiscovery is disabled.

Access	Enables/disables the write access to the device using HiDiscovery.
	
	Possible values:
	▶ `readWrite` (default setting)
	  The HiDiscovery software is given write access to the device.
	  With this setting you can change the IP parameters in the device.
	▶ `readOnly`
	  The HiDiscovery software is given read-only access to the device.
	  With this setting you can view the IP parameters in the device.
	
	Recommendation: Change the setting to `readOnly` exclusively after putting the device into operation.

Signal	Activates/deactivates the flashing of the port LEDs as does the function of the same name in the HiDiscovery software. The function allows you to 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.

Note: With the HiDiscovery software you access the device through ports that are members of the same VLAN as the device management exclusively. You specify which VLAN a certain port is assigned to in the *Switching > VLAN > Configuration* dialog.

■ **IP parameter**

This frame allows you to assign the IP parameters manually. These fields can be edited if you have selected the `Local` radio button in the *Management interface* frame, *IP address assignment* option list.

Parameters	Meaning
IP address	Specifies the IP address under which the device management can be accessed through the network. Possible values: ▶ Valid IPv4 address (default setting: `192.168.1.1`)
Netmask	Specifies the netmask. The netmask identifies the network prefix and the host address of the device in the IP address. Possible values: ▶ Valid IPv4 netmask (default setting: `255.255.255.0`)
Gateway address	Specifies the IP address of a router through which the device accesses other devices outside its own network. Possible values: ▶ Valid IPv4 address

■ **Buttons**

You find the description of the standard buttons in section .

[MAC configuration]

With the default values, the management access is possible through every port. This tab allows you to restrict the management access through one port exclusively. In addition, you have the option of adding a user-specified MAC address to the management.

■ Configuration

Parameters	Meaning
Local admin MAC address	Specifies a user-defined MAC address with which the device management can be accessed. If the value entered here differs from the default setting, the device uses this MAC address after a restart.
	Possible values: ▶ Valid Unicast MAC address (default setting: `00:00:00:00:00:00`) Enter the value in one of the following formats: – without a separator, for example `001122334455` – separated by spaces, for example `00 11 22 33 44 55` – separated by colons, for example `00:11:22:33:44:55` – separated by hyphens, for example `00-11-22-33-44-55` – separated by points, for example `00.11.22.33.44.55` – separated by points after every 4th character, for example `0011.2233.4455`
	Note: Save the changes to this field in the non-volatile memory before you restart the device.
Management port	Specifies the port through which the device management can be accessed through the network.
	Possible values: ▶ `All` (default setting) The device management can be accessed through every port. ▶ `<Port number>` The device management is only accessible through the selected port.

■ Information

Parameters	Meaning
Burned in MAC address	Displays the MAC address of the device specified by the manufacturer.
MAC address type	Displays the MAC address with which the device can be accessed: ▶ `burned-in` The device management is accessible with the MAC address specified by the manufacturer. ▶ `local` The device management is accessible with the user-defined MAC address specified in the ***Configuration*** frame.
Currently used MAC address	Displays the MAC address with which the device management can be accessed.

■ Buttons

You find the description of the standard buttons in section "Buttons" on page 16.

1.3   Software

This dialog allows you to update the device software and display information about the device software.
You also have the option to restore a backup of the device software saved in the device.

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

■ Version

Parameters	Meaning
Stored version	Displays the version number and creation date of the device software stored in the flash memory. The device loads the device software during the next restart.
Running version	Displays the version number and creation date of the device software that the device loaded during the last restart and is currently running.
Backup version	Displays the version number and creation date of the device software saved as a backup in the flash memory. The device copied this device software into the backup memory during the last software update or after you clicked the *Restore* button.
Restore	Restores the device software saved as a backup. In the process, the device changes the *Stored version* and the *Backup version* of the device software. Upon restart, the device loads the *Stored version*.
Bootcode	Displays the version number and creation date of the boot code.

■ Software update

Parameters	Meaning
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
	
	If the file is located on your PC or on a network drive, drag and drop the file in the ⬆ area.
	Alternatively click in the area to select the file.
	▶ Software update from an FTP server
	If the file is located on an FTP server, specify the URL for the file in the following form:
	`ftp://<user>:<password>@<IP address>:<port>/<file name>`
	▶ Software update from a TFTP server
	If the file is located on a TFTP server, specify the URL for the file in the following form:
	`tftp://<IP address>/<path>/<file name>`
	▶ Software update from an SCP or SFTP server
	If the file is located on an SCP or SFTP server, specify the URL for the file in one of the following forms:
	– `scp://` or `sftp://<IP address>/<path>/<file name>`
	   When you click the *Start* button, the device displays the *Credentials* window. There you enter *User name* and *Password*, to log on to the server.
	– `scp://` or `sftp://<user>:<password>@<IP address>/<path>/<file name>`

Start	Updates the device software. The device installs the selected file in the flash memory, replacing the previously saved device software. Upon restart, the device loads the installed device software. The device copies the existing software into the backup memory. To remain logged in to the device during the software update, move the mouse pointer occasionally. Alternatively, specify a sufficiently high value in the *Device Security > Management Access > Web* dialog, field *Web interface session timeout [min]* before the software update.

Alternatively, the device allows you to update the device software by right-clicking in the table if the image file is located in the external memory.

■ **Table**

Parameters	Meaning
File location	Displays the storage location of the device software.
	Possible values: ▶ `ram` 　Volatile memory of the device ▶ `flash` 　Non-volatile memory (`NVM`) of the device ▶ `sd-card` 　External SD memory (ACA31)
Index	Displays the index of the device software. For the device software in the flash memory, the index has the following meaning: ▶ `1` 　Upon restart, the device loads this device software. ▶ `2` 　The device copied this device software into the backup area during the last software update.
File name	Displays the device-internal file name of the device software.
Firmware	Displays the version number and creation date of the device software.

■ **Buttons**

You find the description of the standard buttons in section .

1.4 Load/Save

This dialog allows you to save the device settings permanently in a configuration profile.

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

In the default setting, the device saves the configuration profiles unencrypted. When you enter a password in the *Configuration encryption* frame, the device saves both the current and the future configuration profiles in an encrypted format.

Unintentional changes to the settings may terminate the connection between your PC and the device. To keep the device accessible, enable the *Undo configuration modifications* function before changing any settings. If the connection is lost, the device loads the configuration profile saved in the non-volatile memory (NVM) after the specified time.

■ External memory

Parameters	Meaning
Selected external memory	Displays the type of the external memory.
	Possible values: ▶ `sd` External SD memory (ACA31)
Status	Displays the operating state of the external memory.
	Possible values: ▶ `notPresent` No external memory connected. ▶ `removed` Someone has removed the external memory from the device during operation. ▶ `ok` The external memory is connected and ready for operation. ▶ `outOfMemory` The memory space is occupied on the external memory. ▶ `genericErr` The device has detected an error.

■ Configuration encryption

Parameters	Meaning
Active	Displays whether the configuration encryption is active/inactive on the device.
	Possible values: ▶ `marked` The configuration encryption is active. The device loads a configuration profile from the non-volatile memory (NVM) if it is encrypted and the password matches the password stored in the device. ▶ `unmarked` The configuration encryption is inactive. The device loads a configuration profile from the non-volatile memory solely (NVM) if it is unencrypted.
	If in the *Basic Settings > External Memory* dialog, the *Config priority* column has the value `first` and the configuration profile is unencrypted, the *Security status* frame in the *Basic Settings > System* dialog displays an alarm.
	In the *Diagnostics > Status Configuration > Security Status* dialog, *Global* tab, *Monitor* column you specify whether the device monitors the *Load unencrypted config from external memory* parameter.

Parameters	Meaning
Set password	Opens the *Set password* window that helps you to enter the password needed for the configuration profile encryption. Encrypting the configuration profiles makes unauthorized access more difficult. ☐ When you are changing an existing password, enter the existing password in the *Old password* field. To display the password in plain text instead of ***** (asterisks), mark the *Display content* checkbox. ☐ In the *New password* field, enter the password. To display the password in plain text instead of ***** (asterisks), mark the *Display content* checkbox. ☐ Mark the *Save configuration afterwards* checkbox to use encryption also for the Selected configuration profile in the non-volatile memory (NVM) and in the external memory. **Note:** Use this function solely if a maximum of 1 configuration profile is stored in the non-volatile memory (NVM) of the device. Before creating additional configuration profiles, decide for or against permanently activated configuration encryption in the device. Save additional configuration profiles either unencrypted or encrypted with the same password. If you are replacing a device with an encrypted configuration profile, for example due to a defect, you proceed as follows: ☐ Restart the new device and assign the IP parameters. ☐ Open the *Basic Settings > Load/Save* dialog on the new device. ☐ Encrypt the configuration profile in the new device. See above. Enter the same password you used in the defective device. ☐ Install the external memory from the defective device in the new device. ☐ Restart the new device. When it is restarted, the device loads the configuration profile with the settings of the defective device from the external memory. The device copies the settings into the volatile memory (RAM) and into the non-volatile memory (NVM).
Delete	Opens the *Delete* window which helps you to cancel the configuration encryption in the device. ☐ In the *Old password* field, enter the existing password. To display the password in plain text instead of ***** (asterisks), mark the *Display content* checkbox. ☐ Mark the *Save configuration afterwards* checkbox to remove the encryption also for the Selected configuration profile in the non-volatile memory (NVM) and in the external memory. **Note:** If you keep additional encrypted configuration profiles in the memory, the device helps prevent you from activating or designating these configuration profiles as "Selected".

■ **Information**

Parameters	Meaning
NVM in sync with running config	Displays whether the configuration profile in the volatile memory (RAM) and the "Selected" configuration profile in the non-volatile memory (NVM) are the same. Possible values: ▶ marked The configuration profiles are the same. ▶ unmarked The configuration profiles differ.
External memory in sync with NVM	Displays whether the "Selected" configuration profile in the external memory and the "Selected" configuration profile in the non-volatile memory (NVM) are the same. Possible values: ▶ marked The configuration profiles are the same. ▶ unmarked The configuration profiles differ. Possible causes: – No external memory is connected to the device. – In the *Basic Settings > External Memory* dialog, the *Backup config when saving* function is disabled.

■ Backup config on a remote server when saving

Parameters	Meaning
Operation	Enables/disables the *Backup config on a remote server when saving* function.
	Possible values:
	▶ `Enabled`
	The *Backup config on a remote server when saving* function is enabled.
	When you save the configuration profile in the non-volatile memory (`NVM`), the device automatically backs up the configuration profile on the remote server specified in the *URL* field.
	▶ `Disabled` (default setting)
	The *Backup config on a remote server when saving* function is disabled.
URL	Specifies path and file name of the backed up configuration profile on the remote server.
	Possible values:
	▶ Alphanumeric ASCII character string with 0..128 characters
	Example: `tftp://192.9.200.1/cfg/config.xml`
	The device supports the following wildcards:
	– `%d`
	System date in the format `YYYY-mm-dd`
	– `%t`
	System time in the format `HH_MM_SS`
	– `%i`
	IP address of the device
	– `%m`
	MAC address of the device in the format `AA-BB-CC-DD-EE-FF`
	– `%p`
	Product name of the device
Set credentials	Opens the *Credentials* window which helps you to enter the credentials needed to authenticate on the remote server.
	☐ In the *User name* field, enter the user name.
	To display the user name in plain text instead of ***** (asterisks), mark the *Display content* checkbox.
	Possible values:
	– Alphanumeric ASCII character string with 1..32 characters
	☐ In the *Password* field, enter the password.
	To display the password in plain text instead of ***** (asterisks), mark the *Display content* checkbox.
	Possible values:
	▶ Alphanumeric ASCII character string with 6..64 characters
	The following characters are allowed:
	`a..z`
	`A..Z`
	`0..9`
	`` !#$%&'()*+,-./:;<=>?@[\\]^_`{}~ ``

■ **Undo configuration modifications**

Parameters	Meaning
Operation	Enables/disables the *Undo configuration modifications* function. Using the function, the device continuously checks whether it can still be reached from the IP address of the user's PC. If the connection is lost, after a specified time period the device loads the "Selected" configuration profile from the non-volatile memory (NVM). Afterwards, the device can be accessed again. Possible values: ▶ On 　The function is enabled. 　– You specify the time period between the loss of the connection and the loading of the configuration profile in the field *Timeout [s] to recover after connection loss*. 　– If the non-volatile memory (NVM) contains multiple configuration profiles, the device loads the configuration profile designated as "Selected". ▶ Off (default setting) 　The function is disabled. 　Disable the function again before you close the graphical user interface. You thus prevent the device from restoring the configuration profile designated as "Selected". **Note:** Before you enable the function, save the settings in the configuration profile. Current changes, that are saved temporarily, are therefore maintained in the device.
Timeout [s] to recover after connection loss	Specifies the time in seconds after which the device loads the "Selected" configuration profile from the non-volatile memory (NVM) if the connection is lost. Possible values: ▶ 30..600 (default setting: 600) Specify a sufficiently large value. Take into account the time when you are viewing the dialogs of the graphical user interface without changing or updating them.
Watchdog IP address	Displays the IP address of the PC on which you have enabled the function. Possible values: ▶ IPv4 address (default setting: 0.0.0.0)

■ **Table**

Parameters	Meaning
Storage type	Displays the storage location of the configuration profile. Possible values: ▶ RAM (volatile memory of the device) 　In the volatile memory, the device stores the settings for the current operation. ▶ NVM (non-volatile memory of the device) 　From the non-volatile memory, the device loads the "Selected" configuration profile during a restart or when applying the function *Undo configuration modifications*. 　The non-volatile memory provides space for multiple configuration profiles, depending on the number of settings saved in the configuration profile. The device manages a maximum of 20 configuration profiles in the non-volatile memory. 　You can load a configuration profile into the volatile memory (RAM): 　☐ In the table, highlight the configuration profile. 　☐ Click the ▤ button and then the *Activate* item. ▶ ENVM (external memory) 　On the external memory, the device saves a backup copy of the "Selected" configuration profile. The prerequisite is that in the *Basic Settings > External Memory* dialog you mark the *Backup config when saving* checkbox.

Parameters	Meaning
Profile name	Displays the name of the configuration profile.
	Possible values: ▶ `running-config` Name of the configuration profile in the volatile memory (`RAM`). ▶ `config` Name of the factory setting configuration profile in the non-volatile memory (`NVM`). ▶ User-defined name The device allows you to save a configuration profile with a user-specified name by highlighting an existing configuration profile in the table, clicking the ▤ button and then the *Save As..* item.
	To export the configuration profile as an XML file on your PC, click the link. Then you select the storage location and specify the file name.
	To save the file on a remote server, click the ▤ button and then the *Export...* item.
Modification date (UTC)	Displays the time (UTC) at which a user last saved the configuration profile.
Selected	Displays whether the configuration profile is designated as "Selected".
	Possible values: ▶ `marked` The configuration profile is designated as "Selected". – The device loads the configuration profile into the volatile memory (`RAM`) during a restart or when applying the function *Undo configuration modifications*. – When you click the 🖫 button, the device saves the temporarily saved settings in this configuration profile. ▶ `unmarked` Another configuration profile is designated as "Selected".
	To designate another configuration profile as "Selected", you highlight the desired configuration profile in the table, click the ▤ button and then the *Activate* item.
Encrypted	Displays whether the configuration profile is encrypted.
	Possible values: ▶ `marked` The configuration profile is encrypted. ▶ `unmarked` The configuration profile is unencrypted.
	You activate/deactivate the encryption of the configuration profile in the *Configuration encryption* frame.
Encryption verified	Displays whether the password of the encrypted configuration profile matches the password stored in the device.
	Possible values: ▶ `marked` The passwords match. The device is able to unencrypt the configuration profile. ▶ `unmarked` The passwords are different. The device is unable to unencrypt the configuration profile.
Software version	Displays the version number of the device software that the device ran when it saved the configuration profile.
Fingerprint	Displays the checksum saved in the configuration profile. The device calculates the checksum when saving the settings and inserts it into the configuration profile.

Parameters	Meaning
Fingerprint verified	Displays whether the checksum saved in the configuration profile is valid.
	The device calculates the checksum of the configuration profile marked as "Selected" and compares it with the checksum saved in this configuration profile.

	Possible values:
	▶ `marked`
	  The calculated and the saved checksum match.
	  The saved settings are consistent.
	▶ `unmarked`
	  For the configuration profile marked as "Selected" applies:
	  The calculated and the saved checksum are different.
	  The configuration profile contains modified settings.
	  Possible causes:
	  – The file is damaged.
	  – The file system on the external memory is inconsistent.
	  – A user has exported the configuration profile and changed the XML file outside the device.
	  For the other configuration profiles the device has not calculated the checksum.

	The device verifies the checksum correctly only if the configuration profile has been saved before as follows: – on an identical device – with the same software version, which the device is running
	Note: This function identifies changes to the settings in the configuration profile. The function does not provide protection against operating the device with modified settings.

■ Buttons

You find the description of the standard buttons in section "Buttons" on page 16.

Button	Meaning
	Removes the configuration profile highlighted in the table from the non-volatile memory (`NVM`) or from the external memory.
	If the configuration profile is designated as "Selected", the device helps prevent you from removing the configuration profile.
	Transfers the settings from the volatile memory (`RAM`) into the configuration profile designated as "Selected" in the non-volatile memory (`NVM`).
	If in the *Basic Settings > External Memory* dialog the checkbox in the *Backup config when saving* column is marked , the device generates a copy of the configuration profile on the external memory.
Save As..	Copies the configuration profile highlighted in the table and saves it with a user-specified name in the non-volatile memory (`NVM`). The device designates the new configuration profile as "Selected".
	Note: Before creating additional configuration profiles, decide for or against permanently activated configuration encryption in the device. Save additional configuration profiles either unencrypted or encrypted with the same password.
	If in the *Basic Settings > External Memory* dialog the checkbox in the *Backup config when saving* column is marked, the device designates the configuration profile of the same name on the external memory as "Selected".

Button	Meaning
Activate	Loads the settings of the configuration profile highlighted in the table to the volatile memory (RAM).
	▶ The device terminates the connection to the graphical user interface.
	☐ Reload the graphical user interface.
	☐ Login again.
	▶ The device immediately uses the settings of the configuration profile on the fly.
	Enable the *Undo configuration modifications* function before you activate another configuration profile. If the connection is lost afterwards, the device loads the last configuration profile designated as "Selected" from the non-volatile memory (NVM). The device can then be accessed again.
	If the configuration encryption is inactive, the device loads the configuration profile if it is unencrypted. If the configuration encryption is active, the device loads the configuration profile if it is encrypted and the password matches the password stored in the device.
	When you activate an older configuration profile, the device takes over the settings of the functions contained in this software version. The device sets the values of new functions to their default value.
Select	Designates the configuration profile highlighted in the table as "Selected". In the *Selected* column, the checkbox is then marked.
	The device loads the settings of this configuration profile to the volatile memory (RAM) during a restart or when applying the function *Undo configuration modifications*.
	▶ Designate an unencrypted configuration profile only as "Selected" when the configuration encryption in the device is disabled.
	▶ Designate an encrypted configuration profile only as "Selected" when the following prerequisites are fulfilled:
	– The configuration encryption in the device is enabled.
	– The password of the configuration profile matches the password saved in the device.
	Otherwise, the device is unable to load and encrypt the settings in the configuration profile the next time it restarts. For this case you specify in the *Diagnostics > System > Selftest* dialog whether the device starts with the default settings or terminates the restart and stops.
	Note: You only mark the configuration profiles saved in the non-volatile memory (NVM).
	If in the *Basic Settings > External Memory* dialog the checkbox in the *Backup config when saving* column is marked, the device designates the configuration profile of the same name on the external memory as "Selected".

Button	Meaning
Import...	Opens the *Import...* window to import a configuration profile. The prerequisite is that you have exported the configuration profile using the *Export...* button or using the link in the *Profile name* column. ☐ In the *Select source* drop-down list, select from where the device imports the configuration profile. ▶ PC/URL The device imports the configuration profile from the local PC or from a remote server. ▶ External memory The device imports the configuration profile from the external memory. ☐ If PC/URL is selected above, then in the *Import profile from PC/URL* frame you specify the configuration profile file to be imported. – Import from the PC If the file is located on your PC or on a network drive, drag and drop the file in the ⬆ area. Alternatively click in the area to select the file. – Import from an FTP server If the file is located on an FTP server, specify the URL for the file in the following form: ftp://<user>:<password>@<IP address>:<port>/<file name> – Import from a TFTP server If 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 SCP or SFTP server If the file is located on an SCP or SFTP server, specify the URL for the file in one of the following forms: scp:// or sftp://<IP address>/<path>/<file name> When you click the *Start* button, the device displays the *Credentials* window. There you enter *User name* and *Password*, to log on to the server. scp:// or sftp://<user>:<password>@<IP address>/<path>/<file name> ☐ If External memory is selected above, then in the *Import profile from external memory* frame you specify the configuration profile file to be imported. In the *Profile name* drop-down list, select the name of the configuration profile to be imported. ☐ In the *Destination* frame you specify where the device saves the imported configuration profile. In the *Profile name* field you specify the name under which the device saves the configuration profile. In the *Storage type* field you specify the storage location for the configuration profile. The prerequisite is that in the *Select source* drop-down list you have selected the value PC/URL. ▶ RAM The device saves the configuration profile in the volatile memory (RAM) of the device. This replaces the running-config, the device uses the settings of the imported configuration profile immediately. The device terminates the connection to the graphical user interface. Reload the graphical user interface. Login again. ▶ NVM The device saves the configuration profile in the non-volatile memory (NVM) of the device. When you import a configuration profile, the device takes over the settings as follows: – If the configuration profile was exported on the same device or on an identically equipped device of the same type: The device takes over the settings completely. – If the configuration profile was exported on an other device: 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. Regarding configuration profile encryption, also read the help text of the *Configuration encryption* frame. The device imports a configuration profile under the following conditions: – The configuration encryption of the device is inactive. The configuration profile is unencrypted. – The configuration encryption of the device is active. The configuration profile is encrypted with the same password that the device currently uses.

Button	Meaning

Export...	Exports the configuration profile highlighted in the table and saves it as an XML file on a remote server.
	To save the file on your PC, click the link in the *Profile name* column to select the storage location and specify the file name.
	
	The device gives you the following options for exporting a configuration profile:
	▶ Export to an FTP server
	To save the file on an FTP server, specify the URL for the file in the following form:
	`ftp://<user>:<password>@<IP address>:<port>/<file name>`
	▶ 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 SCP or SFTP server
	To save the file on an SCP or SFTP server, specify the URL for the file in one of the following forms:
	– `scp://` or `sftp://<IP address>/<path>/<file name>`
	When you click the *Ok* button, the device displays the *Credentials* window. There you enter *User name* and *Password*, to log on to the server.
	– `scp://` or `sftp://<user>:<password>@<IP address>/<path>/<file name>`

Load running-config as script	Imports a script file which modifies the current `running config` configuration profile.
	
	The device gives you the following options to import a script file:
	▶ Import from the PC
	
	If the file is located on your PC or on a network drive, drag and drop the file in the ⬆ area.
	Alternatively click in the area to select the file.
	▶ Import from an FTP server
	If the file is located on an FTP server, specify the URL for the file in the following form:
	`ftp://<user>:<password>@<IP address>:<port>/<file name>`
	▶ Import from a TFTP server
	If 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 SCP or SFTP server
	If the file is located on an SCP or SFTP server, specify the URL for the file in one of the following forms:
	`scp://` or `sftp://<IP address>/<path>/<file name>`

Save running-config as script	Saves the `running config` configuration profile as a script file on the local PC. This allows you to backup your current device settings or to use them on various devices.
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`). ▶ The device deletes the HTTPS certificate used by the web server in the device. ▶ The device deletes the RSA key (Host Key) used by the SSH server in the device. ▶ If an external memory is connected, the device deletes the configuration profiles saved on the external memory. ▶ After a brief period, the device reboots and loads the default values.
Back to default	Deletes the current operating (`running config`) settings from the volatile memory (`RAM`).

1.5 External Memory

This dialog allows you to activate functions that the device automatically executes in combination with the external memory. The dialog also displays the operating state and identifying characteristics of the external memory.

■ Table

Parameters	Meaning
Type	Displays the type of the external memory.
	Possible values: ▶ `sd` External SD memory (ACA31)
Status	Displays the operating state of the external memory.

	Possible values:
	▶ `notPresent`
	  No external memory connected.
	▶ `removed`
	  Someone has removed the external memory from the device during operation.
	▶ `ok`
	  The external memory is connected and ready for operation.
	▶ `outOfMemory`
	  The memory space is occupied on the external memory.
	▶ `genericErr`
	  The device has detected an error.

Writable	Displays whether the device has write access to the external memory.

	Possible values:
	▶ `marked`
	  The device has write access to the external memory.
	▶ `unmarked`
	  The device has read-only access to the external memory. Possibly the write protection is activated on the external memory.

Software auto update	Activates/deactivates the automatic device software update during the restart.

	Possible values:
	▶ `marked` (default setting)
	  The automatic device software update during the restart is activated. The device updates the device software when the following files are located in the external memory:
	  – the image file of the device software
	  – a text file "startup.txt" with the content `autoUpdate=<image_file_name>.bin`
	▶ `unmarked`
	  The automatic device software update during the restart is deactivated.

SSH key auto upload	Activates/deactivates the loading of the RSA key from an external memory upon restart.

	Possible values:
	▶ `marked` (default setting)
	  The loading of the RSA key is activated.
	  During a restart, the device loads the RSA key from the external memory when the following files are located on the external memory:
	  – SSH RSA key file
	  – a text file "startup.txt" with the content
	    `autoUpdateRSA=<filename_of_the_SSH_RSA_key>`
	  The device displays messages on the system console of the V.24 interface.
	▶ `unmarked`
	  The loading of the RSA key is deactivated.

	Note: When loading the RSA key from the external memory (`ENVM`), the device overwrites the existing keys in the non-volatile memory (`NVM`).

Parameters	Meaning
Config priority	Specifies the memory from which the device loads the configuration profile upon reboot.
	Possible values:
	▶ `disable`
	The device loads the configuration profile from the non-volatile memory (`NVM`).
	▶ `first`
	The device loads the configuration profile from the external memory.
	If the device does not find a configuration profile on the external memory, it loads the configuration profile from the non-volatile memory (`NVM`).
	Note: When loading the configuration profile from the external memory (`ENVM`), the device overwrites the settings of the Selected configuration profile in the non-volatile memory (`NVM`).
	If the *Config priority* column has the value `first` and the configuration profile is unencrypted, the *Security status* frame in the *Basic Settings > System* dialog displays an alarm.
	In the *Diagnostics > Status Configuration > Security Status* dialog, *Global* tab, *Monitor* column you specify whether the device monitors the *Load unencrypted config from external memory* parameter.
Backup config when saving	Activates/deactivates creating a copy of the configuration profile on the external memory.
	Possible values:
	▶ `marked` (default setting)
	Creating a copy is activated. If you click in the *Basic Settings > Load/Save* dialog the *Save* button, the device generates a copy of the configuration profile on the active external memory.
	▶ `unmarked`
	Creating a copy is deactivated. The device does not generate a copy of the configuration profile.
Manufacturer ID	Displays the name of the memory manufacturer.
Revision	Displays the revision number specified by the memory manufacturer.
Version	Displays the version number specified by the memory manufacturer.
Name	Displays the product name specified by the memory manufacturer.
Serial number	Displays the serial number specified by the memory manufacturer.

■ Buttons

You find the description of the standard buttons in section "Buttons" on page 16.

1.6 Port

This dialog allows you to specify settings for the individual ports. The dialog also displays the operating mode, connection status, bit rate and duplex mode for every port.

The dialog contains the following tabs:
▶ [Configuration]
▶ [Statistics]
▶ [Utilization]

[Configuration]

■ **Table**

Parameters	Meaning
Port	Displays the port number.

Name	Name of the port.
	
	Possible values:
	▶ Alphanumeric ASCII character string with 0..64 characters
	  The following characters are allowed:
	  – `<space>`
	  – `0..9`
	  – `a..z`
	  – `A..Z`
	  – `!#$%&'()*+,-./:;<=>?@[\\]^_`{}~`

Port on	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.

State	Displays whether the port is currently physically enabled or disabled.
	
	Possible values:
	▶ `marked`
	  The port is physically enabled.
	▶ `unmarked`
	  The port is physically disabled.
	  If the *Port on* function is active, the *Auto-Disable* function has disabled the port.
	  You specify the settings of the *Auto-Disable* function in the *Diagnostics > Ports > Auto-Disable* dialog.

Power state (port off)	Specifies, whether the port is physically switched on or off when you deactivate the port with the *Port on* function.
	
	Possible values:
	▶ `marked`
	  The port remains physically enabled. A connected device receives an active link.
	▶ `unmarked` (default setting)
	  The port is physically disabled.

Auto power down	Specifies how the port behaves when no cable is connected.
	
	Possible values:
	▶ `no-power-save` (default setting)
	  The port remains activated.
	▶ `auto-power-down`
	  The port changes to the energy-saving mode.
	▶ `unsupported`
	  The port does not support this function and remains activated.

Automatic configuration	Activates/deactivates the automatic selection of the operating mode for the port.
	
	Possible values:
	▶ `marked` (default setting)
	  The automatic selection of the operating mode is active.
	  The port negotiates the operating mode independently using autonegotiation and detects the devices connected to the TP port automatically (Auto Cable Crossing). This setting has priority over the manual setting of the port.
	  Elapse several seconds until the port has set the operating mode.
	▶ `unmarked`
	  The automatic selection of the operating mode is inactive.
	  The port operates with the values you specify in the *Manual configuration* column and in the *Manual cable crossing (Auto. conf. off)* column.
	▶ Grayed-out display
	  No automatic selection of the operating mode.

Parameters	Meaning
Manual configuration	Specifies the operating mode of the ports when the `Automatic configuration` function is disabled.
	Possible values:
	▶ `10 Mbit/s HDX`
	Half duplex connection
	▶ `10 Mbit/s FDX`
	Full duplex connection
	▶ `100 Mbit/s HDX`
	Half duplex connection
	▶ `100 Mbit/s FDX`
	Full duplex connection
	▶ `1000 Mbit/s FDX`
	Full duplex connection
	Note: The operating modes of the port actually available depend on the device configuration.
Link/Current settings	Displays the operating mode which the port currently uses.
	Possible values:
	▶ `-`
	No cable connected, no link.
	▶ `10 Mbit/s HDX`
	Half duplex connection
	▶ `10 Mbit/s FDX`
	Full duplex connection
	▶ `100 Mbit/s HDX`
	Half duplex connection
	▶ `100 Mbit/s FDX`
	Full duplex connection
	▶ `1000 Mbit/s FDX`
	Full duplex connection
	Note: The operating modes of the port actually available depend on the device configuration.
Manual cable crossing (Auto. conf. off)	Specifies the devices connected to a TP port. The prerequisite is that the `Automatic configuration` function is disabled.
	Possible values:
	▶ `mdi`
	The device interchanges the send- and receive-line pairs on the port.
	▶ `mdix` (default setting on TP ports)
	The device helps prevent the interchange of the send- and receive-line pairs on the port.
	▶ `auto-mdix`
	The device detects the send and receive line pairs of the connected device and automatically adapts to them.
	Example: When you connect an end device with a crossed cable, the device automatically resets the port from `mdix` to `mdi`.
	▶ `unsupported` (default setting on optical ports or TP-SFP ports)
	The port does not support this function.
Flow control	Activates/deactivates the flow control on the port.
	Possible values:
	▶ `marked` (default setting)
	The Flow control on the port is active.
	The sending and evaluating of pause packets (full-duplex operation) or collisions (half-duplex operation) is activated on the port.
	☐ To enable the flow control in the device, also activate the `Flow control` function in the `Switching > Global` dialog.
	☐ Activate the flow control also on the port of the device that is connected to this port.
	On an uplink port, activating the flow control can possibly cause undesired sending breaks in the higher-level network segment ("wandering backpressure").
	▶ `unmarked`
	The Flow control on the port is inactive.
	When you are using a redundancy function, you deactivate the flow control on the participating ports. If the flow control and the redundancy function are active at the same time, there is a risk that the redundancy function will not operate as intended.

Parameters	Meaning
Send trap (Link up/down)	Activates/deactivates the sending of SNMP traps when the device detects changes in the link up/down status for this port. Possible values: ▶ `marked` (default setting) The sending of SNMP traps is active. The device sends an SNMP trap when it detects a link up/down status change. ▶ `unmarked` The sending of SNMP traps is inactive. The prerequisite for sending SNMP traps is that you enable the function in the *Diagnostics > Status Configuration > Alarms (Traps)* dialog and specify at least 1 trap destination.
Signal	Activates/deactivates the port LED flashing. This function allows you to identify the port in the field. Possible values: ▶ `marked` The flashing of the port LED is active. The port LED flashes until you disable the function again. ▶ `unmarked` (default setting) The flashing of the port LED is inactive.
Link monitoring	Activates/deactivates the *Link monitoring* function on the interface. Use the *Link monitoring* function for end devices that do not support Far End Fault Indication (FEFI) on optical links. Possible values: ▶ `marked` The *Link monitoring* function is active. If the device recognizes an established link, the port LED illuminates. When the device recognizes that a link has been lost, the port LED extinguishes. ▶ `unmarked` (default setting) The *Link monitoring* function is inactive.

■ Buttons

You find the description of the standard buttons in section "Buttons" on page 16.

Button	Meaning
Clear port statistics	Resets the counter for the port statistics to `0`.

[Statistics]

This tab displays the following overview per port:

▶ Number of data packets/bytes received on the device
  – *Received packets*
  – *Received octets*
  – *Received unicast packets*
  – *Received multicast packets*
  – *Received broadcast packets*

▶ Number of data packets/bytes sent from the device
  – *Transmitted packets*
  – *Transmitted octets*
  – *Transmitted unicast packets*
  – *Transmitted multicast packets*
  – *Transmitted broadcast packets*

▶ Number of errors detected by the device
  – *Received fragments*
  – *Detected CRC errors*
  – *Detected collisions*

▶ Number of data packets per size category received on and sent from the device
  – *Packets 64 bytes*
  – *Packets 65 to 127 bytes*
  – *Packets 128 to 255 bytes*
  – *Packets 256 to 511 bytes*
  – *Packets 512 to 1023 bytes*
  – *Packets 1024 to 1518 bytes*

▶ Number of data packets discarded by the device
  – *Received discards*
  – *Transmitted discards*

To sort the table by a specific criterion click the header of the corresponding row.
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 counter for the port statistics in the table to 0, proceed as follows:
▶ In the *Basic Settings > Port* dialog, click the ☰ button and then the *Clear port statistics* item.
  or
▶ In the *Basic Settings > Restart* dialog, click the *Clear port statistics* button.

■ Buttons

You find the description of the standard buttons in section "Buttons" on page 16.

Button	Meaning
Clear port statistics	Resets the counter for the port statistics to 0.

[Utilization]

This tab displays the utilization (network load) for the individual ports.

■ Table

Parameters	Meaning
Port	Displays the port number.
Utilization [%]	Displays the current utilization in percent in relation to the time interval specified in the *Control interval [s]* column. The utilization is the relationship of the received data quantity to the maximum possible data quantity at the currently configured data rate.
Lower threshold [%]	Specifies a lower threshold for the utilization. If the utilization of the port falls below this value, the *Alarm* column displays an alarm. Possible values: ▶ 0.00..100.00 (default setting: 0.00) The value 0 deactivates the lower threshold.
Upper threshold [%]	Specifies an upper threshold for the utilization. If the utilization of the port exceeds this value, the *Alarm* column displays an alarm. Possible values: ▶ 0.00..100.00 (default setting: 0.00) The value 0 deactivates the upper threshold.
Control interval [s]	Specifies the interval in seconds. Possible values: ▶ 1..3600 (default setting: 30)
Alarm	Displays the utilization alarm status. Possible values: ▶ marked The utilization of the port is below the value specified in the *Lower threshold [%]* column or above the value specified in the *Upper threshold [%]* column. The device sends an SNMP trap. ▶ unmarked The utilization of the port is above the value specified in the *Lower threshold [%]* column and below the value specified in the *Upper threshold [%]* column. The prerequisite for sending SNMP traps is that you enable the function in the *Diagnostics > Status Configuration > Alarms (Traps)* dialog and specify at least 1 trap destination.

■ Buttons

You find the description of the standard buttons in section "Buttons" on page 16.

Button	Meaning
Clear port statistics	Resets the counter for the port statistics to 0.

1.7 Restart

This dialog allows you to restart the device, reset port counters and address tables, and delete log files.

■ Restart

Parameters	Meaning
Restart in	Displays the remaining time until the device restarts.
	To update the display of the remaining time, click the [⟳] button.
Cancel	Aborts a delayed restart.
Cold start...	Opens the *Restart* dialog to initiate an immediate or delayed restart of the device.
	If the configuration profile in the volatile memory (RAM) and the "Selected" configuration profile in the non-volatile memory (NVM) differ, the device displays the *Warning* dialog. □ To permanently save the changes, click the *Yes* button in the *Warning* dialog. □ To discard the changes, click *No* in the *Warning* dialog.
	▶ In the *Restart in* field you specify the delay time for the delayed restart. Possible values: – `00:00:00..596:31:23` (default setting: `00:00:00`)
	When the delay time elapsed, the device restarts and goes through the following phases: ▶ The device performs a RAM test if this function is activated in the *Diagnostics > System > Selftest* dialog. ▶ The device starts the device software that the *Stored version* field displays in the *Basic Settings > Software* dialog. ▶ The device loads the settings from the "Selected" 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.

■ Buttons

You find the description of the standard buttons in section "Buttons" on page 16.

Button	Meaning
Reset MAC address table	Removes the MAC addresses from the forwarding table that have in the *Switching > Filter for MAC Addresses* dialog the value `learned` in the *Status* column.
Reset ARP table	Removes the dynamically set up addresses from the ARP table. See the *Diagnostics > System > ARP* dialog.
Clear port statistics	Resets the counter for the port statistics to `0`. See the *Basic Settings > Port* dialog, *Statistics* tab.
Reset IGMP snooping data	Removes the IGMP Snooping entries and resets the counter in the *Information* frame to `0`. See the *Switching > IGMP Snooping > Global* dialog.
Delete log file	Removes the logged events from the log file. See the *Diagnostics > Report > System Log* dialog.
Delete persistent log file	Removes the log files from the external memory. See the *Diagnostics > Report > Persistent Logging* dialog.

2 Time

The menu contains the following dialogs:
▶ Basic Settings
▶ SNTP

2.1 Basic Settings

The device is equipped with a buffered hardware clock. This clock maintains the correct time if the power supply fails or you disconnect the device from the power supply. After the device is started, the current time is available to you, for example for log entries.

The hardware clock bridges a power supply downtime of 3 hours. The prerequisite is that the power supply of the device has been connected continually for at least 5 minutes beforehand.
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]

In this tab, you specify the system time in the device and the time zone.

■ **Configuration**

Parameters	Meaning
System time (UTC)	Displays the current date and time with reference to Universal Time Coordinated (UTC).
Set time from PC	The device uses the time on the PC as the system time.
System time	Displays the current date and time with reference to the local time: *System time* = *System time (UTC)* + *Local offset [min]* + *Daylight saving time*

Time source	Displays the time source from which the device gets the time information.
	The device automatically selects the available time source with the greatest accuracy.
	
	Possible values:
	▶ local
	  System clock of the device.
	▶ sntp
	  The *SNTP* client is activated and the device is synchronized by an *SNTP* server.

Local offset [min]	Specifies the difference between the local time and *System time (UTC)* in minutes: *Local offset [min]* = *System time* − *System time (UTC)* Possible values: ▶ -780..840 (default setting: 60)

■ **Buttons**

You find the description of the standard buttons in section .

[Daylight saving time]

In this tab, you activate the automatic daylight saving time function. You specify the beginning and the end of summertime using a pre-defined profile, or you specify these settings individually. During summertime, the device puts the local time forward by 1 hour.

■ **Operation**

Parameters	Meaning
Daylight saving time	Enables/disables the *Daylight saving time* mode. Possible values: ▶ `On` 　The *Daylight saving time* mode is enabled. 　The device automatically changes between summertime and wintertime. ▶ `Off` (default setting) 　The *Daylight saving time* mode is disabled. The times at which the device changes between summertime and wintertime are specified in the *Summertime begin* and *Summertime end* frames.
Profile...	Displays the *Profile...* dialog. There you select a pre-defined profile for the beginning and the end of summertime. This profile overwrites the settings in the *Summertime begin* and *Summertime end* frames.

■ **Summertime begin**

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

The devices switches to summertime when the time in the *System time* field reaches the value entered here.

Parameters	Meaning
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`

Parameters	Meaning
Month	Specifies the month.
	Possible values:
	▶ `none` (default setting)
	▶ `January`
	▶ `February`
	▶ `March`
	▶ `April`
	▶ `May`
	▶ `June`
	▶ `July`
	▶ `August`
	▶ `September`
	▶ `October`
	▶ `November`
	▶ `December`
System time	Specifies the time.
	Possible values:
	▶ `<HH:MM>` (default setting: `00:00`)

■ **Summertime end**

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

The devices switches to wintertime when the time in the `System time` field reaches the value entered here.

Parameters	Meaning
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`

Parameters	Meaning
System time	Specifies the time.
	Possible values:
	▶ `<HH:MM>` (default setting: `00:00`)

■ **Buttons**

You find the description of the standard buttons in section .

2.2   SNTP

The Simple Network Time Protocol (SNTP) is a procedure described in the RFC 4330 for time synchronization in the network.

The device allows you to synchronize the system time in the device as an *SNTP* client. As the *SNTP* server, the device makes the time information available to other devices.

The menu contains the following dialogs:
- ▶ SNTP Client
- ▶ SNTP Server

2.2.1 SNTP Client

In this dialog, you specify the settings with which the device operates as an *SNTP* client.

As an *SNTP* client the device obtains the time information from both *SNTP* servers and *NTP* servers and synchronizes the local clock with the time of the time server.

■ Operation

Parameters	Meaning
Operation	Enables/disables the *SNTP Client* function of the device.

	Possible values:
	▶ `On`
	  The *SNTP Client* function is enabled.
	  The device operates as an *SNTP* client.
	▶ `Off` (default setting)
	  The *SNTP Client* function is disabled.

■ Configuration

Parameters	Meaning
Mode	Specifies whether the device actively requests the time information from an *SNTP* server known and configured in the network (Unicast mode) or passively waits for the time information from a random *SNTP* server (Broadcast mode).

	Possible values:
	▶ `unicast` (default setting)
	  The device takes the time information from the configured *SNTP* server exclusively. The device sends Unicast requests to the *SNTP* server and evaluates its responses.
	▶ `broadcast`
	  The device obtains the time information from one or more *SNTP* or *NTP* servers. The device evaluates the Broadcasts or Multicasts from these servers exclusively.

Request interval [s]	Specifies the interval in seconds at which the device requests time information from the *SNTP* server.
	Possible values: ▶ `5..3600` (default setting: `30`)
Broadcast recv timeout [s]	Specifies the time in seconds a client in broadcast client mode waits before changing the value in the field from `syncToRemoteServer` to `notSynchronized` when the client receives no broadcast packets.
	Possible values: ▶ `128..2048` (default setting: `320`)
Disable client after successful sync	Activates/deactivates the disabling of the *SNTP* client after the device has successfully synchronized the time.

	Possible values:
	▶ `marked`
	  The disabling of the *SNTP* client is active.
	  The device deactivates the *SNTP* client after successful time synchronization.
	▶ `unmarked` (default setting)
	  The disabling of the *SNTP* client is inactive.
	  The *SNTP* client remains active after successful time synchronization.

■ **State**

Parameters	Meaning
State	Displays the status of the `SNTP` client.

	Possible values:
	▶ `disabled`
	  The `SNTP` client is disabled.
	▶ `notSynchronized`
	  The `SNTP` client is not synchronized with any `SNTP` or `NTP` server.
	▶ `synchronizedToRemoteServer`
	  The `SNTP` client is synchronized with an `SNTP` or `NTP` server.

■ **Table**

In the table you specify the settings for up to 4 `SNTP` servers.

Parameters	Meaning
Index	Displays the index number to which the table entry relates.
	Possible values: ▶ `1..4` The device automatically assigns this number. When you delete a table entry, this leaves a gap in the numbering. When you create a new table entry, the device fills the first gap. After starting, the device sends requests to the `SNTP` server configured in the first table entry. If the server does not reply, the device sends its requests to the `SNTP` server configured in the next table entry. If none of the configured `SNTP` servers responds in the meantime, the `SNTP` client loses its synchronization. The device cyclically sends requests to each `SNTP` server until a server delivers a valid time. The device synchronizes itself with this `SNTP` server, even if the other servers can be reached again later.
Name	Specifies the name of the `SNTP` server.
	Possible values: ▶ Alphanumeric ASCII character string with 1..32 characters
Address	Specifies the IP address of the `SNTP` server.
	Possible values: ▶ Valid IPv4 address (default setting: `0.0.0.0`)
Destination UDP port	Specifies the UDP Port on which the `SNTP` server expects the time information.
	Possible values: ▶ `1..65535` (default setting: `123`) Exception: Port `2222` is reserved for internal functions.

Parameters	Meaning
Status	Displays the connection status between the *SNTP* client and the *SNTP* server.
	Possible values: ▶ `success` The device has successfully synchronized the time with the *SNTP* server. ▶ `badDateEncoded` The time information received contains protocol errors - synchronization failed. ▶ `other` – The value `0.0.0.0` is entered for the IP address of the *SNTP* server - synchronization failed. or – The *SNTP* client is using a different *SNTP* server. ▶ `requestTimedOut` The device has not received a reply from the *SNTP* server - synchronization failed. ▶ `serverKissOfDeath` The *SNTP* server is overloaded. The device is requested to synchronize itself with another *SNTP* server. If no other *SNTP* server is available, the device asks at intervals longer than the setting in the *Request interval [s]* field, whether the server is still overloaded. ▶ `serverUnsychronized` The *SNTP* server is not synchronized with either a local or an external reference clock - synchronization failed. ▶ `versionNotSupported` The *SNTP* versions on the client and the server are incompatible with each other - synchronization failed.
Active	Activates/deactivates the connection to the *SNTP* server.
	Possible values: ▶ `marked` The connection to the *SNTP* server is activated. The *SNTP* client has access to the *SNTP* server. ▶ `unmarked` (default setting) The connection to the *SNTP* server is deactivated. The *SNTP* client has no access to the *SNTP* server.

■ Buttons

You find the description of the standard buttons in section .

2.2.2 SNTP Server

In this dialog, you specify the settings with which the device operates as an *SNTP* server.

The *SNTP* server provides the Universal Time Coordinated (UTC) without considering local time differences.

If the setting is appropriate, the *SNTP* server operates in the broadcast mode. In broadcast mode, the *SNTP* server automatically sends broadcast messages or multicast messages according to the broadcast send interval.

■ Operation

Parameters	Meaning
Operation	Enables/disables the *SNTP Server* function of the device.
	Possible values:
	▶ `On`
	The *SNTP Server* function is enabled.
	The device operates as an *SNTP* server.
	▶ `Off` (default setting)
	The *SNTP Server* function is disabled.
	Note the setting in the *Disable server at local time source* checkbox in the *Configuration* frame.

■ Configuration

Parameters	Meaning
UDP port	Specifies the number of the UDP port on which the *SNTP* server of the device receives requests from other clients.
	Possible values:
	▶ `1..65535` (default setting: `123`)
	Exception: Port `2222` is reserved for internal functions.
Broadcast admin mode	Activates/deactivates the Broadcast mode.
	▶ `marked`
	The *SNTP* server replies to requests from *SNTP* clients in Unicast mode and also sends *SNTP* packets in Broadcast mode as Broadcasts or Multicasts.
	▶ `unmarked` (default setting)
	The *SNTP* server replies to requests from *SNTP* clients in the Unicast mode.
Broadcast destination address	Specifies the IP address to which the *SNTP* server of the device sends the *SNTP* packets in Broadcast mode.
	Possible values:
	▶ Valid IPv4 address (default setting: `0.0.0.0`)
	Broadcast and Multicast addresses are permitted.
Broadcast UDP port	Specifies the number of the UDP port on which the *SNTP* server sends the *SNTP* packets in Broadcast mode.
	Possible values:
	▶ `1..65535` (default setting: `123`)
	Exception: Port `2222` is reserved for internal functions.
Broadcast VLAN ID	Specifies the ID of the VLAN in which the *SNTP* server of the device sends the *SNTP* packets in Broadcast mode.
	Possible values:
	▶ `0`
	The *SNTP* server sends the *SNTP* packets in the same VLAN in which the management access to the device is possible. See the *Basic Settings > Network* dialog.
	▶ `1..4042` (default setting: `1`)

Parameters	Meaning
Broadcast send interval [s]	Specifies the time interval at which the *SNTP* server of the device sends *SNTP* broadcast packets.
	Possible values: ▶ `64..1024` (default setting: `128`)
Disable server at local time source	Activates/deactivates the disabling of the *SNTP* server when the device is synchronized to the local clock.
	Possible values: ▶ `marked` The disabling of the *SNTP* server is active. The device disables the *SNTP* server when the device is synchronized to the local clock. The *SNTP* server continues to reply to requests from *SNTP* clients. In the *SNTP* packet, the *SNTP* server informs the clients that it is synchronized locally. ▶ `unmarked` (default setting) The disabling of the *SNTP* server is inactive. The *SNTP* server remains active when the device is synchronized to the local clock.

■ **State**

Parameters	Meaning
State	Displays the state of the *SNTP* server.
	Possible values: ▶ `disabled` The *SNTP* server is disabled. ▶ `notSynchronized` The *SNTP* server is not synchronized with either a local or an external reference clock. ▶ `syncToLocal` The *SNTP* server is synchronized with the hardware clock of the device. ▶ `syncToRefclock` The *SNTP* server is synchronized with an external reference clock. ▶ `syncToRemoteServer` The *SNTP* server is synchronized with an *SNTP* server that is higher than the device in a cascade.

■ **Buttons**

You find the description of the standard buttons in section "Buttons" on page 16.

3 Device Security

The menu contains the following dialogs:
- ▶ User Management
- ▶ Authentication List
- ▶ Management Access
- ▶ Pre-login Banner

3.1   User Management

The device allows users to access its management exclusively when they log in with valid login data.

In this dialog you manage the users of the local user management. You also specify the following settings here:
▶ Settings for the login
▶ Settings for saving the passwords
▶ Specify policy for valid passwords

The methods that the device uses for the authentication you specify in the *Device Security > Authentication List* dialog.

■ Configuration

This frame allows you to specify settings for the login.

Parameters	Meaning
Login attempts	Number of login attempts possible.
	Possible values:
	▶ `0..5` (default setting: `0`)
	If the user makes one more unsuccessful login attempt, the device locks access for the user. The device allows users with the `administrator` authorization to remove the lock exclusively.
	The value `0` deactivates the lock. The user has unlimited attempts to login.
Min. password length	The device accepts the password if it contains at least the number of characters specified here. The device checks the password according to this setting, regardless of the setting for the *Policy check* checkbox.
	Possible values:
	▶ `1..64` (default setting: `6`)

■ Password policy

This frame allows you to specify the policy for valid passwords. The device checks every new password and password change according to this policy.
The settings effect the *Password* column. The prerequisite is that you mark the checkbox in the *Policy check* column.

Parameters	Meaning
Upper-case characters (min.)	The device accepts the password if it contains at least as many upper-case letters as specified here.
	Possible values:
	▶ `0..16` (default setting: `1`)
	The value `0` deactivates this setting.
Lower-case characters (min.)	The device accepts the password if it contains at least as many lower-case letters as specified here.
	Possible values:
	▶ `0..16` (default setting: `1`)
	The value `0` deactivates this setting.
Digits (min.)	The device accepts the password if it contains at least as many numbers as specified here.
	Possible values:
	▶ `0..16` (default setting: `1`)
	The value `0` deactivates this setting.
Special characters (min.)	The device accepts the password if it contains at least as many special characters as specified here.
	Possible values:
	▶ `0..16` (default setting: `1`)
	The value `0` deactivates this setting.

■ **Table**

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

To change settings, click the desired parameter in the table and modify the value.

Parameters	Meaning
User name	Displays the name of the user account.
	To create a new user account, click the ⊞ button.
Active	Activates/deactivates the user account.
	Possible values:
	▶ `marked`
	The user account is active. The device accepts the login of a user with this user name.
	▶ `unmarked` (default setting)
	The user account is inactive. The device rejects the login of a user with this user name.
	When one user account exists with the `administrator` access role, this user account is constantly active.
Password	Displays ***** (asterisks) instead of the password with which the user logs in. To change the password, click the relevant field.
	Possible values:
	▶ Alphanumeric ASCII character string with 6..64 characters
	The following characters are allowed:
	– `a..z`
	– `A..Z`
	– `0..9`
	– `!#$%&'()*+,-./:;<=>?@[\]^_\`{}~`
	The minimum length of the password is specified in the *Configuration* frame. The device differentiates between upper and lower case.
	If the checkbox in the *Policy check* column is marked, the device checks the password according to the policy specified in the *Password policy* frame.
	The device constantly checks the minimum length of the password, even if the checkbox in the *Policy check* column is `unmarked`.
Role	Specifies the user role that regulates the access of the user to the individual functions of the device.
	Possible values:
	▶ `unauthorized`
	The user is blocked, and the device rejects the user log on.
	Assign this value to temporarily lock the user account. If an error occurs when another role is being assigned, the device assigns this role to the user account.
	▶ `guest` (default setting)
	The user is authorized to monitor the device.
	▶ `auditor`
	The user is authorized to monitor the device and to save the log file in the *Diagnostics > Report > Audit Trail* dialog.
	▶ `operator`
	The user is authorized to monitor the device and to change the settings – with the exception of security settings for device access.
	▶ `administrator`
	The user is authorized to monitor the device and to change the settings.
	The device assigns the Service Type transferred in the response of a RADIUS server as follows to a user role:
	– `Administrative-User: administrator`
	– `Login-User: operator`
	– `NAS-Prompt-User: guest`
User locked	Unlocks the user account.
	Possible values:
	▶ `marked`
	The user account is locked. The user has no management access to the device.
	The device automatically locks a user if the user makes too many unsuccessful log in attempts.
	▶ `unmarked` (grayed out) (default setting)
	The user account is unlocked. The user has management access to the device.

Parameters	Meaning
Policy check	Activates/deactivates the password check.
	Possible values: ▶ `marked` The password check is activated. When you set up or change the password, the device checks the password according to the policy specified in the ***Password policy*** frame. ▶ `unmarked` (default setting) The password check is deactivated.
SNMP auth type	Specifies the authentication protocol that the device applies for user access via SNMPv3.
	Possible values: ▶ `hmacmd5` (default value) For this user account, the device uses protocol HMACMD5. ▶ `hmacsha` For this user account, the device uses protocol HMACSHA.
SNMP encryption type	Specifies the encryption protocol that the device applies for user access via SNMPv3.
	Possible values: ▶ `none` No encryption. ▶ `des` (default value) DES encryption ▶ `aesCfb128` AES128 encryption

■ **Buttons**

You find the description of the standard buttons in section "Buttons" on page 16.

Button	Meaning
🖳	Opens the ***Create*** window to add a new entry to the table. ▶ In the ***User name*** field, you specify the name of the user account. Possible values: – Alphanumeric ASCII character string with 1..32 characters

3.2   Authentication List

In this dialog you manage the authentication lists. In a authentication list you specify which method the device uses for the authentication. You also have the option to assign pre-defined applications to the authentication lists.

The device allows users to access its management exclusively when they log in with valid login data. The device authenticates the users using the following methods:
▶ User management of the device
▶ RADIUS

With the port-based access control according to IEEE 802.1X, the device allows connected end devices to access the network if they log in with valid login data. The device authenticates the end devices using the following methods:
▶ RADIUS
▶ IAS (Integrated Authentication Server)

In the default setting the following authentication lists are available:
☐ `defaultDot1x8021AuthList`
☐ `defaultLoginAuthList`
☐ `defaultV24AuthList`

■ **Table**

Parameters	Meaning
Name	Displays the name of the list.
	To create a new list, click the 🔲 button.
	Possible values: ▶ Alphanumeric ASCII character string with 1..32 characters

Parameters	Meaning
Policy 1 Policy 2 Policy 3 Policy 4 Policy 5	Specifies the authentication policy that the device uses for access using the application specified in the *Dedicated applications* column. The device gives you the option of a fall-back solution. For this, you specify another policy in each of the policy fields. Depending on the order of the values entered in each policy, if the authentication with the specified policy is unsuccessful, the device can use the next policy. Possible values: ▶ `local` (default setting) The device authenticates the users by using the local user management. See the *Device Security > User Management* dialog. You cannot assign this value to the authentication list `defaultDot1x8021AuthList`. ▶ `radius` The device authenticates the users with a RADIUS server in the network. You specify the RADIUS server in the *Network Security > RADIUS > Authentication Server* dialog. ▶ `reject` The device accepts or rejects the authentication depending on which policy you try first. The following list contains authentication scenarios: – If the first policy in the authentication list is `local` and the device accepts the credentials of the user, then it logs the user in without attempting the other polices. – If the first policy in the authentication list is `local` and the device denies the credentials of the user, then it attempts to log the user in using the other polices in the order specified. – If the first policy in the authentication list is `radius` and the device rejects a login, then the login is immediately rejected without attempting to login the user using another policy. If there is no response from the RADIUS server, the device attempts to authentication the user with the next policy. – If the first policy in the authentication list is `reject`, then the devices immediately rejects the user login without attempting another policy. – Verify that the authentication list `defaultV24AuthList` contains at least one policy different from `reject`. ▶ `ias` The device authenticates the end devices logging in via 802.1X with the integrated authentication server (IAS). The integrated authentication server manages the log in data in a separate database. See the *Network Security > 802.1X Port Authentication > Integrated Authentication Server* dialog. You can only assign this value to the authentication list `defaultDot1x8021AuthList`.
Dedicated applications	Displays the dedicated applications. When users access the device with the relevant application, the device uses the specified policies for the authentication. To allocate another application to the list or remove the allocation, click the ☰ button and then the *Allocate applications* item. Allocate one application solely to one list.
Active	Activates/deactivates the list. Possible values: ▶ `marked` The list is activated. The device uses the policies in this list when users access the device with the relevant application. ▶ `unmarked` (default setting) The list is deactivated.

Note: If the table does not contain a list, the management access is possible using CLI through the V.24 interface of the device exclusively. In this case, the device authenticates the user by using the local user management. See the *Device Security > User Management* dialog.

■ **Buttons**

You find the description of the standard buttons in section "Buttons" on page 16.

Button	Meaning

Allocate applications	Opens the *Allocate applications* window.
	▶ The left field displays the applications that can be allocated to the highlighted list.
	▶ The right field displays the applications that are allocated to the highlighted list.
	▶ Buttons:
	   ▸ Moves every entry to the right field.
	   ▸ Moves the highlighted entries from the left field to the right field.
	   ◂ Moves the highlighted entries from the right field to the left field.
	   ◂ Moves every entry to the left field.
	
	Do not move the entry `WebInterface` to the left field. Otherwise the connection to the device is lost, after you click the *Ok* button.

3.3 Management Access

The menu contains the following dialogs:
- ▶ Server
- ▶ IP Access Restriction
- ▶ Web
- ▶ Command Line Interface
- ▶ SNMPv1/v2 Community

3.3.1   Server

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

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

[Information]

This tab displays as an overview which server services are enabled.

■ **Table**

Parameters	Meaning

SNMPv1	Displays whether the server service which allows access to the device using SNMP version 1 is active or inactive. See the *SNMP* tab.
	
	Possible values:
	▶ `marked`
	   Server service is active.
	▶ `unmarked`
	   Server service is inactive.

SNMPv2	Displays whether the server service which allows access to the device using SNMP version 2 is active or inactive. See the *SNMP* tab.
	
	Possible values:
	▶ `marked`
	   Server service is active.
	▶ `unmarked`
	   Server service is inactive.

SNMPv3	Displays whether the server service which allows access to the device using SNMP version 3 is active or inactive. See the *SNMP* tab.
	
	Possible values:
	▶ `marked`
	   Server service is active.
	▶ `unmarked`
	   Server service is inactive.

Telnet server	Displays whether the server service which allows access to the device using Telnet is active or inactive. See the *Telnet* tab.
	
	Possible values:
	▶ `marked`
	   Server service is active.
	▶ `unmarked`
	   Server service is inactive.

SSH server	Displays whether the server service which allows access to the device using Secure Shell is active or inactive. See the *SSH* tab.
	
	Possible values:
	▶ `marked`
	   Server service is active.
	▶ `unmarked`
	   Server service is inactive.

HTTP server	Displays whether the server service which allows access to the device using the Graphical User Interface through HTTP is active or inactive. See the *HTTP* tab.
	
	Possible values:
	▶ `marked`
	   Server service is active.
	▶ `unmarked`
	   Server service is inactive.

HTTPS server	Displays whether the server service which allows access to the device using the Graphical User Interface through HTTPS is active or inactive. See the *HTTPS* tab.
	
	Possible values:
	▶ `marked`
	   Server service is active.
	▶ `unmarked`
	   Server service is inactive.

■ **Buttons**

You find the description of the standard buttons in section "Buttons" on page 16.

[**SNMP**]

This tab allows you to specify settings for the SNMP agent of the device and to enable/disable access to the device with different SNMP versions.

The SNMP agent enables management access to the device with SNMP-based applications.

■ Configuration

Parameters	Meaning
SNMPv1	Activates/deactivates the access to the device with SNMP version 1.

	Possible values:
	▶ `marked` (default setting)
	  Access is activated.
	▶ `unmarked`
	  Access is deactivated.

	You specify the community names in the *Device Security > Management Access > SNMPv1/v2 Community* dialog.
SNMPv2	Activates/deactivates the access to the device with SNMP version 2.

	Possible values:
	▶ `marked` (default setting)
	  Access is activated.
	▶ `unmarked`
	  Access is deactivated.

	You specify the community names in the *Device Security > Management Access > SNMPv1/v2 Community* dialog.
SNMPv3	Activates/deactivates the access to the device with SNMP version 3.

	Possible values:
	▶ `marked` (default setting)
	  Access is activated.
	▶ `unmarked`
	  Access is deactivated.

	Network management systems like Industrial HiVision use this protocol to communicate with the device.
UDP port	Specifies the number of the UDP port on which the SNMP agent receives requests from clients.
	Possible values: ▶ `1..65535` (default setting: `161`) Exception: Port `2222` is reserved for internal functions.
	To enable the SNMP agent to use the new port after a change, you proceed as follows:
	☐ Click the ✔ button.
	☐ Select in the *Basic Settings > Load/Save* dialog the active configuration profile.
	☐ Click the 🖫 button to save the current changes.
	☐ Restart the device.
SNMPover802	Activates/deactivates the access to the device through SNMP over IEEE-802.

	Possible values:
	▶ `marked`
	  Access is activated.
	▶ `unmarked` (default setting)
	  Access is deactivated.

■ Buttons

You find the description of the standard buttons in section "Buttons" on page 16.

[Telnet]

This tab allows you to enable/disable the Telnet server in the device and specify its settings.

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

■ Operation

Parameters	Meaning
Operation	Enables/disables the Telnet server.

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

	Note: If the SSH server is disabled and you also disable Telnet, the access to the Command Line Interface is only possible through the V.24 interface of the device.

■ Configuration

Parameters	Meaning
TCP port	Specifies the number of the TCP port on which the device receives Telnet requests from clients.
	Possible values: ▶ 1..65535 (default setting: 23) Exception: Port 2222 is reserved for internal functions.
	The server restarts automatically after the port is changed. Existing connections remain in place.
Connections	Displays how many Telnet connections are currently established to the device.
Connections (max.)	Specifies the maximum number of Telnet connections to the device that can be set up simultaneously.
	Possible values: ▶ 1..2 (default setting: 2)
Session timeout [min]	Specifies the timeout in minutes. After the device has been inactive for this time it ends the session for the user logged on. A change in the value takes effect the next time a user logs on to the device.
	Possible values: ▶ 0 Deactivates the function. The connection remains established in the case of inactivity. ▶ 1..160 (default setting: 5)

■ Buttons

You find the description of the standard buttons in section "Buttons" on page 16.

[**SSH**]

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

The SSH server enables management access to the device 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 via a reliable channel, they have the option to compare both fingerprints. If the character sequences match, the client is connected to the correct server.

The device allows you to create the private and public keys (host keys) required for RSA directly on the device. Otherwise you have the option to copy your own keys to the device in PEM format.
As an alternative, the device allows you to load the RSA key (host key) from an external memory upon restart. You activate this function in the *Basic Settings > External Memory* dialog, *SSH key auto upload* column.

■ Operation

Parameters	Meaning
Operation	Enables/disables the SSH server.

	Possible values:
	▶ `On` (default setting)
	  The SSH server is enabled.
	  The management access to the device is possible through the Command Line Interface using an encrypted SSH connection.
	  The server can solely then be started if there is an RSA signature on the device.
	▶ `Off`
	  The SSH server is disabled.
	  When you disable the SSH server, the existing connections remain established. However, the device helps prevent new connections from being set up.

	Note: If the Telnet server is disabled and you also disable SSH, the access to the Command Line Interface is only possible through the V.24 interface of the device.

■ Configuration

Parameters	Meaning
TCP port	Specifies the number of the TCP port on which the device receives SSH requests from clients.
	Possible values: ▶ `1..65535` (default setting: `22`) Exception: Port `2222` is reserved for internal functions.
	The server restarts automatically after the port is changed. Existing connections remain in place.
Sessions	Displays how many SSH connections are currently established to the device.
Sessions (max.)	Specifies the maximum number of SSH connections to the device that can be set up simultaneously.
	Possible values: ▶ `1..2` (default setting: `2`)
Session timeout [min]	Specifies the timeout in minutes. After the user logged on has been inactive for this time, the ends the connection. A change in the value takes effect the next time a user logs on to the device.
	Possible values: ▶ `0` Deactivates the function. The connection remains established in the case of inactivity. ▶ `1..160` (default setting: `5`)

■ Fingerprint

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

Parameters	Meaning
RSA Fingerprint	Displays the fingerprint of the public host key of the SSH server.

After importing a new host key, the device continues to display the existing fingerprint until you restart the server.

■ Signature

Parameters	Meaning
RSA present	Displays whether an RSA host key is present on the device.
	Possible values:
	▶ `marked`
	A key is present.
	▶ `unmarked`
	No key is present.
Create	Generates a host key on the device. The prerequisite is that the `SSH` server is disabled.
	Length of the key created:
	▶ 2048 bit (RSA)
	To get the SSH server to use the generated host key, re-enable the SSH server.
	Alternatively, you have the option to copy your own host key to the device in PEM format. See the `Key import` frame.
Delete	Removes the host key from the device. The prerequisite is that the SSH server is disabled.
Oper status	Displays whether the device currently generates a host key. It is possible that another user triggered this action.
	Possible values:
	▶ `rsa`
	The device currently generates an RSA host key.
	▶ `none`
	The device does not generate a host key.

■ Key import

Parameters	Meaning
URL	Specifies the path and file name of your own RSA host key.
	The device accepts the RSA key if it has the following key length:
	– 2048 bit (RSA)
	The device gives you the following options for copying the key to the device:
	▶ Import from the PC
	If the host key is located on your PC or on a network drive, drag and drop the file that contains the key in the 🔼 area. Alternatively click in the area to select the file.
	▶ Import from an FTP server
	If the key is on an FTP server, specify the URL for the file in the following form:
	`ftp://<user>:<password>@<IP address>:<port>/<file name>`
	▶ Import from a TFTP server
	If the key is on a TFTP server, specify the URL for the file in the following form:
	`tftp://<IP address>/<path>/<file name>`
	▶ Import from an SCP or SFTP server
	If the key is on an SCP or SFTP server, you specify the URL for the file in the following form:
	– `scp://` or `sftp://<IP address>/<path>/<file name>`
	When you click the `Start` button, the device displays the `Credentials` window. There you enter `User name` and `Password`, to log on to the server.
	– `scp://` or `sftp://<user>:<password>@<IP address>/<path>/<file name>`
Start	Copies the key specified in the `URL` field to the device.

■ **Buttons**

You find the description of the standard buttons in section "Buttons" on page 16.

[**HTTP**]

This tab allows you to enable/disable the HTTP protocol for the web server and specify the settings required for HTTP.

The web server provides the graphical user interface via an unencrypted HTTP connection. For security reasons, disable the HTTP protocol and use the HTTPS protocol instead.

The device supports up to 10 simultaneous connections using HTTP or HTTPS.

Note: If you change the settings in this tab and click the ✓ button, the device ends the session and disconnects every opened connection. To continue working with the graphical user interface, login again.

■ Operation

Parameters	Meaning
Operation	Enables/disables the *HTTP* protocol for the web server.
	Possible values:
	▶ On (default setting) The *HTTP* protocol is enabled. The management access to the device is possible through an unencrypted *HTTP* connection. If the *HTTPS* protocol is also enabled, the device automatically redirects the request for a *HTTP* connection to an encrypted *HTTPS* connection. ▶ Off The *HTTP* protocol is disabled. If the *HTTPS* protocol is enabled, the management access to the device is possible through an encrypted *HTTPS* connection.
	Note: If the *HTTP* and *HTTPS* protocols are disabled, you can enable the *HTTP* protocol using the CLI command `http server` to get to the graphical user interface.

■ Configuration

Parameters	Meaning
TCP port	Specifies the number of the TCP port on which the web server receives HTTP requests from clients.
	Possible values:
	▶ 1..65535 (default setting: 80) Exception: Port 2222 is reserved for internal functions.

■ Buttons

You find the description of the standard buttons in section "Buttons" on page 16.

[**HTTPS**]

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

The web server provides the graphical user interface via an encrypted HTTP connection.
A digital certificate is required for the encryption of the HTTP connection. The device allows you to create this certificate yourself or to load an existing certificate onto the device.

The device supports up to 10 simultaneous connections using HTTP or HTTPS.

Note: If you change the settings in this tab and click the ☑ button, the device ends the session and disconnects every opened connection. To continue working with the graphical user interface, login again.

■ Operation

Parameters	Meaning
Operation	Enables/disables the *HTTPS* protocol for the web server.
	Possible values: ▶ `On` (default setting) The *HTTPS* protocol is enabled. The management access to the device is possible through an encrypted *HTTPS* connection. If there is no digital certificate present, the device generates a digital certificate before it enables the *HTTPS* protocol. ▶ `Off` The *HTTPS* protocol is disabled. If the *HTTP* protocol is enabled, the management access to the device is possible through an unencrypted *HTTP* connection. **Note:** If the *HTTP* and *HTTPS* protocols are disabled, you can enable the *HTTPS* protocol using the CLI command `https server` to get to the graphical user interface.

■ Configuration

Parameters	Meaning
TCP port	Specifies the number of the TCP port on which the web server receives HTTPS requests from clients.
	Possible values: ▶ `1..65535` (default setting: `443`) Exception: Port `2222` is reserved for internal functions.

■ Fingerprint

The fingerprint is an easily verified hexadecimal number sequence that uniquely identifies the digital certificate of the HTTPS server.

After importing a new digital certificate, the device displays the current fingerprint until you restart the server.

Parameters	Meaning
Fingerprint type	Specifies which fingerprint the *Fingerprint* field displays.
	Possible values: ▶ `sha1` The *Fingerprint* field displays the SHA1 fingerprint of the certificate. ▶ `sha256` The *Fingerprint* field displays the SHA256 fingerprint of the certificate.

Parameters	Meaning
Fingerprint	Character sequence of the digital certificate used by the server.
	When you change the settings in the `Fingerprint type` field, click afterwards the ✅ button and then the 🔄 button to update the display.

■ Certificate

Parameters	Meaning
Present	Displays whether the digital certificate is present on the device.
	Possible values:
	▶ `marked`
	The certificate is present.
	▶ `unmarked`
	The certificate has been removed.
Create	Generates a digital certificate on the device. Until restarting the web server uses the previous certificate.
	To get the web server to use the newly generated certificate, restart the web server. Restarting the web server is possible solely through the Command Line Interface (CLI).
	Alternatively, you have the option of copying your own certificate to the device. See the `Certificate import` frame.
Delete	Deletes the digital certificate. Until restarting the web server uses the previous certificate.
Oper status	Displays whether the device currently generates or deletes a digital certificate. It is possible that another user has triggered the action.
	Possible values:
	▶ `none`
	The device does currently not generate or delete a certificate.
	▶ `delete`
	The device currently deletes a certificate.
	▶ `generate`
	The device currently generates a certificate.

Note: When loading the graphical user interface, the web browser displays a warning if the device uses a certificate that is not signed by a certification authority. To continue, add an exception rule for the certificate in the web browser.

■ **Certificate import**

Parameters	Meaning
URL	Specifies the path and file name of the certificate.

	The device accepts certificates with the following properties:
	– X.509 format
	– `.PEM` file name extension
	– Base64-coded, enclosed by
	  • `-----BEGIN PRIVATE KEY-----`
	    and
	    `-----END PRIVATE KEY-----`
	    as well as
	  • `-----BEGIN CERTIFICATE-----`
	    and
	    `-----END CERTIFICATE-----`
	– RSA key with 2048 bit length

	The device gives you the following options for copying the certificate to the device:
	▶ Import from the PC
	If the certificate is located on your PC or on a network drive, drag and drop the certificate in the
	
	  ⬆ area. Alternatively click in the area to select the certificate.
	▶ Import from an FTP server
	If the certificate is on a FTP server, specify the URL for the file in the following form:
	`ftp://<user>:<password>@<IP address>:<port>/<path>/<file name>`
	▶ Import from a TFTP server
	If 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 an SCP or SFTP server
	If the certificate is on an SCP or SFTP server, you specify the URL for the file in the following form:
	– `scp://` or `sftp://<IP address>/<path>/<file name>`
	When you click the *Start* button, the device displays the *Credentials* window. There you enter *User name* and *Password*, to log on to the server.
	– `scp://` or `sftp://<user>:<password>@<IP address>/<path>/<file name>`

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

■ **Buttons**

You find the description of the standard buttons in section "Buttons" on page 16.

3.3.2   IP Access Restriction

This dialog enables you to restrict the management access to the device to specific IP address ranges and selected IP-based applications.
- ▶ If the function is disabled, the management access to the device is possible from any IP address and using every application.
- ▶ If the function is enabled, the access is restricted. You have management access under the following conditions exclusively:
  - – At least one table entry is activated.
    and
  - – You are accessing the device with a permitted application from a permitted IP address range.

■ Operation

Parameters	Meaning
Operation	Enables/disables the **IP Access Restriction** function.

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

Note: Before you enable the function, verify that at least one active entry in the table allows you access. Otherwise, the connection to the device terminates when you change the settings. The management access to the device is possible exclusively using the CLI through the V.24 interface.

■ Table

You have the option of defining up to 16 table entries and activating them separately.

Parameters	Meaning
Index	Displays the index number to which the table entry relates. When you delete a table entry, this leaves a gap in the numbering. When you create a new table entry, the device fills the first gap.
	Possible values: ▶ `1..16`
Address	Specifies the IP address of the network from which you allow the management access to the device. You specify the network range in the **Netmask** column.
	Possible values: ▶ Valid IPv4 address (default setting: `0.0.0.0`)
Netmask	Specifies the range of the network specified in the **Address** column.
	Possible values: ▶ Valid netmask (default setting: `0.0.0.0`)
HTTP	Activates/deactivates the HTTP access.

	Possible values:
	▶ `marked` (default setting)
	    Access is activated for the adjacent IP address range.
	▶ `unmarked`
	    Access is deactivated.

Parameters	Meaning
HTTPS	Activates/deactivates the HTTPS access.

	Possible values:
	▶ `marked` (default setting)
	  Access is activated for the adjacent IP address range.
	▶ `unmarked`
	  Access is deactivated.

SNMP	Activates/deactivates the SNMP access.

	Possible values:
	▶ `marked` (default setting)
	  Access is activated for the adjacent IP address range.
	▶ `unmarked`
	  Access is deactivated.

Telnet	Activates/deactivates the Telnet access.

	Possible values:
	▶ `marked` (default setting)
	  Access is activated for the adjacent IP address range.
	▶ `unmarked`
	  Access is deactivated.

SSH	Activates/deactivates the SSH access.

	Possible values:
	▶ `marked` (default setting)
	  Access is activated for the adjacent IP address range.
	▶ `unmarked`
	  Access is deactivated.

IEC61850-MMS	Activates/deactivates the access to the MMS server.

	Possible values:
	▶ `marked` (default setting)
	  Access is activated for the adjacent IP address range.
	▶ `unmarked`
	  Access is deactivated.

Modbus TCP	Activates/deactivates the access to the *Modbus TCP* server.

	Possible values:
	▶ `marked` (default setting)
	  Access is activated for the adjacent IP address range.
	▶ `unmarked`
	  Access is deactivated.

Active	Activates/deactivates the table entry.

	Possible values:
	▶ `marked` (default setting)
	  Table entry is activated. The device restricts the management access to the adjacent IP address range and the selected IP-based applications.
	▶ `unmarked`
	  Table entry is deactivated.

■ Buttons

You find the description of the standard buttons in section .

3.3.3 Web

In this dialog, you specify settings for the graphical user interface.

■ Configuration

Parameters	Meaning
Web interface session timeout [min]	Specifies the timeout in minutes. After the device has been inactive for this time it ends the session for the user logged on.
	Possible values:
	▶ 0..160 (default setting: 5)
	The value 0 deactivates the function, and the user remains logged on when inactive.

■ Buttons

You find the description of the standard buttons in section "Buttons" on page 16.

3.3.4   Command Line Interface

In this dialog, you specify settings for the Command Line Interface (CLI). You find detailed information about the Command Line Interface in the "Command Line Interface" reference manual.

The dialog contains the following tabs:
▶ [Global]
▶ [Login banner]

[Global]

This tab allows you to change the CLI prompt and to specify the automatic closing of sessions through the V.24 interface when they have been inactive.

■ Configuration

Parameters	Meaning
Login prompt	Specifies the character string that the device displays in the Command Line Interface (CLI) at the start of every command line.
	Possible values: ▶ Alphanumeric ASCII character string with 0..128 characters (`0x20..0x7E`) including space characters Wildcards – `%d` date – `%i` IP address – `%m` MAC address – `%p` product name – `%t` time Default setting: `(EESX)`
	Changes to this setting are immediately effective in the active CLI session.
V.24 timeout [min]	Specifies the time in minutes after which the device automatically closes the session of a logged on user in the Command Line Interface via the V.24 interface when it has been inactive.
	Possible values: ▶ `0..160` (default setting: `5`) The value `0` deactivates the function, and the user remains logged on when inactive.
	A change in the value takes effect the next time a user logs on to the device.
	For Telnet and SSH, you specify the timeout in the *Device Security > Management Access > Server* dialog.

■ Buttons

You find the description of the standard buttons in section "Buttons" on page 16.

[**Login banner**]

In this tab, you replace the CLI start screen with your own text.

In the default setting, the CLI start screen displays information about the device, such as the software version and the device settings. With the function in this tab, you deactivate this information and replace it with an individually specified text.

To display your own text in the CLI and in the graphical user interface before the login, you use the *Device Security > Pre-login Banner* dialog.

■ **Operation**

Parameters	Meaning
Operation	Enables/disables the *Login banner* function.

	Possible values:
	▶ On
	    The *Login banner* function is enabled.
	    The device displays the text information specified in the *Banner text* field to the users that login to the device using the Command Line Interface (CLI).
	▶ Off (default setting)
	    The *Login banner* function is disabled.
	    The CLI start screen displays information about the device. The text information in the *Banner text* field is kept.

■ **Banner text**

Parameters	Meaning
Banner text	Specifies the character string that the device displays in the Command Line Interface at the start of every session.
	Possible values: ▶ Alphanumeric ASCII character string with 0..1024 characters (0x20..0x7E) including space characters ▶ <Tab> ▶ <Line break>
Remaining characters	Displays how many characters are still remaining in the *Banner text* field for the text information.
	Possible values: ▶ 1024..0

■ **Buttons**

You find the description of the standard buttons in section "Buttons" on page 16.

3.3.5 SNMPv1/v2 Community

In this dialog, you specify the community name for SNMPv1/v2 applications.

Applications send requests via SNMPv1/v2 with a community name in the SNMP data packet header. Depending on the community name, the application gets read authorization or read and write authorization for the device.

You activate the access to the device via SNMPv1/v2 in the **Device Security > Management Access > Server** dialog.

■ Table

Parameters	Meaning
Community	Displays the authorization for SNMPv1/v2 applications to the device: ▶ `Write` For requests with the community name entered, the application receives read and write authorization for the device. ▶ `Read` For requests with the community name entered, the application receives read authorization for the device.
Name	Specifies the community name for the adjacent authorization. Possible values: ▶ Alphanumeric ASCII character string with 0..32 characters `private` (default setting for read and write authorizations) `public` (default setting for read authorization)

■ Buttons

You find the description of the standard buttons in section "Buttons" on page 16.

3.4   Pre-login Banner

This dialog allows you to display a greeting or information text to users before they login to the device.

The users see this text in the login dialog of the graphical user interface (GUI) and of the Command Line Interface (CLI). Users logging in with SSH see the text - regardless of the client used - before or during the login.

To display the text in the Command Line Interface (CLI) exclusively, use the settings in the *Device Security > Management Access > CLI* dialog.

■ Operation

Parameters	Meaning

Operation	Enables/disables the *Pre-login Banner* function.
	Using the *Pre-login Banner* function, the device displays a greeting or information text in the login dialog of the Graphical User Interface and of the Command Line Interface.
	
	Possible values:
	▶ `On`
	   The *Pre-login Banner* function is enabled.
	   The device displays the text specified in the *Banner text* field in the login dialog.
	▶ `Off` (default setting)
	   The *Pre-login Banner* function is disabled.
	   The device does not display a text in the login dialog. If you entered a text in the *Banner text* field, this text is saved on the device.

■ Banner text

Parameters	Meaning
Banner text	Specifies information text that the device displays in the Login dialog of the graphical user interface (GUI) and of the Command Line Interface (CLI). Possible values: ▶ Alphanumeric ASCII character string with 0..512 characters (`0x20..0x7E`) including space characters ▶ `<Tab>` ▶ `<Line break>`
Remaining characters	Displays how many characters are still remaining in the *Banner text* field. Possible values: ▶ `512..0`

■ Buttons

You find the description of the standard buttons in section "Buttons" on page 16.

4 Network Security

The menu contains the following dialogs:
- ▶ Network Security Overview
- ▶ Port Security
- ▶ 802.1X Port Authentication
- ▶ RADIUS
- ▶ DoS
- ▶ ACL

4.1 Network Security Overview

This dialog displays the network security rules used in the device.

■ Parameter

Parameters	Meaning
Port/VLAN	Specifies whether the device displays VLAN- and/or port-based rules.
	Possible values:
	▶ `All` (default setting)
	The device displays the VLAN- and port-based rules specified by you.
	▶ `Port: <Port Number>`
	The device displays port-based rules for a specific port. This selection is available if you have specified one or more rules for this port.
	▶ `VLAN: <VLAN ID>`
	The device displays VLAN-based rules for a specific VLAN. This selection is available if you have specified one or more rules for this VLAN.
ACL	Displays the ACL rules in the overview.
	You edit Access Control Lists in the *Network Security > ACL* dialog.
All	Marks the adjacent checkboxes. The device displays the related rules in the overview.
None	Unmarks the adjacent checkboxes. The device does not display any rules in the overview.

■ Buttons

You find the description of the standard buttons in section "Buttons" on page 16.

4.2   Port Security

The device allows you to transmit only data packets from desired senders on one port. When this function is enabled, the device checks the VLAN ID and MAC address of the sender before it transmits a data packet. The device discards data packets from other senders and logs this event. If the *Auto-Disable* function is activated, the device disables the port. This restriction makes MAC Spoofing attacks more difficult. The *Auto-Disable* function enables the relevant port again automatically when the parameters are no longer being exceeded.

In this dialog a *Wizard* window helps you to connect the ports with one or more desired sources. In the device these addresses are known as *Static entries (/)*. To view the specified static addresses, highlight the relevant port and click the ⚡ button.

To keep the setup process as simple as possible, the device allows you to record the desired senders automatically. The device "learns" the senders by evaluating the received data packets. In the device these addresses are known as *Dynamic entries*. When a user-defined upper limit has been reached (*Dynamic limit*), the device stops the "learning" on the relevant port and transmits exclusively the data packets of the senders already recorded. When you adjust 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 1st data packet from unknown senders. Using this 1st data packet, the device checks whether the upper limit has been reached. The device records the sender until the upper limit is reached. Afterwards, the device transmits data packets that it receives on the relevant port from this sender.

■ Operation

Parameters	Meaning
Operation	Enables/disables the *Port Security* function.
	Possible values:
	▶ `On` The *Port Security* function is enabled. The device checks the VLAN ID and MAC address of the source before it transmits a data packet. The device transmits solely a received data packet if its source is desired on the relevant port. Also activate the checking of the source on the relevant ports. ▶ `Off` (default setting) The *Port Security* function is disabled. The device transmits every received data packet without checking the source.

■ Configuration

Parameters	Meaning
Auto-disable	Activates/deactivates the *Auto-Disable* function for *Port Security*.
	Possible values:
	▶ `marked` The *Auto-Disable* function for *Port Security* is active. Also mark the checkbox in the *Auto-disable* column for the relevant ports. ▶ `unmarked` (default setting) The *Auto-Disable* function for *Port Security* is inactive.

■ Table

Parameters	Meaning
Port	Displays the port number.

Parameters	Meaning
Active	Activates/deactivates the checking of the source on the port. Possible values: ▶ `marked` The device checks every data packet received on the port and transmits it if its source is desired. Also enable the function in the `Operation` frame. ▶ `unmarked` (default setting) The device transmits every data packet received on the port without checking the source. **Note:** If you are operating the device as an active subscriber within an MRP ring, we recommend you unmark the checkbox.
Auto-disable	Activates/deactivates the `Auto-Disable` function for the parameters that the `Port Security` function is monitoring on the port. Possible values: ▶ `marked` (default setting) The `Auto-Disable` function is active on the port. The prerequisite is that you mark the checkbox `Auto-disable` in the `Configuration` frame. – The device disables the port if the port registers undesired source MAC addresses or more source MAC addresses than specified in the `Dynamic limit` column. The "Link status" LED for the port flashes 3× per period. – The `Diagnostics > Ports > Auto-Disable` dialog displays which ports are currently disabled due to the parameters being exceeded. – The `Auto-Disable` function reactivates the port automatically. For this you go to the `Diagnostics > Ports > Auto-Disable` dialog and specify a waiting period for the relevant port in the `Reset timer [s]` column. ▶ `unmarked` The `Auto-Disable` function on the port is inactive.
Send trap	Activates/deactivates the sending of SNMP traps when the device discards data packets from an undesired sender on the port. Possible values: ▶ `marked` The device sends an SNMP trap when it discards data packets from an undesired sender on the port. ▶ `unmarked` (default setting) The sending of SNMP traps is deactivated. The prerequisite for sending SNMP traps is that you enable the function in the `Diagnostics > Status Configuration > Alarms (Traps)` dialog and specify at least 1 trap destination.
Trap interval [s]	Specifies the delay time in seconds that the device waits after sending an SNMP trap before sending the next SNMP trap. Possible values: ▶ `0..3600` (default setting: `0`) The value `0` deactivates the delay time.
Dynamic limit	Specifies the upper limit for the number of automatically registered sources (`Dynamic entries`). When the upper limit has been reached, the device stops "learning" on this port. Adjust the value to the number of expected sources. If the port registers more senders than specified here, the port disables the `Auto-Disable` function. The prerequisite is that you mark the checkbox in the `Auto-disable` column and the `Auto-disable` checkbox in the `Configuration` frame. Possible values: ▶ `0` Deactivates the automatic registering of sources on this port. ▶ `1..600` (default setting: `600`)
Static limit	Specifies the upper limit for the number of sources connected to the port (`Static entries (/)`). The `Wizard` window helps you to connect the port with one or more desired sources. Possible values: ▶ `0..64` (default setting: `64`) The value `0` helps prevent you from connecting a source with the port.

Parameters	Meaning
Dynamic entries	Displays the number of senders that the device has automatically determined. See the *Wizard* window, *Dynamic entries* field.
Static entries	Displays the number of senders that are linked with the port. See the *Wizard* window, *Static entries (/)* field.
Last violating VLAN ID/MAC	Displays the VLAN ID and MAC address of an undesired sender whose data packets the device last discarded on this port.
Sent traps	Displays the number of discarded data packets on this port that caused the device to send an SNMP trap.

■ Buttons

You find the description of the standard buttons in section .

Button	Meaning
🪄	Opens the *Wizard* dialog. In the *Wizard* dialog you assign the permitted MAC addresses to a port.

[Wizard : Port security]

■ Select port

The `Wizard` window helps you to connect the ports with one or more desired sources.

Parameters	Meaning
Port	Specifies the port that you assign to the sender in the next step.

■ Addresses

The `Wizard` window helps you to connect the ports with one or more desired sources. When you have specified the settings, click the `Finish` button.

After closing the `Wizard` window, click the ✅ button to save your settings.

Parameters	Meaning
VLAN ID	Specifies the VLAN ID of the desired source.
	Possible values:
	▶ `1..4042`
	To transfer the VLAN ID and the MAC address to the `Static entries (/)` field, click the `Add` button.
MAC address	Specifies the MAC address of the desired source.
	Possible values:
	▶ Valid Unicast MAC address
	Specify the value in one of the following formats:
	– without a separator, for example `001122334455`
	– separated by spaces, for example `00 11 22 33 44 55`
	– separated by colons, for example `00:11:22:33:44:55`
	– separated by hyphens, for example `00-11-22-33-44-55`
	– separated by points, for example `00.11.22.33.44.55`
	– separated by points after every 4th character, for example `0011.2233.4455`
	To transfer the VLAN ID and the MAC address to the `Static entries (/)` field, click the `Add` button.
Add	Transfers the values specified in the `VLAN ID` and `MAC address` fields to the `Static entries (/)` field.
Static entries (/)	Displays the VLAN ID and MAC address of desired senders connected to the port.
	The device uses this field to display the number of senders connected to the port and the upper limit. You specify the upper limit for the number of entries in the table, `Static limit` field.
	Note: You cannot assign a MAC address that you assign to this port to any other port.
Remove	Removes the entries highlighted in the `Static entries (/)` field.
←	Moves the entries highlighted in the `Dynamic entries` field to the `Static entries (/)` field.
«	Moves every entry from the `Dynamic entries` field to the `Static entries (/)` field.
	If the `Dynamic entries` field contains more entries than are allowed in the `Static entries (/)` field, the device moves the foremost entries until the upper limit is reached.
Dynamic entries	Displays in ascending order the VLAN ID and MAC address of the senders automatically recorded on this port. The device transmits data packets from these senders when it receives the data packets on this port.
	You specify the upper limit for the number of entries in the table, `Dynamic limit` field.
	The ← and « buttons allow you to transfer entries from this field into the `Static entries (/)` field. In this way, you connect the relevant senders with the port.

Note: The device saves the sources connected with the port until you deactivate the checking of the source on the relevant port or in the `Operation` frame.

4.3   802.1X Port Authentication

With the port-based access control according to IEEE 802.1X, the device monitors the access to the network from connected end devices. The device (authenticator) allows an end device (supplicant) to access the network if it logs in with valid login data. The authenticator and the end devices communicate via the EAPoL (Extensible Authentication Protocol over LANs) authentication protocol.

The device supports the following methods to authenticate end devices:
▶ `radius`
  A RADIUS server in the network authenticates the end devices.
▶ `ias`
  The Integrated Authentication Server (IAS) implemented in the device authenticates the end devices. Compared to RADIUS, the IAS provides basic functions exclusively.

The menu contains the following dialogs:
▶ 802.1X Global
▶ 802.1X Port Configuration
▶ 802.1X Port Clients
▶ 802.1X EAPOL Port Statistics
▶ 802.1X Port Authentication History
▶ 802.1X Integrated Authentication Server

4.3.1 802.1X Global

This dialog allows you to specify basic settings for the port-based access control.

■ Operation

Parameters	Meaning
Operation	Enables/disables the *802.1X Port Authentication* function. Possible values: ▶ `On` The *802.1X Port Authentication* function is enabled. The device checks the access to the network from connected end devices. The port-based access control is enabled. ▶ `Off` (default setting) The *802.1X Port Authentication* function is disabled. The port-based access control is disabled.

■ Configuration

Parameters	Meaning
VLAN assignment	Activates/deactivates the assigning of the relevant port to a VLAN. This function allows you to provide selected services to the connected end device in this VLAN. Possible values: ▶ `marked` The assigning is active. If the end device successfully authenticates itself, the device assigns to the relevant port the VLAN ID transferred by the RADIUS authentication server. ▶ `unmarked` (default setting) The assigning is inactive. The relevant port is assigned to the VLAN specified in the *Network Security > 802.1X Port Authentication > Port Configuration* dialog, *Assigned VLAN ID* row.
Dynamic VLAN creation	Activates/deactivates the automatic creation of the VLAN assigned by the RADIUS authentication server if the VLAN does not exist. Possible values: ▶ `marked` The automatic VLAN creation is active. The device creates the VLAN if it does not exist. ▶ `unmarked` (default setting) The automatic VLAN creation is inactive. If the assigned VLAN does not exist, the port remains assigned to the original VLAN.
Monitor mode	Activates/deactivates the monitor mode. Possible values: ▶ `marked` The monitor mode is active. The device monitors the authentication and helps with diagnosing detected errors. If an end device has not logged in successfully, the device gives the end device access to the network. ▶ `unmarked` (default setting) The monitor mode is inactive.

■ **Information**

Parameters	Meaning
Monitor mode clients	Displays to how many end devices the device gave network access even though they did not login successfully. The prerequisite is that you activate the *Monitor mode* function. See the *Configuration* frame.
Non monitor mode clients	Displays the number of end devices to which the device gave network access after successful login.
Policy 1	Displays the method that the device currently uses to authenticate the end devices using IEEE 802.1X. You specify the method used in the *Device Security > Authentication List* dialog. □ To authenticate the end devices through a RADIUS server, you assign the `radius` policy to the `8021x` list. □ To authenticate the end devices through the Integrated Authentication Server (IAS) you assign the `ias` policy to the `8021x` list.

■ **Buttons**

You find the description of the standard buttons in section "Buttons" on page 16.

4.3.2   802.1X Port Configuration

This dialog allows you to specify the access settings for every port.

■ Table

Parameters	Meaning
Port	Displays the port number.
Port initialization	Activates/deactivates the port initialization in order to activate the access control on the port or reset it to its initial state. Use this function exclusively to ports in which the *Port control* column contains the value `auto`. Possible values: ▶ `marked` The port initialization is active. When the initialization is complete, the device changes the value to `unmarked` again. ▶ `unmarked` (default setting) The port initialization is inactive. The device keeps the current port status.
Port reauthentication	Activates/deactivates the one-time reauthentication request. Use this function exclusively to ports in which the *Port control* column contains the value `auto`. The device also allows you to periodically request the end device to login again. See the *Periodic reauthentication* column. Possible values: ▶ `marked` The one-time reauthentication request is active. The device requests the end device to login again. Afterwards, the device changes the value to `unmarked` again. ▶ `unmarked` (default setting) The one-time reauthentication request is inactive. The device keeps the end device logged in.
Authentication activity	Displays the current status of the Authenticator (`Authenticator PAE state`). Possible values: ▶ `initialize` ▶ `disconnected` ▶ `connecting` ▶ `authenticating` ▶ `authenticated` ▶ `aborting` ▶ `held` ▶ `forceAuth` ▶ `forceUnauth`
Backend authentication state	Displays the current status of the connection to the authentication server (`Backend Authentication state`). Possible values: ▶ `request` ▶ `response` ▶ `success` ▶ `fail` ▶ `timeout` ▶ `idle` ▶ `initialize`
Authentication state	Displays the current status of the authentication on the port (`Controlled Port Status`). Possible values: ▶ `authorized` The end device is logged in successfully. ▶ `unauthorized` The end device is not logged in.

Parameters	Meaning
Port control	Specifies how the device grants access to the network (`Port control mode`). Possible values: ▶ `forceUnauthorized` The device blocks the access to the network. You use this setting if an end device is connected to the port that does not receive access to the network. ▶ `auto` The device grants access to the network if the end device has logged in successfully. You use this setting if an end device is connected to the port that logs in at the authenticator. **Note:** If other end devices are connected through the same port, they get access to the network without additional authentication. ▶ `forceAuthorized` (default setting) If end devices do not support IEEE 802.1X, the device grants access to the network. You use this setting if an end device is connected to the port that receives access to the network without logging in.
Quiet period [s]	Specifies the time period in seconds in which the authenticator does not accept any more logins from the end device after an unsuccessful log in attempt (`Quiet period [s]`). Possible values: ▶ `0..65535` (default setting: `60`)
Transmit period [s]	Specifies the period in seconds after which the authenticator requests the end device to login again. After this waiting period, the device sends an EAP request/identity data packet to the end device. Possible values: ▶ `1..65535` (default setting: `30`)
Supplicant timeout period [s]	Specifies the period in seconds for which the authenticator waits for the login of the end device. Possible values: ▶ `1..65535` (default setting: `30`)
Server timeout [s]	Specifies the period in seconds for which the authenticator waits for the response from the authentication server (RADIUS or IAS). Possible values: ▶ `1..65535` (default setting: `30`)
Requests (max.)	Specifies how many times the authenticator requests the end device to login until the time specified in the *Supplicant timeout period [s]* column has elapsed. The device sends an EAP request/identity data packet to the end device as often as specified here. Possible values: ▶ `0..10` (default setting: `2`)
Assigned VLAN ID	Displays the ID of the VLAN that the authenticator assigned to the port. This value applies exclusively to ports in which the *Port control* column contains the value `auto`. Possible values: ▶ `0..4042` (default setting: `0`) You find the VLAN ID that the authenticator assigned to the ports in the *Network Security > 802.1X Port Authentication > Port Clients* dialog.
Assignment reason	Displays the cause for the assignment of the VLAN ID. This value applies exclusively to ports in which the *Port control* column contains the value `auto`. Possible values: ▶ `notAssigned` (default setting) ▶ `radius` ▶ `guestVlan` ▶ `unauthenticatedVlan` You find the VLAN ID that the authenticator assigned to the ports for a supplicant in the *Network Security > 802.1X Port Authentication > Port Clients* dialog.
Reauthentication period [s]	Specifies the period in seconds after which the authenticator periodically requests the end device to login again. Possible values: ▶ `1..65535` (default setting: `3600`)

Parameters	Meaning
Periodic reauthentication	Activates/deactivates periodic reauthentication requests.
	Possible values: ▶ `marked` The periodic reauthentication requests are active. The device periodically requests the end device to login again. You specify this time period in the *Reauthentication period [s]* column. This setting becomes ineffective if the authenticator has assigned the end device the ID of a Voice, Unauthenticated or Guest VLAN. ▶ `unmarked` (default setting) The periodic reauthentication requests are inactive. The device keeps the end device logged in.
Guest VLAN ID	Specifies the ID of the VLAN that the authenticator assigns to the port if the end device does not log in during the time period specified in the *Guest VLAN period* column. This value applies exclusively to ports in which the *Port control* column contains the value `auto`.
	This function allows you to grant end devices, without IEEE 802.1X support, access to selected services in the network.
	Possible values: ▶ `0` (default setting) The authenticator does not assign a guest VLAN to the port. ▶ `1..4042`
	Note: The *MAC authorized bypass* function and the *Guest VLAN ID* function cannot be in use simultaneously.
Guest VLAN period	Specifies the period in seconds for which the authenticator waits for EAPOL data packets after the end device is connected. If this period elapses, the authenticator grants the end device access to the network and assigns the port to the guest VLAN specified in the *Guest VLAN ID* column.
	Possible values: ▶ `1..300` (default setting: `90`)
Unauthenticated VLAN ID	Specifies the ID of the VLAN that the authenticator assigns to the port if the end device does not login successfully. This value applies exclusively to ports in which the *Port control* column contains the value `auto`.
	This function allows you to grant end devices without valid login data access to selected services in the network.
	Possible values: ▶ `0..4042` (default setting: `0`)
	The effect of the value `0` is that the authenticator does not assign a Unauthenticated VLAN to the port.
	Note: Assign to the port a VLAN set up statically in the device.

■ Buttons

You find the description of the standard buttons in section .

4.3.3 802.1X Port Clients

This dialog displays information on the connected end devices.

■ Table

Parameters	Meaning
Port	Displays the port number.
User name	Displays the user name with which the end device logged in.
MAC address	Displays the MAC address of the end device.
Assigned VLAN ID	Displays the VLAN ID that the authenticator assigned to the port after the successful authentication of the end device.
Assignment reason	Displays the reason for the assignment of the VLAN. Possible values: ▶ `default` ▶ `radius` ▶ `unauthenticatedVlan` ▶ `guestVlan` ▶ `monitorVlan` ▶ `invalid` The field displays solely a valid value as long as the client is authenticated.
Session timeout	Displays the remaining time in seconds until the log in of the end device expires. This value applies solely if for the port in the *Network Security > 802.1X Port Authentication > Port Configuration* dialog, *Port control* column the value `auto` is specified. The authentication server assigns the timeout period to the device through RADIUS. The value `0` means that the authentication server has not assigned a timeout.
Termination action	Displays the action performed by the device when the login has elapsed. Possible values: ▶ `default` ▶ `reauthenticate`

■ Buttons

You find the description of the standard buttons in section "Buttons" on page 16.

4.3.4　　802.1X EAPOL Port Statistics

This dialog displays which EAPOL data packets the end device has sent and received for the authentication of the end devices.

■ **Table**

Parameters	Meaning
Port	Displays the port number.
Received packets	Displays the total number of EAPOL data packets that the device received on the port.
Transmitted packets	Displays the total number of EAPOL data packets that the device sent on the port.
Start packets	Displays the number of EAPOL start data packets that the device received on the port.
Logoff packets	Displays the number of EAPOL logoff data packets that the device received on the port.
Response/ID packets	Displays the number of EAP response/identity data packets that the device received on the port.
Response packets	Displays the number of valid EAP response data packets that the device received on the port (without EAP response/identity data packets).
Request/ID packets	Displays the number of EAP request/identity data packets that the device received on the port.
Request packets	Displays the number of valid EAP request data packets that the device received on the port (without EAP request/identity data packets).
Invalid packets	Displays the number of EAPOL data packets with an unknown frame type that the device received on the port.
Received error packets	Displays the number of EAPOL data packets with an invalid packet body length field that the device received on the port.
Packet version	Displays the protocol version number of the EAPOL data packet that the device last received on the port.
Source of last received packet	Displays the sender MAC address of the EAPOL data packet that the device last received on the port. The value `00:00:00:00:00:00` means that the port has not received any EAPOL data packets yet.

■ **Buttons**

You find the description of the standard buttons in section "Buttons" on page 16.

4.3.5   802.1X Port Authentication History

The device registers the authentication process of the end devices that are connected to its ports. This dialog displays the information recorded during the authentication.

■ Table

Parameters	Meaning
Port	Displays the port number.
Authentification time stamp	Displays the time at which the authenticator authenticated the end device.
Result age	Displays since when this entry has been entered in the table.
MAC address	Displays the MAC address of the end device.
VLAN ID	Displays the ID of the VLAN that was assigned to the end device before the login.
Authentication status	Displays the status of the authentication on the port. Possible values: ▶ `success` The authentication was successful. ▶ `failure` The authentication failed.
Access status	Displays whether the device grants the end device access to the network. Possible values: ▶ `granted` The device grants the end device access to the network. ▶ `denied` The device denies the end device access to the network.
Assigned VLAN ID	Displays the ID of the VLAN that the authenticator assigned to the port.
Assignment type	Displays the type of the VLAN that the authenticator assigned to the port. Possible values: ▶ `default` ▶ `radius` ▶ `unauthenticatedVlan` ▶ `guestVlan` ▶ `monitorVlan` ▶ `notAssigned`
Assignment reason	Displays the reason for the assignment of the VLAN ID and the VLAN type.

■ 802.1X Port Authentication History

Parameters	Meaning
Port	Simplifies the table and displays solely the entries relating to the port selected here. This makes it easier for you to record the table and sort it as you desire. Possible values: ▶ `all` The table displays the entries for every port. ▶ `<Port number>` The table displays the entries that apply to the port selected here.

■ Buttons

You find the description of the standard buttons in section "Buttons" on page 16.

4.3.6 802.1X Integrated Authentication Server

The Integrated Authentication Server (IAS) allows you to authenticate end devices using IEEE 802.1X. Compared to RADIUS, the IAS has a very limited range of functions. The authentication is based solely on the user name and the password.

In this dialog you manage the login data of the end devices. The device allows you to set up to 100 sets of login data.

To authenticate the end devices through the Integrated Authentication Server you assign in the ***Device Security > Authentication List*** dialog the `ias` policy to the 8021x list.

■ **Table**

Parameters	Meaning
User name	Displays the user name of the end device.
	To create a new user, click the 🔲 button.
Password	Specifies the password with which the user authenticates.
	Possible values: ▶ Alphanumeric ASCII character string with 0..64 characters
	The device differentiates between upper and lower case.
Active	Activates/deactivates the login data.
	Possible values: ▶ `marked` The login data is active. An end device has the option of logging in through IEEE 802.1X using this login data. ▶ `unmarked` (default setting) The login data is inactive.

■ **Buttons**

You find the description of the standard buttons in section "Buttons" on page 16.

Button	Meaning
🔲	Opens the ***Create*** window to add a new entry to the table. In the ***User name*** field, you specify the user name of the end device.

4.4   RADIUS

With its factory settings, the device authenticates users based on the local user management. However, as the size of a network increases, it becomes more difficult to keep the login data of the users consistent across the devices.

RADIUS (Remote Authentication Dial-In User Service) allows you to authenticate and authorize the users at a central point in the network. A RADIUS server performs the following tasks here:
▶ Authentication
  The authentication server authenticates the users when the RADIUS client at the access point forwards the users' login data to the server.
▶ Authorization
  The authentication server authorizes logged in users for selected services by assigning various parameters for the relevant end device to the RADIUS client at the access point.
▶ Accounting
  The accounting server records the traffic data that has occurred during the port authentication according to IEEE 802.1X. This enables you to subsequently determine which services the users have used, and to what extent.

The device operates in the role of the RADIUS client if you assign the `radius` policy to an application in the *Device Security > Authentication List* dialog. The device forwards the users' login data to the primary authentication server. The authentication server decides whether the login data is valid and transfers the user's authorizations to the device.

The device assigns the Service Type transferred in the response of a RADIUS server as follows to a user role existing in the device:
– `Administrative-User: administrator`
– `Login-User: operator`
– `NAS-Prompt-User: guest`

The device also allows you to authenticate end devices with IEEE 802.1X through an authentication server. To do this, you assign the `radius` policy to the `8021x` list in the *Device Security > Authentication List* dialog.

The menu contains the following dialogs:
▶ RADIUS Global
▶ RADIUS Authentication Server
▶ RADIUS Accounting Server
▶ RADIUS Authentication Statistics
▶ RADIUS Accounting Statistics

4.4.1 RADIUS Global

This dialog allows you to specify basic settings for RADIUS.

■ RADIUS configuration

Parameters	Meaning
Retransmits (max.)	Specifies how many times the device retransmits an unanswered request to the authentication server before the device sends the request to an alternative authentication server.
	Possible values: ▶ `1..15` (default setting: `4`)
Timeout [s]	Specifies how many seconds the device waits for a response after a request to an authentication server before it retransmits the request.
	Possible values: ▶ `1..30` (default setting: `5`)
Accounting	Activates/deactivates the accounting.
	Possible values: ▶ `marked` Accounting is active. The device sends the traffic data to an accounting server specified in the *Network Security > RADIUS > Accounting Server* dialog. ▶ `unmarked` (default setting) Accounting is inactive.
NAS IP address (attribute 4)	Specifies the IP address that the device transfers to the authentication server as attribute 4. Specify the IP address of the device or another available address.
	Possible values: ▶ Valid IPv4 address (default setting: `0.0.0.0`)
	In many cases, there is a firewall between the device and the authentication server. In the Network Address Translation (NAT) in the firewall changes the original IP address, and the authentication server receives the translated IP address of the device. The device transfers the IP address in this field unchanged across the Network Address Translation (NAT).

■ Buttons

You find the description of the standard buttons in section "Buttons" on page 16.

Button	Meaning
Reset	Deletes the statistics in the *Network Security > RADIUS > Authentication Statistics* dialog and in the *Network Security > RADIUS > Accounting Statistics* dialog.

4.4.2 RADIUS Authentication Server

This dialog allows you to specify up to 8 authentication servers. An authentication server authenticates and authorizes the users when the device forwards the login data to the server.

The device sends the login data to the specified primary authentication server. If the server does not respond, the device contacts the specified authentication server that is highest in the table. If no response comes from this server either, the device contacts the next server in the table.

■ Table

Parameters	Meaning
Index	Displays the index number to which the table entry relates.
Name	Displays the name of the server. To change the value, click the relevant field. Possible values: ▶ Alphanumeric ASCII character string with 1..32 characters (default setting: `Default-RADIUS-Server`)
Address	Specifies the IP address of the server. Possible values: ▶ Valid IPv4 address
Destination UDP port	Specifies the number of the UDP port on which the server receives requests. Possible values: ▶ `0..65535` (default setting: `1812`) Exception: Port `2222` is reserved for internal functions.
Secret	Displays ****** (asterisks) when you specify a password with which the device logs in to the server. To change the password, click the relevant field. Possible values: ▶ Alphanumeric ASCII character string with 1..64 characters You get the password from the administrator of the authentication server.
Primary server	Specifies the authentication server as primary or secondary. Possible values: ▶ `marked` The server is specified as the primary authentication server. The device sends the login data for authenticating the users to this authentication server. If you activate multiple servers, the device specifies the last server activated as the primary authentication server. ▶ `unmarked` (default setting) The server is the secondary authentication server. The device sends the login data to the secondary authentication server if it does not receive a response from the primary authentication server.
Active	Activates/deactivates the connection to the server. The device uses the server, if you specify in the **Device Security > Authentication List** dialog the value `radius` in one of the rows **Policy 1** to **Policy 5**. Possible values: ▶ `marked` (default setting) The connection is active. The device sends the login data for authenticating the users to this server if the preconditions named above are fulfilled. ▶ `unmarked` The connection is inactive. The device does not send any login data to this server.

■ **Buttons**

You find the description of the standard buttons in section "Buttons" on page 16.

Button	Meaning
	Opens the *Create* window to add a new entry to the table.
	▶ In the *Index* field, you specify the index number.
	▶ In the *Address* field, you specify the IP address of the server.

4.4.3   RADIUS Accounting Server

This dialog allows you to specify up to 8 accounting servers. An accounting server records the traffic data that has occurred during the port authentication according to IEEE 802.1X. The prerequisite is that you activate in the *Network Security > RADIUS > Global* menu the *Accounting* function.

The device sends the traffic data to the first accounting server that can be reached. If it does not respond, the device contacts the next server in the table.

■ Table

Parameters	Meaning
Index	Displays the index number to which the table entry relates. Possible values: ▶ `1..8`
Name	Displays the name of the server. To change the value, click the relevant field. Possible values: ▶ Alphanumeric ASCII character string with 1..32 characters (default setting: `Default-RADIUS-Server`)
Address	Specifies the IP address of the server. Possible values: ▶ Valid IPv4 address
Destination UDP port	Specifies the number of the UDP port on which the server receives requests. Possible values: ▶ `0..65535` (default setting: `1813`) Exception: Port `2222` is reserved for internal functions.
Secret	Displays ****** (asterisks) when you specify a password with which the device logs in to the server. To change the password, click the relevant field. Possible values: ▶ Alphanumeric ASCII character string with 1..16 characters You get the password from the administrator of the authentication server.

Active	Activates/deactivates the connection to the server.
	
	Possible values:
	▶ `marked` (default setting)
	   The connection is active. The device sends traffic data to this server if the preconditions named above are fulfilled.
	▶ `unmarked`
	   The connection is inactive. The device does not send any traffic data to this server.

■ Buttons

You find the description of the standard buttons in section "Buttons" on page 16.

Button	Meaning
	Opens the *Create* window to add a new entry to the table. ▶ In the *Index* field, you specify the index number. ▶ In the *Address* field, you specify the IP address of the server.

4.4.4　　　RADIUS Authentication Statistics

This dialog displays information about the communication between the device and the authentication server. The table displays the information for each server in a separate row.

To delete the statistic, click in the *Network Security > RADIUS > Global* dialog the *Clear RADIUS statistics?* button.

■ Table

Parameters	Meaning
Name	Displays the name of the server.
Address	Displays the IP address of the server.
Round trip time	Displays the time interval in hundredths of a second between the last response received from the server (Access Reply/Access Challenge) and the corresponding data packet sent (Access Request).
Access requests	Displays the number of access data packets that the device sent to the server. This value does not take repetitions into account.
Retransmitted access-request packets	Displays the number of access data packets that the device retransmitted to the server.
Access accepts	Displays the number of access accept data packets that the device received from the server.
Access rejects	Displays the number of access reject data packets that the device received from the server.
Access challenges	Displays the number of access challenge data packets that the device received from the server.
Malformed access responses	Displays the number of malformed access response data packets that the device received from the server (including data packets with an invalid length).
Bad authenticators	Displays the number of access response data packets with an invalid authenticator that the device received from the server.
Pending requests	Displays the number of access request data packets that the device sent to the server to which it has not yet received a response from the server.
Timeouts	Displays how many times no response to the server was received before the specified waiting time elapsed.
Unknown types	Displays the number data packets with an unknown data type that the device received from the server on the authentication port.
Packets dropped	Displays the number of data packets that the device received from the server on the authentication port and then discarded them.

■ Buttons

You find the description of the standard buttons in section "Buttons" on page 16.

4.4.5 RADIUS Accounting Statistics

This dialog displays information about the communication between the device and the accounting server. The table displays the information for each server in a separate row.

To delete the statistic, click in the *Network Security > RADIUS > Global* dialog the *Clear RADIUS statistics?* button.

■ Table

Parameters	Meaning
Name	Displays the name of the server.
Address	Displays the IP address of the server.
Round trip time	Displays the time interval in hundredths of a second between the last response received from the server (Accounting Response) and the corresponding data packet sent (Accounting Request).
Accounting-request packets	Displays the number of accounting request data packets that the device sent to the server. This value does not take repetitions into account.
Retransmitted accounting-request packets	Displays the number of accounting request data packets that the device retransmitted to the server.
Received packets	Displays the number of accounting response data packets that the device received from the server.
Malformed packets	Displays the number of malformed accounting response data packets that the device received from the server (including data packets with an invalid length).
Bad authenticators	Displays the number of accounting response data packets with an invalid authenticator that the device received from the server.
Pending requests	Displays the number of accounting request data packets that the device sent to the server to which it has not yet received a response from the server.
Timeouts	Displays how many times no response to the server was received before the specified waiting time elapsed.
Unknown types	Displays the number data packets with an unknown data type that the device received from the server on the accounting port.
Packets dropped	Displays the number of data packets that the device received from the server on the accounting port and then discarded them.

■ Buttons

You find the description of the standard buttons in section "Buttons" on page 16.

4.5 DoS

Denial of Service (DoS) is a cyber-attack that aims to bring down specific services or devices. In this menu you can set up several filters to protect the device from DoS attacks.

The menu contains the following dialogs:
▶ DoS Global

4.5.1 DoS Global

In this dialog, you specify the DoS settings for the TCP/UDP, IP and ICMP protocols.

■ TCP/UDP

A scanner uses port scans to prepare network attacks. The scanner uses different techniques to determine running devices and open ports. This frame allows you to activate filters for specific scanning techniques.

The device supports the detection of the following scan types:
▶ Null scans
▶ Xmas scans
▶ SYN/FIN scans
▶ TCP Offset attacks
▶ TCP SYN attacks
▶ L4 Port attacks
▶ Minimal Header scans

Parameters	Meaning

Null Scan filter	Activates/deactivates the Null Scan filter.
	The Null Scan filter detects incoming data packets with no TCP flags set and discards them.
	
	Possible values:
	▶ `marked`
	  The filter is active.
	▶ `unmarked` (default setting)
	  The filter is inactive.

Xmas filter	Activates/deactivates the Xmas filter.
	The Xmas filter detects incoming data packets with the TCP flags FIN, URG and PUSH set simultaneously and discards them.
	
	Possible values:
	▶ `marked`
	  The filter is active.
	▶ `unmarked` (default setting)
	  The filter is inactive.

SYN/FIN filter	Activates/deactivates the SYN/FIN filter.
	The SYN/FIN filter detects incoming data packets with the TCP flags SYN and FIN set simultaneously and discards them.
	
	Possible values:
	▶ `marked`
	  The filter is active.
	▶ `unmarked` (default setting)
	  The filter is inactive.

TCP Offset protection	Activates/deactivates the TCP Offset protection.
	The TCP Offset protection detects incoming TCP data packets whose fragment offset field of the IP header is equal to 1 and discards them.
	The TCP Offset protection accepts UDP and ICMP packets whose fragment offset field of the IP header is equal to 1.
	
	Possible values:
	▶ `marked`
	  The protection is active.
	▶ `unmarked` (default setting)
	  The protection is inactive.

Parameters	Meaning

TCP SYN protection	Activates/deactivates the TCP SYN protection.
	The TCP SYN protection detects incoming data packets with the TCP flag SYN set and a L4 source port <1024 and discards them.
	
	Possible values:
	▶ `marked`
	   The protection is active.
	▶ `unmarked` (default setting)
	   The protection is inactive.

L4 Port protection	Activates/deactivates the L4 Port protection.
	The L4 Port protection detects incoming TCP and UDP data packets whose source port number and destination port number are identical and discards them.
	
	Possible values:
	▶ `marked`
	   The protection is active.
	▶ `unmarked` (default setting)
	   The protection is inactive.

Min. Header Size filter	Activates/deactivates the Minimal Header filter.
	The Minimal Header filter compares the TCP header of incoming data packets. If the data offset value multiplied by 4 is smaller than the minimum TCP header size, then the filter discards the data packet.
	
	Possible values:
	▶ `marked`
	   The filter is active.
	▶ `unmarked` (default setting)
	   The filter is inactive.

Min. TCP header size	Displays the minimum size of a valid TCP header.

■ **IP**

This frame allows you to activate or deactivate the Land Attack filter. With the land attack method, the attacking station sends data packets whose source and destination addresses are identical to those of the recipient. When you activate this filter, the device detects data packets with identical source and destination addresses and discards these.

Parameters	Meaning

Land Attack filter	Activates/deactivates the Land Attack filter.
	The Land Attack filter detects incoming IP data packets whose source and destination IP address are identical and discards them.
	
	Possible values:
	▶ `marked`
	   The filter is active.
	▶ `unmarked` (default setting)
	   The filter is inactive.

■ ICMP

This dialog provides you with filter options for the following ICMP parameters:
▶ Fragmented data packets
▶ ICMP packets from a specific size upwards

Parameters	Meaning
Filter fragmented packets	Activates/deactivates the filter for fragmented ICMP packets. The filter detects fragmented ICMP packets and discards them. Possible values: ▶ `marked` The filter is active. ▶ `unmarked` (default setting) The filter is inactive.
Filter by packet size	Activates/deactivates the filter for incoming ICMP packets. The filter detects ICMP packets whose payload size exceeds the size specified in the *Allowed payload size [byte]* field and discards them. Possible values: ▶ `marked` The filter is active. ▶ `unmarked` (default setting) The filter is inactive.
Allowed payload size [byte]	Specifies the maximum allowed payload size of ICMP packets in bytes. Mark the *Filter by packet size* checkbox if you want to discard incoming data packets whose payload size exceeds the maximum allowed size for ICMP packets. Possible values: ▶ `0..1472` (default setting: `512`)

■ Buttons

You find the description of the standard buttons in section "Buttons" on page 16.

4.6 ACL

In this menu, you specify the settings for the Access Control Lists (ACL). Access Control Lists contain rules which the device applies successively to the data stream on its ports or VLANs.

If a data packet complies with the criteria of one or more rules, the device applies the action specified in the first rule applying to the data stream. The device ignores the rules following. Possible actions include:
- ▶ `permit`: The device transmits the data packet to a port or to a VLAN.
- ▶ `deny`: The device drops the data packet.

In the default setting, the device forwards every data packet. Once you assign an Access Control List to an interface or VLAN, there is changing this behavior. The device enters at the end of an Access Control List an implicit Deny-All rule. Consequently, the device discards data packets that do not meet any of the rules. If you want a different behavior, add a "permit" rule at the end of your Access Control Lists.

Proceed as follows to set up Access Control Lists and rules:
- ☐ Create a rule and specify the rule settings. See the *Network Security > ACL > IPv4 Rule* dialog, or the *Network Security > ACL > MAC Rule* dialog.
- ☐ Assign the Access Control List to the Ports and VLANs of the device. See the *Network Security > ACL > Assignment* dialog.

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

4.6.1 ACL IPv4 Rule

In this dialog, you specify the rules that the device applies to the IP data packets.

An Access Control List (group) contains one or more rules. The device applies the rules of an Access Control List successively, beginning with the rule with the lowest value in the *Index* column.

The device allows you to filter according to the following criteria:
▶ Source or destination IP address of a data packet
▶ Type of the transmitting protocol
▶ Source or destination port of a data packet

■ Table

Parameters	Meaning
Group name	Displays the name of the Access Control List. The Access Control List contains the rules.
Index	Displays the number of the rule within the Access Control List. If the Access Control List contains multiple rules, the device processes the rule with the lowest value first.
Match every packet	Specifies to which IP data packets the device applies the rule. Possible values: ▶ `marked` (default setting) The device applies the rule to every IP data packet. ▶ `unmarked` The device applies the rule to IP data packets depending on the value in the fields *Source IP address*, *Destination IP address* and *Protocol*.
Source IP address	Specifies the source address of the IP data packets to which the device applies the rule. Possible values: ▶ `?.?.?.?` (default setting) The device applies the rule to IP data packets with any source address. ▶ Valid IPv4 address The device applies the rule to IP data packets with the specified source address. You use the `?` character as a wild card. Example `192.?.?.32`: The device applies the rule to IP data packets whose source address begins with `192.` and ends with `.32`. ▶ Valid IPv4 address/bit mask The device applies the rule to IP data packets with the specified source address. The inverse bit mask allows you to specify the address range with bit-level accuracy. Example `192.168.1.1/0.0.0.127`: The device applies the rule to IP data packets with a source address in the range from `192.168.1.0` to `….127`.
Destination IP address	Specifies the destination address of the IP data packets to which the device applies the rule. Possible values: ▶ `?.?.?.?` (default setting) The device applies the rule to IP data packets with any destination address. ▶ Valid IPv4 address The device applies the rule to IP data packets with the specified destination address. You use the `?` character as a wild card. Example `192.?.?.32`: The device applies the rule to IP data packets whose source address begins with `192.` and ends with `.32`. ▶ Valid IPv4 address/bit mask The device applies the rule to IP data packets with the specified destination address. The inverse bit mask allows you to specify the address range with bit-level accuracy. Example `192.168.1.1/0.0.0.127`: The device applies the rule to IP data packets with a destination address in the range from `192.168.1.0` to `….127`.

Parameters	Meaning
Protocol	Specifies the protocol type of the IP data packets to which the device applies the rule.
	Possible values: ▶ `any` (default setting) The device applies the rule to every IP data packet without considering the protocol type. ▶ `icmp` ▶ `igmp` ▶ `ip-in-ip` ▶ `tcp` ▶ `udp` ▶ `ip`
Source TCP/UDP port	Specifies the source port of the IP data packets to which the device applies the rule. The prerequisite is that you specify in the *Protocol* column the value `TCP` or `UDP`.
	Possible values: ▶ `any` (default setting) The device applies the rule to every IP data packet without considering the source port. ▶ `1..65535` The device applies the rule solely to IP data packets containing the specified source port.
Destination TCP/UDP port	Specifies the destination port of the IP data packets to which the device applies the rule. The prerequisite is that you specify in the *Protocol* column the value `TCP` or `UDP`.
	Possible values: ▶ `any` (default setting) The device applies the rule to every IP data packet without considering the destination port. ▶ `1..65535` The device applies the rule exclusively to IP data packets containing the specified destination port.
Action	Specifies how the device handles received IP data packets when it applies the rule.
	Possible values: ▶ `permit` (default setting) The device transmits the IP data packets. ▶ `deny` The device drops the IP data packets.
Log	Activates/deactivates the logging in the log file. See the *Diagnostics > Report > System Log* dialog.
	Possible values: ▶ `marked` Logging is activated. The prerequisite is that you assign the Access Control List in the *Network Security > ACL > Assignment* dialog to a VLAN or port. The device registers in the log file, in an interval of 30 s, how many times it applied the deny rule to IP data packets. ▶ `unmarked` (default setting) Logging is deactivated.
	The device allows you to activate this function for up to 128 deny rules.

■ Buttons

You find the description of the standard buttons in section "Buttons" on page 16.

Button	Meaning
🖳	Opens the *Create* window to add a new entry to the table. ▶ In the *Group name* field, you specify the name of the Access Control List to which the rule belongs. ▶ In the *Index* field, you specify the number of the rule within the Access Control List. If the Access Control List contains multiple rules, the device processes the rule with the lowest value first.

4.6.2   ACL MAC Rule

In this dialog, you specify the rules that the device applies to the MAC data packets.

An Access Control List (group) contains one or more rules. The device applies the rules of an Access Control List successively, beginning with the rule with the lowest value in the `Index` column.

The device allows you to filter for the source or destination MAC address of a data packet.

■ Table

Parameters	Meaning
Group name	Displays the name of the Access Control List. The Access Control List contains the rules.
Index	Displays the number of the rule within the Access Control List. If the Access Control List contains multiple rules, the device processes the rule with the lowest value first.
Match every packet	Specifies to which MAC data packets the device applies the rule. Possible values: ▶ `marked` (default setting) The device applies the rule to every MAC data packet. ▶ `unmarked` The device applies the rule to MAC data packets depending on the value in the fields *Source MAC address* and *Destination MAC address*.
Source MAC address	Specifies the source address of the MAC data packets to which the device applies the rule. Possible values: ▶ `??:??:??:??:??:??` (default setting) The device applies the rule to MAC data packets with any source address. ▶ Valid MAC address The device applies the rule to MAC data packets with the specified source address. You use the `?` character as a wild card. Example `00:11:??:??:??:??`: The device applies the rule to MAC data packets whose source address begins with `00:11`. ▶ Valid MAC address/bit mask The device applies the rule to MAC data packets with the specified source address. The bit mask allows you to specify the address range with bit-level accuracy. Example `00:11:22:33:44:54/FF:FF:FF:FF:FF:FC`: The device applies the rule to MAC data packets with a source address in the range from `00:11:22:33:44:54` to …:`57`.
Destination MAC address	Specifies the destination address of the MAC data packets to which the device applies the rule. Possible values: ▶ `??:??:??:??:??:??` (default setting) The device applies the rule to MAC data packets with any destination address. ▶ Valid MAC address The device applies the rule to MAC data packets with the specified destination address. You use the `?` character as a wild card. Example `00:11:??:??:??:??`: The device applies the rule to MAC data packets whose destination address begins with `00:11`. ▶ Valid MAC address/bit mask The device applies the rule to MAC data packets with the specified source address. The bit mask allows you to specify the address range with bit-level accuracy. Example `00:11:22:33:44:54/FF:FF:FF:FF:FF:FC`: The device applies the rule to MAC data packets with a destination address in the range from `00:11:22:33:44:54` to …:`57`.
Action	Specifies how the device handles received MAC data packets when it applies the rule. Possible values: ▶ `permit` (default setting) The device transmits the MAC data packets. ▶ `deny` The device discards the MAC data packets.

Parameters	Meaning
Log	Activates/deactivates the logging in the log file. See the **`Diagnostics > Report > System Log`** dialog.
	Possible values:
	▶ `marked`
	Logging is activated.
	The prerequisite is that you assign the Access Control List in the **`Network Security > ACL > Assignment`** dialog to a VLAN or port.
	The device registers in the log file, in an interval of 30 s, how many times it applied the deny rule to MAC data packets.
	▶ `unmarked` (default setting)
	Logging is deactivated.
	The device allows you to activate this function for up to 128 deny rules.

■ **Buttons**

You find the description of the standard buttons in section "Buttons" on page 16.

Button	Meaning
⊞	Opens the **`Create`** window to add a new entry to the table.
	▶ In the **`Group name`** field, you specify the name of the Access Control List to which the rule belongs.
	▶ In the **`Index`** field, you specify the number of the rule within the Access Control List. If the Access Control List contains multiple rules, the device processes the rule with the lowest value first.

4.6.3 ACL Assignment

This dialog allows you to assign one or more Access Control Lists to the ports and VLANs of the device. By assigning a priority you specify the processing sequence, provided you assign one or more Access Control Lists to a port or VLAN.

The device applies rules successively, namely in the sequence specified by the rule index. You specify the priority of a group in the *Priority* column. The lower the number, the higher the priority. In this process, the device applies the rules with a high priority before the rules with a low priority.

The assignment of Access Control Lists to ports and VLANs results in the following different types of ACL:
▶ Port-based IPv4-ACLs
▶ Port-based MAC ACLs
▶ VLAN-based IPv4 ACLs
▶ VLAN-based MAC ACLs

Note: Before you enable the function, verify that at least one active entry in the table allows you access. Otherwise, the connection to the device terminates when you change the settings. To access the management functions is possible solely using the CLI through the V.24 interface of the device.

■ Table

Parameters	Meaning
Group name	Displays the name of the Access Control List. The Access Control List contains the rules.
Type	Displays whether the Access Control List contains MAC rules or IPv4 rules. Possible values: ▶ `mac` 　The Access Control List contains MAC rules. ▶ `ip` 　The Access Control List contains IPv4 rules. You edit Access Control Lists with IPv4 rules in the *Network Security > ACL > IPv4 Rule* dialog. You edit Access Control Lists with MAC rules in the *Network Security > ACL > IPv4 Rule* dialog.
Port	Displays the port to which the Access Control List is assigned. The field remains empty if the Access Control List is assigned to a VLAN.
VLAN ID	Displays the VLAN to which the Access Control List is assigned. The field remains empty if the Access Control List is assigned to a port.
Direction	Displays that the device applies the Access Control List to received data packets.
Priority	Displays the priority of the Access Control List. Using the priority, you specify the sequence in which the device applies the Access Control Lists to the data stream. The device applies the rules in ascending order starting with priority `1`. Possible values: ▶ `1..4294967295` If an Access Control List is assigned to a port and to a VLAN with the same priority, the device applies the rules first to the port.
Active	Activates/deactivates the Access Control List on the port or in the VLAN. Possible values: ▶ `marked` (default setting) 　The Access Control List is active. ▶ `unmarked` 　The Access Control List is inactive.

■ **Buttons**

You find the description of the standard buttons in section "Buttons" on page 16.

Button	Meaning
	Opens the *Create* dialog to assign a rule to a port or a VLAN.
	▶ In the *Port/VLAN* field, you specify the port or the VLAN ID.
	▶ In the *Priority* field, you specify the source MAC address of the ARP rule.
	▶ In the *Direction* field, you specify the data packets to which the device applies the rule.
	▶ In the *Group name* filed, you specify which rule the device assigns to the port or VLAN.

5 Switching

The menu contains the following dialogs:
▶ Switching Global
▶ Rate Limiter
▶ Filter for MAC Addresses
▶ IGMP Snooping
▶ MRP-IEEE
▶ QoS/Priority
▶ VLAN
▶ L2-Redundancy

5.1 Switching Global

This dialog allows you to specify the following settings:
▶ Change the Aging time of the address table
▶ Enable the flow control in the device
▶ Enable the VLAN Unaware Mode

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

The flow control mechanism described in standard IEEE 802.3 helps ensure that no data packets are lost due to a port memory overflowing. Shortly before a port memory is completely full, the device signals to the connected devices that it is not accepting any more data packets from them.
▶ In full-duplex mode, the device sends a pause data packet.
▶ In half-duplex mode, the device simulates a collision.

Then the connected devices do not send any more data packets for as long as the signaling takes. On uplink ports, this can possibly cause undesired sending breaks in the higher-level network segment ("wandering backpressure").

According to standard IEEE 802.1Q, the device forwards data packets with a VLAN tag in a VLAN ≥1. However, a small number of applications on connected end devices send or receive data packets with a VLAN ID=0. When the device receives one of these data packets, before forwarding it the device overwrites the original value in the data packet with the VLAN ID of the receiving port. When you activate the VLAN Unaware Mode, this deactivates the VLAN settings in the device. The device then transparently forwards the data packets and evaluates the priority information contained in the data packet exclusively.

■ Configuration

Parameters	Meaning
MAC address	Displays the MAC address of the device.
Aging time [s]	Specifies the aging time in seconds.
	Possible values: ▶ `10..500000` (default setting: `30`) The device monitors the age of the learned unicast MAC addresses. The device deletes address entries that exceed a particular age (aging time) from its address table. You find the address table in the *Switching > Filter for MAC Addresses* dialog.
Flow control	Activates/deactivates the flow control in the device.
	Possible values: ▶ `marked` The flow control is active in the device. Additionally activate the flow control on the required ports. See the *Basic Settings > Port* dialog, *Configuration* tab, checkbox in the *Flow control* column. ▶ `unmarked` (default setting) The flow control is inactive in the device.
	When you are using a redundancy function, you deactivate the flow control on the participating ports. If the flow control and the redundancy function are active at the same time, there is a risk that the redundancy function operates sporadically.

Parameters	Meaning

VLAN unaware mode	Activates/deactivates the VLAN unaware mode.
	
	Possible values:
	▶ `marked`
	  The VLAN unaware mode is active.
	  The device works in the VLAN Unaware bridging mode (802.1Q):
	  – The device ignores the VLAN settings in the device and the VLAN tags in the data packets. The device transmits the data packets based on their destination MAC address or destination IP address in VLAN `1`.
	  – The device ignores the VLAN settings specified in the ***Switching > VLAN > Configuration*** and ***Switching > VLAN > Port*** dialogs. Every port is assigned to VLAN `1`.
	  – The device evaluates the priority information contained in the data packet.
	
	  Note: You specify the VLAN ID `1` for every function on the device which uses VLAN settings. Among other things, this applies to static filters, MRP and IGMP Snooping.
	▶ `unmarked` (default setting)
	  The VLAN unaware mode is inactive.
	  The device works in the VLAN-aware bridging mode (802.1Q):
	  – The device evaluates the VLAN tags in the data packets.
	  – The device transmits the data packets based on their destination MAC address or destination IP address in the corresponding VLAN.
	  – The device evaluates the priority information contained in the data packet.

■ **Buttons**

You find the description of the standard buttons in section "Buttons" on page 16.

5.2 Rate Limiter

The device allows you to limit the traffic on the ports in order to help provide reliable operation even with a large traffic volume. If the traffic on a port exceeds the traffic value entered, the device discards the excess traffic on this port.

The rate limiter function operates exclusively on Layer 2, and is used to limit the effects of storms of data packets that flood the device (typically Broadcasts).

The rate limiter function ignores protocol information on higher levels, such as IP or TCP.

The dialog contains the following tabs:
▶ [Ingress]
▶ [Egress]

[Ingress]

In this tab, you enable the **`Rate Limiter`** function. The threshold value specifies the maximum amount of traffic the port receives. If the traffic on this port exceeds the threshold value, the device discards the excess traffic on this port.

■ Table

Parameters	Meaning
Port	Displays the port number.
Threshold	Specifies the threshold value for broadcast, multicast, and unicast traffic on this port:

	Possible values:
	▶ `0` (default setting)
	  The **`Rate Limiter`** function is deactivated on this port.
	▶ `1..24414` at 100 MBit/s
	  `1..244140` at 1000 MBit/s
	  ☐ If the value `percent` is specified in the **`Threshold unit`** column, specify a percentage value between `1` and `100`.
	  ☐ If the value `pps` is specified in the **`Threshold unit`** column, specify an absolute value. The rate limiter function calculates the threshold based on 512-byte-sized packets.

	Note: The operating modes actually available depend on the device configuration.
Threshold unit	Specifies the unit for the threshold value:

	Possible values:
	▶ `percent` (default setting)
	  Specifies the threshold value as a percentage of the data rate of the port.
	▶ `pps`
	  Specifies the threshold value in data packets per second.

Broadcast mode	Activates/deactivates the rate limiter function for received broadcast data packets.
	Possible values: ▶ `marked` ▶ `unmarked` (default setting)
	If the threshold value is exceeded, the device discards the excess broadcast data packets on this port.
Multicast mode	Activates/deactivates the rate limiter function for received multicast data packets.
	Possible values: ▶ `marked` ▶ `unmarked` (default setting)
	If the threshold value is exceeded, the device discards the excess multicast data packets on this port.

Parameters	Meaning
Unknown unicast mode	Activates/deactivates the rate limiter function for received unicast data packets with an unknown destination address. Possible values: ▶ `marked` ▶ `unmarked` (default setting) If the threshold value is exceeded, the device discards the excess unicast data packets on this port.

■ **Buttons**

You find the description of the standard buttons in section "Buttons" on page 16.

[Egress]

In this tab, you specify the egress transmission rate on the port.

■ **Table**

Parameters	Meaning
Port	Displays the port number.
Bandwidth [%]	Specifies the egress transmission rate. Possible values: ▶ `0` (default setting) The bandwidth limitation is disabled. ▶ `1..100` The bandwidth limitation is enabled. This value specifies the percentage of overall link speed for the port in 1% increments.

■ **Buttons**

You find the description of the standard buttons in section "Buttons" on page 16.

5.3   Filter for MAC Addresses

This dialog allows you to display and edit address filters for the address table. Address filters specify the way the data packets are forwarded in the device based on the destination MAC address.

Each row in the table represents one filter. The device automatically sets up the filters. The device allows you to set up additional filters manually.

The device transmits the data packets as follows:
▶ If 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.
▶ If there is no table entry for the destination address, the device transmits the data packet from the receiving port to every other port.

■ Table

Parameters	Meaning
Address	Displays the destination MAC address to which the table entry applies.
VLAN ID	Displays the ID of the VLAN to which the table entry applies.
	The device learns the MAC addresses for every VLAN separately (independent VLAN learning).
Status	Displays how the device has set up the address filter.
	Possible values: ▶ learned Address filter set up automatically by the device based on received data packets. ▶ permanent Address filter set up manually. The address filter stays set up permanently. ▶ IGMP Address filter automatically set up by IGMP Snooping. ▶ mgmt MAC address of the device. The address filter is protected against changes. ▶ MRP-MMRP Multicast address filter automatically set up by MMRP.
\<Port number\>	Displays how the corresponding port transmits data packets which it directs to the adjacent destination address.
	Possible values: ▶ - The port does not transmit any data packets to the destination address. ▶ learned The port transmits data packets to the destination address. The device created the filter automatically based on received data packets. ▶ IGMP learned The port transmits data packets to the destination address. The device created the filter automatically based on IGMP. ▶ unicast static The port transmits data packets to the destination address. A user created the filter. ▶ multicast static The port transmits data packets to the destination address. A user created the filter.

To delete the learned MAC addresses from the address table, click in the *Basic Settings > Restart* dialog the *Reset MAC address table* button.

■ **Buttons**

You find the description of the standard buttons in section .

Button	Meaning

	Opens the ***Create*** window to add a new entry to the table.
	▶ In the ***Address*** field, you specify the destination MAC address.
	▶ In the ***VLAN ID*** field, you specify the ID of the VLAN.
	▶ In the ***Port*** field, you specify the port.
	   – Select one port if the destination MAC address is a unicast address.
	   – Select one or more ports if the destination MAC address is a multicast address.
	   – Select no port to create a discard filter. The device discards data packets with the destination MAC address specified in the table entry.

Reset MAC address table	Removes the MAC addresses from the forwarding table that have the value `learned` in the ***Status*** column.

5.4 IGMP Snooping

The Internet Group Management Protocol (IGMP) 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 allows you to use the IGMP Snooping function to also use the IGMP mechanisms on Layer 2:
▶ Without IGMP Snooping, the device transmits the Multicast data packets to every port.
▶ With the activated IGMP Snooping function, the device transmits the Multicast data packets exclusively 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 not until 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 reports with the entries in its address table. If a multicast receiver joins a multicast group, the device creates a table entry for this port in the *Switching > Filter for MAC Addresses* dialog. If the multicast receiver leaves the multicast group, the device removes the table entry.

The menu contains the following dialogs:
▶ IGMP Snooping Global
▶ IGMP Snooping Configuration
▶ IGMP Snooping Enhancements
▶ IGMP Snooping Querier
▶ IGMP Snooping Multicasts

5.4.1   IGMP Snooping Global

This dialog allows you to enable the *IGMP Snooping* protocol in the device and also configure it for each port and each VLAN.

■ Operation

Parameters	Meaning
Operation	Enables/disables the *IGMP Snooping* function in the device.

	Possible values:
	▶ `On`
	   The *IGMP Snooping* function is enabled in the device according to RFC 4541 (Considerations for Internet Group Management Protocol (IGMP) and Multicast Listener Discovery (MLD) Snooping Switches).
	▶ `Off` (default setting)
	   The *IGMP Snooping* function is disabled in the device.
	   The device transmits received query, report, and leave data packets without evaluating them.
	   Received data packets with a Multicast destination address are transmitted to every port by the device.

■ Information

Parameters	Meaning
Multicast control packets processed	Displays the number of Multicast control data packets processed. This statistic encompasses the following packet types: – IGMP Reports – IGMP Queries version V1 – IGMP Queries version V2 – IGMP Queries version V3 – IGMP Queries with an incorrect version – PIM or DVMRP packets The device uses the Multicast control data packets to create the address table for transmitting the Multicast data packets.
	Possible values: ▶ $0..2^{31}-1$
	You use the *Reset IGMP snooping data* button in the *Basic Settings > Restart* dialog or the `clear igmp-snooping` CLI command to reset the IGMP Snooping entries, including the counter for the processed multicast control data packets.

■ Buttons

You find the description of the standard buttons in section "Buttons" on page 16.

Button	Meaning
Reset IGMP snooping counters	Removes the IGMP Snooping entries and resets the counter in the *Information* frame to `0`.

5.4.2 IGMP Snooping Configuration

This dialog allows you to enable the *IGMP Snooping* function in the device and also configure it for each port and each VLAN.

The dialog contains the following tabs:
▶ [VLAN ID]
▶ [Port]

[V L A N   I D]

In this tab, you configure the *IGMP Snooping* function for every VLAN.

■ **Table**

Parameters	Meaning
VLAN ID	Displays the ID of the VLAN to which the table entry applies.
Active	Activates/deactivates the *IGMP Snooping* function for this VLAN. The prerequisite is that the *IGMP Snooping* function is globally enabled.
	Possible values:
	▶ `marked` IGMP Snooping is activated for this VLAN. The VLAN has joined the Multicast data stream.
	▶ `unmarked` (default setting) IGMP Snooping is deactivated for this VLAN. The VLAN has left the Multicast data stream.
Group membership interval	Specifies the time in seconds for which a VLAN from a dynamic Multicast group remains entered in the address table when the device does not receive any more report data packets from the VLAN. Specify a value larger than the value in the *Max. response time* column.
	Possible values:
	▶ `2..3600` (default setting: `260`)
Max. response time	Specifies the time in seconds in which the members of a multicast group should respond to a query data packet. For their response, the members specify a random time within the response time. You thus help prevent the multicast group members from responding to the query at the same time. Specify a value smaller than the value in the *Group membership interval* column.
	Possible values:
	▶ `1..25` (default setting: `10`)
Fast leave admin mode	Activates/deactivates the Fast Leave function for this VLAN.
	Possible values:
	▶ `marked` If the device receives an IGMP Leave message from a multicast group, when the Fast Leave function is active it removes the entry immediately from its address table.
	▶ `unmarked` (default setting) When the Fast Leave function is inactive, the device first sends MAC-based queries to the members of the multicast group, and removes an entry when a VLAN does not send any more report messages.
MRP expiration time	Multicast Router Present Expiration Time. Specifies the time in seconds for which the device waits for a query on this port that belongs to a VLAN. If the port does not receive a query data packet, the device removes the port from the list of ports with connected multicast routers. You have the option of configuring this parameter solely if the port belongs to an existing VLAN.
	Possible values:
	▶ `0` unlimited timeout - no expiration time
	▶ `1..3600` (default setting: `260`)

■ **Buttons**

You find the description of the standard buttons in section "Buttons" on page 16.

[**Port**]

In this tab, you configure the *IGMP Snooping* function for every port.

■ Table

Parameters	Meaning
Port	Displays the port number.

Active	Activates/deactivates the *IGMP Snooping* function for this port. The prerequisite is that the *IGMP Snooping* function is globally enabled.
	
	Possible values:
	▶ `marked`
	  IGMP Snooping is active on this port. The device includes the port in the multicast data stream.
	▶ `unmarked` (default setting)
	  IGMP Snooping is inactive on this port. The port left the multicast data stream.

Group membership interval	Specifies the time in seconds for which a port, from a dynamic multicast group, remains entered in the address table when the device does not receive any more report data packets from the port. Possible values: ▶ `2..3600` (default setting: `260`) Specify the value larger than the value in the *Max. response time* column.
Max. response time	Specifies the time in seconds in which the members of a multicast group should respond to a query data packet. For their response, the members specify a random time within the response time. You thus help prevent the multicast group members from responding to the query at the same time. Possible values: ▶ `1..25` (default setting: `10`) Specify a value lower than the value in the *Group membership interval* column.
MRP expiration time	Specifies the Multicast Router Present Expiration Time. The MRP expiration time is the time in seconds for which the device waits for a query packet on this port. If the port does not receive a query data packet, the device removes the port from the list of ports with connected multicast routers. Possible values: ▶ `0` unlimited timeout - no expiration time ▶ `1..3600` (default setting: `260`)

Fast leave admin mode	Activates/deactivates the Fast Leave function for this port.
	
	Possible values:
	▶ `marked`
	  If the device receives an IGMP Leave message from a multicast group, when the Fast Leave function is active it removes the entry immediately from its address table.
	▶ `unmarked` (default setting)
	  When the Fast Leave function is inactive, the device first sends MAC-based queries to the members of the multicast group, and removes an entry when a port does not send any more report messages.

Static query port	Activates/deactivates the *Static query port* mode.
	
	Possible values:
	▶ `marked`
	  The *Static query port* mode is active.
	  The port is a static query port in the VLANs that are set up.
	▶ `unmarked` (default setting)
	  The *Static query port* mode is inactive.
	  The port is not a static query port. The device transmits IGMP report messages to the port solely if it receives IGMP queries.

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

■ **Buttons**

You find the description of the standard buttons in section .

5.4.3   IGMP Snooping Enhancements

This dialog allows you to select a port for a VLAN ID and to configure the port.

■ Table

Parameters	Meaning
VLAN ID	Displays the ID of the VLAN to which the table entry applies.
<Port number>	Displays for every VLAN set up in the device whether the relevant port is a query port. Additionally, the field displays whether the device transmits every Multicast stream in the VLAN to this port.
	Possible values:
	▶ `-` The port is not a query port in this VLAN.
	▶ `L` = Learned The device detected the port as a query port because the port received IGMP queries in this VLAN. The port is not a statically configured query port.
	▶ `A` = Automatic The device detected the port as a query port. The prerequisite is that you configure the port as `Learn by LLDP`.
	▶ `S` = Static (manual setting) A user specified the port as a static query port. The device transmits IGMP reports solely to ports on which it previously received IGMP queries – and to statically configured query ports. To assign this value, proceed as follows: ☐ Open the ***Wizard*** window. ☐ On the ***Configuration*** page, mark the `Static` checkbox.
	▶ `P` = Learn by LLDP (manual setting) A user specified the port as `Learn by LLDP`. With the Link Layer Discovery Protocol (LLDP), the device detects Hirschmann devices connected directly to the port. The device denotes the detected query ports with `A`. To assign this value, proceed as follows: ☐ Open the ***Wizard*** window. ☐ On the ***Configuration*** page, mark the `Learn by LLDP` checkbox.
	▶ `F` = Forward All (manual setting) A user specified the port so that the device transmits every received Multicast stream in the VLAN to this port. Use this setting for diagnostics purposes, for example. To assign this value, proceed as follows: ☐ Open the ***Wizard*** window. ☐ On the ***Configuration*** page, mark the `Forward all` checkbox.

Parameters	Meaning
Display categories	Enhances the clarity of the display. The table emphasizes the cells which contain the specified value. This helps to analyze and sort the table according to your needs.
	▶ `Learned (L)` The table displays cells which contain the value `L` and possibly further values. Cells which contain other values than `L` exclusively, the table displays with the "`-`" symbol.
	▶ `Static (S)` The table displays cells which contain the value `S` and possibly further values. Cells which contain other values than `S` exclusively, the table displays with the "`-`" symbol.
	▶ `Automatic (A)` The table displays cells which contain the value `A` and possibly further values. Cells which contain other values than `A` exclusively, the table displays with the "`-`" symbol.
	▶ `Learned by LLDP (P)` The table displays cells which contain the value `P` and possibly further values. Cells which contain other values than `P` exclusively, the table displays with the "`-`" symbol.
	▶ `Forward all (F)` The table displays cells which contain the value `F` and possibly further values. Cells which contain other values than `F` exclusively, the table displays with the "`-`" symbol.

■ **Buttons**

You find the description of the standard buttons in section "Buttons" on page 16.

Button	Meaning
	Opens the `Wizard` window that helps you to select and configure the ports.

[Wizard : Selection VLAN/Port]

After closing the **Wizard** window, click the ✓ button to transfer the changes to the volatile memory (`RAM`) of the device and apply them to the device.

■ Selection VLAN/Port

On this page you assign a VLAN ID to port.

Parameters	Meaning
VLAN ID	Select the ID of the VLAN. Possible values: ▶ `1..4042`
Port	Select the port. Possible values: ▶ `<Port number>`

■ Configuration

On this page you specify the settings for the port.

Parameters	Meaning
VLAN ID	Displays the ID of the selected VLAN.
Port	Displays the number of the selected port.
Static	Specifies the port as a static query port in the VLANs that are set up. The device transmits IGMP report messages to the ports at which it receives IGMP queries. Allows you to also transmit IGMP report messages to other selected ports (enable) or connected Hirschmann devices (`Automatic`).
Learn by LLDP	Specifies the port as `Learn by LLDP`. Allows directly connected Hirschmann devices to be detected via LLDP and learned as query ports.
Forward all	Specifies the port as `Forward all`. With the `Forward all` setting, the device transmits at this port every data packet with a Multicast address in the destination address field.

5.4.4   IGMP Snooping Querier

The device allows you to send a Multicast stream solely to those ports to which a Multicast receiver is connected.

To determine which ports Multicast receivers are connected to, the device sends query data packets to the ports at a definable interval. If a Multicast receiver is connected, it joins the Multicast stream by responding to the device with a report data packet.

This dialog allows you to configure the Snooping Querier settings globally and for the VLANs that are set up.

■ Operation

Parameters	Meaning
Operation	Enables/disables the IGMP Querier function globally in the device. Possible values: ▶ On ▶ Off (default setting)

■ Configuration

In this frame you specify the IGMP Snooping Querier settings for the general query data packets.

Parameters	Meaning

Protocol version	Specifies the IGMP version of the general query data packets.
	
	Possible values:
	▶ 1
	   IGMP v1
	▶ 2 (default setting)
	   IGMP v2
	▶ 3
	   IGMP v3

Query interval [s]	Specifies the time in seconds after which the device generates general query data packets itself when it has received query data packets from the Multicast router. Possible values: ▶ 1..1800 (default setting: 60)
Expiry interval [s]	Specifies the time in seconds after which an active querier switches from the passive state back to the active state if it has not received any query packets for longer than specified here. Possible values: ▶ 60..300 (default setting: 125)

■ Table

In the table you specify the Snooping Querier settings for the VLANs that are set up.

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

Active	Activates/deactivates the IGMP Snooping Querier function for this VLAN.
	
	Possible values:
	▶ marked
	   The IGMP Snooping Querier function is active for this VLAN.
	▶ unmarked (default setting)
	   The IGMP Snooping Querier function is inactive for this VLAN.

Parameters	Meaning
Current state	Displays whether the Snooping Querier is active for this VLAN.
	Possible values: ▶ `marked` The Snooping Querier is active for this VLAN. ▶ `unmarked` The Snooping Querier is inactive for this VLAN.
Address	Specifies the IP address that the device adds as the source address in generated general query data packets. You use the address of the multicast router.
	Possible values: ▶ Valid IPv4 address (default setting: `0.0.0.0`)
Protocol version	Displays the IGMP protocol version of the general query data packets.
	Possible values: ▶ `1` IGMP v1 ▶ `2` IGMP v2 ▶ `3` IGMP v3
Max. response time	Displays the time in seconds in which the members of a Multicast group should respond to a query data packet. For their response, the members specify a random time within the response time. This helps prevent every Multicast group member to respond to the query at the same time.
Last querier address	Displays the IP address of the Multicast router from which the last received IGMP query was sent out..
Last querier version	Displays the IGMP version that the Multicast router used when sending out the last IGMP query received in this VLAN.

■ **Buttons**

You find the description of the standard buttons in section .

5.4.5   IGMP Snooping Multicasts

The device allows you to specify how it transmits data packets with unknown Multicast addresses: Either the device discards these data packets, floods them to every port, or transmits them solely to the ports that previously received query packets.

The device also allows you to transmit the data packets with known Multicast addresses to the query ports.

■ Configuration

Parameters	Meaning
Unknown multicasts	Specifies how the device transmits the data packets with unknown Multicast addresses.

	Possible values:
	▶ `Discard`
	  The device discards data packets with an unknown MAC/IP Multicast address.
	▶ `Send to all ports` (default setting)
	  The device sends data packets with an unknown MAC/IP Multicast address to the registered ports.
	▶ `Send to query ports`
	  The device sends data packets with an unknown MAC/IP Multicast address to the query ports.

■ Table

In the table you specify the settings for known Multicasts for the VLANs that are set up.

Parameters	Meaning
VLAN ID	Displays the ID of the VLAN to which the table entry applies.
Known multicasts	Specifies how the device transmits the data packets with known Multicast addresses.

	Possible values:
	▶ `send to query and registered ports`
	  The device sends data packets with an unknown MAC/IP Multicast address to the query ports and to the registered ports.
	▶ `send to registered ports` (default setting)
	  The device sends data packets with an unknown MAC/IP Multicast address to registered ports.

■ Buttons

You find the description of the standard buttons in section "Buttons" on page 16.

5.5 **MRP-IEEE**

The IEEE 802.1ak amendment to the IEEE 802.1Q standard introduced the Multiple Registration Protocol (MRP) to replace the Generic Attribute Registration Protocol (GARP). The IEEE also modified and replaced the GARP applications, GARP Multicast Registration Protocol (GMRP) and GARP VLAN Registration Protocol (GVRP). The Multiple MAC Registration Protocol (MMRP) and the Multiple VLAN Registration Protocol (MVRP) replace these protocols.

MRP-IEEE helps confine traffic to the required areas of the LAN. To confine traffic, the MRP-IEEE applications distribute attribute values to participating MRP-IEEE devices across a LAN registering and de-registering multicast group membership and VLAN identifiers.

Registering group participants allows you to reserve resources for specific traffic transversing a LAN. Defining resource requirements regulates the level of traffic, allowing the devices to determine the required resources and provides for dynamic maintenance of the allocated resources.

The menu contains the following dialogs:
▶ MRP-IEEE Configuration
▶ MRP-IEEE Multiple MAC Registration Protocol
▶ MRP-IEEE Multiple VLAN Registration Protocol

5.5.1 MRP-IEEE Configuration

This dialog allows you to set the various MRP timers. By maintaining a relationship between the various timer values, the protocol operates efficiently and with less likelihood of unnecessary attribute withdraws and re-registration. The default timer values effectively maintain these relationships.

Maintain the following relationships when you reconfigure the timers:
- ▶ To allow for re-registration after a Leave or LeaveAll event, even if there is a lost message, specify the LeaveTime to: ≥ `(2x JoinTime) + 60`.
- ▶ To minimize the volume of rejoining traffic generated following a LeaveAll event, specify the value for the LeaveAll timer larger than the LeaveTime value.

■ Table

Parameters	Meaning
Port	Displays the port number.
Join time [1/100s]	Specifies the Join timer which controls the interval between transmit opportunities applied to the Applicant state machine. Possible values: ▶ `10..100` (default setting: `20`)
Leave time [1/100s]	Specifies the Leave timer which controls the period that the Registrar state machine waits in the leave (LV) state before transiting to the empty (MT) state. Possible values: ▶ `20..600` (default setting: `60`)
Leave all time [1/100s]	Specifies the LeaveAll timer which controls the frequency with which the LeaveAll state machine generates LeaveAll PDUs. Possible values: ▶ `200..6000` (default setting: `1000`)

■ Buttons

You find the description of the standard buttons in section "Buttons" on page 16.

5.5.2 MRP-IEEE Multiple MAC Registration Protocol

The Multiple MAC Registration Protocol (MMRP) allows end devices and MAC switches to register and de-register group membership and individual MAC address information with switches located in the same LAN. The switches within the LAN disseminate the information through switches that support extended filtering services. Using the MAC address information, MMRP allows you to confine multicast traffic to the required areas of a Layer 2 network.

For an example of how MMRP works, consider a security camera mounted on a mast overlooking a building. The camera sends multicast packets onto a LAN. You have 2 end devices installed for surveillance in separate locations. You register the MAC addresses of the camera and the 2 end devices in the same multicast group. You then specify the MMRP settings on the ports to send the multicast group packets to the 2 end devices.

The dialog contains the following tabs:
▶ [Configuration]
▶ [Service requirement]
▶ [Statistics]

[Configuration]

In this tab, you select active MMRP port participants and set the device to transmit periodic events. The dialog also allows you to enable VLAN registered MAC address broadcasting.

A periodic state machine exists for each port and transmits periodic events regularly to the applicant state machines associated with active ports. Periodic events contain information indicating the status of the devices associated with the active port.

■ Operation

Parameters	Meaning
Operation	Enables/disables the global MMRP function on the device. The device participates in MMRP message exchanges.
	Possible values:
	▶ On The device is a normal participant in MMRP message exchanges.
	▶ Off (default setting) The device ignores MMRP messages.

■ Configuration

Parameters	Meaning
Periodic state machine	Enables/disables the global periodic state machine on the device.
	Possible values:
	▶ On With MMRP *Operation* enabled globally, the device transmits MMRP messages in one-second intervals, on MMRP participating ports.
	▶ Off (default setting) Disables the periodic state machine on the device.

■ Table

Parameters	Meaning
Port	Displays the port number.
Active	Activates/deactivates the port MMRP participation.
	Possible values:
	▶ marked (default setting) With MMRP enabled globally and on this port, the device sends and receives MMRP messages on this port.
	▶ unmarked Disables the port MMRP participation.
Restricted group registration	Activates/deactivates the restriction of dynamic MAC address registration using MMRP on the port.
	Possible values:
	▶ marked When enabled and a static filter entry for the MAC address exists on the VLAN concerned, then the device allows the dynamic registration of MAC address attributes.
	▶ unmarked (default setting) Activates/deactivates the restriction of dynamic MAC address registration using MMRP on the port.

■ **Buttons**

You find the description of the standard buttons in section "Buttons" on page 16.

[Service requirement]

This tab contains forwarding parameters for each active VLAN, specifying the ports on which multicast forwarding applies. The device allows you to statically setup VLAN ports as `Forward all` or `Forbidden`. You set the Forbidden MMRP service requirement statically through the graphical user interface or CLI exclusively.

A port is setup solely as ForwardAll or Forbidden.

■ **Table**

Parameters	Meaning
VLAN ID	Displays the ID of the VLAN.
<Port number>	Specifies the service requirement handling for the port.
	Possible values: ▶ `FA` Specifies the ForwardAll traffic setting on the port. The device forwards traffic destined to MMRP registered multicast MAC addresses on the VLAN. The device forwards traffic to ports which MMRP has dynamically setup or ports which the administrator has statically setup as ForwardAll ports. ▶ `F` Specifies the Forbidden traffic setting on the port. The device blocks dynamic MMRP ForwardAll service requirements. With ForwardAll requests blocked on this port in this VLAN, the device blocks traffic destined to MMRP registered multicast MAC addresses on this port. Furthermore, the device blocks MMRP service request for changing this value on this port. ▶ `-` (default setting) Disables the forwarding functions on this port. ▶ `Learned` Displays values setup by MMRP service requests.

■ **Buttons**

You find the description of the standard buttons in section "Buttons" on page 16.

[Statistics]

Devices on a LAN exchange Multiple MAC Registration Protocol Data Units (MMRPDU) to maintain statuses of devices on an active MMRP port. This tab allows you to monitor the MMRP traffic statistics for each port.

■ Information

Parameters	Meaning
Transmitted MMRP PDU	Displays the number of MMRPDUs transmitted on the device.
Received MMRP PDU	Displays the number of MMRPDUs received on the device.
Received bad header PDU	Displays the number of MMRPDUs received with a bad header on the device.
Received bad format PDU	Displays the number of MMRPDUs with a bad data field that were not transmitted on the device.
Transmission failed	Displays the number of MMRPDUs not transmitted on the device.

■ Table

Parameters	Meaning
Port	Displays the port number.
Transmitted MMRP PDU	Displays the number of MMRPDUs transmitted on the port.
Received MMRP PDU	Displays the number of MMRPDUs received on the port.
Received bad header PDU	Displays the number of MMRPDUs with a bad header that were received on the port.
Received bad format PDU	Displays the number of MMRPDUs with a bad data field that were not transmitted on the port.
Transmission failed	Displays the number of MMRPDUs not transmitted on the port.
Last received MAC address	Displays the last MAC address from which the port received MMRPPDUs.

■ Buttons

You find the description of the standard buttons in section "Buttons" on page 16.

Button	Meaning
Reset	Resets the port statistics counters and the values in the *Last received MAC address* column.

5.5.3   MRP-IEEE Multiple VLAN Registration Protocol

The Multiple VLAN Registration Protocol (MVRP) provides a mechanism that allows you to distribute VLAN information and configure VLANs dynamically. For example, when you configure a VLAN on an active MVRP port, the device distributes the VLAN information to other MVRP enabled devices. Using the information received, an MVRP enabled device dynamically creates the VLAN trunks on other MVRP enabled devices as needed.

The dialog contains the following tabs:
▶ [Configuration]
▶ [Statistics]

[Configuration]

In this tab, you select active MVRP port participants and set the device to transmit periodic events.

A periodic state machine exists for each port and transmits periodic events regularly to the applicant state machines associated with active ports. Periodic events contain information indicating the status of the VLANs associated with the active port. Using the periodic events, MVRP enabled switches dynamically maintain the VLANs.

■ Operation

Parameters	Meaning
Operation	Enables/disables the global Applicant Administrative Control which specifies whether the Applicant state machine participates in MMRP message exchanges.
	Possible values:
	▶ `On` Normal Participant. The Applicant state machine participates in MMRP message exchanges.
	▶ `Off` (default setting) Non-Participant. The Applicant state machine ignores MMRP messages.

■ Configuration

Parameters	Meaning
Periodic state machine	Enables/disables the periodic state machine on the device.
	Possible values:
	▶ `On` The periodic state machine is enabled. With MVRP `Operation` enabled globally, the device transmits MVRP periodic events in 1 second intervals, on MVRP participating ports.
	▶ `Off` (default setting) The periodic state machine is disabled. Disables the periodic state machine on the device.

■ Table

Parameters	Meaning
Port	Displays the port number.
Active	Activates/deactivates the port MVRP participation.
	Possible values:
	▶ `marked` (default setting) With MVRP enabled globally and on this port, the device distributes VLAN membership information to MVRP-aware devices connected to this port.
	▶ `unmarked` Disables the port MVRP participation.
Restricted VLAN registration	Activates/deactivates the `Restricted VLAN registration` function on this port.
	Possible values:
	▶ `marked` When enabled and a static VLAN registration entry exists, then the device allows you to create a dynamic VLAN for this entry.
	▶ `unmarked` (default setting) Disables the `Restricted VLAN registration` function on this port.

■ **Buttons**

You find the description of the standard buttons in section "Buttons" on page 16.

[Statistics]

Devices on a LAN exchange Multiple VLAN Registration Protocol Data Units (MVRPDU) to maintain statuses of VLANs on active ports. This tab allows you to monitor the MVRP traffic.

■ Information

Parameters	Meaning
Transmitted MVRP PDU	Displays the number of MVRPDUs transmitted on the device.
Received MVRP PDU	Displays the number of MVRPDUs received on the device.
Received bad header PDU	Displays the number of MVRPDUs received with a bad header on the device.
Received bad format PDU	Displays the number of MVRPDUs with a bad data field that the device blocked.
Transmission failed	Displays the number of failures while adding a message into the MVRP queue.
Message queue failures	Displays the number of MVRPDUs that the device blocked.

■ Table

Parameters	Meaning
Port	Displays the port number.
Transmitted MVRP PDU	Displays the number of MVRPDUs transmitted on the port.
Received MVRP PDU	Displays the number of MVRPDUs received on the port.
Received bad header PDU	Displays the number of MVRPDUs with a bad header that the device received on the port.
Received bad format PDU	Displays the number of MVRPDUs with a bad data field that the device blocked on the port.
Transmission failed	Displays the number of MVRPDUs that the device blocked on the port.
Registrations failed	Displays the number of failed registration attempts on the port.
Last received MAC address	Displays the last MAC address from which the port received MMRPDUs.

■ Buttons

You find the description of the standard buttons in section .

Button	Meaning
Reset	Resets the port statistics counters and the values in the *Last received MAC address* column.

5.6 QoS/Priority

Communication networks transmit a number of applications at the same time that have different requirements as regards availability, bandwidth and latency periods.

QoS (Quality of Service) is a procedure defined in IEEE 802.1D. It is used to distribute resources in the network. You therefore have the possibility of providing minimum bandwidth for important applications. The prerequisite is that the end devices and the devices in the network support prioritized data transmission. Data packets with high priority are given preference when transmitted by devices in the network. You transfer data packets with lower priority when there are no data packets with a higher priority to be transmitted.

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: Disable flow control if you use the functions in this menu. The flow control is inactive if in the **Switching > Global** dialog, **Configuration** frame the **Flow control** checkbox is `unmarked`.

The menu contains the following dialogs:
- ▶ QoS/Priority Global
- ▶ QoS/Priority Port Configuration
- ▶ 802.1D/p Mapping
- ▶ IP DSCP Mapping
- ▶ Queue Management

5.6.1   QoS/Priority Global

The device allows you to maintain access to the management functions, even in situations with heavy utilization. In this dialog you specify the required QoS/priority settings.

■ Configuration

Parameters	Meaning
VLAN priority for management packets	Specifies the VLAN priority for sending management data packets. Depending on the VLAN priority, the device assigns the data packet to a specific traffic class and thus to a specific priority queue of the port. Possible values: ▶ `0..7` (default setting: `0`) In the *Switching > QoS/Priority > 802.1D/p Mapping* dialog, you assign a traffic class to every VLAN priority.
IP DSCP value for management packets	Specifies the IP DSCP value for sending management data packets. Depending on the IP DSCP value, the device assigns the data packet to a specific traffic class and thus to a specific priority queue of the port. Possible values: ▶ `0 (be/cs0)..63` (default setting: `0 (be/cs0)`) Some values in the list also have a DSCP keyword, for example `0 (be/cs0)`, `10 (af11)` and `46 (ef)`. These values are compatible with the IP precedence model. In the *Switching > QoS/Priority > IP DSCP Mapping* dialog you assign a traffic class to every IP DSCP value.
Queues per port	Displays the number of priority queues per port. The device has 8 priority queues per port. You assign every priority queue to a specific traffic class (traffic class according to IEEE 802.1D).

■ Buttons

You find the description of the standard buttons in section .

5.6.2   QoS/Priority Port Configuration

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

■ Table

Parameters	Meaning
Port	Displays the port number.
Port priority	Specifies what VLAN priority information the device writes into a data packet if the data packet contains no priority information. After this, the device transmits the data packet depending on the value specified in the *Trust mode* column.
	Possible values: ▶ `0..7` (default setting: `0`)
Trust mode	Specifies how the device handles a received data packet if the data packet contains QoS/priority information.
	Possible values: ▶ `untrusted` The device transmits the data packet according to the priority specified in the *Port priority* column. The device ignores the priority information contained in the data packet. In the *Switching > QoS/Priority > 802.1D/p Mapping* dialog, you assign a traffic class to every VLAN priority. ▶ `trustDot1p` (default setting) The device transmits the data packet according to the priority information in the VLAN tag. In the *Switching > QoS/Priority > 802.1D/p Mapping* dialog, you assign a traffic class to every VLAN priority. ▶ `trustIpDscp` – If the data packet is an IP packet: The device transmits the data packet according to the IP DSCP value contained in the data packet. In the *Switching > QoS/Priority > IP DSCP Mapping* dialog you assign a traffic class to every IP DSCP value. – If the data packet is not an IP packet: The device transmits the data packet according to the priority specified in the *Port priority* column. In the *Switching > QoS/Priority > 802.1D/p Mapping* dialog, you assign a traffic class to every VLAN priority.
Untrusted traffic class	Displays the traffic class assigned to the VLAN priority information specified in the *Port priority* column. In the *Switching > QoS/Priority > 802.1D/p Mapping* dialog, you assign a traffic class to every VLAN priority.
	Possible values: ▶ `0..7`

■ Buttons

You find the description of the standard buttons in section "Buttons" on page 16.

5.6.3   802.1D/p Mapping

The device transmits data packets with a VLAN tag according to the contained QoS/priority information with a higher or lower priority.

In this dialog, you assign a traffic class to every VLAN priority. You assign the traffic classes to the priority queues of the ports.

■ Table

Parameters	Meaning
VLAN priority	Displays the VLAN priority.

Traffic class	Specifies the traffic class assigned to the VLAN priority.
	
	Possible values:
	▶ `0..7`
	  `0` assigned to the priority queue with the lowest priority.
	  `7` assigned to the priority queue with the highest priority.
	
	Note: Among other things redundancy mechanisms use the highest traffic class. Therefore, select another traffic class for application data.

■ Buttons

You find the description of the standard buttons in section .

■ Default assignment of the VLAN priority to traffic classes

VLAN Priority	Traffic class	Content description according to IEEE 802.1D
0	2	`Best Effort` Normal data without prioritizing
1	0	`Background` Non-time critical data and background services
2	1	`Standard` Normal data
3	3	`Excellent Effort` Important data
4	4	`Controlled Load` Time-critical data with a high priority
5	5	`Video` Video transmission with delays and jitter < 100 ms
6	6	`Voice` Voice transmission with delays and jitter < 10 ms
7	7	`Network Control` Data for network management and redundancy mechanisms

5.6.4   IP DSCP Mapping

The device transmits IP data packets according to the DSCP value contained in the data packet with a higher or lower priority.

In this dialog, you assign a traffic class to every DSCP value. You assign the traffic classes to the priority queues of the ports.

■ Table

Parameters	Meaning
DSCP value	Displays the DSCP value.
Traffic class	Specifies the traffic class which is assigned to the DSCP value. Possible values: ▶ 0..7 　0 assigned to the priority queue with the lowest priority. 　7 assigned to the priority queue with the highest priority.

■ Buttons

You find the description of the standard buttons in section .

■ Default assignment of the DSCP values to traffic classes

DSCP Value	DSCP Name	Traffic class
0	Best Effort /CS0	2
1-7		2
8	CS1	0
9,11,13,15		0
10,12,14	AF11,AF12,AF13	0
16	CS2	1
17,19,21,23		1
18,20,22	AF21,AF22,AF23	1
24	CS3	3
25,27,29,31		3
26,28,30	AF31,AF32,AF33	3
32	CS4	4
33,35,37,39		4
34,36,38	AF41,AF42,AF43	4
40	CS5	5
41,42,43,44,45,47		5
46	EF	5
48	CS6	6
49-55		6
56	CS7	7
57-63		7

5.6.5   Queue Management

This dialog allows you to enable and disable the *Strict priority* function for the traffic classes. When you disable the *Strict priority* function, the device processes the priority queues of the ports with "Weighted Fair Queuing".

■ Table

Parameters	Meaning
Traffic class	Displays the traffic class.
Strict priority	Activates/deactivates the processing of the port priority queue with *Strict priority* for this traffic class. Possible values: ▶ `marked` (default setting) The processing of the port priority queue with *Strict priority* is active. – The port sends data packets that are in the priority queue with the highest priority exclusively. If this priority queue is empty, the port sends data packets that are in the priority queue with the next lower priority. – The port sends data packets with a lower traffic class after the priority queues with a higher priority are empty. In unfavorable situations, the port does not send these data packets. – If you select this setting for a traffic class, the device enables the function also for traffic classes with a higher priority. – Use this setting for applications such as VoIP or video that require the least possible delay. ▶ `unmarked` The processing of the port priority queue with *Strict priority* is inactive. The device uses "Weighted Fair Queuing"/"Weighted Round Robin" (WRR) to process the port priority queue. – The device assigns a minimum bandwidth to each traffic class. – Even under a high network load the port transmits data packets with a low traffic class. – If you select this setting for a traffic class, the device disables the function also for traffic classes with a lower priority.
Min. bandwidth [%]	Specifies the minimum bandwidth for this traffic class when the device is processing the priority queues of the ports with "Weighted Fair Queuing". Possible values: ▶ `0..100` (default setting: `0` = the device does not reserve any bandwidth for this traffic class) The value specified in percent refers to the available bandwidth on the port. When you disable the *Strict priority* function for every traffic class, the maximum bandwidth is available on the port for the "Weighted Fair Queuing". The maximum total of the assigned bandwidths is 100 %.

■ Buttons

You find the description of the standard buttons in section "Buttons" on page 16.

5.7 VLAN

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

▶ High flexibility
– With VLAN you distribute the data traffic to logical networks in the existing infrastructure. Without VLAN, it would be necessary to have additional devices and complicated cabling.
– With VLAN you specify network segments independently of the location of the individual end devices.

▶ Improved throughput
– In VLANs data packets can be transferred by priority.
If the priority is high, the device transfers the data traffic of a VLAN preferentially, for example for time-critical applications such as VoIP phone calls.
– The network load is considerably reduced if data packets and Broadcasts are distributed in small network segments instead of in the entire network.

▶ Increased security
The distribution of the data traffic among individual logical networks makes unwanted accessing more difficult and strengthens the system against attacks such as MAC Flooding or MAC Spoofing.

The device supports packet-based "tagged" VLANs according to the IEEE 802.1Q standard. The VLAN tagging in the data packet indicates the VLAN to which the data packet belongs.

The device transmits the tagged data packets of a VLAN exclusively via 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:
▶ VLAN Global
▶ VLAN Configuration
▶ VLAN Port

5.7.1   VLAN Global

This dialog allows you to view general VLAN parameters for the device.

■ Configuration

Parameters	Meaning
Max. VLAN ID	Highest ID assignable to a VLAN. See the *Switching > VLAN > Configuration* dialog.
VLANs (max.)	Displays the maximum number of VLANs possible. See the *Switching > VLAN > Configuration* dialog.
VLANs	Number of VLANs currently configured in the device. See the *Switching > VLAN > Configuration* dialog. The VLAN ID 1 is constantly present in the device.

■ Buttons

You find the description of the standard buttons in section "Buttons" on page 16.

Button	Meaning
Clear...	Resets the VLAN settings of the device to the default setting. Caution: You loose your connection to the device if you have changed the VLAN ID for the management in the *Basic Settings > Network* dialog.

5.7.2   VLAN Configuration

In this dialog, you manage the VLANs. To set up a VLAN, create a further row in the table. There you specify for each port if it transmits data packets of the respective VLAN and if the data packets contain a VLAN tag.

You distinguish between the following VLANs:
▶ The user sets up static VLANs.
▶ The device sets up dynamic VLANs automatically and removes them if the prerequisites cease to apply.
  For the following functions the device creates dynamic VLANs:
  – `MRP`: If you assign the ring ports a non-existing VLAN, then the device creates this VLAN.
  – `MVRP`: The device creates a VLAN based on the messages of neighboring devices.

Note: The settings are effective solely if the VLAN Unaware Mode is disabled. See the `Switching > Global` dialog.

■ **Table**

Parameters	Meaning
VLAN ID	ID of the VLAN. The device supports up to 128 VLANs simultaneously set up. Possible values: ▶ `1..4042`

Status	Displays how the VLAN is set up.
	
	Possible values:
	▶ `other`
	  VLAN `1`
	  or
	  VLAN set up using the `802.1X Port Authentication` function. See the `Network Security > 802.1X Port Authentication` dialog.
	▶ `permanent`
	  VLAN set up by the user.
	  or
	  VLAN set up using the `MRP` function. See the `Switching > L2-Redundancy > MRP` dialog.
	  VLANs with this setting remain set up after a restart, if you save the changes in the non-volatile memory.
	▶ `dynamicMvrp`
	  VLAN set up using the `MVRP` function. See the `Switching > MRP-IEEE > MVRP` dialog.
	  VLANs with this setting are write-protected. The device removes a VLAN from the table as soon as the last port leaves the VLAN.

Creation time	Displays the time of VLAN creation. The field displays the time stamp for the operating time (system uptime).
Name	Specifies the name of the VLAN. Possible values: ▶ Alphanumeric ASCII character string with 1..32 characters

Parameters	Meaning
\<Port number\>	Specifies if the respective port transmits data packets of the VLAN and if the data packets contain a VLAN tag. Possible values: ▶ `–` (default setting) The port is not a member of the VLAN and does not transmit data packets of the VLAN. ▶ `T` = Tagged The port is a member of the VLAN and transmits the data packets with a VLAN tag. You use this setting for uplink ports, for example. ▶ `LT` = Tagged Learned The port is a member of the VLAN and transmits the data packets with a VLAN tag. The device created the entry automatically based on the *GVRP* or *MVRP* function. ▶ `F` = Forbidden The port is not a member of the VLAN and does not transmit data packets of this VLAN. Additionally, the device helps prevent the port from becoming a VLAN member through the *MVRP* function. ▶ `U` = Untagged (default setting for VLAN 1) The port is a member of the VLAN and transmits the data packets without a VLAN tag. Use this setting if the connected device does not evaluate any VLAN tags, for example on end ports. ▶ `LU` = Untagged Learned The port is a member of the VLAN and transmits the data packets without a VLAN tag. The device created the entry automatically based on the *GVRP* or *MVRP* function. **Note:** Verify that the port on which the network management station is connected is a member of the VLAN in which the device transmits the management data. In the default setting, the device transmits the management data on VLAN 1. Otherwise, the connection to the device terminates when you transfer the changes to the device. The management access to the device is possible exclusively using the CLI through the V.24 interface.

■ Buttons

You find the description of the standard buttons in section "Buttons" on page 16.

Button	Meaning
	Opens the *Create* window to add a new entry to the table. In the *VLAN ID* field, you specify the ID of the VLAN.

5.7.3 VLAN Port

In this dialog you specify how the device handles received data packets that have no VLAN tag, or whose VLAN tag differs from the VLAN ID of the port.

This dialog allows you to assign a VLAN to the ports and thus specify the port VLAN ID.

Additionally, you also specify for each port how the device transmits data packets when the VLAN Unaware mode is disabled if one of the following situations occurs:
▶ The port receives data packets without a VLAN tagging.
▶ The port receives data packets with VLAN priority information (VLAN ID 0, priority tagged).
▶ The VLAN tagging of the data packet differs from the VLAN ID of the port.

Note: The settings are effective solely if the VLAN Unaware Mode is disabled. See the *Switching > Global* dialog.

■ Table

Parameters	Meaning
Port	Displays the port number.
Port-VLAN ID	Specifies the ID of the VLAN which the devices assigns to data packets without a VLAN tag. The prerequisite is that you specify in the *Acceptable packet types* column the value admitAll.
	Possible values: ▶ ID of a VLAN you set up (default setting: 1)
	When you use the *MRP* function and you have not assigned a VLAN to the ring ports, you specify the value 1 here for the ring ports. Otherwise, the device assigns the value to the ring ports automatically.
Acceptable packet types	Specifies whether the port transmits or discards received data packets without a VLAN tag.
	Possible values: ▶ admitAll (default setting) The port accepts data packets both with and without a VLAN tag. ▶ admitOnlyVlanTagged The port accepts solely data packets tagged with a VLAN ID ≥ 1.
Ingress filtering	Activates/deactivates the ingress filtering.
	Possible values: ▶ marked The ingress filtering is active. The device compares the VLAN ID in the data packet with the VLANs of which the device is a member. See the *Switching > VLAN > Configuration* dialog. If the VLAN ID in the data packet matches one of these VLANs, the port transmits the data packet. Otherwise, the device discards the data packet. ▶ unmarked (default setting) The ingress filtering is inactive. The device transmits received data packets without comparing the VLAN ID. Thus the port also transmits data packets with a VLAN ID of which the port is not a member.

■ Buttons

You find the description of the standard buttons in section .

5.8 L2-Redundancy

The menu contains the following dialogs:
- ▶ MRP
- ▶ Spanning Tree
- ▶ Link Aggregation
- ▶ Link Backup

5.8.1　MRP

The Media Redundancy Protocol (MRP) is a protocol that allows you to set up high-availability, ring-shaped network structures. An MRP ring with Hirschmann devices is made up of up to 100 devices that support the MRP protocol according to IEC 62439.

The ring structure of an MRP ring changes back into a line structure if a section fails. The maximum recovery time can be configured.

The Ring Manager function of the device closes the ends of a backbone in a line structure to a redundant ring.

Note: *Spanning Tree* and Ring Redundancy have an effect on each other. Deactivate the *Spanning Tree* protocol for the ports connected to the MRP ring. See the *Switching > L2-Redundancy > Spanning Tree > Port* dialog.

■ Operation

Parameters	Meaning
Operation	Enables/disables the *MRP* function. After you configured the parameters for the MRP ring, enable the function here. Possible values: ▶ `On` 　The *MRP* function is enabled. 　After you configured the devices in the MRP ring, the redundancy is active. ▶ `Off`　(default setting) 　The *MRP* function is disabled.

■ Ring port 1 /Ring port 2

Parameters	Meaning
Port	Specifies the number of the port that is operating as a ring port. Possible values: ▶ `<Port number>` 　Number of the ring port
Operation	Displays the operating status of the ring port. Possible values: ▶ `forwarding` 　The port is enabled, connection exists. ▶ `blocked` 　The port is blocked, connection exists. ▶ `disabled` 　The port is disabled. ▶ `not-connected` 　No connection exists.
Fixed backup	Activates/deactivates the backup port function for the *Ring port 2*. **Note:** The switch over to the primary port can exceed the maximum ring recovery time. Possible values: ▶ `marked` 　The *Ring port 2* backup function is active. If the ring is closed, the ring manager reverts back to the primary ring port. ▶ `unmarked`　(default setting) 　The *Ring port 2* backup function is inactive. If the ring is closed, the ring manager continues to send data on the secondary ring port.

■ **Configuration**

Parameters	Meaning
Ring manager	Enables/disables the *Ring manager* function. If there is one device at each end of the line, you activate this function. Possible values: ▶ `On` The *Ring manager* function is enabled. The device operates as a ring manager. ▶ `Off` (default setting) The *Ring manager* function is disabled. The device operates as a ring client.
Advanced mode	Activates/deactivates the advanced mode for fast recovery times. Possible values: ▶ `marked` (default setting) Advanced mode active. MRP-capable Hirschmann devices support this mode. ▶ `unmarked` Advanced mode inactive. Select this setting if another device in the ring does not support this mode.
Ring recovery	Specifies the maximum recovery time in milliseconds for reconfiguration of the ring. This setting is effective if the device operates as a ring manager. Possible values: ▶ `500ms` ▶ `200ms` (default setting) Shorter switching times make greater demands on the response time of every individual device in the ring. Use values lower than `500ms` if the other devices in the ring also support this shorter recovery time.
VLAN ID	Specifies the ID of the VLAN which you assign to the ring ports. Possible values: ▶ `0` (default setting) No VLAN assigned. Assign in the *Switching > VLAN > Configuration* dialog to the ring ports for VLAN `1` the value `U`. ▶ `1..4042` VLAN assigned. If you assign to the ring ports a non-existing VLAN, the device creates this VLAN. In the *Switching > VLAN > Configuration* dialog, the device creates an entry in the table for the VLAN and assigns the value `T` to the ring ports.

■ **Information**

Parameters	Meaning
Information	Displays messages for the redundancy configuration and the possible causes of errors. The following messages are possible if the device operates as a ring client or a ring manager: ▶ `Redundancy available` The redundancy is set up. When a component of the ring is down, the redundant line takes over its function. ▶ `Configuration error: Error on ringport link.` Error in the cabling of the ring ports. The following messages are possible if the device operates as a ring manager: ▶ `Configuration error: Packets from another ring manager received.` Another device exists in the ring that operates as the ring manager. Enable the *Ring manager* function only on one device in the ring. ▶ `Configuration error: Ring link is connected to wrong port.` A line in the ring is connected with a different port instead of with a ring port. The device only receives test data packets on 1 ring port.

■ **Buttons**

You find the description of the standard buttons in section "Buttons" on page 16.

Button	Meaning
Delete ring configuration	Disables the redundancy function and resets the settings in the dialog to the default setting.

5.8.2 Spanning Tree

The Spanning Tree Protocol (STP) is a protocol that deactivates redundant paths of a network in order to avoid loops. If a network component fails on the path, the device calculates the new topology and reactivates these paths.

The Rapid Spanning Tree Protocol enables fast switching to a newly calculated topology without interrupting existing connections. RSTP achieves average reconfiguration times of less than a second. When you use RSTP in a ring with 10 to 20 devices, you can achieve reconfiguration times in the order of milliseconds.

Note: If you connect the device to the network through twisted pair SFPs instead of through usual twisted pair ports, the reconfiguration of the network takes slightly longer.

The menu contains the following dialogs:
▶ Spanning Tree Global
▶ Spanning Tree Port

5.8.2.1   Spanning Tree Global

In this dialog, you enable/disable the *Spanning Tree* function and specify the bridge settings.

■ Operation

Parameters	Meaning
Operation	Enables/disables the Spanning Tree function on the device.
	Possible values:
	▶ `On` (default setting)
	▶ `Off`
	The device behaves transparently. The device floods received Spanning Tree data packets like multicast data packets to the ports.

■ Variant

Parameters	Meaning
Variant	Displays the protocol used for the *Spanning Tree* function:
	Possible values:
	▶ `rstp`
	The protocol `RSTP` is active.
	With `RSTP` (IEEE 802.1Q-2005), the *Spanning Tree* function operates for the underlying physical layer.

■ Traps

Parameters	Meaning
Send trap	Activates/deactivates the sending of SNMP traps in case of one of the following events:
	– Another bridge takes over the root bridge role.
	– The topology changes. A port changes its *Port state* from *forwarding* into *discarding* or from *discarding* into *forwarding*.
	Possible values:
	▶ `marked`
	The sending of SNMP traps is active.
	▶ `unmarked` (default setting)
	The sending of SNMP traps is inactive.

■ Bridge configuration

Parameters	Meaning
Bridge ID	Displays the bridge ID of the device. The device with the numerically lowest bridge ID takes over the role of the root bridge in the network.
	Possible values:
	▶ `<Bridge priority> / <MAC address>`
	Value in the *Priority* field / MAC address of the device

Parameters	Meaning
Priority	Specifies the bridge priority of the device.
	Possible values: ▶ `0..61440` in steps of 4096 (default setting: `32768`)
	Assign the lowest numeric priority in the network to the device to make it the root bridge.
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, 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 not changing 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, 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`, `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, the device replaces these values with the last valid values or with the default value.	
Max age	Specifies the maximum permissible branch length, for example 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, 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	Limits the maximum transmission rate for sending BPDUs.
	Possible values: ▶ `1..40` (default setting: `10`)
	When the device sends a BPDU, it increments a counter on this port. When the counter reaches the value specified here, the port stops sending BPDUs. On the one hand, this reduces the load generated by RSTP, and on the other a communication interruption may be caused when the device stops receiving BPDUs.
	The device decrements the counter by `1` every second. In the following second, the device sends a maximum of `1` new BPDU.

Parameters	Meaning

BPDU guard	Activates/deactivates the BPDU Guard function on the device.
	With this function, the device helps protect your network from incorrect configurations, attacks with STP-BPDUs, and undesired topology changes.
	
	Possible values:
	▶ `marked`
	The *BPDU guard* is active.
	  – The device applies the function to manually specified edge ports. For these ports, in the *Switching > L2-Redundancy > Spanning Tree > Port* dialog, *CIST* tab the checkbox in the *Admin edge port* column is marked.
	  – If an edge port receives an STP-BPDU, the device disables the port. For this port, in the *Basic Settings > Port* dialog, *Configuration* tab the checkbox in the *Port on* column is `unmarked`.
	▶ `unmarked` (default setting)
	The *BPDU guard* is inactive.
	
	To reset the status of the port to the value `forwarding`, you proceed as follows:
	☐ If the port is still receiving BPDUs:
	  – In the *Switching > L2-Redundancy > Spanning Tree > Port* dialog, *CIST* tab unmark the checkbox in the *Admin edge port* column.
	    or
	  – In the *Switching > L2-Redundancy > Spanning Tree > Global* dialog, unmark the *BPDU guard* checkbox.
	☐ To re-enable the port again you use the *Auto-Disable* function. Alternatively, proceed as follows:
	  – Open the *Basic Settings > Port* dialog, *Configuration* tab.
	  – Mark the checkbox in the *Port on* column.

BPDU filter (all admin edge ports)	Activates/deactivates the filtering of STP-BPDUs on every manually specified edge port. For these ports, in the *Switching > L2-Redundancy > Spanning Tree > Port* dialog, *CIST* tab the checkbox in the *Admin edge port* column is marked.
	
	Possible values:
	▶ `marked`
	The BPDU filter is active on every edge port.
	The function excludes these ports from *Spanning Tree* operations.
	  – The device does not send STP-BPDUs on these ports.
	  – The device drops any STP-BPDUs received on these ports.
	▶ `unmarked` (default setting)
	The global BPDU filter is inactive.
	You have the option to explicitly activate the BPDU filter for single ports. See the *Port BPDU filter* column in the *Switching > L2-Redundancy > Spanning Tree > Port* dialog.

Auto-disable	Activates/deactivates the *Auto-Disable* function for the parameters that *BPDU guard* is monitoring on the port.
	
	Possible values:
	▶ `marked`
	The *Auto-Disable* function for the *BPDU guard* is active.
	  – The device disables an edge port when the port receives an STP-BPDU. The "Link status" LED for the port flashes 3× per period.
	  – The *Diagnostics > Ports > Auto-Disable* dialog displays which ports are currently disabled due to the parameters being exceeded.
	  – The *Auto-Disable* function reactivates the port automatically. For this you go to the *Diagnostics > Ports > Auto-Disable* dialog and specify a waiting period for the relevant port in the *Reset timer [s]* column.
	▶ `unmarked` (default setting)
	The *Auto-Disable* function for the *BPDU guard* is inactive.

■ Root information

Parameters	Meaning
Bridge ID	Displays the bridge ID of the current root bridge.
	Possible values: ▶ `<Bridge priority> / <MAC address>`
Priority	Displays the bridge priority of the current root bridge.
	Possible values: ▶ `0..61440` in steps of 4096
Hello time [s]	Displays the time in seconds specified by the root bridge between the sending of two configuration messages (Hello data packets).
	Possible values: ▶ `1..2`
	The device uses this specified value. See the **`Bridge configuration`** frame.
Forward delay [s]	Specifies 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, forwarding`.
Max age	Specifies the maximum permissible branch length set up by the root bridge, for example the number of devices to the root bridge.
	Possible values: ▶ `6..40` (default setting: `20`)
	The **`Spanning Tree`** protocol uses the parameter to specify the validity of STP-BPDUs in seconds.

■ Topology information

Parameters	Meaning
Bridge is root	Displays whether the device currently has the role of the root bridge.
	Possible values: ▶ `marked` The device currently has the role of the root bridge. ▶ `unmarked` Another device currently has the role of the root bridge.
Root port	Displays the number of the port from which the current path leads to the root bridge. If the device takes over the role of the root bridge, the field displays the value `0`.
Root path cost	Specifies 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` If the value `0` is specified, the device takes over the role of the root bridge.
Topology changes	Displays how many times the device has put a port into the `forwarding` status via Spanning Tree since it was started.
Time since topology change	Displays the time since the last topology change.
	Possible values: ▶ `<days, hours:minutes:seconds>`

■ Buttons

You find the description of the standard buttons in section "Buttons" on page 16.

5.8.2.2 Spanning Tree Port

In this dialog, you activate the Spanning Tree function on the ports, specify edge ports, and specify the settings for various protection functions.

The dialog contains the following tabs:
▶ [CIST]
▶ [Guards]

[CIST]

In this tab, you have the option to activate the Spanning Tree function on the ports individually, specify the settings for edge ports, and view the current values. The abbreviation CIST stands for Common and Internal Spanning Tree.

Note: Deactivate the *Spanning Tree* function on the ports that are participating in other Layer 2 redundancy protocols. Otherwise the redundancy protocols may operate differently to the way intended. This can cause loops.

■ Table

Parameters	Meaning
Port	Displays the port number.
STP active	Activates/deactivates the Spanning Tree function on the port. Possible values: ▶ `marked` (default setting) ▶ `unmarked` If the *Spanning Tree* function is enabled in the device and disabled on the port, the port does not send STP-BPDUs and drops any STP-BPDUs received.
Port state	Displays the transmission status of the port. Possible values: ▶ `discarding` The port is blocked and forwards STP-BPDUs exclusively. ▶ `learning` The port is blocked, but it learns the MAC addresses of received data packets. ▶ `forwarding` The port forwards data packets. ▶ `disabled` The port is inactive. See the *Basic Settings > Port* dialog, *Configuration* tab. ▶ `manualFwd` The *Spanning Tree* function is disabled on the port. The port forwards STP-BPDUs. ▶ `notParticipate` The port is not participating in STP.
Port role	Displays the current role of the port in CIST. Possible values: ▶ `root` Port with the cheapest path to the root bridge. ▶ `alternate` Port with the alternative path to the root bridge (currently blocking). ▶ `designated` Port for the side of the tree averted from the root bridge (currently blocking). ▶ `backup` Port receives STP-BPDUs from its own device. ▶ `disabled` The port is inactive. See the *Basic Settings > Port* dialog, *Configuration* tab.
Port path cost	Specifies the path costs of the port. Possible values: ▶ `0..200000000` (default setting: `0`) If 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: ▶ `16..240` in steps of 16 (default setting: `128`) This value represents the first 4 bits of the port ID.

Parameters	Meaning
Received bridge ID	Displays the bridge ID of the device from which this port last received an STP-BPDU. Possible values: ▶ For ports with the `designated` role, the device displays the information for the STP-BPDU last received by the port. This helps to diagnose the possible STP problems in the network. ▶ For the `alternate`, `backup`, `master`, and `root` port roles, in the stationary condition (static topology) this information is identical to the information of the `designated` port role. ▶ If a port has no connection, or if it has not received any STP-BDPUs yet, the device displays the values that the port would send with the `designated` role.
Received port ID	Displays the port ID of the device from which this port last received an STP-BPDU. Possible values: ▶ For ports with the `designated` role, the device displays the information for the STP-BPDU last received by the port. This helps to diagnose the possible STP problems in the network. ▶ For the `alternate`, `backup`, `master`, and `root` port roles, in the stationary condition (static topology) this information is identical to the information of the `designated` port role. ▶ If a port has no connection, or if it has not received any STP-BDPUs yet, the device displays the values that the port would send with the `designated` role.
Received path cost	Displays the path cost that the higher-level bridge has from its root port to the root bridge. Possible values: ▶ For ports with the `designated` role, the device displays the information for the STP-BPDU last received by the port. This helps to diagnose the possible STP problems in the network. ▶ For the `alternate`, `backup`, `master`, and `root` port roles, in the stationary condition (static topology) this information is identical to the information of the `designated` port role. ▶ If a port has no connection, or if it has not received any STP-BDPUs yet, the device displays the values that the port would send with the `designated` role.
Admin edge port	Activates/deactivates the *Admin edge port* mode. Use the *Admin edge port* mode if the port is connected to an end device. This setting allows the edge port to change faster to the forwarding state after linkup and thus a faster accessibility of the end device. Possible values: ▶ `marked` The *Admin 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. – If the port receives an STP-BPDU, the device deactivates the port if the BPDU Guard function is active. See the *Switching > L2-Redundancy > Spanning Tree > Global* dialog. ▶ `unmarked` (default setting) The *Admin 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 *Admin 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 has not received 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)
Oper edge port	Displays whether an end device or an STP bridge is connected to the port. Possible values: ▶ `marked` An end device is connected to the port. The port does not receive any STP-BPDUs. ▶ `unmarked` An STP bridge is connected to the port. The port receives STP-BPDUs.

Parameters	Meaning
Oper PointToPoint	Displays whether the port is connected to an STP device via a direct full-duplex link.
	Possible values: ▶ `true` The port is connected directly to an STP device via a full-duplex link. The direct, decentralized communication between 2 bridges enables short reconfiguration times. ▶ `false` The port is connected in another way, for example via a half-duplex link or via a hub.
Port BPDU filter	Activates/deactivates the filtering of STP-BPDUs on the port explicitly. The prerequisite is that the port is a manually specified edge port. For these ports, the checkbox in the *Admin edge port* column is marked.
	Possible values: ▶ `marked` The BPDU filter is active on the port. The function excludes the port from *Spanning Tree* operations. – The device does not send STP-BPDUs on the port. – The device drops any STP-BPDUs received on the port. ▶ `unmarked` (default setting) The BPDU filter is inactive on the port. You have the option to globally activate the BPDU filter for every edge port. See the *Switching > L2-Redundancy > Spanning Tree > Global* dialog, *Bridge configuration* frame. If the *BPDU filter (all admin edge ports)* checkbox is marked, then the BPDU filter is still active on the port.
BPDU filter status	Displays whether or not the BPDU filter is active on the port.
	Possible values: ▶ `marked` The BPDU filter is active on the port as a result of the following settings: – The checkbox in the *Port BPDU filter* column is marked. and/or – The checkbox in the *BPDU filter (all admin edge ports)* column is marked. See the *Switching > L2-Redundancy > Spanning Tree > Global* dialog, *Bridge configuration* frame. ▶ `unmarked` The BPDU filter is inactive on the port.
BPDU flood	Activates/deactivates the *BPDU flood* mode on the port even if the *Spanning Tree* function is inactive on the port. The prerequisite is that the *BPDU flood* mode is also active for these ports.
	Possible values: ▶ `marked` The *BPDU flood* mode is active. The device floods STP-BPDUs received on the port to the ports for which the *Spanning Tree* function is inactive. ▶ `unmarked` (default setting) The *BPDU flood* mode is inactive.

■ **Buttons**

You find the description of the standard buttons in section "Buttons" on page 16.

[**Guards**]

This tab allows you to specify the settings for various protection functions on the ports.

■ **Table**

Parameters	Meaning
Port	Displays the port number.

Root guard	Activates/deactivates the monitoring of STP-BPDUs on the port. The prerequisite is that the *Loop guard* function is inactive.
	
	With this setting the device helps you protect your network from incorrect configurations or attacks with STP-BPDUs that try to change the topology. This setting is relevant solely for ports with the STP role `designated`.
	
	Possible values:
	▶ `marked`
	    The monitoring of STP-BPDUs is active.
	    – If the port receives an STP-BPDU with better path information to the root bridge, the device discards the STP-BPDU and sets the status of the port to the value `discarding` instead of to `root`.
	    – If there are no STP-BPDUs with better path information to the root bridge, the device resets the status of the port after 2 × *Hello time [s]*.
	▶ `unmarked` (default setting)
	    The monitoring of STP-BPDUs is inactive.

TCN guard	Activates/deactivates the monitoring of "Topology Change Notifications" on the port. With this setting the device helps you protect your network from attacks with STP-BPDUs that try to change the topology.
	
	Possible values:
	▶ `marked`
	    The monitoring of "Topology Change Notifications" is enabled.
	    – The port ignores the Topology Change flag in received STP-BPDUs.
	    – If the received BPDU contains other information that causes a topology change, the device processes the BPDU even if the TCN guard is enabled.
	      Example: The device receives better path information for the root bridge.
	▶ `unmarked` (default setting)
	    The monitoring of "Topology Change Notifications" is disabled.
	    If the device receives STP-BPDUs with a Topology Change flag, it deletes the address table of the port and forwards the Topology Change Notifications.

Loop guard	Activates/deactivates the monitoring of loops on the port. The prerequisite is that the *Root guard* function is inactive.
	
	With this setting the device helps prevent loops if the port does not receive any more STP-BPDUs. Use this setting solely for ports with the STP role `alternate`, `backup` or `root`.
	
	Possible values:
	▶ `marked`
	    The monitoring of loops is active. This helps prevent loops for example if you disable the Spanning Tree function on the remote device or if the connection is interrupted solely in the receiving direction.
	    – If the port does not receive any STP-BPDUs for a while, the device sets the status of the port to the value `discarding` and the value in the *Loop state* column to `true`.
	    – If the port then receives STP-BPDUs again, the device sets the status of the port to a value according to *Port role* and the value in the *Loop state* column to `false`.
	▶ `unmarked` (default setting)
	    The monitoring of loops is inactive.
	    If the port does not receive any STP-BPDUs for a while, the device sets the status of the port to the value `forwarding`.

Parameters	Meaning
Loop state	Displays whether the loop state of the port is inconsistent.
	Possible values:
	▶ `true`
	The loop state of the port is inconsistent:
	– The port is not receiving any STP-BPDUs and the *Loop guard* function is enabled.
	– The device sets the state of the port to the value `discarding`. The device thus helps prevent any potential loops.
	▶ `false`
	The loop state of the port is consistent. The port receives STP-BPDUs.
Trans. into loop	Displays how many times the device has set the value in the *Loop state* column from `false` to `true`.
Trans. out of loop	Displays how many times the device has set the value in the *Loop state* column from `true` to `false`.
BPDU guard effect	Displays whether the port received an STP-BPDU as an edge port.
	Prerequisite:
	– The port is a manually specified edge port. In the *Port* dialog, the checkbox for this port in the *Admin edge port* column is `marked`.
	– In the *Switching > L2-Redundancy > Spanning Tree > Global* dialog, the BPDU Guard function is active.
	Possible values:
	▶ `marked`
	The port is an edge port and received an STP-BPDU.
	The device deactivates the port. For this port, in the *Basic Settings > Port* dialog, *Configuration* tab the checkbox in the *Port on* column is `unmarked`.
	▶ `unmarked`
	The port is an edge port and has not received any STP-BPDUs, or the port is not an edge port.
	To reset the status of the port to the value `forwarding`, you proceed as follows:
	☐ If the port is still receiving BPDUs:
	– In the *CIST* tab, unmark the checkbox in the *Admin edge port* column.
	or
	– In the *Switching > L2-Redundancy > Spanning Tree > Global* dialog, unmark the *BPDU guard* checkbox.
	☐ To activate the port, proceed as follows:
	– Open the *Basic Settings > Port* dialog, *Configuration* tab.
	– Mark the checkbox in the *Port on* column.

■ **Buttons**

You find the description of the standard buttons in section .

5.8.3 Link Aggregation

IEEE 802.1ax defines a Link Aggregation Group (LAG) as the combining of 2 or more, full-duplex point-to-point links operating at the same rate, on a single switch to increase bandwidth. Furthermore, Link Aggregation provides for redundancy. When a link goes down, the remaining links in the LAG continue to forward the traffic.

Link Aggregation Control Protocol Data Units (LACPDUs) contain 2 fields with 8 binary bits of information each the Actor periodically sends to a Partner. The fields describe the state of the Actor and what the Actor knows about the Partner. The 8 bits contain information about the state of the Actor and Partner. The port transmits LACPDUs when in the active state. In the passive state, the port transmits LACPDUs solely when requested.

■ Table

Parameters	Meaning
Trunk port	Displays the Link Aggregation port number.
Name	Specifies the name of the Link Aggregation Group. Possible values: ▶ Alphanumeric ASCII character string with 1..15 characters

Active	Activates/deactivates Link Aggregation Group.
	
	Possible values:
	▶ `marked` (default setting)
	   The LAG instance is in an „up" state and processes traffic according to the specified values.
	▶ `unmarked`
	   The LAG instance, including the member ports, is in a "down" state. The member ports remain in the LAG instance and block traffic.

STP active	Activates/deactivates the `Spanning Tree` protocol on this LAG interface. After you create the Link Aggregation instance in the table the device automatically adds the port to the `Switching > L2-Redundancy > Spanning Tree > Port` dialog.
	
	Possible values:
	▶ `marked` (default setting)
	   Enabling the STP mode in this dialog also enables the port in the `Switching > L2-Redundancy > Spanning Tree > Port` dialog.
	▶ `unmarked`
	   Disabling the STP mode in this dialog also disables the port in the `Switching > L2-Redundancy > Spanning Tree > Port` dialog.
	
	The prerequisite is that you enable the function globally in the `Switching > L2-Redundancy > Spanning Tree > Global` dialog.

Static link aggregation	Activates/deactivates the `Static link aggregation` function on the LAG interface.
	
	Possible values:
	▶ `marked`
	   When enabled, the `Static link aggregation` function provides a stable network and the administrator manually propagates the aggregation status of the port.
	▶ `unmarked` (default setting)
	   The device propagates the aggregation status of the port automatically.

Active ports (min.)	Specifies how many active ports the device uses for the Link Aggregation group. Possible values: ▶ `1..2` (default setting: `2`) ▶ `1..4` (default setting: `4`) **Note:** The actual number of ports available depends on the device.

Parameters	Meaning
Type	Displays the type of group Link Aggregation used. Possible values: ▶ `static` The device uses static aggregation on the port, *Static link aggregation* enabled. ▶ `dynamic` The device uses dynamic aggregation on the port, *Static link aggregation* disabled.
Send trap (Link up/ down)	Activates/deactivates the sending of SNMP traps when the device detects changes in the link up/ down status on this interface. Possible values: ▶ `marked` (default setting) The sending of SNMP traps is inactive. The device sends an SNMP trap when it detects a link up/down status change. ▶ `unmarked` The sending of SNMP traps is inactive. The prerequisite for sending SNMP traps is that you enable the function in the *Diagnostics > Status Configuration > Alarms (Traps)* dialog and specify at least 1 trap destination.
LACP admin key	Specifies the administrative value of the local key on this LAG. The aggregator uses the administrative key to group links in a set. It is possible to have the administrative key value differ from the operational key value. Possible values: ▶ `0..65535` (default setting: `0`)
LACP collector max. delay [µs]	Specifies the Frame Collector maximum delay time in microseconds. The LAG uses a Frame Collector to pass frames to the MAC client in the order that the port receives them. The collector delays either delivering the frame to its MAC client or discarding the frame according to this value. Possible values: ▶ `0..65535` (default setting: `0`)
Port	Displays the port members of the LAG instance.
Status	Displays the LAG status of the port. Possible values: ▶ `active` The port is actively participating in the LAG instance. ▶ `inactive` The port is a non-participant in the LAG instance.
LACP active	Activates/deactivates LACP on this port. Possible values: ▶ `marked` (default setting) The port actively participates in the LAG. ▶ `unmarked` The port is a non-participant in the LAG.
LACP port actor admin key	Specifies the administrative key value for the aggregation port. The LAG uses keys to assign membership to local ports on the Actor device. Specify the same key value for the actor ports participating in the same LAG. Possible values: ▶ `0..65535` (default setting: `0`) When the port is in a LAG, then set this value to correspond with the LAG operational key.

Parameters	Meaning
LACP actor admin state	Specifies the administrative values of the Actor State transmitted in LACPDUs. You have the option to combine the values with each other. This allows you administrative control over the LACPDU parameters. In the drop-down list, select one or more values. Possible values: ▶ `lacpActivity` Specifies whether the port is an active or passive participant. An active participant transmits LACPDUs periodically. A passive participant transmits LACPDUs when requested. When selected you set the parameter to active participant. ▶ `lacpTimeout` The Actor periodically transmits LACPDUs at either a slow or fast transmission rate depending on the preference of the partner. You set the parameter to either long timeout or short timeout. When selected you set the parameter to short timeout. ▶ `aggregation` Specifies whether the port is a potential candidate for aggregation or for an individual link. When selected you set the parameter to aggregatable. ▶ `-` The state is unspecified. When the parameter is unspecified the device displays the following values for the LACPDU parameters: – `synchronization` The system considers this link to be allocated to the correct LAG, and the group is associated with a compatible aggregator. Furthermore, the identity of the LAG is consistent with the system ID, and operational key information transmitted. – `collecting` Collection of incoming frames on this link is definitely enabled. For example, collection is currently enabled and remains enabled in the absence of administrative changes or changes in the received protocol information. – `distributing` Distribution is currently disabled and remains disabled in the absence of administrative changes or changes in received protocol information. – `defaulted` The LACPDUs received by the actor is using the statically configured partner information. – `expired` The LACPDUs received by the actor is in the expired state.
LACP actor port priority	Specifies the LACP actor port priority value for this port. Possible values: ▶ `0..65535` (default setting: `128`) The port with the lower value has the higher priority.
LACP partner port admin key	Specifies the default value for the partner key, assigned by administrator or system policy for use when information about the partner is unknown or expired. The LAG uses keys to assign membership to partner ports. Specify the same key value for the local partners participating in the same LAG. Possible values: ▶ `0..65535` (default setting: `0`) If the port is alone in a LAG, then set this value to 0. When the port is in a LAG, then set this value to correspond with the LAG operational key. To manage the partner ports, you use this parameter in conjunction with the settings in the following columns: – *LACP partner admin port* – *LACP partner admin port priority* – *LACP partner admin SysID* – *LACP partner admin sys priority*

Parameters	Meaning
LACP partner admin state	Specifies the partner administrative state values. You have the option to combine the values with each other which allows you administrative control over the LACPDU parameters. In the drop-down list, select one or more values. Possible values: ▶ `lacpActivity` Specifies whether the port is an active or passive participant. An active participant transmits LACPDUs periodically. A passive participant transmits LACPDUs when requested. When selected you set the parameter to active. ▶ `lacpTimeout` The Actor periodically transmits LACPDUs at either a slow or fast transmission rate depending on the preference of the Partner either long timeout or short timeout. When selected you set the parameter to short timeout. ▶ `aggregation` Specifies whether the port is a potential candidate for aggregation or for an individual link. When selected you set the parameter to aggregatable. ▶ `-` The state is unspecified. Possible values: ▶ `synchronization` The system considers this link to be allocated to the correct LAG, and the group is associated with a compatible aggregator. Furthermore, the identity of the LAG is consistent with the system ID, and operational key information transmitted. ▶ `collecting` Collection of incoming frames on this link is definitely enabled. For example, collection is currently enabled and remains enabled in the absence of administrative changes or changes in the received protocol information. ▶ `distributing` Distribution is currently disabled and remains disabled in the absence of administrative changes or changes in received protocol information. ▶ `defaulted` The LACPDUs received by the actor is using the statically configured partner information. ▶ `expired` The LACPDUs received by the partner is in the expired state.
LACP partner admin port	Specifies the port number of the partner port. Possible values: ▶ `0..65535` (default setting: `0`) To manage the partner ports, you use this parameter in conjunction with the settings in the following columns: – *LACP partner port admin key* – *LACP partner admin port priority* – *LACP partner admin SysID* – *LACP partner admin sys priority*
LACP partner admin port priority	Specifies the port priority for the partner port. Possible values: ▶ `0..65535` (default setting: `0`) The port with the lower value has the higher priority. To manage the partner ports, you use this parameter in conjunction with the settings in the following columns: – *LACP partner port admin key* – *LACP partner admin port* – *LACP partner admin SysID* – *LACP partner admin sys priority*

Parameters	Meaning
LACP partner admin SysID	Specifies a MAC Address value representing the Partner System ID. Possible values: ▶ Valid MAC address (default setting: `00:00:00:00:00:00`) To manage the partner ports, you use this parameter in conjunction with the settings in the following columns: – *LACP partner port admin key* – *LACP partner admin port* – *LACP partner admin port priority* – *LACP partner admin sys priority*
LACP partner admin sys priority	Specifies the default value for the system priority component of the system identifier of the partner, assigned by administrator or system policy for use when the information from the partner is unknown or expired. Possible values: ▶ `0..65535` (default setting: `0`) The port with the lower value has the higher priority. To manage the partner ports, you use this parameter in conjunction with the settings in the following columns: – *LACP partner port admin key* – *LACP partner admin port* – *LACP partner admin port priority* – *LACP partner admin SysID*

■ Buttons

You find the description of the standard buttons in section "Buttons" on page 16.

Button	Meaning
🖳	Opens the *Create* window to add a new entry to the table. ▶ In the *Trunk port* drop-down list you select the port number of the Link Aggregation Group trunk. ▶ In the *Port* drop-down list you select the port to assign to the interface.

5.8.4   Link Backup

With Link Backup, you configure pairs of redundant links. Each pair has a primary port and a backup port. The primary port forwards traffic until the device detects an error. When the device detects an error on the primary port, the Link Backup function transfers traffic over to the backup port.

The dialog also allows you to set a fail back option. When you enable the fail back function and the primary port returns to normal operation, the device first blocks traffic on the backup port and then forwards traffic on the primary port. This process helps protect the device from causing loops in the network.

■ Operation

Parameters	Meaning
Operation	Enables/disables the Link Backup function globally on the device.

	Possible values:
	▶ `On`
	  Enables the Link Backup function.
	▶ `Off` (default setting)
	  Disables the Link Backup function.

■ Table

Parameters	Meaning
Primary port	Displays the primary port of the interface pair. When you enable the Link Backup function this port is responsible for forwarding traffic.
	Possible values: ▶ Physical ports
Backup port	Displays the backup port on which the device forwards traffic when the device detects an error on the primary port.
	Possible values: ▶ Physical ports except for the port you set as the primary port.
Description	Specifies the Link Backup pair. Enter a name to identify the Backup pair.
	Possible values: ▶ Alphanumeric ASCII character string with 0..255 characters
Primary port status	Displays the status of the primary port for this Link Backup pair.

	Possible values:
	▶ `forwarding`
	  The link is up, no shutdown, and forwarding traffic.
	▶ `blocking`
	  The link is up, no shutdown, and blocking traffic.
	▶ `down`
	  The port is either link down, cable unplugged, or disabled in software, shutdown.
	▶ `unknown`
	  The Link Backup feature is globally disabled, or the port pair is inactive. Therefore, the device ignores the port pair settings.

Parameters	Meaning
Backup port status	Displays the status of the Backup port for this Link Backup pair.

	Possible values:
	▶ `forwarding`
	  The link is up, no shutdown, and forwarding traffic.
	▶ `blocking`
	  The link is up, no shutdown, and blocking traffic.
	▶ `down`
	  The port is either link down, cable unplugged, or disabled in the software, shutdown.
	▶ `unknown`
	  The Link Backup feature is globally disabled, or the port pair is inactive. Therefore, the device ignores the port pair settings.

Fail back	Activates/deactivates the automatic fail back.

	Possible values:
	▶ `marked` (default setting)
	  The automatic fail back is active.
	  After the delay timer expires, the backup port changes to `blocking` and the primary port changes to `forwarding`.
	▶ `unmarked`
	  The automatic fail back is inactive.
	  The backup port continues forwarding traffic even after the primary port re-establishes a link or you manually change the admin status of the primary port from `shutdown` to `no shutdown`.

Fail back delay [s]	Specifies the delay time in seconds that the device waits after the primary port re-establishes a link. Furthermore, this timer also applies when you manually set the admin status of the primary port from `shutdown` to `no shutdown`. After the delay timer expires, the backup port changes to `blocking` and the primary port changes to `forwarding`.
	Possible values: ▶ `0..3600` (default setting: `30`) When set to `0`, immediately after the primary port re-establishes a link, the backup port changes to `blocking` and the primary port changes to `forwarding`. Furthermore, immediately after you manually set the admin status of from `shutdown` to `no shutdown`, the backup port changes to `blocking` and the primary port changes to `forwarding`.
Active	Activates/deactivates the Link Back up pair configuration.

	Possible values:
	▶ `marked`
	  The Link Backup pair is active. The device senses the link and administration status and forwards traffic according to the pair configuration.
	▶ `unmarked` (default setting)
	  The Link Backup pair is inactive. The ports forward traffic according to standard switching.

■ Buttons

You find the description of the standard buttons in section "Buttons" on page 16.

■ Create

Parameters	Meaning
Primary port	Specifies the primary port of the backup interface pair. During normal operation this port is responsible for forwarding the traffic.
	Possible values: ▶ Physical ports
Backup port	Specifies the backup port to which the device transfers the traffic to when the device detects an error on the primary port.
	Possible values: ▶ Physical ports except for the port you set as the primary port.

6 Diagnostics

The menu contains the following dialogs:
- Status Configuration
- System
- Syslog
- Ports
- LLDP
- Report

6.1 Status Configuration

The menu contains the following dialogs:
▶ Device Status
▶ Security Status
▶ Signal Contact
▶ Alarms (Traps)

6.1.1 Device Status

The device status provides an overview of the overall condition of the device. Many process visualization systems record the device status for a device in order to present its condition in graphic form.

The device displays its current status as `error` or `ok` in the ***Device status*** frame. The device determines this status from the individual monitoring results.

The device displays detected faults in the ***Status*** tab and also in the ***Basic Settings > System*** dialog, ***Device Status*** frame.

The dialog contains the following tabs:
▶ [Global]
▶ [Port]
▶ [Status]

[**Global**]

■ **Device status**

Parameters	Meaning
Device status	Displays the current status of the device. The device determines the status from the individual monitored parameters. Possible values: ▶ `error` The device displays this value to indicate a detected error in one of the monitored parameters. ▶ `ok`

■ **Traps**

Parameters	Meaning

Send trap	Activates/deactivates the sending of SNMP traps when the device detects changes in the monitored functions.
	
	Possible values:
	▶ `marked`
	    The sending of SNMP traps is active.
	    The device sends an SNMP trap when the device detects a change in the monitored functions..
	▶ `unmarked` (default setting)
	    The sending of SNMP traps is inactive.
	
	The prerequisite for sending SNMP traps is that you enable the function in the *Diagnostics > Status Configuration > Alarms (Traps)* dialog and specify at least 1 trap destination.

■ **Table**

Parameters	Meaning

Temperature	Activates/deactivates the monitoring of the temperature in the device.
	
	Possible values:
	▶ `marked` (default setting)
	    Monitoring is active.
	    In the *Device status* frame, the value changes to `error` if the temperature exceeds or falls below the specified limit.
	▶ `unmarked`
	    Monitoring is inactive.
	
	You specify the temperature thresholds in the *Basic Settings > System* dialog, *Upper temp. limit [°C]* field and *Lower temp. limit [°C]* field.

Ring redundancy	Activates/deactivates the monitoring of the ring redundancy.
	
	Possible values:
	▶ `marked`
	    Monitoring is active.
	    In the *Device status* frame, the value changes to `error` in the following situations:
	    – The redundancy function becomes active (loss of redundancy reserve).
	    – The device is a normal ring participant and detects an error in its settings.
	▶ `unmarked` (default setting)
	    Monitoring is inactive.

Parameters	Meaning
Connection errors	Activates/deactivates the monitoring of the port/interface link.
	Possible values: ▶ `marked` Monitoring is active. In the *Device status* frame, the value changes to `error` if the link interrupts on a monitored port/interface. In the *Port* tab, you have the option of selecting the ports/interfaces to be monitored individually. ▶ `unmarked` (default setting) Monitoring is inactive.
External memory removal	Activates/deactivates the monitoring of the active external memory.
	Possible values: ▶ `marked` Monitoring is active. In the *Device status* frame, the value changes to `error` if you remove the active external memory from the device. ▶ `unmarked` (default setting) Monitoring is inactive.
External memory not in sync	Activates/deactivates the monitoring of the configuration profile in the device and in the external memory.
	Possible values: ▶ `marked` Monitoring is active. In the *Device status* frame, the value changes to `error` in the following situations: – The configuration profile solely exists in the device. – The configuration profile in the device differs from the configuration profile in the external memory. ▶ `unmarked` (default setting) Monitoring is inactive.

■ Buttons

You find the description of the standard buttons in section .

[Port]

■ Table

Parameters	Meaning
Port	Displays the port number.

Propagate connection error	Activates/deactivates the monitoring of the link on the port/interface.
	
	Possible values:
	▶ `marked`
	  Monitoring is active.
	  In the *Device status* frame, the value changes to `error` if the link on the selected port/interface is interrupted.
	▶ `unmarked` (default setting)
	  Monitoring is inactive.
	
	This setting takes effect when you mark the *Connection errors* checkbox in the *Global* tab.

■ Buttons

You find the description of the standard buttons in section "Buttons" on page 16.

[Status]

■ Table

Parameters	Meaning
Timestamp	Displays the date and time of the event in the format, `Month Day, Year  hh:mm:ss AM/PM`.
Cause	Displays the event which caused the SNMP trap.

■ Buttons

You find the description of the standard buttons in section "Buttons" on page 16.

6.1.2   Security Status

This dialog gives you an overview of the status of the safety-relevant settings in the device.

The device displays its current status as `error` or `ok` in the ***Security status*** frame. The device determines this status from the individual monitoring results.

The device displays detected faults in the ***Status*** tab and also in the ***Basic Settings > System*** dialog, ***Security status*** frame.

The dialog contains the following tabs:
▶ [Global]
▶ [Port]
▶ [Status]

[Global]

■ Security status

Parameters	Meaning
Security status	Displays the current status of the security-relevant settings in the device. The device determines the status from the individual monitored parameters.
	Possible values: ▶ `error` 　The device displays this value to indicate a detected error in one of the monitored parameters. ▶ `ok`

■ Traps

Parameters	Meaning
Send trap	Activates/deactivates the sending of SNMP traps when the device detects changes in the monitored functions.
	Possible values: ▶ `marked` 　The sending of SNMP traps is active. 　The device sends an SNMP trap when the device detects a change in the monitored functions.. ▶ `unmarked`　(default setting) 　The sending of SNMP traps is inactive.
	The prerequisite for sending SNMP traps is that you enable the function in the *Diagnostics > Status Configuration > Alarms (Traps)* dialog and specify at least 1 trap destination.

■ Table

Parameters	Meaning
Password default settings unchanged	Activates/deactivates the monitoring of the password for the locally set up user accounts `user` and `admin`.
	Possible values: ▶ `marked`　(default setting) 　Monitoring is active. 　In the *Security status* frame, the value changes to `error` if the password for the `user` or `admin` user accounts is the default setting. ▶ `unmarked` 　Monitoring is inactive.
	You set the password in the *Device Security > User Management* dialog.
Min. password length < 8	Activates/deactivates the monitoring of the *Min. password length* policy.
	Possible values: ▶ `marked`　(default setting) 　Monitoring is active. 　In the *Security status* frame, the value changes to `error` if the value for the *Min. password length* policy is less than `8`. ▶ `unmarked` 　Monitoring is inactive.
	You specify the *Min. password length* policy in the *Device Security > User Management* dialog in the *Configuration* frame.

Parameters	Meaning
Password policy settings deactivated	Activates/deactivates the monitoring of the Password policies settings.
	Possible values: ▶ `marked` (default setting) Monitoring is active. In the *`Security status`* frame, the value changes to `error` if the value for at least one of the following policies is less than `1`: – *`Upper-case characters (min.)`* – *`Lower-case characters (min.)`* – *`Digits (min.)`* – *`Special characters (min.)`* ▶ `unmarked` Monitoring is inactive.
	You specify the policy settings in the *`Device Security > User Management`* dialog in the *`Password policy`* frame.
User account password policy check deactivated	Activates/deactivates the monitoring of the *`Policy check`* function.
	Possible values: ▶ `marked` Monitoring is active. In the *`Security status`* frame, the value changes to `error` if for at least 1 user account the *`Policy check`* function is inactive. ▶ `unmarked` (default setting) Monitoring is inactive.
	You activate the *`Policy check`* function in the *`Device Security > User Management`* dialog.
Telnet server active	Activates/deactivates the monitoring of the Telnet server.
	Possible values: ▶ `marked` (default setting) Monitoring is active. In the *`Security status`* frame, the value changes to `error` if you enable the Telnet server. ▶ `unmarked` Monitoring is inactive.
	You enable/disable the Telnet server in the *`Device Security > Management Access > Server`* dialog, *`Telnet`* tab.
HTTP server active	Activates/deactivates the monitoring of the HTTP server.
	Possible values: ▶ `marked` (default setting) Monitoring is active. In the *`Security status`* frame, the value changes to `error` if you enable the HTTP server. ▶ `unmarked` Monitoring is inactive.
	You enable/disable the HTTP server in the *`Device Security > Management Access > Server`* dialog, *`HTTP`* tab.
SNMP unencrypted	Activates/deactivates the monitoring of the SNMP server.
	Possible values: ▶ `marked` (default setting) Monitoring is active. In the *`Security status`* frame, the value changes to `error` if at least one of the following conditions applies: – The *`SNMPv1`* function is enabled. – The *`SNMPv2`* function is enabled. – The encryption for SNMPv3 is disabled. You enable the encryption in the *`Device Security > User Management`* dialog, in the *`SNMP encryption type`* column. ▶ `unmarked` Monitoring is inactive.
	You specify the settings for the SNMP agent in the *`Device Security > Management Access > Server`* dialog, *`SNMP`* tab.

Parameters	Meaning
Access to system monitor with V.24 possible	Activates/deactivates the monitoring of the system monitor. When the system monitor is activated, the user has the possibility to change to the system monitor via a V.24 connection. Possible values: ▶ `marked` Monitoring is active. In the *Security status* frame, the value changes to `error` if you activate the system monitor. ▶ `unmarked` (default setting) Monitoring is inactive. You activate/deactivate the system monitor in the *Diagnostics > System > Selftest* dialog.
Saving the configuration profile on the external memory possible	Activates/deactivates the monitoring of the configuration profile in the external memory. Possible values: ▶ `marked` Monitoring is active. In the *Security status* frame, the value changes to `error` if you activate the saving of the configuration profile in the external memory. ▶ `unmarked` (default setting) Monitoring is inactive. You activate/deactivate the saving of the configuration profile in the external memory in the *Basic Settings > External Memory* dialog.
Load unencrypted config from external memory	Activates/deactivates the monitoring of loading unencrypted configuration profiles from the external memory. Possible values: ▶ `marked` (default setting) Monitoring is active. In the *Security status* frame, the value changes to `error` when the settings allow the device to load an unencrypted configuration profile from the external memory. The *Security status* frame in the *Basic Settings > System* dialog, displays an alarm if the following preconditions are fulfilled: – The configuration profile stored in the external memory is unencrypted. and – The *Config priority* column in the *Basic Settings > External Memory* dialog has the value `first`. ▶ `unmarked` Monitoring is inactive.
Link interrupted on enabled device ports	Activates/deactivates the monitoring of the link on the active ports. Possible values: ▶ `marked` Monitoring is active. In the *Security status* frame, the value changes to `error` if the link interrupts on an active port. In the *Port* tab, you have the option of selecting the ports to be monitored individually. ▶ `unmarked` (default setting) Monitoring is inactive.
Access with HiDiscovery possible	Activates/deactivates the monitoring of the HiDiscovery function. Possible values: ▶ `marked` (default setting) Monitoring is active. In the *Security status* frame, the value changes to `error` if you enable the HiDiscovery function. ▶ `unmarked` Monitoring is inactive. You enable/disable the HiDiscovery function in the *Basic Settings > Network* dialog.

Parameters	Meaning
IEC61850-MMS active	Activates/deactivates the monitoring of the *IEC61850-MMS* function. Possible values: ▶ `marked` (default setting) Monitoring is active. In the *Security status* frame, the value changes to `error` if you enable the *IEC61850-MMS* function. ▶ `unmarked` Monitoring is inactive. You enable/disable the *IEC61850-MMS* function in the *Industrial Protocols > IEC61850-MMS* dialog, *Operation* frame.
Modbus TCP active	Activates/deactivates the monitoring of the *Modbus TCP* function. Possible values: ▶ `marked` (default setting) Monitoring is active. In the *Security status* frame, the value changes to `error` if you enable the *Modbus TCP* function. ▶ `unmarked` Monitoring is inactive. You enable/disable the *Modbus TCP* function in the *Advanced > Industrial Protocols > Modbus TCP* dialog, *Operation* frame.
Self-signed HTTPS certificate present	Activates/deactivates the monitoring of the HTTPS certificate. Possible values: ▶ `marked` (default setting) Monitoring is active. In the *Security status* frame, the value changes to `error` if the HTTPS server uses a self-created digital certificate. ▶ `unmarked` Monitoring is inactive.

■ **Buttons**

You find the description of the standard buttons in section "Buttons" on page 16.

[Port]

■ Table

Parameters	Meaning
Port	Displays the port number.
Link interrupted on enabled device ports	Activates/deactivates the monitoring of the link on the active ports. Possible values: ▶ `marked` Monitoring is active. In the *Security status* frame, the value changes to `error` when the port is enabled (*Basic Settings > Port* dialog, *Configuration* tab, *Port on* checkbox is `marked`) and the link is down on the port. ▶ `unmarked` (default setting) Monitoring is inactive. This setting takes effect when you mark the *Link interrupted on enabled device ports* checkbox in the *Diagnostics > Status Configuration > Security Status* dialog, *Global* tab.

■ Buttons

You find the description of the standard buttons in section "Buttons" on page 16.

[**Status**]

■ **Table**

Parameters	Meaning
Timestamp	Displays the date and time of the event in the format, `Month Day, Year hh:mm:ss AM/PM`.
Cause	Displays the event which caused the SNMP trap.

■ **Buttons**

You find the description of the standard buttons in section "Buttons" on page 16.

6.1.3   Signal Contact

The signal contact is a potential-free relay contact. The device thus allows you to perform remote diagnosis. The device uses the relay contact to signal the occurrence of events by opening the relay contact and interrupting the closed circuit.

Note: The device can contain several signal contacts. Each contact contains the same monitoring functions. Several contacts allow you to group various functions together providing flexibility in system monitoring.

The menu contains the following dialogs:
► Signal Contact 1 / Signal Contact 2

6.1.3.1   Signal Contact 1 / Signal Contact 2

In this dialog you specify the trigger conditions for the signal contact.

The signal contact gives you the following options:
- ▶ Monitoring the correct operation of the device.
- ▶ Signaling the device status of the device.
- ▶ Signaling the security status of the device.
- ▶ Controlling external devices by manually setting the signal contacts.

The device displays detected faults in the *Status* tab and also in the *Basic Settings > System* dialog, *Signal contact status* frame.

The dialog contains the following tabs:
- ▶ [Global]
- ▶ [Port]
- ▶ [Status]

[Global]

■ **Configuration**

Parameters	Meaning
Mode	Specifies which events the signal contact indicates.
	Possible values:
	▶ `Manual setting` (default setting for *Signal Contact 2*, if present) You use this setting to manually open or close the signal contact, for example to turn on or off a remote device. See the *Contact* option list.
	▶ `Monitoring correct operation` (default setting) Using this setting the signal contact indicates the status of the parameters specified in the table below.
	▶ `Device status` Using this setting the signal contact indicates the status of the parameters monitored in the *Diagnostics > Status Configuration > Device Status* dialog. In addition, you can read the status in the *Signal contact status* frame.
	▶ `Security status` Using this setting the signal contact indicates the status of the parameters monitored in the *Diagnostics > Status Configuration > Security Status* dialog. In addition, you can read the status in the *Signal contact status* frame.
	▶ `Device/Security status` Using this setting the signal contact indicates the status of the parameters monitored in the *Diagnostics > Status Configuration > Device Status* and the *Diagnostics > Status Configuration > Security Status* dialog. In addition, you can read the status in the *Signal contact status* frame.
Contact	Toggles the signal contact manually. The prerequisite is that you select in the *Mode* drop-down list the value `Manual setting`.
	Possible values: ▶ `open` The signal contact is opened. ▶ `close` The signal contact is closed.

■ **Signal contact status**

Parameters	Meaning
Signal contact status	Displays the current status of the signal contact.
	Possible values: ▶ `Opened (error)` The signal contact is opened. The circuit is interrupted. ▶ `Closed (ok)` The signal contact is closed. The circuit is closed.

■ Trap configuration

Parameters	Meaning
Send trap	Activates/deactivates the sending of SNMP traps when the device detects changes in the monitored functions.
	Possible values: ▶ `marked` The sending of SNMP traps is active. The device sends an SNMP trap when the device detects a change in the monitored functions.. ▶ `unmarked` (default setting) The sending of SNMP traps is inactive.
	The prerequisite for sending SNMP traps is that you enable the function in the *Diagnostics > Status Configuration > Alarms (Traps)* dialog and specify at least 1 trap destination.

■ Monitoring correct operation

In the table you specify the parameters that the device monitors. The device signals the occurrence of an event by opening the signal contact.

Parameters	Meaning
Temperature	Activates/deactivates the monitoring of the temperature in the device.
	Possible values: ▶ `marked` (default setting) Monitoring is active. The signal contact opens if the temperature exceeds / falls below the threshold values. ▶ `unmarked` Monitoring is inactive.
	You specify the temperature thresholds in the *Basic Settings > System* dialog, *Upper temp. limit [°C]* field and *Lower temp. limit [°C]* field.
Ring redundancy	Activates/deactivates the monitoring of the ring redundancy.
	Possible values: ▶ `marked` Monitoring is active. The signal contact opens in the following situations: – The redundancy function becomes active (loss of redundancy reserve). – The device is a normal ring participant and detects an error in its settings. ▶ `unmarked` (default setting) Monitoring is inactive.
Connection errors	Activates/deactivates the monitoring of the port/interface link.
	Possible values: ▶ `marked` Monitoring is active. The signal contact opens if the link interrupts on a monitored port/interface. In the *Port* tab, you have the option of selecting the ports/interfaces to be monitored individually. ▶ `unmarked` (default setting) Monitoring is inactive.
External memory removed	Activates/deactivates the monitoring of the active external memory.
	Possible values: ▶ `marked` Monitoring is active. The signal contact opens if you remove the active external memory from the device. ▶ `unmarked` (default setting) Monitoring is inactive.

Parameters	Meaning
External memory not in sync with NVM	Activates/deactivates the monitoring of the configuration profile in the device and in the external memory.
	Possible values: ▶ `marked` Monitoring is active. The signal contact opens in the following situations: – The configuration profile solely exists in the device. – The configuration profile in the device differs from the configuration profile in the external memory. ▶ `unmarked` (default setting) Monitoring is inactive.

■ Buttons

You find the description of the standard buttons in section .

[Port]

■ Table

Parameters	Meaning
Port	Displays the port number.

Propagate connection error	Activates/deactivates the monitoring of the link on the port/interface.
	
	Possible values:
	▶ `marked`
	  Monitoring is active.
	  The signal contact opens if the link interrupts on the selected port/interface.
	▶ `unmarked` (default setting)
	  Monitoring is inactive.
	
	This setting takes effect when you mark the ***Connection errors*** checkbox in the ***Global*** tab.

■ Buttons

You find the description of the standard buttons in section "Buttons" on page 16.

[Status]

■ Table

Parameters	Meaning
Timestamp	Displays the date and time of the event in the format, `Month Day, Year  hh:mm:ss AM/PM`.
Cause	Displays the event which caused the SNMP trap.

■ Buttons

You find the description of the standard buttons in section "Buttons" on page 16.

6.1.4 Alarms (Traps)

The device offers you the option of sending an SNMP trap as a reaction to specific events. In this dialog, you specify the trap destinations to which the device sends the SNMP traps.

The events for which the device triggers an SNMP trap, you specify, for example, in the following dialogs:
▶ in the *Diagnostics > Status Configuration > Device Status* dialog
▶ in the *Diagnostics > Status Configuration > Security Status* dialog

■ Operation

Parameters	Meaning
Operation	Enables/disables the sending of SNMP traps to the trap destinations. Possible values: ▶ `On` (default setting) The sending of SNMP traps is enabled. ▶ `Off` The sending of SNMP traps is disabled.

■ Table

Parameters	Meaning
Name	Specifies the name of the trap destination. Possible values: ▶ Alphanumeric ASCII character string with 1..32 characters
Address	Specifies the IP address and the port number of the trap destination. Possible values: ▶ `<Valid IPv4 address>:<port number>`
Active	Activates/deactivates the sending of SNMP traps to this trap destination. Possible values: ▶ `marked` (default setting) The sending of SNMP traps to this trap destination is active. ▶ `unmarked` The sending of SNMP traps to this trap destination is inactive.

■ Buttons

You find the description of the standard buttons in section "Buttons" on page 16.

Button	Meaning
	Opens the *Create* window to add a new entry to the table. ▶ In the *Name* field you specify a name for the trap destination. ▶ In the *Address* field you specify the IP address and the port number of the trap destination. If you choose not to enter a port number, the device automatically adds the port number `162`.

6.2   System

The menu contains the following dialogs:
▶ System Information
▶ Hardware State
▶ Configuration Check
▶ IP Address Conflict Detection
▶ ARP
▶ Selftest

6.2.1 System Information

This dialog displays the current operating condition of individual components in the device. The displayed values are a snapshot; they represent the operating condition at the time the dialog was loaded to the page.

■ Buttons

You find the description of the standard buttons in section "Buttons" on page 16.

Button	Meaning
Save system information	Opens the HTML page in a new web browser window or tab. You can save the HTML page on your PC using the appropriate web bowser command.

6.2.2   Hardware State

This dialog provides information about the distribution and state of the flash memory of the device.

■ Information

Parameters	Meaning
Uptime	Displays the total operating time of the device since it was delivered.
	Possible values:
	▶ ..d ..h ..m ..s
	Day(s) Hour(s) Minute(s) Second(s)

■ Table

Parameters	Meaning
Flash region	Displays the name of the respective memory area.
Description	Displays a description of what the device uses the memory area for.
Flash sectors	Displays how many sectors are assigned to the memory area.
Sector erase operations	Displays how many times the device has overwritten the sectors of the memory area.

■ Buttons

You find the description of the standard buttons in section "Buttons" on page 16.

6.2.3 Configuration Check

The device allows you to compare the settings in the device with the settings in its neighboring devices. For this purpose, the device uses the information that it received from its neighboring devices through topology recognition (LLDP).

The dialog lists the deviations detected, which affect the performance of the communication between the device and the recognized neighboring devices.

You update the content of the table by clicking the 🔄 button. If the table remains empty, the configuration check was successful and the settings in device are compatible with the settings in the detected neighboring devices.

■ Summary

You also find this information, when you position the mouse pointer over the 🔍 button in the Toolbar in the top part of the Navigation area.

Parameters	Meaning
Error	Displays the number of errors that the device detected during the configuration check.
Warning	Displays the number of warnings that the device detected during the configuration check.
Information	Displays the amount of information that the device detected during the configuration check.

■ Table

When you highlight a row in the table, the device displays additional information in the area beneath it.

Parameters	Meaning
ID	Displays the rule ID of the deviations having occurred. The dialog combines several deviations with the same rule ID under one rule ID.

Level	Displays the level of deviation between the settings in this device and the settings in the detected neighboring devices.
	
	The device differentiates between the following access statuses:
	▶ INFORMATION
	  The performance of the communication between the two devices is not impaired.
	▶ WARNING
	  The performance of the communication between the two devices is possibly impaired.
	▶ ERROR
	  The communication between the two devices is impaired.

Message	Displays the information, warnings and errors having occurred more precisely.

Note: The dialog displays the devices detected as connected to the neighboring device as if they were directly connected to the device itself.

Note: If you have set up more than 39 VLANs on the device, then the dialog constantly displays a warning. The reason is the limited number of possible VLAN data sets in LLDP packets with a maximum length. The device compares the first 39 VLANs automatically.
If you have set up 40 or more VLANs on the device, then check the congruence of the further VLANs manually, if necessary.

■ Buttons

You find the description of the standard buttons in section "Buttons" on page 16.

6.2.4 IP Address Conflict Detection

Using the *IP Address Conflict Detection* function the device verifies that its IP address is unique in the network. For this purpose, the device analyzes received ARP packets.

In this dialog you specify the procedure with which the device detects address conflicts and specify the required settings for this.

The device displays detected address conflicts in the table.

■ Operation

Parameters	Meaning
Operation	Enables/disables the *IP Address Conflict Detection* function. Possible values: ▶ `On` (default setting) 　The *IP Address Conflict Detection* function is enabled. 　The device verifies that its IP address is unique in the network. ▶ `Off` 　The *IP Address Conflict Detection* function is disabled.

■ Configuration

Parameters	Meaning
Detection mode	Specifies the procedure with which the device detects address conflicts. Possible values: ▶ `active and passive` (default setting) 　The device uses active and passive address conflict detection. ▶ `active` 　Active address conflict detection. The device actively avoids communicating with an IP address that already exists in the network. The address conflict detection begins as soon as you connect the device to the network or change its IP parameters. 　– The device sends 4 ARP probe data packets at the interval specified in the *Detection delay [ms]* field. If the device receives a response to these data packets, there is an address conflict. 　– If the device does not detect an address conflict, it sends 2 gratuitous ARP data packets as an announcement. The device also sends these data packets when the address conflict detection is disabled. 　– If the IP address already exists in the network, the device changes back to the previously used IP parameters (if possible). 　If the device receives its IP parameters from a DHCP server, it sends a DHCPDECLINE message back to the DHCP server. 　– After the period specified in the *Release delay [s]* field, the device checks whether the address conflict still exists. If the device detects 10 address conflicts one after the other, it extends the waiting time to 60 s for the next check. 　– When the address conflict has been resolved, the device management returns to the network again. ▶ `passive` 　Passive address conflict detection. The device analyzes the data traffic in the network. If another device in the network is using the same IP address, the device initially "defends" its IP address. The device stops sending if the other device keeps sending with the same IP address. 　– As a "defence" the device sends gratuitous ARP data packets. The device repeats this procedure for the number of times specified in the *Address protections* field. 　– If the other device continues sending with the same IP address, after the period specified in the *Release delay [s]* field, the device periodically checks whether the address conflict still exists. 　– When the address conflict has been resolved, the device management returns to the network again.

Parameters	Meaning
Send periodic ARP probes	Activates/deactivates the periodic address conflict detection.
	Possible values: ▶ `marked` (default setting) The periodic address conflict detection is active. – The device periodically sends an ARP probe data packet every 90 to 150 seconds and waits for the time specified in the `Detection delay [ms]` field for a response. – If the device detects an address conflict, it applies the passive detection mode function. If the `Send trap` function is active, the device sends an SNMP trap. ▶ `unmarked` The periodic address conflict detection is inactive.
Detection delay [ms]	Specifies the period in milliseconds for which the device waits for a response after sending a ARP data packets.
	Possible values: ▶ `20..500` (default setting: `200`)
Release delay [s]	Specifies the period in seconds after which the device checks again whether the address conflict still exists.
	Possible values: ▶ `3..3600` (default setting: `15`)
Address protections	Specifies how many times the device sends gratuitous ARP data packets in the passive detection mode to "defend" its IP address.
	Possible values: ▶ `0..100` (default setting: `3`)
Protection interval [ms]	Specifies the period in milliseconds after which the device sends gratuitous ARP data packets again in the passive detection mode to "defend" its IP address.
	Possible values: ▶ `20..5000` (default setting: `200`)
Send trap	Activates/deactivates the sending of SNMP traps when the device detects address conflicts.
	Possible values: ▶ `marked` The sending of SNMP traps is active. The device sends an SNMP trap when it detects an address conflict. ▶ `unmarked` (default setting) The sending of SNMP traps is inactive.
	The prerequisite for sending SNMP traps is that you enable the function in the `Diagnostics > Status Configuration > Alarms (Traps)` dialog and specify at least 1 trap destination.

■ Information

Parameters	Meaning
Conflict detected	Displays whether an address conflict currently exists.
	Possible values: ▶ `marked` The device detects an address conflict. ▶ `unmarked` The device does not detect an address conflict.

■ Table

Parameters	Meaning
Timestamp	Displays the time at which the device detected an address conflict.
Port	Displays the number of the port on which the device detected the address conflict.
IP address	Displays the IP address that is causing the address conflict.
MAC address	Displays the MAC address of the device with which the address conflict exists.

■ **Buttons**

You find the description of the standard buttons in section .

6.2.5 ARP

This dialog displays the MAC and IP addresses of the neighboring devices connected to the device management.

■ Table

Parameters	Meaning
Port	Displays the port number.
IP address	Displays the IP address of a device that responded to an ARP query to this device.
MAC address	Displays the MAC address of a device that responded to an ARP query to this device.
Last updated	Displays the time in seconds since the current settings of the entry were registered in the ARP table.

Type	Displays the type of the ARP entry.
	
	Possible values:
	▶ `static`
	  Static ARP entry. The ARP entry is kept when the ARP table is deleted.
	▶ `dynamic`
	  Dynamic ARP entry. The device deletes the ARP entry when the *Aging time [s]* has been exceeded, if the device does not receive any data from this device during this time.
	▶ `local`
	  IP and MAC address of the device management.

Active	Displays that the ARP table contains the IP/MAC address assignment as an active entry.

■ Buttons

You find the description of the standard buttons in section "Buttons" on page 16.

Button	Meaning
Reset ARP table	Removes the dynamically set up addresses from the ARP table.

6.2.6   Selftest

This dialog allows you to do the following:
▶ Activate/deactivate the RAM test when the device is being started.
▶ Enable/disable the option of entering the system monitor upon the system start.
▶ Specifies how the device behaves in the case of an error.

■ **Configuration**

Parameters	Meaning
RAM test	Activates/deactivates the RAM memory check during the restart.
	Possible values: ▶ `marked` (default setting) The RAM memory check is activated. During the restart, the device checks the RAM memory. ▶ `unmarked` The RAM memory check is deactivated. This shortens the start time for the device.
SysMon1 is available	Activates/deactivates the access to the system monitor during the restart.
	Possible values: ▶ `marked` (default setting) The device allows you to open the system monitor during the restart. ▶ `unmarked` The device starts without the option of opening to the system monitor.
	Among other things, the system monitor allows you to update the device software and to delete saved configuration profiles.
Load default config on error	Activates/deactivates the loading of the default settings if the device does not detect any readable configuration profile when it is restarting.
	Possible values: ▶ `marked` (default setting) The device loads the default settings. ▶ `unmarked` The device interrupts the restart and stops. The management access to the device is possible exclusively using the CLI through the V.24 interface. To regain the access to the device through the network, open the system monitor and reset the settings. Upon restart, the device loads the default settings.

Note: The following settings block your access to the device permanently if the device does not detect any readable configuration profile when it is restarting. This is the case, for example, if the password of the configuration profile that you are loading differs from the password set in the device.
▶ *SysMon1 is available* checkbox is `unmarked`.
▶ *Load default config on error* checkbox is `unmarked`.
To have the device unlocked again, contact your sales partner.

■ Table

In this table you specify how the device behaves in the case of an error.

Parameters	Meaning
Cause	Error causes to which the device reacts.
	Possible values:
	▶ `task`
	The device detects errors in the applications executed, for example if a task terminates or is not available.
	▶ `resource`
	The device detects errors in the resources available, for example if the memory is becoming scarce.
	▶ `software`
	The device detects software errors, for example error in the consistency check.
	▶ `hardware`
	The device detects hardware errors, for example in the chip set.
Action	Specifies how the device behaves if the adjacent event occurs.
	Possible values:
	▶ `reboot` (default setting)
	The device triggers a restart.
	▶ `logOnly`
	The device registers the detected error in the log file. See the ***Diagnostics > Report > System Log*** dialog.
	▶ `sendTrap`
	The device sends an SNMP trap.
	The prerequisite for sending SNMP traps is that you enable the function in the ***Diagnostics > Status Configuration > Alarms (Traps)*** dialog and specify at least 1 trap destination.

■ Buttons

You find the description of the standard buttons in section "Buttons" on page 16.

6.3   Syslog

The device allows you to report selected events, independent of the severity of the event, to different syslog servers. In this dialog, you specify the settings for this function and manage up to 8 syslog servers.

■ Operation

Parameters	Meaning
Operation	Enables/disables the sending of events to the syslog servers.
	Possible values: ▶ `On` 　The sending of events is enabled. 　The device sends the events specified in the table to the specified syslog servers. ▶ `Off` (default setting) 　The sending of events is disabled.

■ Table

Parameters	Meaning
Index	Displays the index number to which the table entry relates. When you delete a table entry, this leaves a gap in the numbering. When you create a new table entry, the device fills the first gap.
	Possible values: ▶ `1..8`
IP address	Specifies the IP address of the syslog server.
	Possible values: ▶ Valid IPv4 address (default setting: `0.0.0.0`)
Destination UDP port	Specifies the UDP port on which the syslog server expects the log entries.
	Possible values: ▶ `1..65535` (default setting: `514`)
Transport type	Displays the transport type the device uses to send the events to the syslog server.
	Possible values: ▶ `udp` 　The device sends the events over the UDP port specified in the ***Destination UDP port*** column.
Min. severity	Specifies the minimum severity of the events. The device sends a log entry for events with this severity and with more urgent severities to the syslog server.
	Possible values: ▶ `emergency` ▶ `alert` ▶ `critical` ▶ `error` ▶ `warning` (default setting) ▶ `notice` ▶ `informational` ▶ `debug`
Type	Specifies the type of the log entry transmitted by the device.
	Possible values: ▶ `systemlog` (default setting) ▶ `audittrail`
Active	Activates/deactivates the transmission of events to the syslog server: ▶ `marked` 　The device sends events to the syslog server. ▶ `unmarked` (default setting) 　The transmission of events to the syslog server is deactivated.

■ **Buttons**

You find the description of the standard buttons in section "Buttons" on page 16.

6.4   Ports

The menu contains the following dialogs:
- ▶ SFP
- ▶ TP cable diagnosis
- ▶ Port Monitor
- ▶ Auto-Disable
- ▶ Port Mirroring

6.4.1 SFP

This dialog allows you to look at the SFP transceivers currently connected to the device and their properties.

■ Table

The table displays valid values if the device is equipped with SFP transceivers.

Parameters	Meaning
Port	Displays the port number.
Module type	Type of the SFP transceiver, for example M-SFP-SX/LC.
Serial number	Displays the serial number of the SFP transceiver.
Connector type	Displays the connector type.
Supported	Displays whether the device supports the SFP transceiver.
Temperature [°C]	Operating temperature of the SFP transceiver in °Celsius.
Tx power [mW]	Transmission power of the SFP transceiver in mW.
Rx power [mW]	Receiving power of the SFP transceiver in mW.
Tx power [dBm]	Transmission power of the SFP transceiver in dBm.
Rx power [dBm]	Receiving power of the SFP transceiver in dBm.

■ Buttons

You find the description of the standard buttons in section "Buttons" on page 16.

6.4.2   TP cable diagnosis

This feature tests the cable attached to an interface for short or open circuit. The table displays the cable status and estimated length. The device also displays the individual cable pairs connected to the port. When the device detects a short circuit or an open circuit in the cable, it also displays the estimated distance to the problem.

Note: This test interrupts traffic on the port.

■ Information

Parameters	Meaning
Port	Displays the port number.
Status	Status of the Virtual Cable Tester.
	Possible values:
	▶ `active` Cable testing is in progress.
	To start the test, click the ☰ button and then the ***Start cable diagnosis...*** item. This action opens the ***Select port*** dialog.
	▶ `success` The device displays this entry after performing a successful test.
	▶ `failure` The device displays this entry after an interruption in the test.
	▶ `uninitialized` The device displays this entry while in standby.

■ Table

Parameters	Meaning
Cable pair	Displays the cable pair to which this entry relates. The device uses the first PHY index supported to display the values.
Result	Displays the results of the cable test.
	Possible values:
	▶ `normal` The cable is functioning properly.
	▶ `open` There is a break in the cable causing an interruption.
	▶ `short` Wires in the cable are touching together causing a short circuit.
	▶ `unknown` The device displays this value for untested cable pairs.
	Note: The device displays different values than expected in the following cases: – If no cable is connected to the port, the device displays the value `unknown` instead of `open`. – If the port is deactivated, the device displays the value `short`.
Min. length	Displays the minimum estimated length of the cable in meters. The device displays the value `0` if the cable length is unknown or in the ***Information*** frame the ***Status*** field displays the value `active`, `failure` or `uninitialized`.
Max. length	Displays the maximum estimated length of the cable in meters. The device displays the value `0` if the cable length is unknown or in the ***Information*** frame the ***Status*** field displays the value `active`, `failure` or `uninitialized`.
Distance [m]	Displays the estimated distance in meters from the end of the cable to the failure location. The device displays the value `0` if the cable length is unknown or in the ***Information*** frame the ***Status*** field displays the value `active`, `failure` or `uninitialized`.

■ **Buttons**

You find the description of the standard buttons in section .

Button	Meaning
Start cable diagnosis...	Opens the *Select port* dialog. In the *Port* drop-down list you select the port to be tested. Use for copper-based ports exclusively. To initiate the cable test on the selected port, click the *Ok* button.

6.4.3 Port Monitor

The *Port Monitor* function monitors the adherence to the specified parameters on the ports. If the *Port Monitor* function detects that the parameters are being exceeded, the device performs an action.

To apply the *Port Monitor* function, proceed as follows:
▶ *Global* tab
　☐ Enable the *Operation* function in the *Port Monitor* frame.
　☐ Activate for each port those parameters that you want the *Port Monitor* function to monitor.
▶ *Link flap*, *CRC/Fragments* and *Overload detection* tabs
　☐ Specify the threshold values for the parameters for each port.
▶ *Link speed/Duplex mode detection* tab
　☐ Activate the allowed combinations of speed and duplex mode for each port.
▶ *Global* tab
　☐ Specify for each port an action that the device carries out when the *Port Monitor* function detects that the parameters have been exceeded.
▶ *Auto-disable* tab
　☐ Mark the *Auto-disable* checkbox for the monitored parameters when you have specified the auto-disable action at least once.

The dialog contains the following tabs:
▶ [Global]
▶ [Auto-disable]
▶ [Link flap]
▶ [CRC/Fragments]
▶ [Overload detection]
▶ [Link speed/Duplex mode detection]

[**Global**]

In this tab, you enable the *Port Monitor* function and specify the parameters that the *Port Monitor* function is monitoring. Also specify the action that the device carries out when the *Port Monitor* function detects that the parameters have been exceeded.

■ Operation

Parameters	Meaning
Operation	Enables/disables the *Port Monitor* function globally.
	Possible values: ▶ On 　The *Port Monitor* function is enabled. ▶ Off　(default setting) 　The *Port Monitor* function is disabled.

■ Table

Parameters	Meaning
Port	Displays the port number.

Parameters	Meaning
Link flap on	Activates/deactivates the monitoring of link flaps on the port.
	Possible values:
	▶ `marked` Monitoring is active.
	– The `Port Monitor` function monitors link flaps on the port.
	– If the device detects too many link flaps, the device executes the action specified in the `Action` column.
	– On the `Link flap` tab, specify the parameters to be monitored.
	▶ `unmarked` (default setting) Monitoring is inactive.
CRC/Fragments on	Activates/deactivates the monitoring of CRC/fragment errors on the port.
	Possible values:
	▶ `marked` Monitoring is active.
	– The `Port Monitor` function monitors CRC/fragment errors on the port.
	– If the device detects too many CRC/fragment errors, the device executes the action specified in the `Action` column.
	– On the `CRC/Fragments` tab, specify the parameters to be monitored.
	▶ `unmarked` (default setting) Monitoring is inactive.
Duplex mismatch detection active	Activates/deactivates the monitoring of duplex mismatches on the port.
	Possible values:
	▶ `marked` Monitoring is active.
	– The `Port Monitor` function monitors duplex mismatches on the port.
	– If the device detects a duplex mismatch, the device executes the action specified in the `Action` column.
	▶ `unmarked` (default setting) Monitoring is inactive.
Overload detection on	Activates/deactivates the overload detection on the port.
	Possible values:
	▶ `marked` Monitoring is active.
	– The `Port Monitor` function monitors the data load on the port.
	– If the device detects a data overload on the port, the device executes the action specified in the `Action` column.
	– On the `Overload detection` tab, specify the parameters to be monitored.
	▶ `unmarked` (default setting) Monitoring is inactive.
Link speed/Duplex mode detection on	Activates/deactivates the monitoring of the link speed and duplex mode on the port.
	Possible values:
	▶ `marked` Monitoring is active.
	– The `Port Monitor` function monitors the link speed and duplex mode on the port.
	– If the device detects an unpermitted combination of link speed and duplex mode, the device executes the action specified in the `Action` column.
	– On the `Link speed/Duplex mode detection` tab, specify the parameters to be monitored.
	▶ `unmarked` (default setting) Monitoring is inactive.

Parameters	Meaning
Active condition	Displays the monitored parameter that led to the action on the port.
	Possible values: ▶ `-` No monitored parameter. The device does not carry out any action. ▶ `Link flap` Too many link changes in the observed period. ▶ `CRC/Fragments` Too many CRC/fragment errors in the observed period. ▶ `Duplex mismatch` Duplex mismatch detected. ▶ `Overload detection` Overload detected in the observed period. ▶ `Link speed/Duplex mode detection` Impermissible combination of speed and duplex mode detected.
Action	Specifies the action that the device carries out when the *Port Monitor* function detects that the parameters have been exceeded.
	Possible values: ▶ `disable port` The device disables the port and sends an SNMP trap. The "Link status" LED for the port flashes 3× per period. – To re-enable the port, highlight the port and click the ☰ button and then the *Reset* item. – The *Auto-Disable* function enables the port again after the specified waiting period when the parameters are no longer being exceeded. The prerequisite is that on the *Auto-disable* tab the checkbox for the monitored parameter is marked. ▶ `send trap` The device sends an SNMP trap. The prerequisite for sending SNMP traps is that you enable the function in the *Diagnostics > Status Configuration > Alarms (Traps)* dialog and specify at least 1 trap destination. ▶ `auto-disable` (default setting) The device disables the port and sends an SNMP trap. The "Link status" LED for the port flashes 3× per period. The prerequisite is that on the *Auto-disable* tab the checkbox for the monitored parameter is marked. – The *Diagnostics > Ports > Auto-Disable* dialog displays which ports are currently disabled due to the parameters being exceeded. – The *Auto-Disable* function reactivates the port automatically. For this you go to the *Diagnostics > Ports > Auto-Disable* dialog and specify a waiting period for the relevant port in the *Reset timer [s]* column.
Port status	Displays the operating state of the port.
	Possible values: ▶ `up` The port is enabled. ▶ `down` The port is disabled. ▶ `notPresent` Physical port unavailable.

■ Buttons

You find the description of the standard buttons in section "Buttons" on page 16.

Button	Meaning
Reset	Enables the port highlighted in the table again and resets its counter to `0`. This affects the counters in the following dialogs: ▶ *Diagnostics > Ports > Port Monitor* dialog – *Link flap* tab – *CRC/Fragments* tab – *Overload detection* tab ▶ *Diagnostics > Ports > Auto-Disable* dialog

[**Auto-disable**]

In this tab, you activate the *Auto-Disable* function for the parameters monitored by the *Port Monitor* function.

■ **Table**

Parameters	Meaning
Reason	Displays the parameters monitored by the *Port Monitor* function. Mark the adjacent checkbox so that the *Port Monitor* function carries out the auto-disable action when it detects that the monitored parameters have been exceeded.

Auto-disable	Activates/deactivates the *Auto-Disable* function for the adjacent parameters.
	
	Possible values:
	▶ marked
	   The *Auto-Disable* function for the adjacent parameters is active.
	   When the adjacent parameters are exceeded, the device carries out the *Auto-Disable* function when the value auto-disable is specified in the *Action* column.
	▶ unmarked (default setting)
	   The *Auto-Disable* function for the adjacent parameters is inactive.

■ **Buttons**

You find the description of the standard buttons in section "Buttons" on page 16.

Button	Meaning

Reset	Enables the port highlighted in the table again and resets its counter to 0. This affects the counters in the following dialogs:
	▶ *Diagnostics > Ports > Port Monitor* dialog
	  – *Link flap* tab
	  – *CRC/Fragments* tab
	  – *Overload detection* tab
	▶ *Diagnostics > Ports > Auto-Disable* dialog

[**Link flap**]

In this tab, you specify individually for every port the following settings:
▶ The number of link changes.
▶ The period during which the *Port Monitor* function monitors a parameter to detect discrepancies.

You also see how many link changes the *Port Monitor* function has detected up to now.

The *Port Monitor* function monitors those ports for which the checkbox in the *Link flap on* column is marked on the *Global* tab.

■ **Table**

Parameters	Meaning
Port	Displays the port number.
Sampling interval [s]	Specifies in seconds, the period during which the *Port Monitor* function monitors a parameter to detect discrepancies. Possible values: ▶ 1..180 (default setting: 10)
Link flaps	Specifies the number of link changes. If the *Port Monitor* function detects this number of link changes in the monitored period, the device performs the specified action. Possible values: ▶ 1..100 (default setting: 5)

Parameters	Meaning
Last sampling interval	Displays the number of errors that the device has detected during the period that has elapsed.
Total	Displays the total number of errors that the device has detected since the port was enabled.

■ **Buttons**

You find the description of the standard buttons in section "Buttons" on page 16.

Button	Meaning
Reset	Enables the port highlighted in the table again and resets its counter to `0`. This affects the counters in the following dialogs: ▶ *Diagnostics > Ports > Port Monitor* dialog – *Link flap* tab – *CRC/Fragments* tab – *Overload detection* tab ▶ *Diagnostics > Ports > Auto-Disable* dialog

[CRC/Fragments]

In this tab, you specify individually for every port the following settings:
▶ The fragment error rate.
▶ The period during which the *Port Monitor* function monitors a parameter to detect discrepancies.

You also see the fragment error rate that the device has detected up to now.

The *Port Monitor* function monitors those ports for which the checkbox in the *CRC/Fragments on* column is marked on the *Global* tab.

■ **Table**

Parameters	Meaning
Port	Displays the port number.
Sampling interval [s]	Specifies in seconds, the period during which the *Port Monitor* function monitors a parameter to detect discrepancies. Possible values: ▶ `5..180` (default setting: `10`)
CRC/Fragments count [ppm]	Specifies the fragment error rate (in parts per million). If the *Port Monitor* function detects this fragment error rate in the monitored period, the device performs the specified action. Possible values: ▶ `1..1000000` (default setting: `1000`)
Last active interval [ppm]	Displays the fragment error rate that the device has detected during the period that has elapsed.
Total [ppm]	Displays the fragment error rate that the device has detected since the port was enabled.

■ **Buttons**

You find the description of the standard buttons in section "Buttons" on page 16.

Button	Meaning
Reset	Enables the port highlighted in the table again and resets its counter to `0`. This affects the counters in the following dialogs: ▶ *Diagnostics > Ports > Port Monitor* dialog – *Link flap* tab – *CRC/Fragments* tab – *Overload detection* tab ▶ *Diagnostics > Ports > Auto-Disable* dialog

[Overload detection]

In this tab, you specify individually for every port the following settings:
▶ The load threshold values.
▶ The period during which the *Port Monitor* function monitors a parameter to detect discrepancies.

You also see the number of data packets that the device has detected up to now.

The *Port Monitor* function monitors those ports for which the checkbox in the *Overload detection on* column is marked on the *Global* tab.
The *Port Monitor* function does not monitor any ports that are members of a link aggregation group.

■ **Table**

Parameters	Meaning
Port	Displays the port number.
Traffic type	Specifies the type of data packets that the device considers when monitoring the load on the port.
	Possible values: ▶ `all` The *Port Monitor* function monitors Broadcast, Multicast and Unicast packets. ▶ `bc` (default setting) The *Port Monitor* function monitors only Broadcast packets. ▶ `bc-mc` The *Port Monitor* function monitors only Broadcast and Multicast packets.
Threshold type	Specifies the unit for the data rate.
	Possible values: ▶ `pps` (default setting) packets per second ▶ `kbps` kbit per second The prerequisite is that the value in the *Traffic type* column = `all`.
Lower threshold	Specifies the lower threshold value for the data rate. The *Auto-Disable* function enables the port again only when the load on the port is lower than the value specified here.
	Possible values: ▶ `0..10000000` (default setting: `0`)
Upper threshold	Specifies the upper threshold value for the data rate. If the *Port Monitor* function detects this load in the monitored period, the device performs the specified action.
	Possible values: ▶ `0..10000000` (default setting: `0`))
Interval [s]	Specifies in seconds, the period that the *Port Monitor* function observes a parameter to detect that a parameter is being exceeded.
	Possible values: ▶ `1..20` (default setting: `1`)

Parameters	Meaning
Packets	Displays the number of Broadcast, Multicast and Unicast packets that the device has detected during the period that has elapsed.
Broadcast packets	Displays the number of Broadcast packets that the device has detected during the period that has elapsed.
Multicast packets	Displays the number of Multicast packets that the device has detected during the period that has elapsed.
Kbit/s	Displays the data rate in Kbits per second that the device has detected during the period that has elapsed.

■ **Buttons**

You find the description of the standard buttons in section "Buttons" on page 16.

Button	Meaning

Reset	Enables the port highlighted in the table again and resets its counter to `0`. This affects the counters in the following dialogs:
	▶ *Diagnostics > Ports > Port Monitor* dialog
	  – *Link flap* tab
	  – *CRC/Fragments* tab
	  – *Overload detection* tab
	▶ *Diagnostics > Ports > Auto-Disable* dialog

[Link speed/Duplex mode detection]

In this tab, you activate the allowed combinations of speed and duplex mode for each port.

The *Port Monitor* function monitors those ports for which the checkbox in the *Link speed/Duplex mode detection on* column is marked on the *Global* tab.
The *Port Monitor* function monitors only enabled physical ports.

■ **Table**

Parameters	Meaning
Port	Displays the port number.
10 Mbit/s HDX	Activates/deactivates the port monitor to accept a half-duplex and 10 Mbit/s data rate combination on the port. Possible values: ▶ `marked` The port monitor allows the speed and duplex combination. ▶ `unmarked` If the port monitor detects the speed and duplex combination on the port, then the device executes the action specified in the *Global* tab.
10 Mbit/s FDX	Activates/deactivates the port monitor to accept a full-duplex and 10 Mbit/s data rate combination on the port. Possible values: ▶ `marked` The port monitor allows the speed and duplex combination. ▶ `unmarked` If the port monitor detects the speed and duplex combination on the port, then the device executes the action specified in the *Global* tab.

Parameters	Meaning
100 Mbit/s HDX	Activates/deactivates the port monitor to accept a half-duplex and 100 Mbit/s data rate combination on the port.
	Possible values:
	▶ `marked` The port monitor allows the speed and duplex combination.
	▶ `unmarked` If the port monitor detects the speed and duplex combination on the port, then the device executes the action specified in the *Global* tab.
100 Mbit/s FDX	Activates/deactivates the port monitor to accept a full-duplex and 100 Mbit/s data rate combination on the port.
	Possible values:
	▶ `marked` The port monitor allows the speed and duplex combination.
	▶ `unmarked` If the port monitor detects the speed and duplex combination on the port, then the device executes the action specified in the *Global* tab.
1,000 Mbit/s FDX	Activates/deactivates the port monitor to accept a full-duplex and 1 Gbit/s data rate combination on the port.
	Possible values:
	▶ `marked` The port monitor allows the speed and duplex combination.
	▶ `unmarked` If the port monitor detects the speed and duplex combination on the port, then the device executes the action specified in the *Global* tab.

■ Buttons

You find the description of the standard buttons in section "Buttons" on page 16.

Button	Meaning

Reset	Enables the port highlighted in the table again and resets its counter to `0`. This affects the counters in the following dialogs:
	▶ *Diagnostics > Ports > Port Monitor* dialog
	  – *Link flap* tab
	  – *CRC/Fragments* tab
	  – *Overload detection* tab
	▶ *Diagnostics > Ports > Auto-Disable* dialog

6.4.4 Auto-Disable

The *Auto-Disable* function allows you to disable monitored ports automatically and enable them again as you desire.

For example, the *Port Monitor* function and selected functions in the *Network Security* menu use the *Auto-Disable* function to disable ports when monitored parameters are exceeded.

When the parameters are no longer being exceeded, the *Auto-Disable* function enables the relevant port again after a specified waiting period.

The dialog contains the following tabs:
▶ [Port]
▶ [Status]

[Port]

This tab displays which ports are currently disabled due to the parameters being exceeded. When you specify a waiting period in the *Reset timer [s]* column, the *Auto-Disable* function automatically enables the relevant port again when the parameters are no longer being exceeded.

■ Table

Parameters	Meaning
Port	Displays the port number.
Reset timer [s]	Specifies the waiting period in seconds, after which the *Auto-Disable* function enables the port again. Possible values: ▶ 0 (default setting) The timer is inactive. The port remains disabled. ▶ 30..4294967295 The *Auto-Disable* function enables the port again after the waiting period specified here and when the parameters are no longer being exceeded.
Error time	Displays when the device disabled the port due to the parameters being exceeded.
Remaining time [s]	Displays the remaining time in seconds, until the *Auto-Disable* function enables the port again.
Component	Displays the software component in the device that disabled the port. Possible values: ▶ PORT_MON *Port Monitor* See the *Diagnostics > Ports > Port Monitor* dialog. ▶ PORT_ML *Port Security* See the *Network Security > Port Security* dialog. ▶ DOT1S *BPDU guard* See the *Switching > L2-Redundancy > Spanning Tree > Global* dialog.

Parameters	Meaning
Reason	Displays the monitored parameter that led to the port being disabled.
	Possible values: ▶ `none` No monitored parameter. The port is enabled. ▶ `link-flap` Too many link changes. See the ***Diagnostics > Ports > Port Monitor*** dialog, ***Link flap*** tab. ▶ `crc-error` Too many CRC/fragment errors. See the ***Diagnostics > Ports > Port Monitor*** dialog, ***CRC/Fragments*** tab. ▶ `duplex-mismatch` Duplex mismatch detected. See the ***Diagnostics > Ports > Port Monitor*** dialog, ***Global*** tab. ▶ `bpdu-rate` STP-BPDUs received. See the ***Switching > L2-Redundancy > Spanning Tree > Global*** dialog. ▶ `mac-based-port-security` Too many data packets from undesired senders. See the ***Network Security > Port Security*** dialog. ▶ `overload-detection` Overload. See the ***Diagnostics > Ports > Port Monitor*** dialog, ***Overload detection*** tab. ▶ `speed-duplex` Impermissible combination of speed and duplex mode detected. See the ***Diagnostics > Ports > Port Monitor*** dialog, ***Link speed/Duplex mode detection*** tab.
Active	Displays whether the port is currently disabled due to the parameters being exceeded.
	Possible values: ▶ `marked` The port is currently disabled. ▶ `unmarked` The port is enabled.

■ **Buttons**

You find the description of the standard buttons in section "Buttons" on page 16.

[Status]

This tab displays the monitored parameters for which the ***Auto-Disable*** function is activated.

■ **Table**

Parameters	Meaning
Reason	Displays the parameters that the device monitors. Mark the adjacent checkbox so that the ***Auto-Disable*** function disables and, if applicable, enables the port again when the monitored parameters are exceeded.
Category	Displays which function the adjacent parameter belongs to.
	Possible values: ▶ `port-monitor` The parameter belongs to the ***Port Monitor*** function. See the ***Diagnostics > Port > Port Monitor*** dialog. ▶ `network-security` The parameter belongs to the functions in the ***Network Security*** menu. ▶ `l2-redundancy` The parameter belongs to the ***L2-Redundancy*** functions. See the ***Switching > L2-Redundancy*** dialog.

Parameters	Meaning
Auto-disable	Displays whether the `Auto-Disable` function is activated/deactivated for the adjacent parameter.
	Possible values:
	▶ `marked`
	The `Auto-Disable` function for the adjacent parameters is active.
	The `Auto-Disable` function disables and, if applicable, enables the relevant port again when the monitored parameters are exceeded.
	▶ `unmarked` (default setting)
	The `Auto-Disable` function for the adjacent parameters is inactive.

■ Buttons

You find the description of the standard buttons in section "Buttons" on page 16.

Button	Meaning
Reset	Enables the port highlighted in the table again and resets its counter to `0`. This affects the counters in the following dialogs:
	▶ *Diagnostics > Ports > Port Monitor* dialog
	– *Link flap* tab
	– *CRC/Fragments* tab
	– *Overload detection* tab
	▶ *Diagnostics > Ports > Auto-Disable* dialog

6.4.5   Port Mirroring

The *Port Mirroring* function allows you to copy received and sent data packets from selected ports to a destination port. You can watch and process the data stream using an analyzer or an RMON probe, connected to the destination port. The data packets remain unmodified on the source port.

Note: To enable the management access using the destination port, mark the checkbox *Allow management* in the *Destination port* frame before you enable the *Port Mirroring* function.

■ Operation

Parameters	Meaning
Operation	Enables/disables the *Port Mirroring* function.
	Possible values:
	▶ On
	The *Port Mirroring* function is enabled.
	The device copies the data packets from the selected source ports to the destination port.
	▶ Off (default setting)
	The *Port Mirroring* function is disabled.

■ Destination port

Parameters	Meaning
Primary port	Specifies the destination port.
	Suitable ports are those ports that are not used for the following purposes:
	– Source port
	– L2 redundancy protocols
	Possible values:
	▶ no Port (default setting)
	No destination port selected.
	▶ <Port number>
	Number of the destination port. The device copies the data packets from the source ports to this port.
	On the destination port, the device adds a VLAN tag to the data packets that the source port transmits. The destination port transmits unmodified the data packets that the source port receives.
	Note: The destination port needs sufficient bandwidth to absorb the data stream. When the copied data stream exceeds the bandwidth of the destination port, the device discards surplus data packets on the destination port.
Secondary port	Specifies a second destination port.
	The port transmits the same data as the port specified above.
	Possible values:
	▶ no Port (default setting)
	No destination port selected.
	▶ <Port number>
	Number of the destination port. The device copies the data packets from the source ports to this port.

Parameters	Meaning
Allow management	Activates/deactivates the management access using the destination port.
	Possible values: ▶ `marked` The management access using the destination port is active. The device allows the management access to the device using the destination port without interrupting the active *Port Mirroring* session. – The device duplicates multicasts, broadcasts and unknown unicasts on the destination port. – The VLAN settings on the destination port remain unchanged. The prerequisite for management access via the destination port is that the destination port is not a member of the management VLAN. ▶ `unmarked` (default setting) The management access using the destination port is inactive. The device prohibits the management access to the device using the destination port.

■ Table

Parameters	Meaning
Source port	Specifies the port number.
	Possible values: ▶ `<Port number>`
Enabled	Activates/deactivates the copying of the data packets from this source port to the destination port.
	Possible values: ▶ `marked` The copying of the data packets is active. The port is specified as a source port. ▶ `unmarked` (default setting) The copying of the data packets is inactive. ▶ (Grayed-out display) It is not possible to copy the data packets for this port. Possible causes: – The port is already specified as a destination port. – The port is a logical port, not a physical port. **Note:** The device allows you to activate every physical port as source port except for the destination port.
Type	Specifies which data packets the device copies to the destination port.
	Possible values: ▶ `none` (default setting) No data packets. ▶ `tx` Data packets that the source port transmits. ▶ `rx` Data packets that the source port receives. ▶ `txrx` Data packets that the source port transmits and receives. **Note:** With the `txrx` setting the device copies transmitted and received data packets. The destination ports needs at least a bandwidth that corresponds to the sum of the send and receive channel of the source ports. For example, for similar ports the destination port is at 100 % capacity when the send and receive channel of a source port are at 50 % capacity respectively. On the destination port, the device adds a VLAN tag to the data packets that the source port transmits. The destination port transmits unmodified the data packets that the source port receives.

■ **Buttons**

You find the description of the standard buttons in section "Buttons" on page 16.

Button	Meaning
Reset config	Resets the settings in the dialog to the default settings and transfers the changes to the volatile memory of the device (`RAM`).

6.5 LLDP

The device allows you to gather information about neighboring devices. For this, the device uses the Link Layer Discovery Protocol (LLDP). This information enables a network management station to map the structure of your network.

This menu allows you to configure the topology discovery and to display the information received in table form.

The menu contains the following dialogs:
- ▶ LLDP Configuration
- ▶ LLDP Topology Discovery

6.5.1   LLDP Configuration

This dialog allows you to configure the topology discovery for every port.

■ Operation

Parameters	Meaning
Operation	Enables/disables the `LLDP` function.

	Possible values:
	▶ `On` (default setting)
	  The `LLDP` function is enabled.
	  The topology discovery using LLDP is active on the device.
	▶ `Off`
	  The `LLDP` function is disabled.

■ Configuration

Parameters	Meaning
Transmit interval [s]	Specifies the interval in seconds at which the device transmits LLDP data packets.
	Possible values: ▶ `5..32768` (default setting: `30`)
Transmit interval multiplier	Specifies the factor for determining the time-to-live value for the LLDP data packets.
	Possible values: ▶ `2..10` (default setting: `4`)
	The time-to-live value coded in the LLDP header results from multiplying this value with the value in the `Transmit interval [s]` field.
Reinit delay [s]	Specifies the delay in seconds for the reinitialization of a port.
	Possible values: ▶ `1..10` (default setting: `2`)
	If in the `Operation` column the value `Off` is specified, the device tries to reinitialize the port after the time specified here has elapsed.
Transmit delay [s]	Specifies the delay in seconds for transmitting successive LLDP data packets after configuration changes in the device occur.
	Possible values: ▶ `1..8192` (default setting: `2`)
	The recommended value is between a minimum of `1` and a maximum of a quarter of the value in the `Transmit interval [s]` field.
Notification interval [s]	Specifies the interval in seconds for transmitting LLDP notifications.
	Possible values: ▶ `5..3600` (default setting: `5`)
	After transmitting a notification trap, the device waits for a minimum of the time specified here before transmitting the next notification trap.

■ Table

Parameters	Meaning
Port	Displays the port number.

Parameters	Meaning
Operation	Specifies whether the port transmits and receives LLDP data packets.
	Possible values:
	▶ `transmit`
	The port transmits LLDP data packets but does not save any information about neighboring devices.
	▶ `receive`
	The port receives LLDP data packets but does not transmit any information to neighboring devices.
	▶ `receive and transmit` (default setting)
	The port transmits LLDP data packets and saves information about neighboring devices.
	▶ `disabled`
	The port does not transmit LLDP data packets and does not save information about neighboring devices.
Notification	Activates/deactivates the LLDP notifications on the port.
	Possible values:
	▶ `marked`
	LLDP notifications are active on the port.
	▶ `unmarked` (default setting)
	LLDP notifications are inactive on the port.
Transmit port description	Activates/deactivates the transmitting of a TLV (Type Length Value) with the port description.
	Possible values:
	▶ `marked` (default setting)
	The transmitting of the TLV is active.
	The device transmits the TLV with the port description.
	▶ `unmarked`
	The transmitting of the TLV is inactive.
	The device does not transmit a TLV with the port description.
Transmit system name	Activates/deactivates the transmitting of a TLV (Type Length Value) with the device name.
	Possible values:
	▶ `marked` (default setting)
	The transmitting of the TLV is active.
	The device transmits the TLV with the device name.
	▶ `unmarked`
	The transmitting of the TLV is inactive.
	The device does not transmit a TLV with the device name.
Transmit system description	Activates/deactivates the transmitting of the TLV (Type Length Value) with the system description.
	Possible values:
	▶ `marked` (default setting)
	The transmitting of the TLV is active.
	The device transmits the TLV with the system description.
	▶ `unmarked`
	The transmitting of the TLV is inactive.
	The device does not transmit a TLV with the system description.
Transmit system capabilities	Activates/deactivates the transmitting of the TLV (Type Length Value) with the system capabilities.
	Possible values:
	▶ `marked` (default setting)
	The transmitting of the TLV is active.
	The device transmits the TLV with the system capabilities.
	▶ `unmarked`
	The transmitting of the TLV is inactive.
	The device does not transmit a TLV with the system capabilities.
Neighbors (max.)	Limits the number of neighboring devices to be recorded for this port.
	Possible values:
	▶ `1..50` (default setting: `10`)

Parameters	Meaning
FDB mode	Specifies which function the device uses to record neighboring devices on this port.
	Possible values: ▶ `lldpOnly` The device uses LLDP data packets exclusively to record neighboring devices on this port. ▶ `macOnly` The device uses learned MAC addresses to record neighboring devices on this port. The device uses the MAC address exclusively if there is no other entry in the address table (FDB, Forwarding Database) for this port. ▶ `both` The device uses LLDP data packets and learned MAC addresses to record neighboring devices on this port. ▶ `autoDetect` (default setting) If the device receives LLDP data packets at this port, the device works the same as with the `lldpOnly` setting. Otherwise, the device works the same as with the `macOnly` setting.

■ **Buttons**

You find the description of the standard buttons in section .

6.5.2   LLDP Topology Discovery

Devices in networks send notifications in the form of packets which are also known as "LLDPDU" (LLDP data units). The data that is sent and received via LLDPDU are useful for many reasons. Thus the device detects which devices in the network are neighbors and via which ports they are connected.

The dialog allows you to display the network and to detect the connected devices along with their specific features.

This dialog displays the collected LLDP information for the neighboring devices. This information enables a network management station to map the structure of your network.

When devices both with and without an active topology discovery function are connected to a port, the topology table hides the devices without active topology discovery.

When devices without active topology discovery are connected to a port exclusively, then the table contains one line for this port to represent every device. This line contains the number of connected devices.

The Forwarding Database (FDB) address table contains MAC addresses of devices that the topology table hides for the sake of clarity.

If you use 1 port to connect several devices, for example via a hub, the table contains 1 line for each connected device.

■ Table

Parameters	Meaning
Port	Displays the port number.
Neighbor identifier	Displays the chassis ID of the neighboring device. This can be the basis MAC address of the neighboring device, for example.
FDB	Displays whether or not the connected device has active LLDP support.

	Possible values:
	▶ `marked`
	  The connected device does not have active LLDP support.
	  The device uses information from its address table (FDB, Forwarding Database)
	▶ `unmarked` (default setting)
	  The connected device has active LLDP support.

Neighbor IP address	Displays the IP address with which the management access to the neighboring device is possible.
Neighbor port description	Displays a description for the port of the neighboring device.
Neighbor system name	Displays the device name of the neighboring device.
Neighbor system description	Displays a description for the neighboring device.
Port ID	Displays the ID of the port through which the neighboring device is connected to the device.
Autonegotiation supported	Displays whether the port of the neighboring device supports autonegotiation.
Autonegotiation	Displays whether autonegotiation is enabled on the port of the neighboring device.
PoE supported	Displays whether the port of the neighboring device supports Power over Ethernet (PoE).
PoE enabled	Displays whether Power over Ethernet (PoE) is enabled on the port of the neighboring device.

■ Buttons

You find the description of the standard buttons in section "Buttons" on page 16.

6.6 Report

The menu contains the following dialogs:
- ▶ Report Global
- ▶ Persistent Logging
- ▶ System Log
- ▶ Audit Trail

6.6.1 Report Global

The device allows you to log specific events using the following outputs:
▶ on the console
▶ on one or more syslog servers
▶ on a CLI connection set up using SSH
▶ on a CLI connection set up using Telnet

In this dialog, you specify the required settings. By assigning the severity you specify which events the device registers.

The dialog allows you to save a ZIP archive with system information on your PC.

■ Console logging

Parameters	Meaning
Operation	Enables/disables the `Console logging` function.

	Possible values:
	▶ `On`
	   The `Console logging` function is enabled.
	   The device logs the events on the console.
	▶ `Off` (default setting)
	   The `Console logging` function is disabled.

Severity	Specifies the minimum severity for the events. The device logs events with this severity and with more urgent severities. The device outputs the messages on the V.24 interface.
	Possible values: ▶ `emergency` ▶ `alert` ▶ `critical` ▶ `error` ▶ `warning` (default setting) ▶ `notice` ▶ `informational` ▶ `debug`

■ Buffered logging

The device buffers logged events in 2 separate storage areas so that the log entries for urgent events are kept.

This dialog allows you to specify the minimum severity for events that the device buffers in the storage area with a higher priority.

Parameters	Meaning
Severity	Specifies the minimum severity for the events. The device buffers log entries for events with this severity and with more urgent severities in the storage area with a higher priority.
	Possible values: ▶ `emergency` ▶ `alert` ▶ `critical` ▶ `error` ▶ `warning` (default setting) ▶ `notice` ▶ `informational` ▶ `debug`

■ **SNMP logging**

Parameters	Meaning
Log SNMP get request	Enables/disables the logging of SNMP Get requests.
	Possible values:
	▶ On
	The logging is enabled.
	The device registers SNMP Get requests as events in the syslog.
	In the *Severity get request* drop-down list, you select the severity for this event.
	▶ Off (default setting)
	The logging is disabled.
Log SNMP set request	Enables/disables the logging of SNMP Set requests.
	Possible values:
	▶ On
	The logging is enabled.
	The device registers SNMP Set requests as events in the syslog.
	In the *Severity set request* drop-down list, you select the severity for this event.
	▶ Off (default setting)
	The logging is disabled.
Severity get request	Specifies the severity of the event that the device registers for SNMP Get requests.
	Possible values:
	▶ emergency
	▶ alert
	▶ critical
	▶ error
	▶ warning
	▶ notice (default setting)
	▶ informational
	▶ debug
Severity set request	Specifies the severity of the event that the device registers for SNMP Set requests.
	Possible values:
	▶ emergency
	▶ alert
	▶ critical
	▶ error
	▶ warning
	▶ notice (default setting)
	▶ informational
	▶ debug

When you enable the logging of SNMP requests, the device sends these as events with the preset severity notice to the list of syslog servers. The preset minimum severity for a syslog server entry is critical.

To send SNMP requests to a syslog server, you have a number of options to change the default settings. Select the ones that meet your requirements best.

☐ Set the severity for which the device creates SNMP requests as events to `warning` or `error` and change the minimum severity for a syslog entry for one or more syslog servers to the same value.
You also have the option of creating a separate syslog server entry for this.

☐ When you set the severity for SNMP requests to `critical` or higher. The device then sends SNMP requests as events with the severity `critical` or higher to the syslog servers.

☐ When you set the minimum severity for one or more syslog server entries to `notice` or lower. Then it is possible that the device sends many events to the syslog servers.

■ CLI logging

Parameters	Meaning
Operation	Enables/disables the *CLI logging* function.
	Possible values: ▶ `On` 　The *CLI logging* function is enabled. 　The device logs every command received using the Command Line Interface (CLI). ▶ `Off`　(default setting) 　The *CLI logging* function is disabled.

■ Buttons

You find the description of the standard buttons in section "Buttons" on page 16.

Button	Meaning
Download support information	Generates a ZIP archive which the web browser offers to you for download on your PC. The ZIP archive contains system information about the device. You will find an explanation of the files contained in the ZIP archive in the following section.

■ Support Information: Files contained in ZIP archive

File name	Format	Comments
`audittrail.html`	HTML	Contains the chronological recording of the system events and saved user changes in the Audit Trail.
`defaultconfig.xml`	XML	Contains the configuration profile with the default settings.
`script`	TEXT	Contains the output of CLI command `show running-config script`.
`runningconfig.xml`	XML	Contains the configuration profile with the current operating settings.
`supportinfo.html`	TEXT	Contains device internal service information.
`systeminfo.html`	HTML	Contains information about the current settings and operating parameters.
`systemlog.html`	HTML	Contains the logged events in the Log file. See the *Diagnostics > Report > System Log* dialog.

■ Meaning of the severities for events

Severity	Meaning
`emergency`	Device not ready for operation
`alert`	Immediate user intervention required
`critical`	Critical status

Severity	Meaning
error	Error status
warning	Warning
notice	Significant, normal status
informational	Informal message
debug	Debug message

6.6.2 Persistent Logging

The device allows you to save log entries permanently in a file on the external memory. Therefore, even after the device is restarted you have access to the log entries.

In this dialog, you limit the size of the log file and specify the minimum severity for the events to be saved. If the log file attains the specified size, the device archives this file and saves the following log entries in a newly created file.

In the table the device displays you the log files held on the external memory. As soon as the specified maximum number of files has been attained, the device deletes the oldest file and renames the remaining files. This helps ensure that there is enough memory space on the external memory.

Note: Verify that an external memory is connected. To verify if an external memory is connected, see the *Status* column in the *Basic Settings > External Memory* dialog. We recommend to monitor the external memory connection using the *Device Status* function, see the *External memory removal* parameter in the *Diagnostics > Status Configuration > Device Status* dialog.

■ Operation

Parameters	Meaning

Operation	Enables/disables the *Persistent Logging* function.
	Only activate this function when the external memory is available on the device.
	
	Possible values:
	▶ `On` (default setting)
	  The *Persistent Logging* function is enabled.
	  The device saves the log entries in a file on the external memory.
	▶ `Off`
	  The *Persistent Logging* function is disabled.

■ Configuration

Parameters	Meaning
Max. file size [kbyte]	Specifies the maximum size of the log file in KBytes. If the log file attains the specified size, the device archives this file and saves the following log entries in a newly created file. Possible values: ▶ `0..4096` (default setting: `1024`) The value `0` deactivates saving of log entries in the log file.
Files (max.)	Specifies the number of log files that the device keeps on the external memory. As soon as the specified maximum number of files has been attained, the device deletes the oldest file and renames the remaining files. Possible values: ▶ `0..25` (default setting: `4`) The value `0` deactivates saving of log entries in the log file.
Severity	Specifies the minimum severity of the events. The device saves the log entry for events with this severity and with more urgent severities in the log file on the external memory. Possible values: ▶ `emergency` ▶ `alert` ▶ `critical` ▶ `error` ▶ `warning` (default setting) ▶ `notice` ▶ `informational` ▶ `debug`

Parameters	Meaning
Log file target	Specifies the external memory device for logging.
	Possible values: ▶ `sd` External SD memory (ACA31)

■ Table

Parameters	Meaning
Index	Displays the index number to which the table entry relates.
	Possible values: ▶ `1..25` The device automatically assigns this number.
File name	Displays the file name of the log file on the external memory.
	Possible values: ▶ `messages` ▶ `messages.X`
File size [byte]	Displays the size of the log file on the external memory in bytes.

■ Buttons

You find the description of the standard buttons in section .

Button	Meaning
Delete persistent log file	Removes the log files from the external memory.

6.6.3 System Log

The device logs important device-internal events in a log file (System Log).

This dialog displays the log file (System Log). The dialog allows you to save the log file in HTML format on your PC.

In order to search the log file for search terms, use the search function of your web browser.

The log file is kept until a restart is performed on the device. After the restart the device creates the file again.

■ Buttons

You find the description of the standard buttons in section "Buttons" on page 16.

Button	Meaning
Save log file	Opens the HTML page in a new web browser window or tab. You can save the HTML page on your PC using the appropriate web bowser command.
Delete log file	Removes the logged events from the log file.

6.6.4 Audit Trail

This dialog displays the log file (Audit Trail). The dialog allows you to save the log file as an HTML file on your PC. In order to search the log file for search terms, use the search function of your web browser.

The device logs system events and writing user actions on the device. This gives you the option of following WHO changes WHAT on the device WHEN. The prerequisite is that the user role `auditor` or `administrator` is assigned to your user account.

The device logs the following user actions, among others:
▶ A user logging on via CLI (local or remote)
▶ A user logging off manually
▶ Automatic logging off of a user in CLI after a specified period of inactivity
▶ Device restart
▶ Locking of a user account due to too many failed logon attempts
▶ Locking of the management access due to failed logon attempts
▶ Commands executed in CLI, apart from show commands
▶ Changes to configuration variables
▶ Changes to the system time
▶ File transfer operations, including firmware updates
▶ Configuration changes via HiDiscovery
▶ Firmware updates and automatic configuration of the device via the external memory
▶ Opening and closing of SNMP via an HTTPS tunnel

The device does not log passwords. The logged entries are write-protected and remain saved in the device after a restart.

Note: During the restart, access to the system monitor is possible using the default settings of the device. When an attacker gains physical access to the device, they are able to reset the device settings to its default values using the system monitor. After this, the device and log file are accessible using the standard password. Take appropriate measures to restrict physical access to the device. Otherwise, deactivate access to the system monitor. See the *Diagnostics > System > Selftest* dialog, *SysMon1 is available* checkbox.

■ Buttons

You find the description of the standard buttons in section "Buttons" on page 16.

Button	Meaning
Save audit trail file	Opens the HTML page in a new web browser window or tab. You can save the HTML page on your PC using the appropriate web bowser command.

7 Advanced

The menu contains the following dialogs:
- ▶ DHCP L2 Relay
- ▶ Industrial Protocols
- ▶ Command Line Interface

7.1 DHCP L2 Relay

A network administrator uses the DHCP L2 Relay Agent to add DHCP client information. L3 Relay Agents and DHCP servers need the DHCP client information to assign an IP address and a configuration to the clients.

When active, the relay adds Option 82 information configured in this dialog to the packets before it relays DHCP requests from the clients to the server. The Option 82 fields provide unique information about the client and relay. This unique identifier consists of a Circuit ID for the client and a Remote ID for the relay.

In addition to the type, length, and multicast fields, the Circuit ID includes the VLAN ID, unit number, slot number, and port number for the connected client.

The Remote ID consists of a type and length field and either a MAC address, IP address, client identifier, or a user-defined device description. A client identifier is the user-defined system name for the device.

The menu contains the following dialogs:
▶ DHCP L2 Relay Configuration
▶ DHCP L2 Relay Statistics

7.1.1 DHCP L2 Relay Configuration

This dialog allows you to activate the relay function on an interface and VLAN. When you activate this function on a port, the device either relays the Option 82 information or drops the information on untrusted ports. Furthermore, the device allows you to specify the remote identifier.

The dialog contains the following tabs:
▶ [Interface]
▶ [VLAN ID]

■ Operation

Parameters	Meaning
Operation	Enables/disables the DHCP L2 Relay function of the device globally.

	Possible values:
	▶ On
	   Enables the DHCP Layer 2 Relay function of the device.
	▶ Off (default setting)
	   Disables the DHCP Layer 2 Relay function of the device.

[Interface]

■ Table

Parameters	Meaning
Port	Displays the port number.
Active	Activates/deactivates the `DHCP L2 Relay` function on the port. The prerequisite is that you enable the function globally.
	Possible values: ▶ `marked` The `DHCP L2 Relay` function is active. ▶ `unmarked` (default setting) The `DHCP L2 Relay` function is inactive.
Trusted port	Activates/deactivates the secure `DHCP L2 Relay` mode for the corresponding port.
	Possible values: ▶ `marked` The device accepts DHCP packets with Option 82 information. ▶ `unmarked` (default setting) The device discards DHCP packets received on non-secure ports that contain Option 82 information.

■ Buttons

You find the description of the standard buttons in section "Buttons" on page 16.

[VLAN ID]

■ Table

Parameters	Meaning
VLAN ID	VLAN to which the table entry relates.
Active	Activates/deactivates the DHCP Layer 2 Relay function on the VLAN. The prerequisite is that you enable the function globally.
	Possible values: ▶ `marked` The DHCP Layer 2 Relay function is active. ▶ `unmarked` (default setting) The DHCP Layer 2 Relay function is inactive.
Circuit ID	Activates or deactivates the addition of the Circuit ID to the Option 82 information.
	Possible values: ▶ `marked` (default setting) Enables Circuit ID and Remote ID to be sent together. ▶ `unmarked` The device sends the Remote ID exclusively.
Remote ID type	Specifies the components of the Remote ID for this VLAN.
	Possible values: ▶ `ip` Specifies the IP address of the device as Remote ID. ▶ `mac` (default setting) Specifies the MAC address of the device as Remote ID. ▶ `client-id` Specifies the system name of the device as Remote ID. ▶ `other` Enter in the *Remote ID* column user-defined information if you use this value.
Remote ID	Displays the Remote ID for the VLAN. Specify the identifier when you specify the value `other` in the *Remote ID type* column.

■ Buttons

You find the description of the standard buttons in section .

7.1.2 DHCP L2 Relay Statistics

The device monitors the traffic on the ports and displays the results in tabular form.

This table is divided into various categories to aid you in traffic analysis.

■ Table

Parameters	Meaning
Port	Displays the port number.
Untrusted server messages with Option 82	Displays the number of DHCP server messages received with Option 82 information on the untrusted interface.
Untrusted client messages with Option 82	Displays the number of DHCP client messages received with Option 82 information on the untrusted interface.
Trusted server messages without Option 82	Displays the number of DHCP server messages received without Option 82 information on the trusted interface.
Trusted client messages without Option 82	Displays the number of DHCP client messages received without Option 82 information on the trusted interface.

■ Buttons

You find the description of the standard buttons in section "Buttons" on page 16.

Button	Meaning
Reset	Resets the entire table.

7.2 Industrial Protocols

The menu contains the following dialogs:
▶ IEC61850-MMS
▶ Modbus TCP

7.2.1 IEC61850-MMS

The IEC61850-MMS is a standardized industrial communication protocol from the International Electrotechnical Commission (IEC). For example, automatic switching equipment uses this protocol when communicating with power station equipment.

The packet orientated protocol defines a uniform communication language based on the transport protocol, TCP/IP. The protocol uses a Manufacturing Message Specification (MMS) server for client server communications. The protocol includes functions for SCADA, Intelligent Electronic Device (IED) and the network control systems.

Note: IEC61850/MMS does not provide any authentication mechanisms. If the write access for IEC61850/MMS is activated, every client that can access the device using TCP/IP is capable of changing the settings of the device. This in turn can result in an incorrect configuration of the device and to failures in the network.
Activate the write access exclusively if you have taken additional measures (for example Firewall, VPN, etc.) to reduce the risk of unauthorized access.

This dialog allows you to specify the following MMS server settings:
▶ Activates/deactivates the MMS server.
▶ Activates/deactivates the write access to the MMS server.
▶ The MMS server TCP Port.
▶ The maximum number of MMS server sessions.

■ Operation

Parameters	Meaning
Operation	Enables/disables the `IEC61850-MMS` server.
	Possible values: ▶ `On` The `IEC61850-MMS` server is enabled. ▶ `Off` (default setting) The `IEC61850-MMS` server is disabled. The IEC61850 MIBs stay accessible.

■ Configuration

Parameters	Meaning
Write access	Activates/deactivates the write access to the MMS server.
	Possible values: ▶ `marked` The write access to the MMS server is activated. This setting allows you to change the device settings using the IEC 61850 MMS protocol. ▶ `unmarked` (default setting) The write access to the MMS server is deactivated. The MMS server is accessible as read-only.
Technical key	Specifies the IED name. The IED name is eligible independently of the system name.
	Possible values: ▶ Alphanumeric ASCII character string with 0..32 characters The following characters are allowed: – `_` – `0..9` – `a..z` – `A..Z` (default setting: `KEY`)
	To get the MMS server to use the IED name, click the ☑ button and restart the MMS server. The connection to connected clients is then interrupted.

Parameters	Meaning
TCP port	Specifies TCP port for MMS server access.
	Possible values: ▶ `1..65535` (default setting: `102`) Exception: Port `2222` is reserved for internal functions. **Note:** The server restarts automatically after you change the port. In the process, the device terminates open connections to the server.
Sessions (max.)	Specifies the maximum number of MMS server connections.
	Possible values: ▶ `1..15` (default setting: `5`)

■ Information

Parameters	Meaning
Status	Displays the current *IEC61850-MMS* server status.
	Possible values: ▶ `unavailable` ▶ `starting` ▶ `running` ▶ `stopping` ▶ `halted` ▶ `error`
Active sessions	Displays the number of active MMS server connections.

■ Buttons

You find the description of the standard buttons in section "Buttons" on page 16.

Button	Meaning
Download	Copies the ICD file to your PC.

7.2.2　Modbus TCP

Modbus TCP is a protocol used for Supervisory Control and Data Acquisition (SCADA) system integration. *Modbus TCP* is a vendor-neutral protocol used to monitor and control industrial automation equipment such as Programmable Logic Controllers (PLC), sensors and meters.

This dialog allows you to specify the parameters of the protocol. To monitor and control the parameters of the device, you need Human-Machine Interface (HMI) software and the memory mapping table. Refer to the tables located in the Industrial Protocol user manual for the supported objects and memory mapping.

The dialog allows you to enable the function, activate the write access, control which TCP port the Human-Machine Interface (HMI) polls for data. You can also specify the number of sessions allowed to be open at the same time.

Note: Activating the *Modbus TCP* write-access can cause a possible security risk, because the protocol does not authenticate user access.

To help minimize the security risks, specify the IP address range located in the *Device Security > Management Access* dialog. Enter only the IP addresses assigned to your devices before enabling the function. Furthermore, the default setting for monitoring function activation in the *Diagnostics > Status Configuration > Security Status > Global* tab, is active.

■ Operation

Parameters	Meaning
Operation	Enables/disables the *Modbus TCP* server on the device. Possible values: ▶ `On` 　The *Modbus TCP* server is enabled. ▶ `Off` (default setting) 　The *Modbus TCP* server is disabled.

■ Configuration

Parameters	Meaning
Write access	Activates/deactivates the write access to the *Modbus TCP* parameters. **Note:** Activating the *Modbus TCP* write-access can cause a possible security risk, because the protocol does not authenticate user access. Possible values: ▶ `marked` (default setting) 　The *Modbus TCP* server read/write access is active. This allows you to change the device configuration using the *Modbus TCP* protocol. ▶ `unmarked` 　The *Modbus TCP* server read-only access is active.
TCP port	Specifies the TCP port number that the *Modbus TCP* server uses for communication. Possible values: ▶ `<TCP Port number>` (default setting: `502`) 　Specifying `0` is not allowed.
Sessions (max.)	Specifies the maximum number of concurrent sessions that the *Modbus TCP* server allows. Possible values: ▶ `1..5` (default setting: `5`)

■ **Buttons**

You find the description of the standard buttons in section .

7.3 Command Line Interface

This dialog allows you to access the device using the Command Line Interface.

The prerequisites are:
☐ In the device, enable the SSH server in the *Device Security > Management Access > Server* dialog, tab *SSH*.
☐ On your workstation, install a SSH-capable client application which registers a handler for URLs starting with `ssh://` in your operating system.

■ **Buttons**

You find the description of the standard buttons in section "Buttons" on page 16.

Parameters	Meaning
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 on 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.

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 http://www.hirschmann.com.

A list of local telephone numbers and email addresses for technical support directly from Hirschmann is available at https://hirschmann-support.belden.com.

This site also includes a free of charge knowledge base and a software download section.

Hirschmann Competence Center

The Hirschmann Competence 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 http://www.hicomcenter.com.
▶ Support ranges from the first installation through the standby service to maintenance concepts.

With the Hirschmann Competence Center, you decided against making any compromises. Our client-customized package leaves you free to choose the service components you want to use.

Internet:
http://www.hicomcenter.com

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 01RD-NT
Stuttgarter Str. 45-51
72654 Neckartenzlingen

Reference Manual

Command Line Interface
HiOS-2E EESX (Embedded Ethernet Switch eXtend)

Contents

Contents

Contents

Contents

Contents

Contents

Contents

37   Management Access   341

38   Management Address   347

39   Modbus   351

40   Media Redundancy Protocol (MRP)   355

Contents

Contents

Contents

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

The "GUI" reference manual contains detailed information on using the graphical interface to operate the individual functions of the device.

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 "Basic 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 "Redundancy Configuration" user manual document contains the information you require to select the suitable redundancy procedure and configure it.

The document "HiView User Manual" contains information about the GUI application HiView. This application offers you the possibility to use the graphical user interface without other applications such as a Web browser or an installed Java Runtime Environment (JRE).

The Industrial HiVision Network Management software provides you with additional options for smooth configuration and monitoring:
▶ ActiveX control for SCADA integration
▶ 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

1 Command reference

2 Address Conflict Detection (ACD)

2.1 address-conflict

Configure the address conflict settings.

2.1.1 address-conflict operation

Enable or disable the address conflict component.
▶ **Mode:** `Global Config Mode`
▶ **Privilege Level:** `Operator`
▶ **Format:** `address-conflict operation`

■ no address-conflict operation
Disable the option
  ▶ **Mode:** `Global Config Mode`
  ▶ **Privilege Level:** `Operator`
  ▶ **Format:** `no address-conflict operation`

2.1.2 address-conflict detection-mode

Configure the detection mode.
▶ **Mode:** `Global Config Mode`
▶ **Privilege Level:** `Operator`
▶ **Format:** `address-conflict detection-mode <P-1>`

Paramete r	Value	Meaning
P-1	active-and-passive	Configure active and passive detection. During the ip address configuration, if you set the detection to 'active', then the device sends ARP or NDP probes into the network, and if you set the detection to 'passive', then the device listens continuously on the network.
	active-only	Configure only active detection. During ip address configuration 'active' the device sends only one ARP or NDP probe into the network.
	passive-only	Configure passive detection. The device listens passively on the network to verify that another device does not have the same ip address assigned.

2.1.3   address-conflict detection-ongoing

Enable or disable the ongoing detection. If enabled, the device sends periodic ARP or NDP probes.
▶ Mode: `Global Config Mode`
▶ Privilege Level: `Operator`
▶ Format: `address-conflict detection-ongoing`

■ **no address-conflict detection-ongoing**
  Disable the option
    ▶ Mode: `Global Config Mode`
    ▶ Privilege Level: `Operator`
    ▶ Format: `no address-conflict detection-ongoing`

2.1.4   address-conflict delay

The maximum detection delay time in milliseconds. Time gap between ARP or NDP probes.
▶ Mode: `Global Config Mode`
▶ Privilege Level: `Operator`
▶ Format: `address-conflict delay <P-1>`

Paramete r	Value	Meaning
P-1	20..500	Time gap between consecutive ARP or NDP probes ([ms], default 200).

2.1.5   address-conflict release-delay

Delay in seconds to the next ARP or NDP probe cycle after an ip address conflict was detected.
▶ Mode: `Global Config Mode`
▶ Privilege Level: `Operator`
▶ Format: `address-conflict release-delay <P-1>`

Paramete r	Value	Meaning
P-1	3..3600	Delay between consecutive probe cycles after a conflict was detected ([sec], default 15).

2.1.6   address-conflict max-protection

Maximum number of frequent address protections.
▶ Mode: `Global Config Mode`
▶ Privilege Level: `Operator`
▶ Format: `address-conflict max-protection <P-1>`

Parameter	Value	Meaning
P-1	0..100	Maximum number of frequent address protections (default 1).

2.1.7   address-conflict protect-interval

Delay in milliseconds between two consecutive address protections.
▶ Mode: `Global Config Mode`
▶ Privilege Level: `Operator`
▶ Format: `address-conflict protect-interval <P-1>`

Parameter	Value	Meaning
P-1	20..10000	Delay between two consecutive protections ([ms], default 10000).

2.1.8   address-conflict trap-status

If enabled, this trap reports an address conflict.
▶ Mode: `Global Config Mode`
▶ Privilege Level: `Operator`
▶ Format: `address-conflict trap-status`

■ **no address-conflict trap-status**
Disable the option
▶ Mode: `Global Config Mode`
▶ Privilege Level: `Operator`
▶ Format: `no address-conflict trap-status`

2.2 show

Display device options and settings.

2.2.1 show address-conflict global

Displays the component mode.
▶ Mode: Command is in all modes available.
▶ Privilege Level: Guest
▶ Format: show address-conflict global

2.2.2 show address-conflict detected

Displays the last detected address conflict.
▶ Mode: Command is in all modes available.
▶ Privilege Level: Guest
▶ Format: show address-conflict detected

2.2.3 show address-conflict fault-state

Displays the current conflict status.
▶ Mode: Command is in all modes available.
▶ Privilege Level: Guest
▶ Format: show address-conflict fault-state

2.2.4   show mac-address-conflict global

Displays the component mode.
- ▶ Mode: `Command is in all modes available.`
- ▶ Privilege Level: `Guest`
- ▶ Format: `show mac-address-conflict global`

3   Application Lists

3.1 appllists

Configure an application list.

3.1.1 appllists set-authlist

Set an authentication list reference that shall be used by given application.
- ▶ Mode: `Global Config Mode`
- ▶ Privilege Level: `Administrator`
- ▶ Format: `appllists set-authlist <P-1> <P-2>`

Parameter	Value	Meaning
P-1	string	`<application>` Name of an application list.
P-2	string	`<authlist_name>` Name of referenced authentication list.

3.1.2 appllists enable

Activate a login application list.
- ▶ Mode: `Global Config Mode`
- ▶ Privilege Level: `Administrator`
- ▶ Format: `appllists enable <P-1>`

Parameter	Value	Meaning
P-1	string	`<application>` Name of an application list.

3.1.3 appllists disable

Deactivate a login application list.
- ▶ Mode: `Global Config Mode`
- ▶ Privilege Level: `Administrator`
- ▶ Format: `appllists disable <P-1>`

Parameter	Value	Meaning
P-1	string	`<application>` Name of an application list.

3.2 show

Display device options and settings.

3.2.1 show appllists

Display ordered methods for application lists.
▶ Mode: `Command is in all modes available.`
▶ Privilege Level: `Administrator`
▶ Format: `show appllists`

4   Authentication Lists

4.1 authlists

Configure an authentication list.

4.1.1 authlists add

Create a new login authentication list.
▶ Mode: `Global Config Mode`
▶ Privilege Level: `Administrator`
▶ Format: `authlists add <P-1>`

Parameter	Value	Meaning
P-1	string	`<authlist_name>` Name of an authentication list.

4.1.2 authlists delete

Delete an existing login authentication list.
▶ Mode: `Global Config Mode`
▶ Privilege Level: `Administrator`
▶ Format: `authlists delete <P-1>`

Parameter	Value	Meaning
P-1	string	`<authlist_name>` Name of an authentication list.

4.1.3 authlists set-policy

Set the policies of a login authentication list.
▶ Mode: `Global Config Mode`
▶ Privilege Level: `Administrator`
▶ Format: `authlists set-policy <P-1> <P-2> [<P-3> [<P-4> [<P-5> [<P-6>]]]]`

Parameter	Value	Meaning
P-1	string	`<authlist_name>` Name of an authentication list.

Paramete r	Value	Meaning
P-2	reject	Authentication is rejected / not allowed
	local	Authentication by local user DB
	radius	Authentication by RADIUS server
	ias	Authentication by IAS server
	cam	Authentication by CAM server
	ldap	Authentication by remote server
P-3	reject	Authentication is rejected / not allowed
	local	Authentication by local user DB
	radius	Authentication by RADIUS server
	ias	Authentication by IAS server
	cam	Authentication by CAM server
	ldap	Authentication by remote server
P-4	reject	Authentication is rejected / not allowed
	local	Authentication by local user DB
	radius	Authentication by RADIUS server
	ias	Authentication by IAS server
	cam	Authentication by CAM server
	ldap	Authentication by remote server
P-5	reject	Authentication is rejected / not allowed
	local	Authentication by local user DB
	radius	Authentication by RADIUS server
	ias	Authentication by IAS server
	cam	Authentication by CAM server
	ldap	Authentication by remote server
P-6	reject	Authentication is rejected / not allowed
	local	Authentication by local user DB
	radius	Authentication by RADIUS server
	ias	Authentication by IAS server
	cam	Authentication by CAM server
	ldap	Authentication by remote server

4.1.4   authlists enable

Activate a login authentication list.
▶ Mode: Global Config Mode
▶ Privilege Level: Administrator
▶ Format: authlists enable <P-1>

Paramete r	Value	Meaning
P-1	string	<authlist_name> Name of an authentication list.

4.1.5   authlists disable

Deactivate a login authentication list.
▶ Mode: `Global Config Mode`
▶ Privilege Level: `Administrator`
▶ Format: `authlists disable <P-1>`

Parameter	Value	Meaning
P-1	string	`<authlist_name>` Name of an authentication list.

4.2 show

Display device options and settings.

4.2.1 show authlists

Display ordered methods for authentication lists.
▶ Mode: `Command is in all modes available.`
▶ Privilege Level: `Administrator`
▶ Format: `show authlists`

5 Auto Disable

5.1 auto-disable

Configure the Auto Disable condition settings.

5.1.1 auto-disable reason

Enables/disables port Recovery by reason on this device.
▶ Mode: `Global Config Mode`
▶ Privilege Level: `Operator`
▶ Format: `auto-disable reason <P-1>`

Paramete r	Value	Meaning
P-1	link-flap	`Enable/disable link-flap.`
	crc-error	`Enable/disable crc-error.`
	duplex-mismatch	`Enable/disable duplex-mismatch.`
	dhcp-snooping	`Enable/disable dhcp-snooping.`
	arp-rate	`Enable/disable arp-rate.`
	bpdu-rate	`Enable/disable bpdu-rate.`
	port-security	`Enable/disable MAC based port security.`
	overload-detection	`Enable/disable overload-detection.`
	speed-duplex	`Enable/disable link speed and duplex monitor.`

■ **no auto-disable reason**
Disable the option
▶ Mode: `Global Config Mode`
▶ Privilege Level: `Operator`
▶ Format: `no auto-disable reason <P-1>`

5.2 auto-disable

Configure the Auto Disable condition settings.

5.2.1 auto-disable timer

Timer value in seconds after a deactivated port is activated again. Possible values are: 30-4294967295.
A value of 0 disables the timer.
▶ Mode: `Interface Range Mode`
▶ Privilege Level: `Operator`
▶ Format: `auto-disable timer <P-1>`

Paramete r	Value	Meaning
P-1	xxx_30..4294967295	Timer value in seconds.

5.2.2 auto-disable reset

Reset the specific interface and reactivate the port.
▶ Mode: `Interface Range Mode`
▶ Privilege Level: `Operator`
▶ Format: `auto-disable reset [<P-1>]`

Paramete r	Value	Meaning
P-1	port	Press Enter to execute the command.

■ **no auto-disable reset**
Disable the option
▶ Mode: `Interface Range Mode`
▶ Privilege Level: `Operator`
▶ Format: `no auto-disable reset [<P-1>]`

5.3 show

Display device options and settings.

5.3.1 show auto-disable brief

Display Auto Disable summary by interface.
▶ **Mode:** `Command is in all modes available.`
▶ **Privilege Level:** `Guest`
▶ **Format:** `show auto-disable brief`

5.3.2 show auto-disable reasons

Display summary of Auto Disable error reasons.
▶ **Mode:** `Command is in all modes available.`
▶ **Privilege Level:** `Guest`
▶ **Format:** `show auto-disable reasons`

6 Cabletest

6.1 cable-test

6.1.1 cable-test

Select port on which to perform the cable test.
▶ Mode: `Privileged Exec Mode`
▶ Privilege Level: `Operator`
▶ Format: `cable-test <P-1>`

Parameter	Value	Meaning
P-1	slot no./port no.	

7 Class Of Service

7.1 classofservice

Class of service configuration.

7.1.1 classofservice ip-dscp-mapping

ip-dscp-mapping configuration
▶ **Mode:** `Global Config Mode`
▶ **Privilege Level:** `Operator`
▶ **Format:** `classofservice ip-dscp-mapping <P-1> <P-2> <P-3>`

Parameter	Value	Meaning
P-1	af11	
	af12	
	af13	
	af21	
	af22	
	af23	
	af31	
	af32	
	af33	
	af41	
	af42	
	af43	
	be	
	cs0	
	cs1	
	cs2	
	cs3	
	cs4	
	cs5	
	cs6	
	cs7	
	ef	
	0	
	1	
	2	
	3	
	4	
	5	
	6	
	7	
	8	
	9	
	10	
	11	
	12	
	13	
	14	
	15	
	16	
	17	
	18	
	19	
	20	
	21	
	22	
	23	
	24	
	25	
	26	
	27	
	28	
	29	
	30	
	31	
	32	
	33	
	34	

Paramete r	Value	Meaning
P-2	0..7	Enter the Traffic Class value.
P-3	0..3	Enter the Traffic Class value.

7.1.2 classofservice dot1p-mapping

Enter a VLAN priority and the traffic class it should be mapped to.
▶ Mode: Global Config Mode
▶ Privilege Level: Operator
▶ Format: classofservice dot1p-mapping <P-1> <P-2> <P-3>

Paramete r	Value	Meaning
P-1	0..7	Enter the 802.1p priority.
P-2	0..7	Enter the Traffic Class value.
P-3	0..3	Enter a number in the given range.

7.2 classofservice

Interface classofservice configuration.

7.2.1 classofservice trust

trust configuration
- ▶ **Mode:** `Interface Range Mode`
- ▶ **Privilege Level:** `Operator`
- ▶ **Format:** `classofservice trust <P-1>`

Parameter	Value	Meaning
P-1	untrusted	Sets the class of service trust mode to untrusted
	dot1p	Sets the class of service trust mode to dot1p.
	ip-dscp	Sets the class of service trust mode to IP DSCP.

7.3 cos-queue

COS queue configuration

7.3.1 cos-queue strict

strict priority scheduler (default)
▶ Mode: `Global Config Mode`
▶ Privilege Level: `Operator`
▶ Format: `cos-queue strict <P-1> <P-2>`

Parameter	Value	Meaning
P-1	0..7	Enter a Queue Id from 0 to 7.
P-2	0..3	Enter a number in the given range.

7.3.2 cos-queue weighted

weighted scheduler
▶ Mode: `Global Config Mode`
▶ Privilege Level: `Operator`
▶ Format: `cos-queue weighted <P-1> <P-2>`

Parameter	Value	Meaning
P-1	0..7	Enter a Queue Id from 0 to 7.
P-2	0..3	Enter a number in the given range.

7.3.3 cos-queue min-bandwidth

Minimum/guaranteed bandwidth for the queues when in weighted mode
▶ Mode: `Global Config Mode`
▶ Privilege Level: `Operator`
▶ Format: `cos-queue min-bandwidth <P-1> <P-2> <P-3>`

Parameter	Value	Meaning
P-1	0..3	Enter a number in the given range.
P-2	0..7	Enter a Queue Id from 0 to 7.
P-3	0..100	Enter a number in the given range.

7.4 show

Display device options and settings.

7.4.1 show classofservice ip-dscp-mapping

Show ip-dscp-mapping configuration.
- ▶ Mode: `Command is in all modes available.`
- ▶ Privilege Level: `Guest`
- ▶ Format: `show classofservice ip-dscp-mapping`

7.4.2 show classofservice dot1p-mapping

Display a table containing the vlan priority to traffic class mappings.
- ▶ Mode: `Command is in all modes available.`
- ▶ Privilege Level: `Guest`
- ▶ Format: `show classofservice dot1p-mapping`

7.4.3 show classofservice trust

Show a table containing the trust mode of all interfaces.
- ▶ Mode: `Command is in all modes available.`
- ▶ Privilege Level: `Guest`
- ▶ Format: `show classofservice trust`

7.4.4 show cos-queue

Show cosqueue parameters
▶ Mode: `Command is in all modes available.`
▶ Privilege Level: `Guest`
▶ Format: `show cos-queue`

8 Command Line Interface (CLI)

8.1 cli

Set the CLI preferences.

8.1.1 cli serial-timeout

Set login timeout for serial line connection to CLI. Setting to 0 will disable the timeout. The value is active after next login.
▶ Mode: `Privileged Exec Mode`
▶ Privilege Level: `Operator`
▶ Format: `cli serial-timeout <P-1>`

Parameter	Value	Meaning
P-1	0..160	Enter a number in the given range. Setting to 0 will disable the timeout.

8.1.2 cli prompt

Change the system prompt. Following wildcards are allowed: %d date, %t time, %i IP address, %m MAC address ,%p product name
▶ Mode: `Privileged Exec Mode`
▶ Privilege Level: `Operator`
▶ Format: `cli prompt <P-1>`

Parameter	Value	Meaning
P-1	string	Enter a user-defined text, max. 128 characters. Following wildcards are allowed: %d date, %t time, %i IP address, %m MAC address ,%p product name

8.1.3 cli numlines

Screen size for 'more' (23 = default). Enter a 0 will disable the feature. The value is only valid for the current session.
▶ Mode: `Command is in all modes available.`
▶ Privilege Level: `Guest`
▶ Format: `cli numlines <P-1>`

Paramete r	Value	Meaning
P-1	0..250	Screen size for 'more' (23 = default). Enter a 0 will disable the feature. The value is only valid for the current session.

8.1.4 cli banner operation

Enable or disable the CLI login banner.
▶ Mode: `Privileged Exec Mode`
▶ Privilege Level: `Administrator`
▶ Format: `cli banner operation`

■ **no cli banner operation**
Disable the option
▶ Mode: `Privileged Exec Mode`
▶ Privilege Level: `Administrator`
▶ Format: `no cli banner operation`

8.1.5 cli banner text

Set the text for the CLI login banner (C printf format syntax allowed: \\n \\t).
▶ Mode: `Privileged Exec Mode`
▶ Privilege Level: `Administrator`
▶ Format: `cli banner text <P-1>`

Paramete r	Value	Meaning
P-1	string	Enter a user-defined text, max. 1024 characters (allowed characters are from ASCII 32 to 127).

8.2 show

Display device options and settings.

8.2.1 show cli global

Display CLI preferences.
▶ Mode: `Command is in all modes available.`
▶ Privilege Level: `Guest`
▶ Format: `show cli global`

8.2.2 show cli command-tree

Show a list of all commands.
▶ Mode: `Command is in all modes available.`
▶ Privilege Level: `Guest`
▶ Format: `show cli command-tree`

8.3 logging

Logging configuration.

8.3.1 logging cli-command

Enable or disable the CLI command logging.
- ▶ Mode: `Global Config Mode`
- ▶ Privilege Level: `Administrator`
- ▶ Format: `logging cli-command`

■ **no logging cli-command**
Disable the option
- ▶ Mode: `Global Config Mode`
- ▶ Privilege Level: `Administrator`
- ▶ Format: `no logging cli-command`

8.4　show

Display device options and settings.

8.4.1　show logging cli-command

Show the CLI command logging preferences.
▶ **Mode:** `Command is in all modes available.`
▶ **Privilege Level:** `Guest`
▶ **Format:** `show logging cli-command`

9   Clock

9.1 clock

Configure local and DST clock settings.

9.1.1 clock set

Edit current local time.
- ▶ Mode: `Global Config Mode`
- ▶ Privilege Level: `Administrator`
- ▶ Format: `clock set <P-1> <P-2>`

Parameter	Value	Meaning
P-1	YYYY-MM-DD	Local date (range: 2004-01-01 - 2037-12-31).
P-2	HH:MM:SS	Local time.

9.1.2 clock timezone offset

Local time offset (in minutes) with respect to UTC (positive values for locations east of\nGreenwich).
- ▶ Mode: `Global Config Mode`
- ▶ Privilege Level: `Administrator`
- ▶ Format: `clock timezone offset <P-1>`

Parameter	Value	Meaning
P-1	-780..840	Edit the timezone offset (in minutes).

9.1.3 clock timezone zone

Edit the timezone acronym (max. 4 characters).
- ▶ Mode: `Global Config Mode`
- ▶ Privilege Level: `Administrator`
- ▶ Format: `clock timezone zone <P-1>`

Parameter	Value	Meaning
P-1	string	Edit the timezone acronym (max 4 characters).

9.1.4 clock summer-time mode

Configure summer-time mode parameters.
▶ Mode: `Global Config Mode`
▶ Privilege Level: `Administrator`
▶ Format: `clock summer-time mode <P-1>`

Parameter	Value	Meaning
P-1	disable	Disable recurring summer-time mode.
	recurring	Enable recurring summer-time mode.
	eu	Enable recurring summer-time used in most parts of the European Union.
	usa	Enable recurring summer-time used in most parts of the USA.

9.1.5 clock summer-time recurring start

Edit the starting date and time for daylight saving time.
▶ Mode: `Global Config Mode`
▶ Privilege Level: `Administrator`
▶ Format: `clock summer-time recurring start <P-1> <P-2> <P-3> <P-4>`

Parameter	Value	Meaning
P-1	none	
	first	
	second	
	third	
	fourth	
	last	
P-2	none	
	sun	Sunday
	mon	Monday
	tue	Tuesday
	wed	Wednesday
	thu	Thursday
	fri	Friday
	sat	Saturday
P-3	none	
	jan	January
	feb	February
	mar	March
	apr	April
	may	May
	jun	June
	jul	July
	aug	August
	sep	September
	oct	October
	nov	November
	dec	December
P-4	string	<hh:mm> Present time in hh:mm format (00:00-23:59).

9.1.6 clock summer-time recurring end

Edit the ending date and time for daylight saving time.
▶ Mode: `Global Config Mode`
▶ Privilege Level: `Administrator`
▶ Format: `clock summer-time recurring end <P-1> <P-2> <P-3> <P-4>`

Parameter	Value	Meaning
P-1	none	
	first	
	second	
	third	
	fourth	
	last	
P-2	none	
	sun	`Sunday`
	mon	`Monday`
	tue	`Tuesday`
	wed	`Wednesday`
	thu	`Thursday`
	fri	`Friday`
	sat	`Saturday`
P-3	none	
	jan	`January`
	feb	`February`
	mar	`March`
	apr	`April`
	may	`May`
	jun	`June`
	jul	`July`
	aug	`August`
	sep	`September`
	oct	`October`
	nov	`November`
	dec	`December`
P-4	string	`<hh:mm> Present time in hh:mm format (00:00-23:59).`

9.1.7 clock summer-time zone

Edit timezone acronym for summer-time (max. 4 characters).
▶ Mode: `Global Config Mode`
▶ Privilege Level: `Administrator`
▶ Format: `clock summer-time zone <P-1>`

Parameter	Value	Meaning
P-1	string	`Edit the timezone acronym (max 4 characters).`

9.2   show

Display device options and settings.

9.2.1   show clock

Display the current time information.
▶ Mode: `Command is in all modes available.`
▶ Privilege Level: `Guest`
▶ Format: `show clock [summer-time]`
`[summer-time]`: Display summer-time parameters.

10 Configuration

10.1 save

Save the configuration to the specified destination.

10.1.1 save profile

Save the configuration to the specific profile.
- ▶ Mode: `All Privileged Modes`
- ▶ Privilege Level: `Operator`
- ▶ Format: `save profile <P-1>`

Paramete r	Value	Meaning
P-1	string	Enter a user-defined text, max. 32 characters.

10.2 config

Configure the configuration saving settings.

10.2.1 config watchdog admin-state

Enable or disable the configuration undo feature.
- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Operator
- ▶ Format: config watchdog admin-state

■ no config watchdog admin-state
Disable the option
- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Operator
- ▶ Format: no config watchdog admin-state

10.2.2 config watchdog timeout

Configure the configuration undo timeout (unit: seconds).
- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Operator
- ▶ Format: config watchdog timeout <P-1>

Parameter	Value	Meaning
P-1	30..600	Enter a number in the given range.

10.2.3   config encryption password set

Set the configuration file password.
▶ Mode: `Global Config Mode`
▶ Privilege Level: `Administrator`
▶ Format: `config encryption password set [<P-1>] [<P-2>]`

Paramete r	Value	Meaning
P-1	string	Enter a user-defined text, max. 64 characters.
P-2	string	Enter a user-defined text, max. 64 characters.

10.2.4   config encryption password clear

Clear the configuration file password.
▶ Mode: `Global Config Mode`
▶ Privilege Level: `Administrator`
▶ Format: `config encryption password clear [<P-1>]`

Paramete r	Value	Meaning
P-1	string	Enter a user-defined text, max. 64 characters.

10.2.5   config envm auto-update

Allow automatic firmware updates with this memory device.
▶ Mode: `Global Config Mode`
▶ Privilege Level: `Administrator`
▶ Format: `config envm auto-update <P-1>`

Paramete r	Value	Meaning
P-1	sd	SD-Card
	usb	USB Storage Device

■ **no config envm auto-update**
Disable the option
▶ Mode: `Global Config Mode`
▶ Privilege Level: `Administrator`
▶ Format: `no config envm auto-update <P-1>`

10.2.6 config envm sshkey-auto-update

Allow automatic ssh key updates with this memory device.
▶ Mode: `Global Config Mode`
▶ Privilege Level: `Administrator`
▶ Format: `config envm sshkey-auto-update <P-1>`

Paramete r	Value	Meaning
P-1	sd	SD-Card
	usb	USB Storage Device

■ **no config envm sshkey-auto-update**
  Disable the option
  ▶ Mode: `Global Config Mode`
  ▶ Privilege Level: `Administrator`
  ▶ Format: `no config envm sshkey-auto-update <P-1>`

10.2.7 config envm config-save

Allow the configuration to be saved to this memory device.
▶ Mode: `Global Config Mode`
▶ Privilege Level: `Operator`
▶ Format: `config envm config-save <P-1>`

Paramete r	Value	Meaning
P-1	sd	SD-Card
	usb	USB Storage Device

■ **no config envm config-save**
  Disable the option
  ▶ Mode: `Global Config Mode`
  ▶ Privilege Level: `Operator`
  ▶ Format: `no config envm config-save <P-1>`

10.2.8 config envm load-priority

Configure the order of configuration load attempts from memory devices at boot time. If one load is successful, then the device discards further attempts.

▶ Mode: `Global Config Mode`
▶ Privilege Level: `Operator`
▶ Format: `config envm load-priority <P-1> <P-2>`

Parameter	Value	Meaning
P-1	sd	SD-Card
	usb	USB Storage Device
P-2	disable	Config will not be loaded at all
	first	Config will be loaded first. If successful, no other config will be tried.
	second	Config will be loaded if first one does not succeed.

10.2.9 config profile select

Select a configuration profile to be the active configuration.

▶ Mode: `Global Config Mode`
▶ Privilege Level: `Administrator`
▶ Format: `config profile select <P-1> <P-2>`

Parameter	Value	Meaning
P-1	nvm	You can only select nvm for this command.
P-2	1..20	Index of the profile entry.

10.2.10 config profile delete

Delete a specific configuration profile.

▶ Mode: `Global Config Mode`
▶ Privilege Level: `Administrator`
▶ Format: `config profile delete <P-1> num <P-2> profile <P-3>`

`num`: Select the index of a profile to delete.
`profile`: Select the name of a profile to delete.

Parameter	Value	Meaning
P-1	nvm	non-volatile memory
	envm	external non-volatile memory device
P-2	1..20	Index of the profile entry.
P-3	string	Enter a user-defined text, max. 32 characters.

10.2.11 config fingerprint verify

Verify the fingerprint of the selected profile.
- ▶ Mode: `Global Config Mode`
- ▶ Privilege Level: `Administrator`
- ▶ Format: `config fingerprint verify <P-1> profile <P-2> <P-3> num <P-4> <P-5>`

`profile`: Select the name of a profile to be verified.

`num`: Select the index number of a profile to be verified.

Parameter	Value	Meaning
P-1	nvm	non-volatile memory
	envm	external non-volatile memory device
P-2	string	Enter a user-defined text, max. 32 characters.
P-3	string	Enter hash as 40 hexa-decimal characters.
P-4	1..20	Index of the profile entry.
P-5	string	Enter hash as 40 hexa-decimal characters.

10.3   copy

Copy different kinds of items.

10.3.1   copy sysinfo system envm

Copy the system information to external non-volatile memory.
▶ Mode: `Privileged Exec Mode`
▶ Privilege Level: `Operator`
▶ Format: `copy sysinfo system envm [filename <P-1>]`
`[filename]`: Enter the filename (format xyz.html) to be saved in external non-volatile memory.

Paramete r	Value	Meaning
P-1	string	Enter a user-defined text, max. 32 characters.

10.3.2   copy sysinfoall system envm

Copy the system information and the event log from the device to external non-volatile memory.
▶ Mode: `Privileged Exec Mode`
▶ Privilege Level: `Operator`
▶ Format: `copy sysinfoall system envm`

10.3.3   copy firmware envm

Copy a firmware image to the device from external non-volatile memory.
▶ Mode: `Privileged Exec Mode`
▶ Privilege Level: `Administrator`
▶ Format: `copy firmware envm <P-1> system`
`system`: Copy a firmware image to the device from external non-volatile memory.

Paramete r	Value	Meaning
P-1	string	Filename.

10.3.4 copy firmware remote

Copy a firmware image to the device from a server.
- ▶ Mode: `Privileged Exec Mode`
- ▶ Privilege Level: `Administrator`
- ▶ Format: `copy firmware remote <P-1> system`

`system`: Copy a firmware image to the device from a file server.

Parameter	Value	Meaning
P-1	string	Enter a user-defined text, max. 128 characters.

10.3.5 copy config running-config nvm

Copy the running-config to non-volatile memory.
- ▶ Mode: `Privileged Exec Mode`
- ▶ Privilege Level: `Operator`
- ▶ Format: `copy config running-config nvm [profile <P-1>]`

`[profile]`: Save the configuration as a specific profile name.

Parameter	Value	Meaning
P-1	string	Enter a user-defined text, max. 32 characters.

10.3.6 copy config running-config remote

Copy the running-config to a file server.
- ▶ Mode: `Privileged Exec Mode`
- ▶ Privilege Level: `Administrator`
- ▶ Format: `copy config running-config remote <P-1>`

Parameter	Value	Meaning
P-1	string	Enter a user-defined text, max. 128 characters.

10.3.7 copy config nvm

Load a configuration from non-volatile memory to the running-config.
- ▶ Mode: `Privileged Exec Mode`
- ▶ Privilege Level: `Administrator`
- ▶ Format: `copy config nvm [profile <P-1>] running-config remote <P-2>`

`[profile]`: Load a configuration from a specific profile name.
`running-config`: (Re)-load a configuration from non-volatile memory to the running-config.
`remote`: Copy a configuration from non-volatile memory to a server.

Parameter	Value	Meaning
P-1	string	Filename.
P-2	string	Enter a user-defined text, max. 128 characters.

10.3.8 copy config envm

Copy a configuration from external non-volatile memory to non-volatile memory.
- ▶ Mode: `Privileged Exec Mode`
- ▶ Privilege Level: `Administrator`
- ▶ Format: `copy config envm [profile <P-1>] nvm`

`[profile]`: Copy a specfic configuration profile from external non-volatile memory to non-volatile memory.
`nvm`: Copy a specific profile from external non-volatile memory to non-volatile memory.

Parameter	Value	Meaning
P-1	string	Filename.

10.3.9 copy config remote

Copy a configuration file to the device from a server.
- ▶ Mode: `Privileged Exec Mode`
- ▶ Privilege Level: `Administrator`
- ▶ Format: `copy config remote <P-1> nvm [profile <P-2>] running-config`

`nvm`: Copy a configuration file from a server to non-volatile memory.
`[profile]`: Copy a configuration from a server to a specific profile in non-volatile memory.
`running-config`: Copy a configuration file from a server to the running-config.

Parameter	Value	Meaning
P-1	string	Enter a user-defined text, max. 128 characters.
P-2	string	Enter a user-defined text, max. 32 characters.

10.3.10 copy sfp-white-list remote

Copy the SFP WhiteList from server to the device.
- ▶ Mode: `Privileged Exec Mode`
- ▶ Privilege Level: `Operator`
- ▶ Format: `copy sfp-white-list remote <P-1> nvm`

`nvm`: Copy the SFP WhiteList from server to the device.

Parameter	Value	Meaning
P-1	string	Enter a user-defined text, max. 128 characters.

10.3.11 copy sfp-white-list envm

Copy the SFP WhiteList from external non-volatile memory.
- ▶ Mode: `Privileged Exec Mode`
- ▶ Privilege Level: `Operator`
- ▶ Format: `copy sfp-white-list envm <P-1> nvm`

`nvm`: Copy the SFP WhiteList from external non-volatile memory to the device.

Parameter	Value	Meaning
P-1	string	Enter a user-defined text, max. 128 characters.

10.4 clear

Clear several items.

10.4.1 clear config

Clear the running configuration.
▶ **Mode:** `Privileged Exec Mode`
▶ **Privilege Level:** `Administrator`
▶ **Format:** `clear config`

10.4.2 clear factory

Set the device back to the factory settings (use with care).
▶ **Mode:** `Privileged Exec Mode`
▶ **Privilege Level:** `Administrator`
▶ **Format:** `clear factory [erase-all]`
`[erase-all]`: Set to factory settings and also erase file systems (use with extreme care).

10.5 show

Display device options and settings.

10.5.1 show running-config xml

Show the currently running configuration (XML file).
▶ Mode: `Command is in all modes available.`
▶ Privilege Level: `Administrator`
▶ Format: `show running-config xml`

10.5.2 show running-config script

Show the currently running configuration (CLI script).
▶ Mode: `Command is in all modes available.`
▶ Privilege Level: `Administrator`
▶ Format: `show running-config script [all]`
`[all]`: Show the currently running configuration (CLI script).

10.6 show

Display device options and settings.

10.6.1 show config envm settings

Show the settings of the external non-volatile memory.
- ▶ Mode: `Command is in all modes available.`
- ▶ Privilege Level: `Guest`
- ▶ Format: `show config envm settings`

10.6.2 show config envm properties

Show the properties of the external non-volatile memory.
- ▶ Mode: `Command is in all modes available.`
- ▶ Privilege Level: `Guest`
- ▶ Format: `show config envm properties`

10.6.3 show config watchdog

Show the Auto Configuration Undo settings.
- ▶ Mode: `Command is in all modes available.`
- ▶ Privilege Level: `Guest`
- ▶ Format: `show config watchdog`

10.6.4   show config encryption

Show the settings for config encryption.
▶ Mode: `Command is in all modes available.`
▶ Privilege Level: `Guest`
▶ Format: `show config encryption`

10.6.5   show config profiles

Show the configuration profiles.
▶ Mode: `Command is in all modes available.`
▶ Privilege Level: `Administrator`
▶ Format: `show config profiles <P-1> [<P-2>]`

Paramete r	Value	Meaning
P-1	nvm	non-volatile memory
	envm	external non-volatile memory device
P-2	1..20	Index of the profile entry.

10.6.6   show config status

Show the sync status of the running-config with non-volatile memory and ACA.
▶ Mode: `Command is in all modes available.`
▶ Privilege Level: `Guest`
▶ Format: `show config status`

10.7 swap

Swap software images.

10.7.1 swap firmware system backup

Swap the main and backup images.
▶ **Mode:** `Privileged Exec Mode`
▶ **Privilege Level:** `Administrator`
▶ **Format:** `swap firmware system backup`

11 Debugging

11.1 debug

Different tools to assist in debugging the device.

11.1.1 debug tcpdump help

Display help file for the tcpdump tool.
▶ **Mode:** `Privileged Exec Mode`
▶ **Privilege Level:** `Operator`
▶ **Format:** `debug tcpdump help`

11.1.2 debug tcpdump start cpu

Start capture with default values.
▶ **Mode:** `Privileged Exec Mode`
▶ **Privilege Level:** `Operator`
▶ **Format:** `debug tcpdump start cpu [filter <P-1>] [parms <P-2>]`
`[filter]`: Start capture with values from a filter file.
`[parms]`: Start capture with the tcpdump parameters (for details see tcpdump help).

Paramete r	Value	Meaning
P-1	string	`<filename> Enter a valid filename.`
P-2	string	`Enter a user-defined text, max. 255 characters.`

11.1.3 debug tcpdump stop

Abort capture of network traffic.
▶ **Mode:** `Privileged Exec Mode`
▶ **Privilege Level:** `Operator`
▶ **Format:** `debug tcpdump stop`

11.1.4 debug tcpdump filter show

Display a known filter file.
- ▶ Mode: `Privileged Exec Mode`
- ▶ Privilege Level: `Operator`
- ▶ Format: `debug tcpdump filter show <P-1>`

Parameter	Value	Meaning
P-1	string	`<filename> Enter a valid filename.`

11.1.5 debug tcpdump filter list

Display all available filter files.
- ▶ Mode: `Privileged Exec Mode`
- ▶ Privilege Level: `Operator`
- ▶ Format: `debug tcpdump filter list`

11.1.6 debug tcpdump filter delete

Delete a known filter file.
- ▶ Mode: `Privileged Exec Mode`
- ▶ Privilege Level: `Operator`
- ▶ Format: `debug tcpdump filter delete <P-1>`

Parameter	Value	Meaning
P-1	string	`<filename> Enter a valid filename.`

11.2 show

Display device options and settings.

11.2.1 show debug logic-modules

List logic module information
▶ **Mode:** `Privileged Exec Mode`
▶ **Privilege Level:** `Administrator`
▶ **Format:** `show debug logic-modules`

11.3 copy

Copy different kinds of items.

11.3.1 copy tcpdumpcap nvm envm

Copy the capture file from non-volatile memory to external non-volatile memory.
▶ Mode: `Privileged Exec Mode`
▶ Privilege Level: `Operator`
▶ Format: `copy tcpdumpcap nvm envm [<P-1>]`

Paramete r	Value	Meaning
P-1	string	`<filename> Enter a valid filename.`

11.3.2 copy tcpdumpcap nvm remote

Copy the capture file from the device to a server.
▶ Mode: `Privileged Exec Mode`
▶ Privilege Level: `Operator`
▶ Format: `copy tcpdumpcap nvm remote <P-1>`

Paramete r	Value	Meaning
P-1	string	`Enter a user-defined text, max. 128 characters.`

11.3.3 copy tcpdumpfilter remote

Copy the filter file from a server to the specified destination.
▶ Mode: `Privileged Exec Mode`
▶ Privilege Level: `Operator`
▶ Format: `copy tcpdumpfilter remote <P-1> nvm <P-2>`
`nvm`: Copy the filter file from a server to non-volatile memory.

Paramete r	Value	Meaning
P-1	string	`Enter a user-defined text, max. 128 characters.`

Paramete r	Value	Meaning
P-2	string	<filename> Enter a valid filename.

11.3.4 copy tcpdumpfilter envm

Copy the capture filter from external non-volatile memory to the specified destination.
▶ Mode: `Privileged Exec Mode`
▶ Privilege Level: `Operator`
▶ Format: `copy tcpdumpfilter envm <P-1> nvm [<P-2>]`
`nvm`: Copy the capture filter from external non-volatile memory to non-volatile memory.

Paramete r	Value	Meaning
P-1	string	<filename> Enter a valid filename.
P-2	string	<filename> Enter a valid filename.

11.3.5 copy tcpdumpfilter nvm

Copy the capture filter from non-volatile memory to the specified destination.
▶ Mode: `Privileged Exec Mode`
▶ Privilege Level: `Operator`
▶ Format: `copy tcpdumpfilter nvm <P-1> envm [<P-2>] remote <P-3>`
`envm`: Copy the capture filter from non-volatile memory to external non-volatile memory.
`remote`: Copy the capture file from non-volatile memory to a server.

Paramete r	Value	Meaning
P-1	string	Filename.
P-2	string	<filename> Enter a valid filename.
P-3	string	Enter a user-defined text, max. 128 characters.

12   Device Monitoring

12.1   device-status

Configure various device conditions to be monitored.

12.1.1   device-status monitor link-failure

Enable or disable monitor state of network connection(s).
▶ Mode: `Global Config Mode`
▶ Privilege Level: `Administrator`
▶ Format: `device-status monitor link-failure`

■ no device-status monitor link-failure
Disable the option
▶ Mode: `Global Config Mode`
▶ Privilege Level: `Administrator`
▶ Format: `no device-status monitor link-failure`

12.1.2   device-status monitor temperature

Enable or disable monitoring of the device temperature.
▶ Mode: `Global Config Mode`
▶ Privilege Level: `Administrator`
▶ Format: `device-status monitor temperature`

■ no device-status monitor temperature
Disable the option
▶ Mode: `Global Config Mode`
▶ Privilege Level: `Administrator`
▶ Format: `no device-status monitor temperature`

12.1.3 device-status monitor envm-removal

Enable or disable monitoring the presence of the external non-volatile memory.
▶ Mode: `Global Config Mode`
▶ Privilege Level: `Administrator`
▶ Format: `device-status monitor envm-removal`

■ no device-status monitor envm-removal
Disable the option
▶ Mode: `Global Config Mode`
▶ Privilege Level: `Administrator`
▶ Format: `no device-status monitor envm-removal`

12.1.4 device-status monitor envm-not-in-sync

Enable or disable monitoring synchronization between the external non-volatile memory\n and the running configuration.
▶ Mode: `Global Config Mode`
▶ Privilege Level: `Administrator`
▶ Format: `device-status monitor envm-not-in-sync`

■ no device-status monitor envm-not-in-sync
Disable the option
▶ Mode: `Global Config Mode`
▶ Privilege Level: `Administrator`
▶ Format: `no device-status monitor envm-not-in-sync`

12.1.5 device-status monitor ring-redundancy

Enable or disable monitoring if ring-redundancy is present.
▶ Mode: `Global Config Mode`
▶ Privilege Level: `Administrator`
▶ Format: `device-status monitor ring-redundancy`

■ **no device-status monitor ring-redundancy**

Disable the option
▶ Mode: `Global Config Mode`
▶ Privilege Level: `Administrator`
▶ Format: `no device-status monitor ring-redundancy`

12.1.6 device-status trap

Configure the device to send a trap when the device status changes.
▶ Mode: `Global Config Mode`
▶ Privilege Level: `Administrator`
▶ Format: `device-status trap`

■ **no device-status trap**

Disable the option
▶ Mode: `Global Config Mode`
▶ Privilege Level: `Administrator`
▶ Format: `no device-status trap`

12.2　device-status

Configure various device conditions to be monitored.

12.2.1　device-status link-alarm

Configure the monitor settings of the port link.
▶ Mode: `Interface Range Mode`
▶ Privilege Level: `Administrator`
▶ Format: `device-status link-alarm`

■ **no device-status link-alarm**
　Disable the option
　▶ Mode: `Interface Range Mode`
　▶ Privilege Level: `Administrator`
　▶ Format: `no device-status link-alarm`

12.3 show

Display device options and settings.

12.3.1 show device-status monitor

Display the device monitoring configurations.
▶ **Mode:** `Command is in all modes available.`
▶ **Privilege Level:** `Guest`
▶ **Format:** `show device-status monitor`

12.3.2 show device-status state

Display the current state of the device.
▶ **Mode:** `Command is in all modes available.`
▶ **Privilege Level:** `Guest`
▶ **Format:** `show device-status state`

12.3.3 show device-status trap

Display the device trap information and configurations.
▶ **Mode:** `Command is in all modes available.`
▶ **Privilege Level:** `Guest`
▶ **Format:** `show device-status trap`

12.3.4   show device-status events

Display occurred device status events.
- ▶ Mode: `Command is in all modes available.`
- ▶ Privilege Level: `Guest`
- ▶ Format: `show device-status events`

12.3.5   show device-status link-alarm

Display the monitor configurations of the network ports.
- ▶ Mode: `Command is in all modes available.`
- ▶ Privilege Level: `Guest`
- ▶ Format: `show device-status link-alarm`

12.3.6   show device-status all

Display the configurable device status settings.
- ▶ Mode: `Command is in all modes available.`
- ▶ Privilege Level: `Guest`
- ▶ Format: `show device-status all`

13 Device Security

13.1 security-status

Configure the security status settings.

13.1.1 security-status monitor pwd-change

Sets the monitoring of default password change for\n'user' and 'admin'.
▶ Mode: `Global Config Mode`
▶ Privilege Level: `Administrator`
▶ Format: `security-status monitor pwd-change`

■ **no security-status monitor pwd-change**
Disable the option
▶ Mode: `Global Config Mode`
▶ Privilege Level: `Administrator`
▶ Format: `no security-status monitor pwd-change`

13.1.2 security-status monitor pwd-min-length

Sets the monitoring of minimum length of the password\n(smaller 8).
▶ Mode: `Global Config Mode`
▶ Privilege Level: `Administrator`
▶ Format: `security-status monitor pwd-min-length`

■ **no security-status monitor pwd-min-length**
Disable the option
▶ Mode: `Global Config Mode`
▶ Privilege Level: `Administrator`
▶ Format: `no security-status monitor pwd-min-length`

13.1.3   security-status monitor pwd-policy-config

Sets the monitoring whether the minimum password policy is configured. The device changes the security status to the value "error" if the value for at least one of the following password rules is 0:\n"minimum upper cases","minimum lower cases","minimum numbers","minimum special characters".
- ▶ Mode: `Global Config Mode`
- ▶ Privilege Level: `Administrator`
- ▶ Format: `security-status monitor pwd-policy-config`

■ **no security-status monitor pwd-policy-config**
   Disable the option
   - ▶ Mode: `Global Config Mode`
   - ▶ Privilege Level: `Administrator`
   - ▶ Format: `no security-status monitor pwd-policy-config`

13.1.4   security-status monitor pwd-str-not-config

Sets the monitoring whether the password minimum\nstrength check is configured.
- ▶ Mode: `Global Config Mode`
- ▶ Privilege Level: `Administrator`
- ▶ Format: `security-status monitor pwd-str-not-config`

■ **no security-status monitor pwd-str-not-config**
   Disable the option
   - ▶ Mode: `Global Config Mode`
   - ▶ Privilege Level: `Administrator`
   - ▶ Format: `no security-status monitor pwd-str-not-config`

13.1.5   security-status monitor pwd-policy-inactive

Sets the monitoring whether at least one user is\nconfigured with inactive policy check.\nThe device changes the security status to the value "error" if the function "policy check" is inactive for at least 1 user account.
- ▶ Mode: `Global Config Mode`
- ▶ Privilege Level: `Administrator`
- ▶ Format: `security-status monitor pwd-policy-inactive`

■ **no security-status monitor pwd-policy-inactive**
   Disable the option
   ▶ Mode: `Global Config Mode`
   ▶ Privilege Level: `Administrator`
   ▶ Format: `no security-status monitor pwd-policy-inactive`

13.1.6 security-status monitor bypass-pwd-strength

Sets the monitoring whether at least one user is\nconfigured to bypass strength check.
▶ Mode: `Global Config Mode`
▶ Privilege Level: `Administrator`
▶ Format: `security-status monitor bypass-pwd-strength`

■ **no security-status monitor bypass-pwd-strength**
   Disable the option
   ▶ Mode: `Global Config Mode`
   ▶ Privilege Level: `Administrator`
   ▶ Format: `no security-status monitor bypass-pwd-strength`

13.1.7 security-status monitor telnet-enabled

Sets the monitoring of the activation of telnet on\nthe switch.
▶ Mode: `Global Config Mode`
▶ Privilege Level: `Administrator`
▶ Format: `security-status monitor telnet-enabled`

■ **no security-status monitor telnet-enabled**
   Disable the option
   ▶ Mode: `Global Config Mode`
   ▶ Privilege Level: `Administrator`
   ▶ Format: `no security-status monitor telnet-enabled`

13.1.8 security-status monitor http-enabled

Sets the monitoring of the activation of http on the switch.
- ▶ Mode: `Global Config Mode`
- ▶ Privilege Level: `Administrator`
- ▶ Format: `security-status monitor http-enabled`

■ **no security-status monitor http-enabled**
Disable the option
- ▶ Mode: `Global Config Mode`
- ▶ Privilege Level: `Administrator`
- ▶ Format: `no security-status monitor http-enabled`

13.1.9 security-status monitor snmp-unsecure

Sets the monitoring of SNMP security\n(SNMP v1/v2 is enabled or v3 encryption is disabled).
- ▶ Mode: `Global Config Mode`
- ▶ Privilege Level: `Administrator`
- ▶ Format: `security-status monitor snmp-unsecure`

■ **no security-status monitor snmp-unsecure**
Disable the option
- ▶ Mode: `Global Config Mode`
- ▶ Privilege Level: `Administrator`
- ▶ Format: `no security-status monitor snmp-unsecure`

13.1.10 security-status monitor sysmon-enabled

Sets the monitoring of the activation of System Monitor 1 on the switch.
- ▶ Mode: `Global Config Mode`
- ▶ Privilege Level: `Administrator`
- ▶ Format: `security-status monitor sysmon-enabled`

■ **no security-status monitor sysmon-enabled**
Disable the option
▶ Mode: `Global Config Mode`
▶ Privilege Level: `Administrator`
▶ Format: `no security-status monitor sysmon-enabled`

13.1.11 security-status monitor extnvm-upd-enabled

Sets the monitoring of activation of the configuration\n saving to external non volatile memory.
▶ Mode: `Global Config Mode`
▶ Privilege Level: `Administrator`
▶ Format: `security-status monitor extnvm-upd-enabled`

■ **no security-status monitor extnvm-upd-enabled**
Disable the option
▶ Mode: `Global Config Mode`
▶ Privilege Level: `Administrator`
▶ Format: `no security-status monitor extnvm-upd-enabled`

13.1.12 security-status monitor no-link-enabled

Sets the monitoring of no link detection.
▶ Mode: `Global Config Mode`
▶ Privilege Level: `Administrator`
▶ Format: `security-status monitor no-link-enabled`

■ **no security-status monitor no-link-enabled**
Disable the option
▶ Mode: `Global Config Mode`
▶ Privilege Level: `Administrator`
▶ Format: `no security-status monitor no-link-enabled`

13.1.13 security-status monitor hidisc-write-enabled

Sets the monitoring of HiDiscovery write enabled.
▶ Mode: `Global Config Mode`
▶ Privilege Level: `Administrator`
▶ Format: `security-status monitor hidisc-write-enabled`

■ **no security-status monitor hidisc-write-enabled**
Disable the option
▶ Mode: `Global Config Mode`
▶ Privilege Level: `Administrator`
▶ Format: `no security-status monitor hidisc-write-enabled`

13.1.14 security-status monitor extnvm-load-unsecure

Sets the monitoring of security of the configuration loading from extnvm.
▶ Mode: `Global Config Mode`
▶ Privilege Level: `Administrator`
▶ Format: `security-status monitor extnvm-load-unsecure`

■ **no security-status monitor extnvm-load-unsecure**
Disable the option
▶ Mode: `Global Config Mode`
▶ Privilege Level: `Administrator`
▶ Format: `no security-status monitor extnvm-load-unsecure`

13.1.15 security-status monitor iec61850-mms-enabled

Sets the monitoring of the activation of IEC 61850 MMS on the switch.
▶ Mode: `Global Config Mode`
▶ Privilege Level: `Administrator`
▶ Format: `security-status monitor iec61850-mms-enabled`

■ **no security-status monitor iec61850-mms-enabled**
Disable the option
▶ Mode: `Global Config Mode`
▶ Privilege Level: `Administrator`
▶ Format: `no security-status monitor iec61850-mms-enabled`

13.1.16 security-status monitor https-certificate

Sets the monitoring whether auto generated self-signed HTTPS certificate is in use.
▶ Mode: `Global Config Mode`
▶ Privilege Level: `Administrator`
▶ Format: `security-status monitor https-certificate`

■ **no security-status monitor https-certificate**
Disable the option
▶ Mode: `Global Config Mode`
▶ Privilege Level: `Administrator`
▶ Format: `no security-status monitor https-certificate`

13.1.17 security-status monitor modbus-tcp-enabled

Sets the monitoring of the activation of Modbus/TCP server on the switch.
▶ Mode: `Global Config Mode`
▶ Privilege Level: `Administrator`
▶ Format: `security-status monitor modbus-tcp-enabled`

■ **no security-status monitor modbus-tcp-enabled**
Disable the option
▶ Mode: `Global Config Mode`
▶ Privilege Level: `Administrator`
▶ Format: `no security-status monitor modbus-tcp-enabled`

13.1.18 security-status trap

Configure if a trap is sent when the security status\nchanges.
▶ Mode: `Global Config Mode`
▶ Privilege Level: `Administrator`
▶ Format: `security-status trap`

■ no security-status trap
Disable the option
▶ Mode: `Global Config Mode`
▶ Privilege Level: `Administrator`
▶ Format: `no security-status trap`

13.2 security-status

Configure the security status interface settings.

13.2.1 security-status no-link

Configure the monitoring of the specific ports.
▶ **Mode:** `Interface Range Mode`
▶ **Privilege Level:** `Administrator`
▶ **Format:** `security-status no-link`

■ **no security-status no-link**
  Disable the option
  ▶ **Mode:** `Interface Range Mode`
  ▶ **Privilege Level:** `Administrator`
  ▶ **Format:** `no security-status no-link`

13.3 show

Display device options and settings.

13.3.1 show security-status monitor

Display the security status monitoring settings.
- ▶ Mode: `Command is in all modes available.`
- ▶ Privilege Level: `Guest`
- ▶ Format: `show security-status monitor`

13.3.2 show security-status state

Display the current security status.
- ▶ Mode: `Command is in all modes available.`
- ▶ Privilege Level: `Guest`
- ▶ Format: `show security-status state`

13.3.3 show security-status no-link

Display the settings of the monitoring of the specific\nnetwork ports.
- ▶ Mode: `Command is in all modes available.`
- ▶ Privilege Level: `Guest`
- ▶ Format: `show security-status no-link`

13.3.4 show security-status trap

Display the security status trap information and settings.
- ▶ Mode: `Command is in all modes available.`
- ▶ Privilege Level: `Guest`
- ▶ Format: `show security-status trap`

13.3.5 show security-status events

Display occurred security status events.
- ▶ Mode: `Command is in all modes available.`
- ▶ Privilege Level: `Guest`
- ▶ Format: `show security-status events`

13.3.6 show security-status all

Display all security status settings.
- ▶ Mode: `Command is in all modes available.`
- ▶ Privilege Level: `Guest`
- ▶ Format: `show security-status all`

14 DHCP Layer 2 Relay

14.1 dhcp-l2relay

Configure DHCP Layer 2 Relay.

14.1.1 dhcp-l2relay mode

Enables or disables DHCP Layer 2 Relay globally.
▶ Mode: `Global Config Mode`
▶ Privilege Level: `Operator`
▶ Format: `dhcp-l2relay mode`

■ no dhcp-l2relay mode
Disable the option
▶ Mode: `Global Config Mode`
▶ Privilege Level: `Operator`
▶ Format: `no dhcp-l2relay mode`

14.2   dhcp-l2relay

Group of commands that configure DHCP Layer 2 Relay on existing VLANs.

14.2.1   dhcp-l2relay mode

Enables or disables DHCP Layer 2 Relay on a VLAN.
▶ Mode: `VLAN Database Mode`
▶ Privilege Level: `Operator`
▶ Format: `dhcp-l2relay mode <P-1>`

Paramete r	Value	Meaning
P-1	1..4042	Enter the VLAN ID.

■ **no dhcp-l2relay mode**
   Disable the option
   ▶ Mode: `VLAN Database Mode`
   ▶ Privilege Level: `Operator`
   ▶ Format: `no dhcp-l2relay mode`

14.2.2   dhcp-l2relay circuit-id

This commands enables setting the Option-82 Circuit ID in DHCP messages to an interface descriptor.
▶ Mode: `VLAN Database Mode`
▶ Privilege Level: `Operator`
▶ Format: `dhcp-l2relay circuit-id <P-1>`

Paramete r	Value	Meaning
P-1	1..4042	Enter the VLAN ID.

■ **no dhcp-l2relay circuit-id**
   Disable the option
   ▶ Mode: `VLAN Database Mode`
   ▶ Privilege Level: `Operator`
   ▶ Format: `no dhcp-l2relay circuit-id <P-1>`

14.2.3 dhcp-l2relay remote-id ip

This commands sets the Option-82 Remote ID to the IP address of device (if any assigned, else fails).
- ▶ Mode: `VLAN Database Mode`
- ▶ Privilege Level: `Operator`
- ▶ Format: `dhcp-l2relay remote-id ip <P-1>`

Parameter	Value	Meaning
P-1	1..4042	Enter the VLAN ID.

14.2.4 dhcp-l2relay remote-id mac

This commands sets the Option-82 Remote ID to the MAC address of device.
- ▶ Mode: `VLAN Database Mode`
- ▶ Privilege Level: `Operator`
- ▶ Format: `dhcp-l2relay remote-id mac <P-1>`

Parameter	Value	Meaning
P-1	1..4042	Enter the VLAN ID.

14.2.5 dhcp-l2relay remote-id client-id

This commands sets the Option-82 Remote ID to the system name (sysName) of device.
- ▶ Mode: `VLAN Database Mode`
- ▶ Privilege Level: `Operator`
- ▶ Format: `dhcp-l2relay remote-id client-id <P-1>`

Parameter	Value	Meaning
P-1	1..4042	Enter the VLAN ID.

14.2.6 dhcp-l2relay remote-id other

This commands sets the Option-82 Remote ID manually. If it is omitted then only the Circuit ID is inserted into a relayed DHCP message.

▶ Mode: `VLAN Database Mode`
▶ Privilege Level: `Operator`
▶ Format: `dhcp-l2relay remote-id other <P-1> [<P-2>]`

Parameter	Value	Meaning
P-1	1..4042	Enter the VLAN ID.
P-2	string	`<remote-id> Option 82 Remote ID`

14.3   dhcp-l2relay

Configure DHCP Layer 2 Relay for an interface (list/range)

14.3.1   dhcp-l2relay mode

Enables or disables DHCP Layer 2 Relay on an interface.
▶ Mode: `Interface Range Mode`
▶ Privilege Level: `Operator`
▶ Format: `dhcp-l2relay mode`

■ **no dhcp-l2relay mode**
   Disable the option
   ▶ Mode: `Interface Range Mode`
   ▶ Privilege Level: `Operator`
   ▶ Format: `no dhcp-l2relay mode`

14.3.2   dhcp-l2relay trust

This command configures an interface as trusted (typically connected to a DHCP server) or untrusted.
▶ Mode: `Interface Range Mode`
▶ Privilege Level: `Operator`
▶ Format: `dhcp-l2relay trust`

■ **no dhcp-l2relay trust**
   Disable the option
   ▶ Mode: `Interface Range Mode`
   ▶ Privilege Level: `Operator`
   ▶ Format: `no dhcp-l2relay trust`

14.4 clear

Clear several items.

14.4.1 clear dhcp-l2relay statistics

This command clears the DHCP Layer 2 Relay statistics.
▶ Mode: `Privileged Exec Mode`
▶ Privilege Level: `Operator`
▶ Format: `clear dhcp-l2relay statistics`

14.5 show

Display device options and settings.

14.5.1 show dhcp-l2relay global

This command displays the global DHCP Layer 2 Relay configuration.
▶ **Mode:** `Command is in all modes available.`
▶ **Privilege Level:** `Guest`
▶ **Format:** `show dhcp-l2relay global`

14.5.2 show dhcp-l2relay statistics

This command displays interface statistics specific to DHCP Layer 2 Relay.
▶ **Mode:** `Command is in all modes available.`
▶ **Privilege Level:** `Guest`
▶ **Format:** `show dhcp-l2relay statistics`

14.5.3 show dhcp-l2relay interfaces

This command displays the DHCP Layer 2 Relay status of all interfaces.
▶ **Mode:** `Command is in all modes available.`
▶ **Privilege Level:** `Guest`
▶ **Format:** `show dhcp-l2relay interfaces`

14.5.4   show dhcp-l2relay vlan

This command displays the VLAN based DHCP Layer 2 Relay status.
- ▶ Mode: `Command is in all modes available.`
- ▶ Privilege Level: `Guest`
- ▶ Format: `show dhcp-l2relay vlan`

15 DHCP Snooping

15.1 ip

Set IP parameters.

15.1.1 ip dhcp-snooping verify-mac

If enabled verifies the source MAC address in the ethernet packet against the client hardware address in the received DHCP Message. If disabled does not perform this additional security check.
▶ Mode: `Global Config Mode`
▶ Privilege Level: `Operator`
▶ Format: `ip dhcp-snooping verify-mac`

■ no ip dhcp-snooping verify-mac
Disable the option
▶ Mode: `Global Config Mode`
▶ Privilege Level: `Operator`
▶ Format: `no ip dhcp-snooping verify-mac`

15.1.2 ip dhcp-snooping mode

Enable or disable DHCP Snooping.
▶ Mode: `Global Config Mode`
▶ Privilege Level: `Operator`
▶ Format: `ip dhcp-snooping mode`

■ no ip dhcp-snooping mode
Disable the option
▶ Mode: `Global Config Mode`
▶ Privilege Level: `Operator`
▶ Format: `no ip dhcp-snooping mode`

15.1.3   ip dhcp-snooping database storage

This command specifies a location for the persistent DHCP Snooping bindings database. This can be a local file or a remote file on a given host.
▶ Mode: `Global Config Mode`
▶ Privilege Level: `Operator`
▶ Format: `ip dhcp-snooping database storage <P-1>`

Parameter	Value	Meaning
P-1	local	Save persistent DHCP Snooping bindings database to a local file.
	tftp-loc	Save persistent DHCP Snooping bindings database to a remote file: <tftp-loc> := tftp://<ip-addr>/<filename>.

15.1.4   ip dhcp-snooping database write-delay

This command configures the interval in seconds at which the DHCP Snooping binding database will be saved (persistent).
▶ Mode: `Global Config Mode`
▶ Privilege Level: `Operator`
▶ Format: `ip dhcp-snooping database write-delay <P-1>`

Parameter	Value	Meaning
P-1	15..86400	Interval in seconds at which the persistent DHCP Snooping binding database will be saved. The interval value ranges from 15 to 86400 seconds.

15.1.5   ip dhcp-snooping binding add

This command creates a new static DHCP Snooping binding (and optionally an associated dynamic IP Source Guard binding) between a MAC address and an IP address, for a specific VLAN at a particular interface.
▶ Mode: `Global Config Mode`
▶ Privilege Level: `Operator`
▶ Format: `ip dhcp-snooping binding add <P-1> <P-2> <P-3> <P-4> [<P-5>]`

Parameter	Value	Meaning
P-1	aa:bb:cc:dd:ee:ff	MAC address.
P-2	A.B.C.D	IP address.
P-3	slot no./port no.	
P-4	1..4042	Enter the VLAN ID.
P-5	active	Activate the option.
	inactive	Inactivate the option.

15.1.6 ip dhcp-snooping binding delete all

This command deletes all static DHCP Snooping bindings (and optionally all associated dynamic IP Source Guard bindings) at all interfaces.
▶ Mode: `Global Config Mode`
▶ Privilege Level: `Operator`
▶ Format: `ip dhcp-snooping binding delete all`

15.1.7 ip dhcp-snooping binding delete interface

This command deletes all static DHCP Snooping bindings (and optionally all associated dynamic IP Source Guard bindings), associated with a particular interface.
▶ Mode: `Global Config Mode`
▶ Privilege Level: `Operator`
▶ Format: `ip dhcp-snooping binding delete interface <P-1>`

Parameter	Value	Meaning
P-1	slot no./port no.	

15.1.8 ip dhcp-snooping binding delete mac

This command deletes one DHCP Snooping binding (and optionally the associated dynamic IP Source Guard binding), associated with a MAC address.
▶ Mode: `Global Config Mode`
▶ Privilege Level: `Operator`
▶ Format: `ip dhcp-snooping binding delete mac <P-1>`

Parameter	Value	Meaning
P-1	aa:bb:cc:dd:ee:ff	MAC address.

15.1.9   ip dhcp-snooping binding mode

This command activates or deactivates a configured static DHCP Snooping binding, associated with a MAC address.

▶ Mode: `Global Config Mode`
▶ Privilege Level: `Operator`
▶ Format: `ip dhcp-snooping binding mode <P-1> <P-2>`

Parameter	Value	Meaning
P-1	aa:bb:cc:dd:ee:ff	MAC address.
P-2	active	Activate the option.
	inactive	Inactivate the option.

15.2 clear

Clear several items.

15.2.1 clear ip dhcp-snooping bindings

This command clears all dynamic DHCP Snooping (and IP Source Guard) bindings on all interfaces or on a specific interface.

▶ Mode: `Privileged Exec Mode`
▶ Privilege Level: `Operator`
▶ Format: `clear ip dhcp-snooping bindings [<P-1>]`

Parameter	Value	Meaning
P-1	slot no./port no.	

15.2.2 clear ip dhcp-snooping statistics

This command clears the DHCP Snooping statistics.

▶ Mode: `Privileged Exec Mode`
▶ Privilege Level: `Operator`
▶ Format: `clear ip dhcp-snooping statistics`

15.3 ip

IP interface commands.

15.3.1 ip dhcp-snooping trust

This command configures an interface as trusted (typically connected to a DHCP server) or un-trusted. DHCP Snooping forwards valid DHCP client messages on trusted interfaces. On un-trusted interfaces the application compares the receive interface with the clients interface in the binding database.
▶ Mode: `Interface Range Mode`
▶ Privilege Level: `Operator`
▶ Format: `ip dhcp-snooping trust`

■ no ip dhcp-snooping trust
Disable the option
▶ Mode: `Interface Range Mode`
▶ Privilege Level: `Operator`
▶ Format: `no ip dhcp-snooping trust`

15.3.2 ip dhcp-snooping log

This command configures an interface to log invalid DHCP messages, or not to log.
▶ Mode: `Interface Range Mode`
▶ Privilege Level: `Operator`
▶ Format: `ip dhcp-snooping log`

■ no ip dhcp-snooping log
Disable the option
▶ Mode: `Interface Range Mode`
▶ Privilege Level: `Operator`
▶ Format: `no ip dhcp-snooping log`

15.3.3   ip dhcp-snooping auto-disable

Enables or disables the auto-disable feature for an interface, applicable when the DHCP packet rate exceeds the limit.
- ▶ **Mode:** `Interface Range Mode`
- ▶ **Privilege Level:** `Operator`
- ▶ **Format:** `ip dhcp-snooping auto-disable`

■ no ip dhcp-snooping auto-disable
Disable the option
- ▶ **Mode:** `Interface Range Mode`
- ▶ **Privilege Level:** `Operator`
- ▶ **Format:** `no ip dhcp-snooping auto-disable`

15.3.4   ip dhcp-snooping limit

This command configures an interface for a maximum DHCP packet rate in a burst interval, or disables it. If the rate of DHCP packets exceed this limit in consecutive intervals then all further packets are dropped. If that happens and additionally the auto-disable feature is enabled, then the port is disabled automatically.
- ▶ **Mode:** `Interface Range Mode`
- ▶ **Privilege Level:** `Operator`
- ▶ **Format:** `ip dhcp-snooping limit <P-1> [<P-2>]`

Parameter	Value	Meaning
P-1	-1..150	Specifies the rate limit value (in packets per seconds, pps) for DHCP snooping purposes. The value -1 switches rate limiting off.
P-2	1..15	Specifies the burst interval value for DHCP snooping purposes. Because this parameter is optional it leaves unchanged if omitted.

15.4 show

Display device options and settings.

15.4.1 show ip dhcp-snooping global

This command displays the global DHCP Snooping configuration.
▶ **Mode:** `Command is in all modes available.`
▶ **Privilege Level:** `Guest`
▶ **Format:** `show ip dhcp-snooping global`

15.4.2 show ip dhcp-snooping statistics

This command displays statistics for DHCP Snooping security violations on untrusted ports.
▶ **Mode:** `Command is in all modes available.`
▶ **Privilege Level:** `Guest`
▶ **Format:** `show ip dhcp-snooping statistics`

15.4.3 show ip dhcp-snooping interfaces

This command shows the DHCP Snooping status of all interfaces.
▶ **Mode:** `Command is in all modes available.`
▶ **Privilege Level:** `Guest`
▶ **Format:** `show ip dhcp-snooping interfaces`

15.4.4 show ip dhcp-snooping vlan

This command displays the VLAN based DHCP Snooping status.
▶ Mode: `Command is in all modes available.`
▶ Privilege Level: `Guest`
▶ Format: `show ip dhcp-snooping vlan`

15.4.5 show ip dhcp-snooping bindings

This command displays the DHCP Snooping binding entries from the static and/or dynamic bindings table.
▶ Mode: `Command is in all modes available.`
▶ Privilege Level: `Guest`
▶ Format: `show ip dhcp-snooping bindings [<P-1>] [interface <P-2>] [vlan <P-3>]`
`[interface]`: Restrict the output based on a specific interface.
`[vlan]`: Restrict the output based on VLAN.

Parameter	Value	Meaning
P-1	static	Restrict the output based on static bindings.
	dynamic	Restrict the output based on dynamic bindings.
P-2	slot no./port no.	
P-3	1..4042	Enter the VLAN ID.

16 DoS Mitigation

16.1   dos

Manage DoS Mitigation

16.1.1   dos tcp-null

Enables TCP Null scan protection - all TCP flags and TCP sequence number zero.
- ▶ **Mode:** `Global Config Mode`
- ▶ **Privilege Level:** `Operator`
- ▶ **Format:** `dos tcp-null`

■ no dos tcp-null
Disable the option
- ▶ **Mode:** `Global Config Mode`
- ▶ **Privilege Level:** `Operator`
- ▶ **Format:** `no dos tcp-null`

16.1.2   dos tcp-xmas

Enables TCP XMAS scan protection - TCP FIN, URG, PSH equal 1 and SEQ equals 0.
- ▶ **Mode:** `Global Config Mode`
- ▶ **Privilege Level:** `Operator`
- ▶ **Format:** `dos tcp-xmas`

■ no dos tcp-xmas
Disable the option
- ▶ **Mode:** `Global Config Mode`
- ▶ **Privilege Level:** `Operator`
- ▶ **Format:** `no dos tcp-xmas`

16.1.3   dos tcp-syn-fin

Enables TCP SYN/FIN scan protection - TCP with SYN and FIN flags set.
- ▶ Mode: `Global Config Mode`
- ▶ Privilege Level: `Operator`
- ▶ Format: `dos tcp-syn-fin`

■ **no dos tcp-syn-fin**
Disable the option
- ▶ Mode: `Global Config Mode`
- ▶ Privilege Level: `Operator`
- ▶ Format: `no dos tcp-syn-fin`

16.1.4   dos tcp-min-header

Enables TCP minimal header size check.
- ▶ Mode: `Global Config Mode`
- ▶ Privilege Level: `Operator`
- ▶ Format: `dos tcp-min-header`

■ **no dos tcp-min-header**
Disable the option
- ▶ Mode: `Global Config Mode`
- ▶ Privilege Level: `Operator`
- ▶ Format: `no dos tcp-min-header`

16.1.5   dos icmp-fragmented

Enables fragmented ICMP protection.
- ▶ Mode: `Global Config Mode`
- ▶ Privilege Level: `Operator`
- ▶ Format: `dos icmp-fragmented`

■ **no dos icmp-fragmented**
Disable the option
▶ Mode: `Global Config Mode`
▶ Privilege Level: `Operator`
▶ Format: `no dos icmp-fragmented`

16.1.6 dos icmp payload-check

Enables ICMP max payload size protection for IPv4 and IPv6.
▶ Mode: `Global Config Mode`
▶ Privilege Level: `Operator`
▶ Format: `dos icmp payload-check`

■ **no dos icmp payload-check**
Disable the option
▶ Mode: `Global Config Mode`
▶ Privilege Level: `Operator`
▶ Format: `no dos icmp payload-check`

16.1.7 dos icmp payload-size

Configures maximum ICMP payload size (default: 512).
▶ Mode: `Global Config Mode`
▶ Privilege Level: `Operator`
▶ Format: `dos icmp payload-size <P-1>`

Paramete r	Value	Meaning
P-1	0..1472	Max. ICMP payload size (default: 512)

16.1.8   dos ip-land

Enables LAND attack protection - source IP equals destination IP.
▶ Mode: `Global Config Mode`
▶ Privilege Level: `Operator`
▶ Format: `dos ip-land <P-1>`

Paramete r	Value	Meaning
P-1	enable	`Enable the option.`
	disable	`Disable the option.`

16.1.9   dos tcp-offset

Enables TCP offset check - ingress TCP packets with fragment offset 1 are dropped.
▶ Mode: `Global Config Mode`
▶ Privilege Level: `Operator`
▶ Format: `dos tcp-offset`

■ **no dos tcp-offset**
Disable the option
  ▶ Mode: `Global Config Mode`
  ▶ Privilege Level: `Operator`
  ▶ Format: `no dos tcp-offset`

16.1.10 dos tcp-syn

Enables TCP source port smaller than 1024 protection.
▶ Mode: `Global Config Mode`
▶ Privilege Level: `Operator`
▶ Format: `dos tcp-syn`

■ **no dos tcp-syn**
Disable the option
  ▶ Mode: `Global Config Mode`
  ▶ Privilege Level: `Operator`
  ▶ Format: `no dos tcp-syn`

16.1.11 dos l4-port

Enables UDP or TCP source port equals destination port check.
▶ Mode: `Global Config Mode`
▶ Privilege Level: `Operator`
▶ Format: `dos l4-port`

■ **no dos l4-port**
Disable the option
▶ Mode: `Global Config Mode`
▶ Privilege Level: `Operator`
▶ Format: `no dos l4-port`

16.2 show

Display device options and settings.

16.2.1 show dos

Show DoS Mitigation parameters
- ▶ Mode: `Command is in all modes available.`
- ▶ Privilege Level: `Guest`
- ▶ Format: `show dos`

17 IEEE 802.1x (Dot1x)

17.1   dot1x

Configure 802.1X parameters.

17.1.1   dot1x dynamic-vlan

Creates VLANs dynamically when a RADIUS-assigned VLAN does not exist.
- ▶ Mode: `Global Config Mode`
- ▶ Privilege Level: `Operator`
- ▶ Format: `dot1x dynamic-vlan`

■ no dot1x dynamic-vlan
Disable the option
- ▶ Mode: `Global Config Mode`
- ▶ Privilege Level: `Operator`
- ▶ Format: `no dot1x dynamic-vlan`

17.1.2   dot1x system-auth-control

Enable or disable 802.1X authentication support on the switch.
- ▶ Mode: `Global Config Mode`
- ▶ Privilege Level: `Operator`
- ▶ Format: `dot1x system-auth-control`

■ no dot1x system-auth-control
Disable the option
- ▶ Mode: `Global Config Mode`
- ▶ Privilege Level: `Operator`
- ▶ Format: `no dot1x system-auth-control`

17.1.3   dot1x monitor

Enable or disable 802.1X monitor mode.
- ▶ Mode: `Global Config Mode`
- ▶ Privilege Level: `Operator`
- ▶ Format: `dot1x monitor`

■ **no dot1x monitor**
Disable the option
- ▶ Mode: `Global Config Mode`
- ▶ Privilege Level: `Operator`
- ▶ Format: `no dot1x monitor`

17.2 dot1x

Configure 802.1X interface parameters.

17.2.1 dot1x guest-vlan

Configure a VLAN as 802.1X guest VLAN.
▶ **Mode:** `Interface Range Mode`
▶ **Privilege Level:** `Operator`
▶ **Format:** `dot1x guest-vlan <P-1>`

Parameter	Value	Meaning
P-1	0..4042	Enter the VLAN ID. Entering of ID 0 disables the feature.

17.2.2 dot1x max-req

Configure the maximum number of requests to be sent.
▶ **Mode:** `Interface Range Mode`
▶ **Privilege Level:** `Operator`
▶ **Format:** `dot1x max-req <P-1>`

Parameter	Value	Meaning
P-1	1..10	Maximum number of requests (default: 2).

17.2.3 dot1x port-control

Set the authentication mode on the specified port.
▶ **Mode:** `Interface Range Mode`
▶ **Privilege Level:** `Operator`
▶ **Format:** `dot1x port-control <P-1>`

Parameter	Value	Meaning
P-1	auto	Port is actually controlled by protocol.
	force-authorized	Port is authorized unconditionally (default).
	force-unauthorized	Port is unauthorized unconditionally.
	multi-client	If more than one client is attached to the port, then each client needs to authenticate separately.

17.2.4 dot1x re-authentication

Enable or disable re-authentication for the given interface.
▶ **Mode:** `Interface Range Mode`
▶ **Privilege Level:** `Operator`
▶ **Format:** `dot1x re-authentication`

■ **no dot1x re-authentication**
Disable the option
▶ **Mode:** `Interface Range Mode`
▶ **Privilege Level:** `Operator`
▶ **Format:** `no dot1x re-authentication`

17.2.5 dot1x unauthenticated-vlan

Configure a VLAN as 802.1X unauthenticated VLAN.
▶ **Mode:** `Interface Range Mode`
▶ **Privilege Level:** `Operator`
▶ **Format:** `dot1x unauthenticated-vlan <P-1>`

Parameter	Value	Meaning
P-1	0..4042	Enter the VLAN ID. Entering of ID 0 disables the feature.

17.2.6 dot1x timeout guest-vlan-period

Configure the guest-vlan period value.
▶ Mode: `Interface Range Mode`
▶ Privilege Level: `Operator`
▶ Format: `dot1x timeout guest-vlan-period <P-1>`

Parameter	Value	Meaning
P-1	1..300	Guest-vlan timeout in seconds (default: 90).

17.2.7 dot1x timeout reauth-period

Configure the re-authentication period.
▶ Mode: `Interface Range Mode`
▶ Privilege Level: `Operator`
▶ Format: `dot1x timeout reauth-period <P-1>`

Parameter	Value	Meaning
P-1	1..65535	Timeout in seconds.

17.2.8 dot1x timeout quiet-period

Configure the quiet period value.
▶ Mode: `Interface Range Mode`
▶ Privilege Level: `Operator`
▶ Format: `dot1x timeout quiet-period <P-1>`

Parameter	Value	Meaning
P-1	0..65535	Quiet period in seconds (default: 60).

17.2.9 dot1x timeout tx-period

Configure the transmit timeout period.
▶ Mode: `Interface Range Mode`
▶ Privilege Level: `Operator`
▶ Format: `dot1x timeout tx-period <P-1>`

Paramete r	Value	Meaning
P-1	1..65535	Timeout in seconds.

17.2.10 dot1x timeout supp-timeout

Configure the supplicant timeout period.
▶ Mode: `Interface Range Mode`
▶ Privilege Level: `Operator`
▶ Format: `dot1x timeout supp-timeout <P-1>`

Paramete r	Value	Meaning
P-1	1..65535	Timeout in seconds.

17.2.11 dot1x timeout server-timeout

Configure the server timeout period.
▶ Mode: `Interface Range Mode`
▶ Privilege Level: `Operator`
▶ Format: `dot1x timeout server-timeout <P-1>`

Paramete r	Value	Meaning
P-1	1..65535	Timeout in seconds.

17.2.12 dot1x initialize

Begins the initialization sequence on the specified port (port-control mode must be 'auto').
▶ Mode: `Interface Range Mode`
▶ Privilege Level: `Operator`
▶ Format: `dot1x initialize`

■ **no dot1x initialize**

Disable the option
▶ Mode: `Interface Range Mode`
▶ Privilege Level: `Operator`
▶ Format: `no dot1x initialize`

17.2.13 dot1x re-authenticate

Begins the re-authentication sequence on the specified port (port-control mode must be 'auto').
▶ Mode: `Interface Range Mode`
▶ Privilege Level: `Operator`
▶ Format: `dot1x re-authenticate`

■ **no dot1x re-authenticate**

Disable the option
▶ Mode: `Interface Range Mode`
▶ Privilege Level: `Operator`
▶ Format: `no dot1x re-authenticate`

17.3   show

Display device options and settings.

17.3.1   show dot1x global

Display global 802.1X configuration.
- ▶ Mode: `Command is in all modes available.`
- ▶ Privilege Level: `Guest`
- ▶ Format: `show dot1x global`

17.3.2   show dot1x auth-history

Display 802.1X authentication events and information.
- ▶ Mode: `Command is in all modes available.`
- ▶ Privilege Level: `Guest`
- ▶ Format: `show dot1x auth-history [<P-1> [<P-2>]]`

Paramete r	Value	Meaning
P-1	slot no./port no.	
P-2	1..4294967294	802.1X history log entry index. This can be specified only if interface is provided.\nParameter Usage:[<slot/port> [index]]

17.3.3   show dot1x detail

Display the detailed 802.1X configuration for the specified port.
- ▶ Mode: `Command is in all modes available.`
- ▶ Privilege Level: `Guest`
- ▶ Format: `show dot1x detail <P-1>`

Paramete r	Value	Meaning
P-1	slot no./port no.	

17.3.4 show dot1x summary

Display summary information of the 802.1X configuration for a specified port or all ports.
- ▶ Mode: `Command is in all modes available.`
- ▶ Privilege Level: `Guest`
- ▶ Format: `show dot1x summary [<P-1>]`

Parameter	Value	Meaning
`P-1`	slot no./port no.	

17.3.5 show dot1x clients

Display 802.1X client information.
- ▶ Mode: `Command is in all modes available.`
- ▶ Privilege Level: `Guest`
- ▶ Format: `show dot1x clients [<P-1>]`

Parameter	Value	Meaning
`P-1`	aa:bb:cc:dd:ee:ff	`MAC address.`

17.3.6 show dot1x statistics

Display the 802.1X statistics for the specified port.
- ▶ Mode: `Command is in all modes available.`
- ▶ Privilege Level: `Guest`
- ▶ Format: `show dot1x statistics <P-1>`

Parameter	Value	Meaning
`P-1`	slot no./port no.	

17.4 clear

Clear several items.

17.4.1 clear dot1x statistics port

Resets the 802.1X statistics for specified port.
▶ Mode: `Privileged Exec Mode`
▶ Privilege Level: `Operator`
▶ Format: `clear dot1x statistics port <P-1>`

Parameter	Value	Meaning
`P-1`	slot no./port no.	

17.4.2 clear dot1x statistics all

Resets the 802.1X statistics for all ports.
▶ Mode: `Privileged Exec Mode`
▶ Privilege Level: `Operator`
▶ Format: `clear dot1x statistics all`

17.4.3 clear dot1x auth-history port

Clears the 802.1X authentication history for specified port.
▶ Mode: `Privileged Exec Mode`
▶ Privilege Level: `Operator`
▶ Format: `clear dot1x auth-history port <P-1>`

Parameter	Value	Meaning
`P-1`	slot no./port no.	

17.4.4   clear dot1x auth-history all

Clears the 802.1X authentication history for all ports.
- ▶ Mode: `Privileged Exec Mode`
- ▶ Privilege Level: `Operator`
- ▶ Format: `clear dot1x auth-history all`

18 IEEE 802.3ad (Dot3ad)

18.1 link-aggregation

Configure 802.3ad link aggregation parameters to increase bandwidth and provide redundancy by combining connections.

18.1.1 link-aggregation add

Create a new Link Aggregation Group to increase bandwidth and provide link redundancy. If desired, enter a name up to 15 alphanumeric characters in length.
- ▶ Mode: `Global Config Mode`
- ▶ Privilege Level: `Operator`
- ▶ Format: `link-aggregation add <P-1>`

Paramete r	Value	Meaning
P-1	lag/<lagport>	`lag/<lagport>  Enter a lag interface in lag/lagport format.`

18.1.2 link-aggregation modify

Modify the parameters for the specified Link Aggregation Group.
- ▶ Mode: `Global Config Mode`
- ▶ Privilege Level: `Operator`
- ▶ Format: `link-aggregation modify <P-1> name <P-2> addport <P-3> deleteport <P-4> adminmode linktrap static hashmode <P-5> min-links <P-6>`

`name`: Modify the name of the specified Link Aggregation Group.
`addport`: Add the specified port to the Link Aggregation Group.
`deleteport`: Delete the specified port from the Link Aggregation Group.
`adminmode`: Modify the administration mode of the specified Link Aggregation Group. To activate the group, enable the administration mode.
`linktrap`: Enable/Disable link trap notifications for the specified Link Aggregation Group
`static`: Enable or disable static capability for the specified Link Aggregation Group on a device. When enabled, LACP automatically helps prevent loops and allows non-link aggregation partners to support LACP.
`hashmode`: Set the hash mode to be used by the load balancing algorithm for specified Link Aggregation Group.
`min-links`: Set the minimum links for the specified Link Aggregation Group.

Paramete r	Value	Meaning
P-1	slot no./port no.	
P-2	string	`Enter a user-defined text, max. 15 characters.`
P-3	slot no./port no.	

Paramete r	Value	Meaning
P-4	slot no./port no.	
P-5	src-mac	Source MAC, VLAN, EtherType, and incoming port associated with the packet.
	dst-mac	Destination MAC, VLAN, EtherType, and incoming port associated with the packet.
	src-dst-mac	Source/Destination MAC, VLAN, EtherType, and incoming port associated with the packet.
	src-ip	Source IP and Source TCP/UDP fields of the packet.
	dst-ip	Destination IP and Destination TCP/UDP Port fields of the packet.
	src-dst-ip	Source/Destination IP and source/destination TCP/UDP Port fields of the packet.
P-6	slot no./port no.	

■ **no link-aggregation modify**
  Disable the option
  ▶ Mode: `Global Config Mode`
  ▶ Privilege Level: `Operator`
  ▶ Format: `no link-aggregation modify <P-1> name addport deleteport adminmode linktrap static hashmode min-links`

18.1.3 link-aggregation delete

Delete the Link Aggregation Group to divide the group into individual connections.
▶ Mode: `Global Config Mode`
▶ Privilege Level: `Operator`
▶ Format: `link-aggregation delete <P-1>`

Paramete r	Value	Meaning
P-1	slot no./port no.	

18.2 lacp

Configure lacp parameters.

18.2.1 lacp admin-key

Configure the administrative value of the key on this LAG.
▶ Mode: `Interface Range Mode`
▶ Privilege Level: `Operator`
▶ Format: `lacp admin-key <P-1>`

Parameter	Value	Meaning
P-1	0..65535	Enter a number between 0 and 65535

18.2.2 lacp collector-max-delay

Configure the collector max delay on this LAG (default is 0).
▶ Mode: `Interface Range Mode`
▶ Privilege Level: `Operator`
▶ Format: `lacp collector-max-delay <P-1>`

Parameter	Value	Meaning
P-1	0..65535	Enter a number between 0 and 65535

18.2.3 lacp lacpmode

Activate/deactivate LACP on an interface.
▶ Mode: `Interface Range Mode`
▶ Privilege Level: `Operator`
▶ Format: `lacp lacpmode`

■ **no lacp lacpmode**
Disable the option
▶ Mode: `Interface Range Mode`
▶ Privilege Level: `Operator`
▶ Format: `no lacp lacpmode`

18.2.4 lacp actor admin key

Configure the value of the LACP actor admin key on this port(default 0).
▶ Mode: `Interface Range Mode`
▶ Privilege Level: `Operator`
▶ Format: `lacp actor admin key <P-1>`

Paramete r	Value	Meaning
P-1	0..65535	Enter a number between 0 and 65535

18.2.5 lacp actor admin state lacp-activity

Enable/disable the LACP activity on the actor admin state.
▶ Mode: `Interface Range Mode`
▶ Privilege Level: `Operator`
▶ Format: `lacp actor admin state lacp-activity`

■ **no lacp actor admin state lacp-activity**
Disable the option
▶ Mode: `Interface Range Mode`
▶ Privilege Level: `Operator`
▶ Format: `no lacp actor admin state lacp-activity`

18.2.6 lacp actor admin state lacp-timeout

Enable/disable the LACP timeout on the actor admin state.
- ▶ Mode: `Interface Range Mode`
- ▶ Privilege Level: `Operator`
- ▶ Format: `lacp actor admin state lacp-timeout`

■ no lacp actor admin state lacp-timeout
Disable the option
- ▶ Mode: `Interface Range Mode`
- ▶ Privilege Level: `Operator`
- ▶ Format: `no lacp actor admin state lacp-timeout`

18.2.7 lacp actor admin state aggregation

Enable/disable the aggregation on the actor admin state.
- ▶ Mode: `Interface Range Mode`
- ▶ Privilege Level: `Operator`
- ▶ Format: `lacp actor admin state aggregation`

■ no lacp actor admin state aggregation
Disable the option
- ▶ Mode: `Interface Range Mode`
- ▶ Privilege Level: `Operator`
- ▶ Format: `no lacp actor admin state aggregation`

18.2.8 lacp actor admin port priority

Set LACP actor port priority value (default 128).
- ▶ Mode: `Interface Range Mode`
- ▶ Privilege Level: `Operator`
- ▶ Format: `lacp actor admin port priority <P-1>`

Paramete r	Value	Meaning
P-1	0..65535	Enter a number between 0 and 65535

18.2.9   lacp partner admin key

Configure the administrative value of the LACP key for the protocol partner on this LAG (default 0).
▶ Mode: `Interface Range Mode`
▶ Privilege Level: `Operator`
▶ Format: `lacp partner admin key <P-1>`

Paramete r	Value	Meaning
P-1	0..65535	Enter a number between 0 and 65535

18.2.10 lacp partner admin state lacp-activity

Enable/disable the LACP activity on the partner admin state.
▶ Mode: `Interface Range Mode`
▶ Privilege Level: `Operator`
▶ Format: `lacp partner admin state lacp-activity`

■ **no lacp partner admin state lacp-activity**
Disable the option
   ▶ Mode: `Interface Range Mode`
   ▶ Privilege Level: `Operator`
   ▶ Format: `no lacp partner admin state lacp-activity`

18.2.11 lacp partner admin state lacp-timeout

Enable/disable the LACP timeout on the partner admin state.
▶ Mode: `Interface Range Mode`
▶ Privilege Level: `Operator`
▶ Format: `lacp partner admin state lacp-timeout`

■ **no lacp partner admin state lacp-timeout**
Disable the option
   ▶ Mode: `Interface Range Mode`
   ▶ Privilege Level: `Operator`
   ▶ Format: `no lacp partner admin state lacp-timeout`

18.2.12 lacp partner admin state aggregation

Enable/disable the state aggregation on the partner admin state.
- ▶ Mode: `Interface Range Mode`
- ▶ Privilege Level: `Operator`
- ▶ Format: `lacp partner admin state aggregation`

■ **no lacp partner admin state aggregation**
   Disable the option
- ▶ Mode: `Interface Range Mode`
- ▶ Privilege Level: `Operator`
- ▶ Format: `no lacp partner admin state aggregation`

18.2.13 lacp partner admin port priority

Set LACP partener port priority value (default 128).
- ▶ Mode: `Interface Range Mode`
- ▶ Privilege Level: `Operator`
- ▶ Format: `lacp partner admin port priority <P-1>`

Paramete r	Value	Meaning
P-1	0..65535	Enter a number between 0 and 65535

18.2.14 lacp partner admin port id

Set LACP partener port value (default 0).
- ▶ Mode: `Interface Range Mode`
- ▶ Privilege Level: `Operator`
- ▶ Format: `lacp partner admin port id <P-1>`

Paramete r	Value	Meaning
P-1	0..65535	Enter a number between 0 and 65535

18.2.15 lacp partner admin system-priority

Configure the partener system priority.
- ▶ Mode: `Interface Range Mode`
- ▶ Privilege Level: `Operator`
- ▶ Format: `lacp partner admin system-priority <P-1>`

Parameter	Value	Meaning
P-1	0..65535	Enter a number between 0 and 65535

18.2.16 lacp partner admin system-id

Configure the MAC address representing the administrative value of the LAG ports protocol partner system ID default (00:00:00:00:00:00).
- ▶ Mode: `Interface Range Mode`
- ▶ Privilege Level: `Operator`
- ▶ Format: `lacp partner admin system-id <P-1>`

Parameter	Value	Meaning
P-1	aa:bb:cc:dd:ee:ff	MAC address.

18.3 show

Display device options and settings.

18.3.1 show link-aggregation port

Show LAG configuration of a single port.
▶ Mode: `Command is in all modes available.`
▶ Privilege Level: `Guest`
▶ Format: `show link-aggregation port [<P-1>]`

Paramete r	Value	Meaning
`P-1`	slot no./port no.	

18.3.2 show link-aggregation statistics

Show ports LAG statistics.
▶ Mode: `Command is in all modes available.`
▶ Privilege Level: `Guest`
▶ Format: `show link-aggregation statistics [<P-1>]`

Paramete r	Value	Meaning
`P-1`	slot no./port no.	

18.3.3 show link-aggregation members

Show the member ports for specified LAG.
▶ Mode: `Command is in all modes available.`
▶ Privilege Level: `Guest`
▶ Format: `show link-aggregation members <P-1>`

Paramete r	Value	Meaning
`P-1`	slot no./port no.	

18.3.4   show lacp interface

Show LAG iterfaces attributes.
- ▶ Mode: `Command is in all modes available.`
- ▶ Privilege Level: `Guest`
- ▶ Format: `show lacp interface [<P-1>]`

Paramete r	Value	Meaning
P-1	slot no./port no.	

18.3.5   show lacp mode

Show lacp mode.
- ▶ Mode: `Command is in all modes available.`
- ▶ Privilege Level: `Guest`
- ▶ Format: `show lacp mode [<P-1>]`

Paramete r	Value	Meaning
P-1	slot no./port no.	

18.3.6   show lacp actor

Show Link Aggregation Control protocol actor attributes.
- ▶ Mode: `Command is in all modes available.`
- ▶ Privilege Level: `Guest`
- ▶ Format: `show lacp actor [<P-1>]`

Paramete r	Value	Meaning
P-1	slot no./port no.	

18.3.7   show lacp partner operational

Show Operational partner attributes.
- ▶ Mode: `Command is in all modes available.`
- ▶ Privilege Level: `Guest`
- ▶ Format: `show lacp partner operational [<P-1>]`

Paramete r	Value	Meaning
P-1	slot no./port no.	

18.3.8   show lacp partner admin

Show administrative partner attributes.
- ▶ Mode: `Command is in all modes available.`
- ▶ Privilege Level: `Guest`
- ▶ Format: `show lacp partner admin [<P-1>]`

Paramete r	Value	Meaning
P-1	slot no./port no.	

19 Filtering Database (FDB)

19.1   mac-filter

19.1.1   mac-filter

Static MAC filter configuration.
▶ Mode: `Global Config Mode`
▶ Privilege Level: `Operator`
▶ Format: `mac-filter <P-1> <P-2>`

Paramete r	Value	Meaning
P-1	aa:bb:cc:dd:ee:ff	MAC address.
P-2	1..4042	Enter the VLAN ID.

■ **no mac-filter**
Disable the option
▶ Mode: `Global Config Mode`
▶ Privilege Level: `Operator`
▶ Format: `no mac-filter <P-1> <P-2>`

19.2 bridge

Bridge configuration.

19.2.1 bridge aging-time

Aging time configuration.
▶ Mode: `Global Config Mode`
▶ Privilege Level: `Operator`
▶ Format: `bridge aging-time <P-1>`

Parameter	Value	Meaning
P-1	10..500000	Enter a number in the given range.

19.3   show

Display device options and settings.

19.3.1   show mac-filter-table static

Displays the MAC address filter table.
▶ Mode: `Command is in all modes available.`
▶ Privilege Level: `Guest`
▶ Format: `show mac-filter-table static`

19.4 show

Display device options and settings.

19.4.1 show bridge aging-time

Address aging time.
- ▶ Mode: `Command is in all modes available.`
- ▶ Privilege Level: `Guest`
- ▶ Format: `show bridge aging-time`

19.5 show

Display device options and settings.

19.5.1 show mac-addr-table

Displays the MAC address table.
- ▶ Mode: `Command is in all modes available.`
- ▶ Privilege Level: `Guest`
- ▶ Format: `show mac-addr-table [<P-1>]`

Paramete r	Value	Meaning
P-1	a:b:c:d:e:f	Enter a MAC address.
	1..4042	Enter a VLAN ID.

19.6 clear

Clear several items.

19.6.1 clear mac-addr-table

Clears the MAC address table.
▶ Mode: `Privileged Exec Mode`
▶ Privilege Level: `Operator`
▶ Format: `clear mac-addr-table`

20 HiDiscovery

20.1 network

Configure the inband and outband connectivity.

20.1.1 network hidiscovery operation

Enable/disable the HiDiscovery protocol on this device.
▶ Mode: `Privileged Exec Mode`
▶ Privilege Level: `Operator`
▶ Format: `network hidiscovery operation <P-1>`

Parameter	Value	Meaning
P-1	enable	Enable the HiDiscovery protocol.
	disable	Disable the HiDiscovery protocol.

■ **no network hidiscovery operation**
  Disable the option
  ▶ Mode: `Privileged Exec Mode`
  ▶ Privilege Level: `Operator`
  ▶ Format: `no network hidiscovery operation <P-1>`

20.1.2 network hidiscovery mode

Set the access level for HiDiscovery.
▶ Mode: `Privileged Exec Mode`
▶ Privilege Level: `Operator`
▶ Format: `network hidiscovery mode <P-1>`

Parameter	Value	Meaning
P-1	read-write	Allow detection and configuration.
	read-only	Allow only detection, no configuration.

20.1.3   network hidiscovery blinking

Enable/disable the HiDiscovery blinking sequence on this device. This preference is not saved in configuration
▶ Mode: `Privileged Exec Mode`
▶ Privilege Level: `Operator`
▶ Format: `network hidiscovery blinking`

■ **no network hidiscovery blinking**
   Disable the option
   ▶ Mode: `Privileged Exec Mode`
   ▶ Privilege Level: `Operator`
   ▶ Format: `no network hidiscovery blinking`

20.1.4   network hidiscovery relay

Enable/disable the HiDiscovery relay status.
▶ Mode: `Privileged Exec Mode`
▶ Privilege Level: `Operator`
▶ Format: `network hidiscovery relay`

■ **no network hidiscovery relay**
   Disable the option
   ▶ Mode: `Privileged Exec Mode`
   ▶ Privilege Level: `Operator`
   ▶ Format: `no network hidiscovery relay`

20.2 show

Display device options and settings.

20.2.1 show network hidiscovery

Show the HiDiscovery settings.
- ▶ Mode: `Command is in all modes available.`
- ▶ Privilege Level: `Guest`
- ▶ Format: `show network hidiscovery`

21 Hypertext Transfer Protocol (HTTP)

21.1 http

Set HTTP parameters.

21.1.1 http port

Set the HTTP port number.
▶ Mode: `Global Config Mode`
▶ Privilege Level: `Administrator`
▶ Format: `http port <P-1>`

Paramete r	Value	Meaning
P-1	1..65535	Port number of the HTTP server (default: 80).

21.1.2 http server

Enable or disable the HTTP server.
▶ Mode: `Global Config Mode`
▶ Privilege Level: `Administrator`
▶ Format: `http server`

■ no http server
Disable the option
▶ Mode: `Global Config Mode`
▶ Privilege Level: `Administrator`
▶ Format: `no http server`

21.2   show

Display device options and settings.

21.2.1   show http

Show HTTP server information.
▶ **Mode:** `Command is in all modes available.`
▶ **Privilege Level:** `Guest`
▶ **Format:** `show http`

22 HTTP Secure (HTTPS)

22.1 https

Set HTTPS parameters.

22.1.1 https server

Enable or disable the HTTPS server.
▶ **Mode:** `Global Config Mode`
▶ **Privilege Level:** `Administrator`
▶ **Format:** `https server`

■ no https server
Disable the option
▶ **Mode:** `Global Config Mode`
▶ **Privilege Level:** `Administrator`
▶ **Format:** `no https server`

22.1.2 https port

Set the HTTPS port number.
▶ **Mode:** `Global Config Mode`
▶ **Privilege Level:** `Administrator`
▶ **Format:** `https port <P-1>`

Paramete r	Value	Meaning
P-1	1..65535	Port number of the web server (default: 443).

22.1.3 https certificate

Generate/Delete HTTPS X509/PEM certificate.
▶ Mode: `Global Config Mode`
▶ Privilege Level: `Administrator`
▶ Format: `https certificate <P-1>`

Parameter	Value	Meaning
P-1	generate	Generates the item
	delete	Deletes the item

22.2   copy

Copy different kinds of items.

22.2.1   copy httpscert remote

Copy X509/PEM certificate from a server to the specified destination.
▶ Mode: `Privileged Exec Mode`
▶ Privilege Level: `Administrator`
▶ Format: `copy httpscert remote <P-1> nvm`
`nvm`: Copy HTTPS certificate (PEM) from a server to the device.

Paramete r	Value	Meaning
P-1	string	Enter a user-defined text, max. 128 characters.

22.2.2   copy httpscert envm

Copy X509/PEM certificate from external non-volatile memory to the specified destination.
▶ Mode: `Privileged Exec Mode`
▶ Privilege Level: `Administrator`
▶ Format: `copy httpscert envm <P-1> nvm`
`nvm`: Copy X509/PEM certificate from external non-volatile memory to the device.

Paramete r	Value	Meaning
P-1	string	Enter a user-defined text, max. 128 characters.

22.3 show

Display device options and settings.

22.3.1 show https

Show HTTPS server information.
▶ **Mode:** `Command is in all modes available.`
▶ **Privilege Level:** `Guest`
▶ **Format:** `show https`

23 Integrated Authentification Server (IAS)

23.1 ias-users

Manage IAS Users and User Accounts.

23.1.1 ias-users add

Add a new IAS user.
▶ Mode: `Global Config Mode`
▶ Privilege Level: `Administrator`
▶ Format: `ias-users add <P-1>`

Parameter	Value	Meaning
P-1	string	`<user>` User name (up to 32 characters).

23.1.2 ias-users delete

Delete an existing IAS user.
▶ Mode: `Global Config Mode`
▶ Privilege Level: `Administrator`
▶ Format: `ias-users delete <P-1>`

Parameter	Value	Meaning
P-1	string	`<user>` User name (up to 32 characters).

23.1.3 ias-users enable

Enable IAS user.
▶ Mode: `Global Config Mode`
▶ Privilege Level: `Administrator`
▶ Format: `ias-users enable <P-1>`

Parameter	Value	Meaning
P-1	string	`<user>` User name (up to 32 characters).

23.1.4   ias-users disable

Disable IAS user.
▶ Mode: `Global Config Mode`
▶ Privilege Level: `Administrator`
▶ Format: `ias-users disable <P-1>`

Parameter	Value	Meaning
P-1	string	`<user> User name (up to 32 characters).`

23.1.5   ias-users password

Change IAS user password.
▶ Mode: `Global Config Mode`
▶ Privilege Level: `Administrator`
▶ Format: `ias-users password <P-1> [<P-2>]`

Parameter	Value	Meaning
P-1	string	`<user> User name (up to 32 characters).`
P-2	string	`Enter a user-defined text, max. 64 characters.`

23.2   show

Display device options and settings.

23.2.1   show ias-users

Display IAS users and user accounts information.
- ▶ **Mode:** `Command is in all modes available.`
- ▶ **Privilege Level:** `Administrator`
- ▶ **Format:** `show ias-users`

24 IEC 61850 MMS Server

24.1 iec61850-mms

Configure the IEC61850 MMS Server settings.

24.1.1 iec61850-mms operation

Enable or disable the IEC61850 MMS Server. The MMS server facilitates real-time distribution of data and supervisory control functions for substations.
▶ Mode: `Global Config Mode`
▶ Privilege Level: `Operator`
▶ Format: `iec61850-mms operation`

■ no iec61850-mms operation
Disable the option
▶ Mode: `Global Config Mode`
▶ Privilege Level: `Operator`
▶ Format: `no iec61850-mms operation`

24.1.2 iec61850-mms write-access

Enable or disable the Write-Access on IEC61850 bridge objects via MMS. Write services allow the MMS client to access application content. - Possible security risk, as MMS communication is not authenticated -
▶ Mode: `Global Config Mode`
▶ Privilege Level: `Operator`
▶ Format: `iec61850-mms write-access`

■ no iec61850-mms write-access
Disable the option
▶ Mode: `Global Config Mode`
▶ Privilege Level: `Operator`
▶ Format: `no iec61850-mms write-access`

24.1.3   iec61850-mms port

Defines the port number of the IEC61850 MMS server (default: 102).
- ▶ Mode: `Global Config Mode`
- ▶ Privilege Level: `Operator`
- ▶ Format: `iec61850-mms port <P-1>`

Paramete r	Value	Meaning
P-1	1..65535	Port number of the IEC61850 MMS server (default: 102).

24.1.4   iec61850-mms max-sessions

Defines the maximum number of concurrent IEC61850 MMS sessions (default: 5).
- ▶ Mode: `Global Config Mode`
- ▶ Privilege Level: `Operator`
- ▶ Format: `iec61850-mms max-sessions <P-1>`

Paramete r	Value	Meaning
P-1	1..15	Maximum number of concurrent IEC61850 MMS sessions (default: 5).

24.1.5   iec61850-mms technical-key

Defines the IEC61850 MMS Technical Key (default: KEY).
- ▶ Mode: `Global Config Mode`
- ▶ Privilege Level: `Operator`
- ▶ Format: `iec61850-mms technical-key <P-1>`

Paramete r	Value	Meaning
P-1	string	Enter a IEC61850-7-2 Ed. VisibleString, max. 32 characters. The following characters are allowed: VisibleString (FROM ('A'|'a'|'B'|'b'|'C'|'c'|'D'|'d'|'E'|'e'|'F'|'f'| 'G'|'g'|'H'|'h'|'I'|'i'|'J'|'j'|'K'|'k'|'L'|'l'| 'M'|'m'|'N'|'n'|'O'|'o'|'P'|'p'|'Q'|'q'|'R'|'r'| 'S'|'s'|'T'|'t'|'U'|'u'|'V'|'v'|'W'|'w'|'X'|'x'| 'Y'|'y'|'Z'|'z'|'_'|'0'|'1'|'2'|'3'|'4'|'5'|'6'| '7'|'8'|'9')

24.2 show

Display device options and settings.

24.2.1 show iec61850-mms

Show the IEC61850 MMS Server settings.
- ▶ Mode: `Command is in all modes available.`
- ▶ Privilege Level: `Guest`
- ▶ Format: `show iec61850-mms`

25 Internet Group Management Protocol (IGMP)

25.1 ip

Set IP parameters.

25.1.1 ip igmp operation

Enable or disable IGMP globally on the device.
▶ **Mode:** `Global Config Mode`
▶ **Privilege Level:** `Operator`
▶ **Format:** `ip igmp operation`

■ **no ip igmp operation**
Disable the option
  ▶ **Mode:** `Global Config Mode`
  ▶ **Privilege Level:** `Operator`
  ▶ **Format:** `no ip igmp operation`

25.2 ip

IP interface commands.

25.2.1 ip igmp operation

Enables or disables IGMP on the interface.
- ▶ Mode: `Interface Range Mode`
- ▶ Privilege Level: `Operator`
- ▶ Format: `ip igmp operation`

■ no ip igmp operation
Disable the option
- ▶ Mode: `Interface Range Mode`
- ▶ Privilege Level: `Operator`
- ▶ Format: `no ip igmp operation`

25.2.2 ip igmp version

Configure IGMP version.
- ▶ Mode: `Interface Range Mode`
- ▶ Privilege Level: `Operator`
- ▶ Format: `ip igmp version <P-1>`

Parameter	Value	Meaning
P-1	1..3	Enter igmp version (default: 3).

25.2.3 ip igmp robustness

Configure IGMP router robustness.
▶ Mode: `Interface Range Mode`
▶ Privilege Level: `Operator`
▶ Format: `ip igmp robustness <P-1>`

Parameter	Value	Meaning
P-1	1..255	Enter igmp query robustness (default: 2).

25.2.4 ip igmp querier query-interval

Configure IGMP query interval in seconds.
▶ Mode: `Interface Range Mode`
▶ Privilege Level: `Operator`
▶ Format: `ip igmp querier query-interval <P-1>`

Parameter	Value	Meaning
P-1	1..3600	Enter igmp query interval (default: 125).

25.2.5 ip igmp querier last-member-interval

Configure last member query interval in tenths of seconds.
▶ Mode: `Interface Range Mode`
▶ Privilege Level: `Operator`
▶ Format: `ip igmp querier last-member-interval <P-1>`

Parameter	Value	Meaning
P-1	1..255	Enter igmp last member query interval (default: 10).

25.2.6 ip igmp querier max-response-time

Configure maximum response time in tenths of seconds.
▶ Mode: `Interface Range Mode`
▶ Privilege Level: `Operator`
▶ Format: `ip igmp querier max-response-time <P-1>`

Paramete r	Value	Meaning
P-1	1..255	Enter igmp query maximum response time (default: 100).

25.3 show

Display device options and settings.

25.3.1 show ip igmp global

Display IGMP global configuration.
- ▶ **Mode:** `Command is in all modes available.`
- ▶ **Privilege Level:** `Operator`
- ▶ **Format:** `show ip igmp global`

25.3.2 show ip igmp interface

Display IGMP interface information.
- ▶ **Mode:** `Command is in all modes available.`
- ▶ **Privilege Level:** `Operator`
- ▶ **Format:** `show ip igmp interface [<P-1>]`

Paramete r	Value	Meaning
`P-1`	slot no./port no.	

25.3.3 show ip igmp membership

Display interfaces subscribed to the multicast group.
- ▶ **Mode:** `Command is in all modes available.`
- ▶ **Privilege Level:** `Operator`
- ▶ **Format:** `show ip igmp membership`

25.3.4   show ip igmp groups

Display the subscribed multicast groups.
▶ Mode: `Command is in all modes available.`
▶ Privilege Level: `Operator`
▶ Format: `show ip igmp groups`

25.3.5   show ip igmp statistics

Display IGMP statistical information.
▶ Mode: `Command is in all modes available.`
▶ Privilege Level: `Operator`
▶ Format: `show ip igmp statistics [<P-1>]`

Paramete r	Value	Meaning
`P-1`	slot no./port no.	

26 IGMP Proxy

26.1   ip

Set IP parameters.

26.1.1   ip igmp-proxy interface

This command enables/disables IGMP Proxy on the router and configures the host interface.
- ▶ Mode: `Global Config Mode`
- ▶ Privilege Level: `Operator`
- ▶ Format: `ip igmp-proxy interface <P-1>`

Paramete r	Value	Meaning
P-1	slot no./port no.	

■ **no ip igmp-proxy interface**
   Disable the option
   - ▶ Mode: `Global Config Mode`
   - ▶ Privilege Level: `Operator`
   - ▶ Format: `no ip igmp-proxy interface <P-1>`

26.1.2   ip igmp-proxy report-interval

Sets the unsolicited report interval in seconds.
- ▶ Mode: `Global Config Mode`
- ▶ Privilege Level: `Operator`
- ▶ Format: `ip igmp-proxy report-interval <P-1>`

Paramete r	Value	Meaning
P-1	1..260	Enter a number in the given range.

26.2 show

Display device options and settings.

26.2.1 show ip igmp-proxy global

Displays a summary of the host interface status parameters.
▶ Mode: `Command is in all modes available.`
▶ Privilege Level: `Guest`
▶ Format: `show ip igmp-proxy global`

26.2.2 show ip igmp-proxy groups

Displays informations about the subscribed multicast groups that IGMP Proxy reported.
▶ Mode: `Command is in all modes available.`
▶ Privilege Level: `Guest`
▶ Format: `show ip igmp-proxy groups`

26.2.3 show ip igmp-proxy source-list

Displays the source-list of each subscribed multicast group that IGMP Proxy reported.
▶ Mode: `Command is in all modes available.`
▶ Privilege Level: `Guest`
▶ Format: `show ip igmp-proxy source-list`

27 IGMP Snooping

27.1 igmp-snooping

Configure IGMP snooping.

27.1.1 igmp-snooping mode

Enable or disable IGMP snooping.
▶ **Mode:** `Global Config Mode`
▶ **Privilege Level:** `Operator`
▶ **Format:** `igmp-snooping mode`

■ **no igmp-snooping mode**
   Disable the option
   ▶ **Mode:** `Global Config Mode`
   ▶ **Privilege Level:** `Operator`
   ▶ **Format:** `no igmp-snooping mode`

27.1.2 igmp-snooping querier mode

Enable or disable IGMP snooping querier on the system.
▶ **Mode:** `Global Config Mode`
▶ **Privilege Level:** `Operator`
▶ **Format:** `igmp-snooping querier mode`

■ **no igmp-snooping querier mode**
   Disable the option
   ▶ **Mode:** `Global Config Mode`
   ▶ **Privilege Level:** `Operator`
   ▶ **Format:** `no igmp-snooping querier mode`

27.1.3 igmp-snooping querier query-interval

Sets the IGMP querier query interval time (1-1800) in seconds.
- ▶ Mode: `Global Config Mode`
- ▶ Privilege Level: `Operator`
- ▶ Format: `igmp-snooping querier query-interval <P-1>`

Paramete r	Value	Meaning
P-1	1..1800	Enter a number in the given range.

27.1.4 igmp-snooping querier timer-expiry

Sets the IGMP querier timer expiration period (60-300) in seconds.
- ▶ Mode: `Global Config Mode`
- ▶ Privilege Level: `Operator`
- ▶ Format: `igmp-snooping querier timer-expiry <P-1>`

Paramete r	Value	Meaning
P-1	60..300	Enter a number in the given range.

27.1.5 igmp-snooping querier version

Sets the IGMP version (1-3) of the query.
- ▶ Mode: `Global Config Mode`
- ▶ Privilege Level: `Operator`
- ▶ Format: `igmp-snooping querier version <P-1>`

Paramete r	Value	Meaning
P-1	1..3	IGMP snooping querier's protocol version(1 to 3,default: 2).

27.1.6 igmp-snooping forward-unknown

Configure if and how unknown multicasts are forwarded.The setting can be discard, flood or query-ports.The default is flood.

▶ Mode: `Global Config Mode`
▶ Privilege Level: `Operator`
▶ Format: `igmp-snooping forward-unknown <P-1>`

Parameter	Value	Meaning
P-1	discard	Unknown multicast frames will be discarded.
	flood	Unknown multicast frames will be flooded.
	query-ports	Unknown multicast frames will be forwarded only to query ports.

27.2   igmp-snooping

Configure IGMP snooping.

27.2.1   igmp-snooping vlan-id

Configure the VLAN parameters.
- ▶ **Mode:** `VLAN Database Mode`
- ▶ **Privilege Level:** `Operator`
- ▶ **Format:** `igmp-snooping vlan-id <P-1> mode fast-leave groupmembership-interval <P-2> maxresponse <P-3> mcrtrexpiretime <P-4> querier mode address <P-5> forward-known <P-6> forward-all <P-7> static-query-port <P-8> automatic-mode <P-9>`

`mode`: Enable or disable IGMP snooping per VLAN.
`fast-leave`: Enable or disable IGMP snooping fast-leave per VLAN.
`groupmembership-interval`: Set IGMP group membership interval time (2-3600) in seconds per VLAN.
`maxresponse`: Set the igmp maximum response time (1-25) in seconds per VLAN.
`mcrtrexpiretime`: Sets the multicast router present expiration time (0-3600) in seconds per VLAN.
`querier`: Set IGMP snooping querier on the system.
`mode`: Enable or disable IGMP snooping querier per VLAN.
`address`: Set IGMP snooping querier address on the system using a VLAN.
`forward-known`: Sets the mode how known multicast packets will be treated.The default value is registered-ports-only(2).
`forward-all`: Enable or disable IGMP snooping forward-all.
`static-query-port`: Enable or disable IGMP snooping static-query-port.
`automatic-mode`: Enable or disable IGMP snooping automatic-mode.

Parameter	Value	Meaning
P-1	1..4042	Enter the VLAN ID.
P-2	2..3600	Enter a number in the given range.
P-3	1..25	Enter a number in the given range.
P-4	0..3600	Enter a number in the given range.
P-5	a.b.c.d	IP address.
P-6	query-and-registered-ports	Addition of query ports to multicast filter portmasks.
	registered-ports-only	No addition of query ports to multicast filter portmasks.
P-7	slot no./port no.	
P-8	slot no./port no.	
P-9	slot no./port no.	

■ **no igmp-snooping vlan-id**

Disable the option

▶ Mode: `VLAN Database Mode`

▶ Privilege Level: `Operator`

▶ Format: `no igmp-snooping vlan-id <P-1> mode fast-leave groupmembership-interval maxresponse mcrtrexpiretime querier mode address forward-known forward-all <P-7> static-query-port <P-8> automatic-mode <P-9>`

27.3 igmp-snooping

Configure IGMP snooping.

27.3.1 igmp-snooping mode

Enable or disable IGMP snooping per interface.
▶ Mode: `Interface Range Mode`
▶ Privilege Level: `Operator`
▶ Format: `igmp-snooping mode`

■ no igmp-snooping mode
Disable the option
▶ Mode: `Interface Range Mode`
▶ Privilege Level: `Operator`
▶ Format: `no igmp-snooping mode`

27.3.2 igmp-snooping fast-leave

Enable or disable IGMP snooping fast-leave per interface.
▶ Mode: `Interface Range Mode`
▶ Privilege Level: `Operator`
▶ Format: `igmp-snooping fast-leave`

■ no igmp-snooping fast-leave
Disable the option
▶ Mode: `Interface Range Mode`
▶ Privilege Level: `Operator`
▶ Format: `no igmp-snooping fast-leave`

27.3.3 igmp-snooping groupmembership-interval

Set IGMP group membership interval time (2-3600) in seconds per interface.
▶ Mode: `Interface Range Mode`
▶ Privilege Level: `Operator`
▶ Format: `igmp-snooping groupmembership-interval <P-1>`

Paramete r	Value	Meaning
P-1	2..3600	Enter a number in the given range.

27.3.4 igmp-snooping maxresponse

Set the igmp maximum response time (1-25) in seconds per interface.
▶ Mode: `Interface Range Mode`
▶ Privilege Level: `Operator`
▶ Format: `igmp-snooping maxresponse <P-1>`

Paramete r	Value	Meaning
P-1	1..25	Enter a number in the given range.

27.3.5 igmp-snooping mcrtrexpiretime

Sets the multicast router present expiration time (0-3600) in seconds per interface.
▶ Mode: `Interface Range Mode`
▶ Privilege Level: `Operator`
▶ Format: `igmp-snooping mcrtrexpiretime <P-1>`

Paramete r	Value	Meaning
P-1	0..3600	Enter a number in the given range.

27.3.6 igmp-snooping static-query-port

Configures the interface as a static query interface in all VLANs.
▶ Mode: `Interface Range Mode`
▶ Privilege Level: `Operator`
▶ Format: `igmp-snooping static-query-port`

■ **no igmp-snooping static-query-port**
Disable the option
▶ Mode: `Interface Range Mode`
▶ Privilege Level: `Operator`
▶ Format: `no igmp-snooping static-query-port`

27.4 show

Display device options and settings.

27.4.1 show igmp-snooping global

Show IGMP snooping global information.
- ▶ Mode: `Command is in all modes available.`
- ▶ Privilege Level: `Guest`
- ▶ Format: `show igmp-snooping global`

27.4.2 show igmp-snooping interface

Show IGMP snooping interface information.
- ▶ Mode: `Command is in all modes available.`
- ▶ Privilege Level: `Guest`
- ▶ Format: `show igmp-snooping interface [<P-1>]`

Paramete r	Value	Meaning
`P-1`	slot no./port no.	

27.4.3 show igmp-snooping vlan

Show IGMP snooping VLAN information.
- ▶ Mode: `Command is in all modes available.`
- ▶ Privilege Level: `Guest`
- ▶ Format: `show igmp-snooping vlan [<P-1>]`

Paramete r	Value	Meaning
`P-1`	1..4042	`Enter the VLAN ID.`

27.4.4 show igmp-snooping querier global

Show IGMP snooping querier information per VLAN.
▶ **Mode:** `Command is in all modes available.`
▶ **Privilege Level:** `Guest`
▶ **Format:** `show igmp-snooping querier global`

27.4.5 show igmp-snooping querier vlan

Show IGMP snooping querier VLAN information.
▶ **Mode:** `Command is in all modes available.`
▶ **Privilege Level:** `Guest`
▶ **Format:** `show igmp-snooping querier vlan [<P-1>]`

Paramete r	Value	Meaning
P-1	1..4042	Enter the VLAN ID.

27.4.6 show igmp-snooping enhancements vlan

Show IGMP snooping VLAN information.
▶ **Mode:** `Command is in all modes available.`
▶ **Privilege Level:** `Guest`
▶ **Format:** `show igmp-snooping enhancements vlan [<P-1>]`

Paramete r	Value	Meaning
P-1	1..4042	Enter the VLAN ID.

27.4.7 show igmp-snooping enhancements unknown-filtering

Show unknown multicast filtering information.
▶ **Mode:** `Command is in all modes available.`
▶ **Privilege Level:** `Guest`
▶ **Format:** `show igmp-snooping enhancements unknown-filtering`

27.4.8   show igmp-snooping statistics global

Show number of control packets processed by CPU.
- ▶ Mode: `Command is in all modes available.`
- ▶ Privilege Level: `Guest`
- ▶ Format: `show igmp-snooping statistics global`

27.4.9   show igmp-snooping statistics interface

Show number of control packets processed by CPU per interface.
- ▶ Mode: `Command is in all modes available.`
- ▶ Privilege Level: `Guest`
- ▶ Format: `show igmp-snooping statistics interface [<P-1>]`

Parameter	Value	Meaning
`P-1`	slot no./port no.	

27.5 show

Display device options and settings.

27.5.1 show mac-filter-table igmp-snooping

Display IGMP snooping entries in the MFDB table.
▶ Mode: `Command is in all modes available.`
▶ Privilege Level: `Guest`
▶ Format: `show mac-filter-table igmp-snooping`

27.6 clear

Clear several items.

27.6.1 clear igmp-snooping

Clear all IGMP snooping entries.
▶ **Mode:** `Privileged Exec Mode`
▶ **Privilege Level:** `Operator`
▶ **Format:** `clear igmp-snooping`

28 Interface

28.1 shutdown

28.1.1 shutdown

Enable or disable the interface.
▶ **Mode:** `Interface Range Mode`
▶ **Privilege Level:** `Operator`
▶ **Format:** `shutdown`

■ no shutdown
Disable the option
▶ **Mode:** `Interface Range Mode`
▶ **Privilege Level:** `Operator`
▶ **Format:** `no shutdown`

28.2 auto-negotiate

28.2.1 auto-negotiate

Enable or disable automatic negotiation on the interface. The cable crossing settings have no effect if auto-negotiation is enabled. In this case cable crossing is always set to auto. Cable crossing is set to the value chosen by the user if auto-negotiation is disabled.
- ▶ Mode: `Interface Range Mode`
- ▶ Privilege Level: `Operator`
- ▶ Format: `auto-negotiate`

■ **no auto-negotiate**
Disable the option
- ▶ Mode: `Interface Range Mode`
- ▶ Privilege Level: `Operator`
- ▶ Format: `no auto-negotiate`

28.3 auto-power-down

28.3.1 auto-power-down

Set the auto-power-down mode on the interface.
▶ Mode: `Interface Range Mode`
▶ Privilege Level: `Operator`
▶ Format: `auto-power-down <P-1>`

Parameter	Value	Meaning
P-1	auto-power-save	The port goes in a low power mode.
	no-power-save	The port does not use the automatic power save mode.

28.4 cable-crossing

28.4.1 cable-crossing

Cable crossing settings on the interface. The cable crossing settings have no effect if auto-negotiation is enabled. In this case cable crossing is always set to auto. Cable crossing is set to the value chosen by the user if auto-negotiation is disabled.

▶ Mode: `Interface Range Mode`
▶ Privilege Level: `Operator`
▶ Format: `cable-crossing <P-1>`

Parameter	Value	Meaning
P-1	mdi	The port does not use the crossover mode.
	mdix	The port uses the crossover mode.
	auto-mdix	The port uses the auto crossover mode.

28.5   linktraps

28.5.1   linktraps

Enable/disable link up/down traps on the interface.
▶ Mode: `Interface Range Mode`
▶ Privilege Level: `Operator`
▶ Format: `linktraps`

■ no linktraps
Disable the option
▶ Mode: `Interface Range Mode`
▶ Privilege Level: `Operator`
▶ Format: `no linktraps`

28.6 link-loss-alert

Configure Link Loss Alert on the interface.

28.6.1 link-loss-alert operation

Enable or disable Link Loss Alert on the interface.
- ▶ Mode: `Interface Range Mode`
- ▶ Privilege Level: `Operator`
- ▶ Format: `link-loss-alert operation`

■ **no link-loss-alert operation**
Disable the option
- ▶ Mode: `Interface Range Mode`
- ▶ Privilege Level: `Operator`
- ▶ Format: `no link-loss-alert operation`

28.7 speed

28.7.1 speed

Sets the speed and duplex setting for the interface.
▶ Mode: `Interface Range Mode`
▶ Privilege Level: `Operator`
▶ Format: `speed <P-1> [<P-2>]`

Parameter	Value	Meaning
P-1	10	`10 MBit/s.`
	100	`100 MBit/s.`
	1000	`1000 MBit/s.`
P-2	full	`full duplex.`
	half	`half duplex.`

28.8 name

28.8.1 name

Set or remove a descriptive name for the interface.
▶ Mode: `Interface Range Mode`
▶ Privilege Level: `Operator`
▶ Format: `name <P-1>`

Parameter	Value	Meaning
P-1	string	Enter a user-defined text, max. 64 characters.

28.9 power-state

28.9.1 power-state

Enable or disable the power state on the interface. The interface power state settings have no effect if the interface admin state is enabled.

▶ Mode: `Interface Range Mode`
▶ Privilege Level: `Operator`
▶ Format: `power-state`

■ no power-state
Disable the option

▶ Mode: `Interface Range Mode`
▶ Privilege Level: `Operator`
▶ Format: `no power-state`

28.10 mac-filter

28.10.1 mac-filter

static mac filter configuration
▶ Mode: `Interface Range Mode`
▶ Privilege Level: `Operator`
▶ Format: `mac-filter <P-1> <P-2>`

Paramete r	Value	Meaning
P-1	aa:bb:cc:dd:ee:ff	MAC address.
P-2	1..4042	Enter the VLAN ID.

■ **no mac-filter**
Disable the option
▶ Mode: `Interface Range Mode`
▶ Privilege Level: `Operator`
▶ Format: `no mac-filter <P-1> <P-2>`

28.11 led-signaling

Enable or disable Port LED signaling.

28.11.1 led-signaling operation

Enable or disable Port LED signaling.
- ▶ **Mode:** `Interface Range Mode`
- ▶ **Privilege Level:** `Operator`
- ▶ **Format:** `led-signaling operation`

■ **no led-signaling operation**
  Disable the option
  - ▶ **Mode:** `Interface Range Mode`
  - ▶ **Privilege Level:** `Operator`
  - ▶ **Format:** `no led-signaling operation`

28.12 show

Display device options and settings.

28.12.1 show port

Show interface parameters.
▶ Mode: `Command is in all modes available.`
▶ Privilege Level: `Guest`
▶ Format: `show port [<P-1>]`

Paramete r	Value	Meaning
P-1	slot no./port no.	

28.13 show

Display device options and settings.

28.13.1 show link-loss-alert

Show link-loss-alert parameters.
▶ Mode: `Command is in all modes available.`
▶ Privilege Level: `Guest`
▶ Format: `show link-loss-alert [<P-1>]`

Paramete r	Value	Meaning
`P-1`	slot no./port no.	

28.14 show

Display device options and settings.

28.14.1 show led-signaling operation

Show Port LED signaling operation.
- ▶ **Mode:** `Command is in all modes available.`
- ▶ **Privilege Level:** `Guest`
- ▶ **Format:** `show led-signaling operation`

29 Interface Statistics

29.1 utilization

Configure the interface utilization parameters.

29.1.1 utilization control-interval

Add interval time to monitor the bandwidth utilization of the interface.
▶ Mode: `Interface Range Mode`
▶ Privilege Level: `Operator`
▶ Format: `utilization control-interval <P-1>`

Parameter	Value	Meaning
P-1	1..3600	Add interval time to monitor the bandwidth utilization.

29.1.2 utilization alarm-threshold lower

Lower threshold value
▶ Mode: `Interface Range Mode`
▶ Privilege Level: `Operator`
▶ Format: `utilization alarm-threshold lower <P-1>`

Parameter	Value	Meaning
P-1	0..10000	Add alarm threshold lower value for monitoring bandwidth utilization in hundredths of a percent.

29.1.3 utilization alarm-threshold upper

Upper threshold value
▶ Mode: `Interface Range Mode`
▶ Privilege Level: `Operator`
▶ Format: `utilization alarm-threshold upper <P-1>`

Paramete r	Value	Meaning
P-1	0..10000	Add alarm threshold upper value for monitoring bandwidth utilization in hundredths of a percent.

29.2 clear

Clear several items.

29.2.1 clear port-statistics

Clear all statistics counter.
- ▶ Mode: `Privileged Exec Mode`
- ▶ Privilege Level: `Operator`
- ▶ Format: `clear port-statistics`

29.3 show

Display device options and settings.

29.3.1 show interface counters

Show Table with interface counters.
- ▶ **Mode:** `Command is in all modes available.`
- ▶ **Privilege Level:** `Guest`
- ▶ **Format:** `show interface counters`

29.3.2 show interface layout

Show interface layout of the device.
- ▶ **Mode:** `Command is in all modes available.`
- ▶ **Privilege Level:** `Guest`
- ▶ **Format:** `show interface layout`

29.3.3 show interface utilization

Show interface utilization.
- ▶ **Mode:** `Command is in all modes available.`
- ▶ **Privilege Level:** `Guest`
- ▶ **Format:** `show interface utilization [<P-1>]`

Paramete r	Value	Meaning
`P-1`	slot no./port no.	

29.3.4 show interface statistics

Show summary interface statistics.
- ▶ Mode: `Command is in all modes available.`
- ▶ Privilege Level: `Guest`
- ▶ Format: `show interface statistics [<P-1>]`

Parameter	Value	Meaning
`P-1`	slot no./port no.	

29.3.5 show interface ether-stats

Show detailed interface statistics.
- ▶ Mode: `Command is in all modes available.`
- ▶ Privilege Level: `Guest`
- ▶ Format: `show interface ether-stats [<P-1>]`

Parameter	Value	Meaning
`P-1`	slot no./port no.	

30 Intern

30.1 help

Display help for various special keys.
▶ Mode: `Command is in all modes available.`
▶ Privilege Level: `Guest`
▶ Format: `help`

30.2   logout

Exit this session.
▶ Mode: `Command is in all modes available.`
▶ Privilege Level: `any`
▶ Format: `logout`

30.3 history

Show a list of previously run commands.
- Mode: `Command is in all modes available.`
- Privilege Level: `Guest`
- Format: `history`

30.4 vlan-mode

30.4.1 vlan-mode

Enter VLAN Configuration Mode.
▶ **Mode:** `Global Config Mode`
▶ **Privilege Level:** `Operator`
▶ **Format:** `vlan-mode <P-1>`

Parameter	Value	Meaning
P-1	all	Select all VLAN configured.
	vlan	Enter single VLAN.
	vlan range	Enter VLAN range separated by hyphen e.g 1-4.
	vlan list	Enter VLAN list separated by comma e.g 2,4,6,... .
	complex range	Enter VLAN range and several VLAN separated by comma for a list and hyphen for ranges e.g 2-4,6-9,11.

30.5   exit

Exit from vlan mode.
▶ **Mode:** `VLAN Mode`
▶ **Privilege Level:** `Operator`
▶ **Format:** `exit`

30.6 end

Exit to exec mode.
- ▶ **Mode:** `Interface Range Mode`
- ▶ **Privilege Level:** `Operator`
- ▶ **Format:** `end`

30.7   serviceshell

Enter system mode.

30.7.1   serviceshell deactivate

Disable the service shell access permanently (Cannot be undone).
▶ **Mode:** `Privileged Exec Mode`
▶ **Privilege Level:** `Administrator`
▶ **Format:** `serviceshell deactivate`

30.8 serviceshell-f

Enter system mode.

30.8.1 serviceshell-f deactivate

Disable the service shell access permanently (Cannot be undone).
- ▶ **Mode:** `Factory Mode`
- ▶ **Privilege Level:** `Administrator`
- ▶ **Format:** `serviceshell-f deactivate`

30.9 traceroute

Trace route to a specified host.

30.9.1 traceroute maxttl

Set max TTL value.
▶ Mode: `Privileged Exec Mode`
▶ Privilege Level: `Operator`
▶ Format: `traceroute <P-1> maxttl <P-2> [initttl <P-3>] [interval <P-4>] [count <P-5>] [maxFail <P-6>] [size <P-7>] [port <P-8>]`

`[initttl]`: Initial TTL value.
`[interval]`: Timeout until probe failure.
`[count]`: Number of probes for each TTL.
`[maxFail]`: Maximum number of consecutive probes that can fail.
`[size]`: Size of payload in bytes.
`[port]`: UDP destination port.

Parameter	Value	Meaning
`P-1`	string	Hostname or IP address.
`P-2`	1..255	Enter a number in the given range.
`P-3`	0..255	Enter a number in the given range.
`P-4`	1..60	Enter a number in the given range.
`P-5`	1..10	Enter a number in the given range.
`P-6`	0..255	Enter a number in the given range.
`P-7`	0..65507	Enter a number in the given range.
`P-8`	1..65535	Enter port number between 1 and 65535

30.10 traceroute

Trace route to a specified host.

30.10.1 traceroute source

Source address for traceroute command.
▶ Mode: `Privileged Exec Mode`
▶ Privilege Level: `Operator`
▶ Format: `traceroute <P-1> source <P-2>`

Parameter	Value	Meaning
P-1	string	Hostname or IP address.
P-2	A.B.C.D	IP address.

30.11 reboot

Reset the device (cold start).

30.11.1 reboot after

Schedule reboot after specified time.
▶ Mode: `All Privileged Modes`
▶ Privilege Level: `any`
▶ Format: `reboot after <P-1>`

Parameter	Value	Meaning
P-1	0..2147483	Enter Seconds Between 0 to 2147483. Setting 0 will clear scheduled Reboot if configured.

30.12 ping

30.12.1 ping

Send ICMP echo packets to a specified IP address.
- ▶ Mode: `Command is in all modes available.`
- ▶ Privilege Level: `Guest`
- ▶ Format: `ping <P-1>`

Parameter	Value	Meaning
P-1	string	Hostname or IP address.

30.13 ping

Send ICMP echo packets to a specified host or IP address.

30.13.1 ping source

Source address for ping command.
- ▶ Mode: `Command is in all modes available.`
- ▶ Privilege Level: `Guest`
- ▶ Format: `ping <P-1> source <P-2>`

Paramete r	Value	Meaning
`P-1`	string	Hostname or IP address.
`P-2`	A.B.C.D	`IP address.`

30.14 show

Display device options and settings.

30.14.1 show reboot

Display Configured reboot in seconds
- ▶ Mode: `Command is in all modes available.`
- ▶ Privilege Level: `Guest`
- ▶ Format: `show reboot`

30.14.2 show serviceshell

Display the service shell access.
- ▶ Mode: `Command is in all modes available.`
- ▶ Privilege Level: `Guest`
- ▶ Format: `show serviceshell`

31 Open Shortest Path First (OSPF)

31.1 ip

Set IP parameters.

31.1.1 ip ospf area

Configure the OSPF router area. A router area is a sub-division of an OSPF autonomous system and you identify an area by an area-id. OSPF networks, routers, and links that have the same area-id form a logical set.
- ▶ Mode: `Global Config Mode`
- ▶ Privilege Level: `Operator`
- ▶ Format: `ip ospf area <P-1> range add <P-2> <P-3> <P-4> modify <P-5> <P-6> <P-7> <P-8> delete <P-9> <P-10> <P-11> add delete stub add <P-12> modify <P-13> summarylsa <P-14> default-cost <P-15> delete <P-16> virtual-link add <P-17> delete <P-18> modify <P-19> authentication type <P-20> key <P-21> key-id <P-22> hello-interval <P-23> dead-interval <P-24> transmit-delay <P-25> retransmit-interval <P-26> nssa add <P-27> delete <P-28> modify translator role <P-29> stability-interval <P-30> summary no-redistribute default-info originate [metric <P-31>] [metric-type <P-32>]`

`range`: Configure the range for the area. You summarize the networks within this range into a single routing domain.
`add`: Create a router area.
`modify`: Modify the parameters of a router area.
`delete`: Delete a specific router area.
`add`: Create a new area.
`delete`: Delete a existing area.
`stub`: Configure the preferences for a stub area. You shield stub areas from external route advertisements, but the area receives advertisements from networks that belong to other areas of the same autonomous system.
`add`: Create a stub area. The command also allows you to convert an existing area to a stub area.
`modify`: Modify the stub area parameters.
`summarylsa`: Configure the summary LSA mode for a stub area. When enabled, the router both summarizes and propagates summary LSAs.
`default-cost`: Set the default cost for the stub area.
`delete`: Remove a stub area. After removal, the area receives external route advertisements.
`virtual-link`: Configure a virtual link. You use the virtual link to connect the router to the backbone area (0.0.0.0) through a non-backbone area or to connect two parts of a partitioned backbone area (0.0.0.0) through a non-backbone area.
`add`: Add a virtual neighbor.
`delete`: Delete a virtual neighbor.
`modify`: Modify the parameters of a virtual neighbor.
`authentication`: Configure the authentication type. The device authenticates the OSPF protocol exchanges in the OSPF packet header which includes an authentication type field.
`type`: Configure the authentication type. Authentication types are 0 for null authentication, 1 for simple password authentication, and 2 for cryptographic authentication.
`key`: Configure the authentication key.

`key-id`: Configure the authentication key-id for md5 authentication. This field identifies the algorithm and secret key used to create the message digest appended to the OSPF packet.

`hello-interval`: Configure the OSPF hello-interval for the virtual link, in seconds. The hello timer controls the time interval between sending two consecutive hello packets. Set this value to the same hello-interval value of the virtual neighbors.

`dead-interval`: Configure the OSPF dead-interval for the virtual link, in seconds. If the timer expires without the router receiving hello packets from a virtual neighbor, the router declares the neighbor router as down. Set the timer to at least four times the value of the hello-interval.

`transmit-delay`: Configure the OSPF transmit-delay for the virtual link, in seconds. Transmit delay is the time that you estimate it takes to transmit a link-state update packet over the virtual link.

`retransmit-interval`: Configure the OSPF retransmit-interval for the virtual link, in seconds. The retransmit interval is the time between two consecutive link-state advertisement transmissions. Link-state advertisements contain such information as database descriptions and link-state request packets for adjacencies belonging to virtual link.

`nssa`: Configure a NSSA(Not-So-Stubby-Area).

`add`: Add a NSSA.

`delete`: Delete a NSSA.

`modify`: Modify the parameters of a NSSA.

`translator`: Configure the NSSA translator related parameters.

`role`: Configure the NSSA translator role.

`stability-interval`: Configure the translator stability interval for the NSSA, in seconds.

`summary`: Configure the import summary for the specified NSSA.

`no-redistribute`: Configure route redistribution for the specified NSSA.

`default-info`: Configure the nssa default information origination parameters.

`originate`: Configuration whether a Type-7 LSA should be originated into the NSSA.

`[metric]`: Configure the metric for the NSSA.

`[metric-type]`: Configure the metric type for default information.

Paramete r	Value	Meaning
P-1	A.B.C.D	IP address.
P-2	summary-link	Configure summary links LSDB type optional mode.
	nssa-external-link	Configure nssa external link LSDB type optional mode.
P-3	A.B.C.D	IP address.
P-4	a.b.c.d	IP subnet mask.
P-5	summary-link	Configure summary links LSDB type optional mode.
	nssa-external-link	Configure nssa external link LSDB type optional mode.
P-6	A.B.C.D	IP address.
P-7	a.b.c.d	IP subnet mask.
P-8	advertise	Set as advertise.
	do-not-advertise	Set as do-not-advertise.
P-9	summary-link	Configure summary links LSDB type optional mode.
	nssa-external-link	Configure nssa external link LSDB type optional mode.
P-10	A.B.C.D	IP address.
P-11	a.b.c.d	IP subnet mask.
P-12	0	Configure the TOS (0 is for Normal Service).
P-13	0	Configure the TOS (0 is for Normal Service).
P-14	no-area-summary	Disable the router from sending area link state advertisement summaries.
	send-area-summary	Enable the router to send area link state advertisement summaries. The router floods LSAs within the area using multicast. Every topology change starts a new flood of LSAs.
P-15	0..16777215	Configure the default cost.
P-16	0	Configure the TOS (0 is for Normal Service).
P-17	A.B.C.D	IP address.
P-18	A.B.C.D	IP address.
P-19	A.B.C.D	IP address.

Paramete r	Value	Meaning
P-20	none	Configure the authentication type as none (Key and key ID is not required).
	simple	Configure the authentication type as simple (Key ID is not required).
	md5	Configure the authentication type as md5 for the interface.
P-21	string	<key> Configure the authentication key.
P-22	0..255	Enter a number in the given range.
P-23	1..65535	Enter a number between 1 and 65535
P-24	1..65535	Enter a number between 1 and 65535
P-25	0..3600	Enter a number in the given range.
P-26	0..3600	Enter a number in the given range.
P-27	import-nssa	Configure the area as NSSA only.
P-28	import-external	Change the area to support external LSAs also.
P-29	always	Configure the NSSA translator role as always. When used as a border router, the router translates LSAs regardless of the translator states of the other NSSA border routers.
	candidate	Configure the NSSA translator role as a candidate. When used as a border router, the router participates in the translator election process. The router maintains a list of reachable NSSA border routers.
P-30	0..65535	Enter a number between 0 and 65535
P-31	1..16777214	Configure the metric value.
P-32	ospf-metric	Set the metric type as ospf Metric.
	comparable-cost	Set the metric type as comparable cost.
	non-comparable	Set the metric type as non-comparable.

■ **no ip ospf area**

Disable the option
▶ Mode: `Global Config Mode`
▶ Privilege Level: `Operator`
▶ Format: `no ip ospf area <P-1> range add modify delete add delete stub add modify summarylsa default-cost delete virtual-link add delete modify authentication type key key-id hello-interval dead-interval transmit-delay retransmit-interval nssa add delete modify translator role stability-interval summary no-redistribute default-info originate [metric] [metric-type]`

31.1.2   ip ospf trapflags all

Set all trapflags at once.
▶ Mode: `Global Config Mode`
▶ Privilege Level: `Operator`
▶ Format: `ip ospf trapflags all <P-1>`

Paramete r	Value	Meaning
P-1	[cr]	Enable the Bit.

■ **no ip ospf trapflags all**
Disable the option
▶ Mode: `Global Config Mode`
▶ Privilege Level: `Operator`
▶ Format: `no ip ospf trapflags all <P-1>`

31.1.3   ip ospf operation

Enable or disable the OSPF admin mode. When enabled, the device initiates the OSPF process if the OSPF function is active on at least one interface.
▶ Mode: `Global Config Mode`
▶ Privilege Level: `Operator`
▶ Format: `ip ospf operation`

■ **no ip ospf operation**
Disable the option
▶ Mode: `Global Config Mode`
▶ Privilege Level: `Operator`
▶ Format: `no ip ospf operation`

31.1.4   ip ospf 1583compatability

Enable or disable the 1583compatibility for calculating routes external to the autonomous system. When enabled, the router is compatible with the preference rules defined in RFC1583, section 16.4.
▶ Mode: `Global Config Mode`
▶ Privilege Level: `Operator`
▶ Format: `ip ospf 1583compatability`

■ **no ip ospf 1583compatability**
Disable the option
▶ Mode: `Global Config Mode`
▶ Privilege Level: `Operator`
▶ Format: `no ip ospf 1583compatability`

31.1.5 ip ospf default-metric

Configure the default metric for re-distributed routes, when OSPF redistributes routes from other protocols.

▶ Mode: `Global Config Mode`
▶ Privilege Level: `Operator`
▶ Format: `ip ospf default-metric <P-1>`

Paramete r	Value	Meaning
P-1	1..16777214	Configure the default metric for redistributed routes.

■ **no ip ospf default-metric**

Disable the option

▶ Mode: `Global Config Mode`
▶ Privilege Level: `Operator`
▶ Format: `no ip ospf default-metric <P-1>`

31.1.6 ip ospf router-id

Configure the router ID to uniquely identify this OSPF router in the autonomous system.

▶ Mode: `Global Config Mode`
▶ Privilege Level: `Operator`
▶ Format: `ip ospf router-id <P-1>`

Paramete r	Value	Meaning
P-1	A.B.C.D	IP address.

31.1.7 ip ospf external-lsdb-limit

Configure the OSPF external lsdb limitation, which is the maximum number of non-default AS-external-LSA entries that the router stores in the link-state database. When the value -1 is configured, you disable the limitation.

▶ Mode: `Global Config Mode`
▶ Privilege Level: `Operator`
▶ Format: `ip ospf external-lsdb-limit <P-1>`

Paramete r	Value	Meaning
P-1	-1..2147483647	Configure the external lsdb limit.

31.1.8   ip ospf exit-overflow

Configure the OSPF exit overflow interval, in seconds. After the timer expires the router will attempt to leave the overflow-state. To disable the exit overflow interval function set the value to 0.

▶ Mode: `Global Config Mode`
▶ Privilege Level: `Operator`
▶ Format: `ip ospf exit-overflow <P-1>`

Parameter	Value	Meaning
P-1	0..2147483647	Configure the exit overflow interval.

31.1.9   ip ospf spf-delay

Configure the SPF delay, in seconds. The Shortest Path First (SPF) delay is the time that the device waits for the network to stabilize before calculating the shortest path tree, after a topology change.

▶ Mode: `Global Config Mode`
▶ Privilege Level: `Operator`
▶ Format: `ip ospf spf-delay <P-1>`

Parameter	Value	Meaning
P-1	0..65535	Enter a number between 0 and 65535

31.1.10 ip ospf spf-holdtime

Configure the minimum time between two consecutive SPF calculations, in seconds.

▶ Mode: `Global Config Mode`
▶ Privilege Level: `Operator`
▶ Format: `ip ospf spf-holdtime <P-1>`

Parameter	Value	Meaning
P-1	0..65535	Enter a number between 0 and 65535

31.1.11 ip ospf auto-cost

Set the auto cost reference bandwidth of the router interfaces for ospf metric calculations. The default reference bandwidth is 100 Mbps.
▶ Mode: `Global Config Mode`
▶ Privilege Level: `Operator`
▶ Format: `ip ospf auto-cost <P-1>`

Parameter	Value	Meaning
P-1	1..4294967	Configure the auto cost for OSPF calculation.

31.1.12 ip ospf distance intra

Enter the preference type as intra. Use intra-area routing when the device routes packets solely within an area, such as an internal router.
▶ Mode: `Global Config Mode`
▶ Privilege Level: `Operator`
▶ Format: `ip ospf distance intra <P-1>`

Parameter	Value	Meaning
P-1	1..255	Enter the value.

31.1.13 ip ospf distance inter

Enter the preference type as inter. Use inter-area routing when the device routes packets into or out of an area, such as an area border router.
▶ Mode: `Global Config Mode`
▶ Privilege Level: `Operator`
▶ Format: `ip ospf distance inter <P-1>`

Parameter	Value	Meaning
P-1	1..255	Enter the value.

31.1.14 ip ospf distance external

Enter the preference type as external. Use external-area routing when the device routes packets into or out of an autonomous system, such as an autonomous system boundary router (ASBR).
▶ Mode: `Global Config Mode`
▶ Privilege Level: `Operator`
▶ Format: `ip ospf distance external <P-1>`

Parameter	Value	Meaning
P-1	1..255	`Enter the value.`

31.1.15 ip ospf re-distribute

Configure the OSPF route re-distribution. An ASBR is able to translate information from other OSPF processes in separate areas and routes from other sources, such as static routes or other dynamic routing protocols, into the OSPF protocol.
▶ Mode: `Global Config Mode`
▶ Privilege Level: `Operator`
▶ Format: `ip ospf re-distribute <P-1> [metric <P-2>] [metric-type <P-3>] [tag <P-4>] [subnets <P-5>]`

`[metric]`: Configure the OSPF route re-distribution metric parameters.
`[metric-type]`: Configure the OSPF route redistribution metric-type.
`[tag]`: Configure the OSPF route redistribution tag parameters.
`[subnets]`: Allow the router to redistribute subnets into OSPF.

Parameter	Value	Meaning
P-1	connected	`Select the source protocol as connected.`
	static	`Select the source protocol as static.`
	rip	`Select the source protocol as RIP.`
P-2	0..16777214	`Configure the metric.`
P-3	1..2	`Configure the metric type.`
P-4	0..4294967295	`Configure the tag.`
P-5	enable	`Enable the option.`
	disable	`Disable the option.`

■ **no ip ospf re-distribute**
Disable the option
▶ Mode: `Global Config Mode`
▶ Privilege Level: `Operator`
▶ Format: `no ip ospf re-distribute <P-1> [metric] [metric-type] [tag] [subnets]`

31.1.16 ip ospf distribute-list

Configure the distribute list for the routes from other source protocols.
▶ Mode: `Global Config Mode`
▶ Privilege Level: `Operator`
▶ Format: `ip ospf distribute-list <P-1> <P-2> <P-3>`

Parameter	Value	Meaning
P-1	out	Configure as out to re-distribute routes with ACL rules
P-2	connected	Select the source protocol as connected.
	static	Select the source protocol as static.
	rip	Select the source protocol as RIP.
P-3	<1000..1099>	Enter the access list number.

■ **no ip ospf distribute-list**
   Disable the option
   ▶ Mode: `Global Config Mode`
   ▶ Privilege Level: `Operator`
   ▶ Format: `no ip ospf distribute-list <P-1> <P-2> <P-3>`

31.1.17 ip ospf default-info originate

Originate the OSPF default information.
▶ Mode: `Global Config Mode`
▶ Privilege Level: `Operator`
▶ Format: `ip ospf default-info originate [always] [metric <P-1>] [metric-type <P-2>]`

`[always]`: Always advertise the 0.0.0.0/0.0.0.0 route information.
`[metric]`: Configure the metric for default information.
`[metric-type]`: Configure the metric type for default information.

Parameter	Value	Meaning
P-1	1..16777214	Configure the metric value.
P-2	external-type1	Set the metric type for default information as external type-1. The type 1 value sets the metric to the sum of the internal and external OSPF metrics.
	external-type2	Set the metric type for default information as external type-2. The type 2 value sets the metric to the sum of external OSPF metrics from the source AS to the destination AS.

■ **no ip ospf default-info originate**
Disable the option
▶ Mode: `Global Config Mode`
▶ Privilege Level: `Operator`
▶ Format: `no ip ospf default-info originate [always] [metric <P-1>] [metric-type]`

31.2   ip

IP interface commands.

31.2.1   ip ospf operation

Enable or disable OSPF on port.
▶ Mode: `Interface Range Mode`
▶ Privilege Level: `Operator`
▶ Format: `ip ospf operation`

■ **no ip ospf operation**
   Disable the option
   ▶ Mode: `Interface Range Mode`
   ▶ Privilege Level: `Operator`
   ▶ Format: `no ip ospf operation`

31.2.2   ip ospf area-id

Configure the router ID that uniquely identifies the area to which the interface is connected. If a tie occurs during the designated router election the router with the higher router ID is the designated router.
▶ Mode: `Interface Range Mode`
▶ Privilege Level: `Operator`
▶ Format: `ip ospf area-id <P-1>`

Parameter	Value	Meaning
P-1	A.B.C.D	IP address.

31.2.3 ip ospf link-type

Configure the OSPF link type.
▶ Mode: `Interface Range Mode`
▶ Privilege Level: `Operator`
▶ Format: `ip ospf link-type <P-1>`

Paramete r	Value	Meaning
P-1	broadcast	Configure the link-type as broadcast for the interface. In broadcast networks, routers discover their neighbors dynamically using the OSPF hello protocol.
	nbma	Configure the link-type as Non-Broadcast Multi-Access for the interface. The nbma mode, emulates OSPF operation over a broadcast network. The nbma mode is the most efficient way to run OSPF over non-broadcast networks, both in terms of the LSDB size and the amount of routing protocol traffic. However, this mode requires direct communication between every router in the nbma network.
	point-to-point	Configure the link-type as point-to-point for the interface. Use the point-to-point link-type in a network that joins a single pair of routers.
	point-to-multipoint	Configure the link-type as point-to-multipoint for the interface. In the point-to-multipoint mode, OSPF treats each router-to-router link over non-broadcast networks as if they were point-to-point links.

31.2.4 ip ospf priority

Configure the OSPF router priority which the router uses in multi-access networks for the designated router election algorithm. The router with the higher router priority is the designated router. A value of 0 declares the router as ineligible for designated router elections.
▶ Mode: `Interface Range Mode`
▶ Privilege Level: `Operator`
▶ Format: `ip ospf priority <P-1>`

Paramete r	Value	Meaning
P-1	0..255	Configure the priority.

31.2.5 ip ospf transmit-delay

Configure the OSPF transmit-delay for the interface, in seconds. The transmit-delay is the time that you estimate it takes to transmit a link-state update packet over the interface.
▶ Mode: `Interface Range Mode`
▶ Privilege Level: `Operator`
▶ Format: `ip ospf transmit-delay <P-1>`

Paramete r	Value	Meaning
P-1	0..3600	Enter a number in the given range.

31.2.6   ip ospf retransmit-interval

Configure the OSPF retransmit-interval for the interface, in seconds. The retransmit-interval is the interval after which link-state advertisements containing database description and link-state request packets, are re-transmitted for adjacencies belonging to this interface.

▶ Mode: `Interface Range Mode`
▶ Privilege Level: `Operator`
▶ Format: `ip ospf retransmit-interval <P-1>`

Paramete r	Value	Meaning
P-1	0..3600	Enter a number in the given range.

31.2.7   ip ospf hello-interval

Configure the OSPF hello-interval for the interface, in seconds. The hello timer controls the time interval between two consecutive hello packets. Set this value to the same hello-interval value of the neighbor.

▶ Mode: `Interface Range Mode`
▶ Privilege Level: `Operator`
▶ Format: `ip ospf hello-interval <P-1>`

Paramete r	Value	Meaning
P-1	1..65535	Enter a number between 1 and 65535

31.2.8   ip ospf dead-interval

Configure the OSPF dead-interval for the interface, in seconds. If the timer expires without the router receiving hello packets from the neighbor, the router declares the neighbor router as down. Set the timer to at least four times the value of the hello-interval.

▶ Mode: `Interface Range Mode`
▶ Privilege Level: `Operator`
▶ Format: `ip ospf dead-interval <P-1>`

Paramete r	Value	Meaning
P-1	1..65535	Enter a number between 1 and 65535

31.2.9 ip ospf cost

Configure the OSPF cost for the interface. The cost of a specific interface indicates the overhead required to send packets across the link. If set to 0, OSPF calculates the cost from the reference bandwidth and the interface speed.
▶ Mode: `Interface Range Mode`
▶ Privilege Level: `Operator`
▶ Format: `ip ospf cost <P-1>`

Paramete r	Value	Meaning
P-1	<1..65535>	Configure the cost for the specified interface.
	auto	Automatic calculation from reference bandwidth and link speed.

31.2.10 ip ospf mtu-ignore

Enable/Disable OSPF MTU mismatch on interface.
▶ Mode: `Interface Range Mode`
▶ Privilege Level: `Operator`
▶ Format: `ip ospf mtu-ignore`

■ **no ip ospf mtu-ignore**
Disable the option
▶ Mode: `Interface Range Mode`
▶ Privilege Level: `Operator`
▶ Format: `no ip ospf mtu-ignore`

31.2.11 ip ospf authentication type

Configure authentication type.
- ▶ Mode: `Interface Range Mode`
- ▶ Privilege Level: `Operator`
- ▶ Format: `ip ospf authentication type <P-1>`

Parameter	Value	Meaning
P-1	none	Configure the authentication type as none (Key and key ID is not required).
	simple	Configure the authentication type as simple (Key ID is not required).
	md5	Configure the authentication type as md5 for the interface.

31.2.12 ip ospf authentication key

Configure authentication key.
- ▶ Mode: `Interface Range Mode`
- ▶ Privilege Level: `Operator`
- ▶ Format: `ip ospf authentication key <P-1>`

Parameter	Value	Meaning
P-1	string	<key> Configure the authentication key.

31.2.13 ip ospf authentication key-id

Configure authentication key-id for md5 authentication.
- ▶ Mode: `Interface Range Mode`
- ▶ Privilege Level: `Operator`
- ▶ Format: `ip ospf authentication key-id <P-1>`

Parameter	Value	Meaning
P-1	0..255	Enter a number in the given range.

31.3 show

Display device options and settings.

31.3.1 show ip ospf global

Display OSPF global configurations.
- ▶ Mode: `Command is in all modes available.`
- ▶ Privilege Level: `Guest`
- ▶ Format: `show ip ospf global`

31.3.2 show ip ospf area

Display OSPF area related information.
- ▶ Mode: `Command is in all modes available.`
- ▶ Privilege Level: `Guest`
- ▶ Format: `show ip ospf area [<P-1>]`

Paramete r	Value	Meaning
P-1	A.B.C.D	IP address.

31.3.3 show ip ospf stub

Display OSPF stub area related information.
- ▶ Mode: `Command is in all modes available.`
- ▶ Privilege Level: `Guest`
- ▶ Format: `show ip ospf stub`

31.3.4   show ip ospf database internal

Display the internal LSA database information.
- ▶ Mode: `Command is in all modes available.`
- ▶ Privilege Level: `Guest`
- ▶ Format: `show ip ospf database internal`

31.3.5   show ip ospf database external

Display the external LSA database information.
- ▶ Mode: `Command is in all modes available.`
- ▶ Privilege Level: `Guest`
- ▶ Format: `show ip ospf database external`

31.3.6   show ip ospf range

Display OSPF area range information.
- ▶ Mode: `Command is in all modes available.`
- ▶ Privilege Level: `Guest`
- ▶ Format: `show ip ospf range`

31.3.7   show ip ospf interface

Display OSPF interface related information.
- ▶ Mode: `Command is in all modes available.`
- ▶ Privilege Level: `Guest`
- ▶ Format: `show ip ospf interface [<P-1>]`

Parameter	Value	Meaning
`P-1`	slot no./port no.	

31.3.8 show ip ospf virtual-link

Display OSPF virtual-link related information.
- ▶ Mode: `Command is in all modes available.`
- ▶ Privilege Level: `Guest`
- ▶ Format: `show ip ospf virtual-link <P-1> <P-2>`

Parameter	Value	Meaning
P-1	A.B.C.D	IP address.
P-2	A.B.C.D	IP address.

31.3.9 show ip ospf virtual-neighbor

Display OSPF Virtual-link neighbor information
- ▶ Mode: `Command is in all modes available.`
- ▶ Privilege Level: `Guest`
- ▶ Format: `show ip ospf virtual-neighbor`

31.3.10 show ip ospf neighbor

Display OSPF neighbor related information.
- ▶ Mode: `Command is in all modes available.`
- ▶ Privilege Level: `Guest`
- ▶ Format: `show ip ospf neighbor [<P-1>]`

Parameter	Value	Meaning
P-1	slot no./port no.	

31.3.11 show ip ospf statistics

Display OSPF statistics.
- ▶ Mode: `Command is in all modes available.`
- ▶ Privilege Level: `Guest`
- ▶ Format: `show ip ospf statistics`

31.3.12 show ip ospf re-distribute

Display OSPF re-distribute related information
- ▶ Mode: `Command is in all modes available.`
- ▶ Privilege Level: `Guest`
- ▶ Format: `show ip ospf re-distribute <P-1>`

Paramete r	Value	Meaning
P-1	connected	Select the source protocol as connected.
	static	Select the source protocol as static.
	rip	Select the source protocol as RIP.

31.3.13 show ip ospf nssa

Display OSPF NSSA related information.
- ▶ Mode: `Command is in all modes available.`
- ▶ Privilege Level: `Guest`
- ▶ Format: `show ip ospf nssa <P-1>`

Paramete r	Value	Meaning
P-1	A.B.C.D	IP address.

31.3.14 show ip ospf route

Display OSPF routes.
- ▶ Mode: `Command is in all modes available.`
- ▶ Privilege Level: `Guest`
- ▶ Format: `show ip ospf route`

32   Internet Protocol Version 4 (IPv4)

32.1   network

Configure the inband and outband connectivity.

32.1.1   network protocol

Select DHCP, BOOTP or none as the network configuration protocol.
▶ Mode: `Privileged Exec Mode`
▶ Privilege Level: `Operator`
▶ Format: `network protocol <P-1>`

Parameter	Value	Meaning
P-1	none	No network config protocol
	bootp	BOOTP
	dhcp	DHCP

32.1.2   network parms

Set network address, netmask and gateway
▶ Mode: `Privileged Exec Mode`
▶ Privilege Level: `Operator`
▶ Format: `network parms <P-1> <P-2> [<P-3>]`

Parameter	Value	Meaning
P-1	A.B.C.D	IP address.
P-2	A.B.C.D	IP address.
P-3	A.B.C.D	IP address.

32.2 clear

Clear several items.

32.2.1 clear arp-table-switch

Clear the agent's ARP table (cache).
- ▶ Mode: `Privileged Exec Mode`
- ▶ Privilege Level: `Operator`
- ▶ Format: `clear arp-table-switch`

32.3   show

Display device options and settings.

32.3.1   show network parms

Show network settings.
- ▶ Mode: `Command is in all modes available.`
- ▶ Privilege Level: `Guest`
- ▶ Format: `show network parms`

32.4   show

Display device options and settings.

32.4.1   show arp

Show ARP table.
- ▶ Mode: `Command is in all modes available.`
- ▶ Privilege Level: `Guest`
- ▶ Format: `show arp`

33 Link Backup

33.1 link-backup

Configure Link Backup parameters.

33.1.1 link-backup operation

Enable or disable Link Backup.
▶ Mode: `Global Config Mode`
▶ Privilege Level: `Administrator`
▶ Format: `link-backup operation`

■ **no link-backup operation**
 Disable the option
  ▶ Mode: `Global Config Mode`
  ▶ Privilege Level: `Administrator`
  ▶ Format: `no link-backup operation`

33.2 link-backup

Configure Link Backup parameters.

33.2.1 link-backup add

Add a Link Backup interface pair.
- ▶ Mode: `Interface Range Mode`
- ▶ Privilege Level: `Administrator`
- ▶ Format: `link-backup add <P-1> [failback-time <P-2>] [description <P-3>]`
`[failback-time]`: FailBack time in seconds for the interface pair.
`[description]`: Description for the interface pair.

Parameter	Value	Meaning
P-1	slot no./port no.	
P-2	0..3600	`FailBack time interval.(default: 30)`
P-3	string	`Enter a user-defined text, max. 256 characters.`

33.2.2 link-backup delete

Delete the associated backup interface.
- ▶ Mode: `Interface Range Mode`
- ▶ Privilege Level: `Administrator`
- ▶ Format: `link-backup delete <P-1>`

Parameter	Value	Meaning
P-1	slot no./port no.	

33.2.3   link-backup modify

Modify a Link Backup interface pair.
- ▶ Mode: `Interface Range Mode`
- ▶ Privilege Level: `Administrator`
- ▶ Format: `link-backup modify <P-1> [failback-status <P-2>] [failback-time <P-3>] [description <P-4>] [status <P-5>]`

`[failback-status]`: Modify failback status.(default: enabled)
`[failback-time]`: Modify failback time.(default: 30)
`[description]`: Description for the interface pair.
`[status]`: Enable or disable a Link Backup interface pair entry.

Parameter	Value	Meaning
P-1	slot no./port no.	
P-2	enable	Enable the option.
	disable	Disable the option.
P-3	0..3600	FailBack time interval.(default: 30)
P-4	string	Enter a user-defined text, max. 256 characters.
P-5	enable	Enable the option.
	disable	Disable the option.

33.3 show

Display device options and settings.

33.3.1 show link-backup operation

Display Link Backup global information.
- ▶ Mode: `Command is in all modes available.`
- ▶ Privilege Level: `Guest`
- ▶ Format: `show link-backup operation`

33.3.2 show link-backup pairs

Display Link Backup interface pairs.
- ▶ Mode: `Command is in all modes available.`
- ▶ Privilege Level: `Guest`
- ▶ Format: `show link-backup pairs [<P-1>] [<P-2>]`

Parameter	Value	Meaning
`P-1`	slot no./port no.	
`P-2`	slot no./port no.	

34 Link Layer Discovery Protocol (LLDP)

34.1 lldp

Configure of Link Layer Discovery Protocol.

34.1.1 lldp operation

Enable or disable the LLDP operational state.
▶ Mode: `Global Config Mode`
▶ Privilege Level: `Operator`
▶ Format: `lldp operation`

■ no lldp operation
Disable the option
▶ Mode: `Global Config Mode`
▶ Privilege Level: `Operator`
▶ Format: `no lldp operation`

34.1.2 lldp config chassis admin-state

Enable or disable the LLDP operational state.
▶ Mode: `Global Config Mode`
▶ Privilege Level: `Operator`
▶ Format: `lldp config chassis admin-state <P-1>`

Parameter	Value	Meaning
P-1	enable	Enable the option.
	disable	Disable the option.

34.1.3 lldp config chassis notification-interval

Enter the LLDP notification interval in seconds.
- ▶ Mode: `Global Config Mode`
- ▶ Privilege Level: `Operator`
- ▶ Format: `lldp config chassis notification-interval <P-1>`

Paramete r	Value	Meaning
P-1	5..3600	Enter a number in the given range.

34.1.4 lldp config chassis re-init-delay

Enter the LLDP re-initialization delay in seconds.
- ▶ Mode: `Global Config Mode`
- ▶ Privilege Level: `Operator`
- ▶ Format: `lldp config chassis re-init-delay <P-1>`

Paramete r	Value	Meaning
P-1	1..10	Enter a number in the given range.

34.1.5 lldp config chassis tx-delay

Enter the LLDP transmit delay in seconds (tx-delay smaller than (0.25 × tx-interval))
- ▶ Mode: `Global Config Mode`
- ▶ Privilege Level: `Operator`
- ▶ Format: `lldp config chassis tx-delay <P-1>`

Paramete r	Value	Meaning
P-1	1..8192	Enter a number in the given range (tx-delay smaller than (0.25 × tx-interval)

34.1.6 lldp config chassis tx-hold-multiplier

Enter the LLDP transmit hold multiplier.
▶ Mode: `Global Config Mode`
▶ Privilege Level: `Operator`
▶ Format: `lldp config chassis tx-hold-multiplier <P-1>`

Parameter	Value	Meaning
P-1	2..10	Enter a number in the given range.

34.1.7 lldp config chassis tx-interval

Enter the LLDP transmit interval in seconds.
▶ Mode: `Global Config Mode`
▶ Privilege Level: `Operator`
▶ Format: `lldp config chassis tx-interval <P-1>`

Parameter	Value	Meaning
P-1	5..32768	Enter a number in the given range.

34.2　show

Display device options and settings.

34.2.1　show lldp global

Display the LLDP global configurations.
▶ Mode: `Command is in all modes available.`
▶ Privilege Level: `Guest`
▶ Format: `show lldp global`

34.2.2　show lldp port

Display port specific LLDP configurations.
▶ Mode: `Command is in all modes available.`
▶ Privilege Level: `Guest`
▶ Format: `show lldp port [<P-1>]`

Paramete r	Value	Meaning
`P-1`	slot no./port no.	

34.2.3　show lldp remote-data

Remote information collected with LLDP.
▶ Mode: `Command is in all modes available.`
▶ Privilege Level: `Guest`
▶ Format: `show lldp remote-data [<P-1>]`

Paramete r	Value	Meaning
`P-1`	slot no./port no.	

34.3 lldp

Configure of Link Layer Discovery Protocol on a port.

34.3.1 lldp admin-state

Configure how the interface processes LLDP frames.
- ▶ Mode: `Interface Range Mode`
- ▶ Privilege Level: `Operator`
- ▶ Format: `lldp admin-state <P-1>`

Parameter	Value	Meaning
P-1	tx-only	Interface will only transmit LLDP frames. Received frames are not processed.
	rx-only	Interface will only receive LLDP frames. Frames are not transmitted.
	tx-and-rx	Interface will transmit and receive LLDP frames. This is the default setting.
	disable	Interface will neither transmit nor process received LLDP frames.

34.3.2 lldp fdb-mode

Configure the LLDP FDB mode for this interface.
- ▶ Mode: `Interface Range Mode`
- ▶ Privilege Level: `Operator`
- ▶ Format: `lldp fdb-mode <P-1>`

Parameter	Value	Meaning
P-1	lldp-only	Collected remote data will be based on received LLDP frames only.
	mac-only	Collected remote data will be based on the switch's FDB entries only.
	both	Collected remote data will be based on received LLDP frames as well as on the switch's FDB entries.
	auto-detect	As long as no LLDP frames are received, the collected remote data will be based on the switch's FDB entries only. After the first LLDP frame is received, the remote data will be based on received LLDP frames only. This is the default setting.

34.3.3 lldp max-neighbors

Enter the LLDP max neighbors for interface.
▶ Mode: `Interface Range Mode`
▶ Privilege Level: `Operator`
▶ Format: `lldp max-neighbors <P-1>`

Paramete r	Value	Meaning
P-1	1..50	Enter a number in the given range.

34.3.4 lldp notification

Enable or disable the LLDP notification operation for interface.
▶ Mode: `Interface Range Mode`
▶ Privilege Level: `Operator`
▶ Format: `lldp notification`

■ **no lldp notification**
Disable the option
▶ Mode: `Interface Range Mode`
▶ Privilege Level: `Operator`
▶ Format: `no lldp notification`

34.3.5 lldp tlv inline-power

Enable or disable inline-power TLV transmission.
▶ Mode: `Interface Range Mode`
▶ Privilege Level: `Operator`
▶ Format: `lldp tlv inline-power <P-1>`

Paramete r	Value	Meaning
P-1	[cr]	Enable the Bit.

■ **no lldp tlv inline-power**
Disable the option
▶ Mode: `Interface Range Mode`
▶ Privilege Level: `Operator`
▶ Format: `no lldp tlv inline-power <P-1>`

34.3.6 lldp tlv link-aggregation

Enable or disable link-aggregation TLV transmission.
▶ Mode: Interface Range Mode
▶ Privilege Level: Operator
▶ Format: lldp tlv link-aggregation <P-1>

Paramete r	Value	Meaning
P-1	[cr]	Enable the Bit.

■ no lldp tlv link-aggregation
Disable the option
▶ Mode: Interface Range Mode
▶ Privilege Level: Operator
▶ Format: no lldp tlv link-aggregation <P-1>

34.3.7 lldp tlv mac-phy-config-state

Enable or disable mac-phy-config-state TLV transmission.
▶ Mode: Interface Range Mode
▶ Privilege Level: Operator
▶ Format: lldp tlv mac-phy-config-state <P-1>

Paramete r	Value	Meaning
P-1	[cr]	Enable the Bit.

■ no lldp tlv mac-phy-config-state
Disable the option
▶ Mode: Interface Range Mode
▶ Privilege Level: Operator
▶ Format: no lldp tlv mac-phy-config-state <P-1>

34.3.8 lldp tlv max-frame-size

Enable or disable max-frame-size TLV transmission.
▶ Mode: Interface Range Mode
▶ Privilege Level: Operator
▶ Format: lldp tlv max-frame-size <P-1>

Paramete r	Value	Meaning
P-1	[cr]	Enable the Bit.

■ no lldp tlv max-frame-size
Disable the option
▶ Mode: `Interface Range Mode`
▶ Privilege Level: `Operator`
▶ Format: `no lldp tlv max-frame-size <P-1>`

34.3.9 lldp tlv mgmt-addr

Enable or disable mgmt-addr TLV transmission.
▶ Mode: `Interface Range Mode`
▶ Privilege Level: `Operator`
▶ Format: `lldp tlv mgmt-addr`

■ no lldp tlv mgmt-addr
Disable the option
▶ Mode: `Interface Range Mode`
▶ Privilege Level: `Operator`
▶ Format: `no lldp tlv mgmt-addr`

34.3.10 lldp tlv port-desc

Enable or disable port description TLV transmission.
▶ Mode: `Interface Range Mode`
▶ Privilege Level: `Operator`
▶ Format: `lldp tlv port-desc <P-1>`

Paramete r	Value	Meaning
P-1	[cr]	Enable the Bit.

■ **no lldp tlv port-desc**
Disable the option
- ▶ Mode: `Interface Range Mode`
- ▶ Privilege Level: `Operator`
- ▶ Format: `no lldp tlv port-desc <P-1>`

34.3.11 lldp tlv port-vlan

Enable or disable port-vlan TLV transmission.
- ▶ Mode: `Interface Range Mode`
- ▶ Privilege Level: `Operator`
- ▶ Format: `lldp tlv port-vlan`

■ **no lldp tlv port-vlan**
Disable the option
- ▶ Mode: `Interface Range Mode`
- ▶ Privilege Level: `Operator`
- ▶ Format: `no lldp tlv port-vlan`

34.3.12 lldp tlv protocol

Enable or disable protocol TLV transmission.
- ▶ Mode: `Interface Range Mode`
- ▶ Privilege Level: `Operator`
- ▶ Format: `lldp tlv protocol`

■ **no lldp tlv protocol**
Disable the option
- ▶ Mode: `Interface Range Mode`
- ▶ Privilege Level: `Operator`
- ▶ Format: `no lldp tlv protocol`

34.3.13 lldp tlv sys-cap

Enable or disable system capabilities TLV transmission.
▶ Mode: `Interface Range Mode`
▶ Privilege Level: `Operator`
▶ Format: `lldp tlv sys-cap <P-1>`

Parameter	Value	Meaning
P-1	[cr]	Enable the Bit.

■ **no lldp tlv sys-cap**
Disable the option
▶ Mode: `Interface Range Mode`
▶ Privilege Level: `Operator`
▶ Format: `no lldp tlv sys-cap <P-1>`

34.3.14 lldp tlv sys-desc

Enable or disable system description TLV transmission.
▶ Mode: `Interface Range Mode`
▶ Privilege Level: `Operator`
▶ Format: `lldp tlv sys-desc <P-1>`

Parameter	Value	Meaning
P-1	[cr]	Enable the Bit.

■ **no lldp tlv sys-desc**
Disable the option
▶ Mode: `Interface Range Mode`
▶ Privilege Level: `Operator`
▶ Format: `no lldp tlv sys-desc <P-1>`

34.3.15 lldp tlv sys-name

Enable or disable system name TLV transmission.
▶ Mode: `Interface Range Mode`
▶ Privilege Level: `Operator`
▶ Format: `lldp tlv sys-name <P-1>`

Paramete r	Value	Meaning
P-1	[cr]	Enable the Bit.

■ **no lldp tlv sys-name**
Disable the option
▶ Mode: `Interface Range Mode`
▶ Privilege Level: `Operator`
▶ Format: `no lldp tlv sys-name <P-1>`

34.3.16 lldp tlv vlan-name

Enable or disable vlan name TLV transmission.
▶ Mode: `Interface Range Mode`
▶ Privilege Level: `Operator`
▶ Format: `lldp tlv vlan-name`

■ **no lldp tlv vlan-name**
Disable the option
▶ Mode: `Interface Range Mode`
▶ Privilege Level: `Operator`
▶ Format: `no lldp tlv vlan-name`

34.3.17 lldp tlv protocol-based-vlan

Enable or disable protocol-based vlan TLV transmission.
▶ Mode: `Interface Range Mode`
▶ Privilege Level: `Operator`
▶ Format: `lldp tlv protocol-based-vlan`

■ **no lldp tlv protocol-based-vlan**
Disable the option
▶ Mode: `Interface Range Mode`
▶ Privilege Level: `Operator`
▶ Format: `no lldp tlv protocol-based-vlan`

34.3.18 lldp tlv igmp

Enable or disable igmp TLV transmission.
- ▶ Mode: `Interface Range Mode`
- ▶ Privilege Level: `Operator`
- ▶ Format: `lldp tlv igmp`

■ no lldp tlv igmp
Disable the option
- ▶ Mode: `Interface Range Mode`
- ▶ Privilege Level: `Operator`
- ▶ Format: `no lldp tlv igmp`

34.3.19 lldp tlv portsec

Enable or disable portsec TLV transmission.
- ▶ Mode: `Interface Range Mode`
- ▶ Privilege Level: `Operator`
- ▶ Format: `lldp tlv portsec`

■ no lldp tlv portsec
Disable the option
- ▶ Mode: `Interface Range Mode`
- ▶ Privilege Level: `Operator`
- ▶ Format: `no lldp tlv portsec`

34.3.20 lldp tlv ptp

Enable or disable PTP TLV transmission.
- ▶ Mode: `Interface Range Mode`
- ▶ Privilege Level: `Operator`
- ▶ Format: `lldp tlv ptp`

■ **no lldp tlv ptp**
Disable the option
▶ Mode: `Interface Range Mode`
▶ Privilege Level: `Operator`
▶ Format: `no lldp tlv ptp`

35 Media Endpoint Discovery LLDP-MED

35.1 lldp

Configure of Link Layer Discovery Protocol on a port.

35.1.1 lldp med confignotification

Enable or disable LLDP-MED notification send for this interface.
▶ Mode: `Interface Range Mode`
▶ Privilege Level: `Operator`
▶ Format: `lldp med confignotification`

■ no lldp med confignotification
Disable the option
▶ Mode: `Interface Range Mode`
▶ Privilege Level: `Operator`
▶ Format: `no lldp med confignotification`

35.1.2 lldp med transmit-tlv capabilities

Include/Exclude LLDP MED capabilities TLV.
▶ Mode: `Interface Range Mode`
▶ Privilege Level: `Operator`
▶ Format: `lldp med transmit-tlv capabilities`

■ no lldp med transmit-tlv capabilities
Disable the option
▶ Mode: `Interface Range Mode`
▶ Privilege Level: `Operator`
▶ Format: `no lldp med transmit-tlv capabilities`

35.1.3 lldp med transmit-tlv network-policy

Include/Exclude LLDP network policy TLV.
- ▶ Mode: `Interface Range Mode`
- ▶ Privilege Level: `Operator`
- ▶ Format: `lldp med transmit-tlv network-policy`

- ■ **no lldp med transmit-tlv network-policy**
  Disable the option
  - ▶ Mode: `Interface Range Mode`
  - ▶ Privilege Level: `Operator`
  - ▶ Format: `no lldp med transmit-tlv network-policy`

35.2   lldp

Configure of Link Layer Discovery Protocol.

35.2.1   lldp med faststartrepeatcount

Configure LLDP-MED fast start repeat count.
▶ **Mode:** `Global Config Mode`
▶ **Privilege Level:** `Operator`
▶ **Format:** `lldp med faststartrepeatcount <P-1>`

Paramete r	Value	Meaning
P-1	1..10	Enter a value representing the number of LLDP PDUs that will be transmitted.Default is 3.

35.3 show

Display device options and settings.

35.3.1 show lldp med global

Display a summary of the current LLDP-MED configuration.
- ▶ Mode: `Command is in all modes available.`
- ▶ Privilege Level: `Guest`
- ▶ Format: `show lldp med global`

35.3.2 show lldp med interface

Display the current LLDP-MED configuration on a specific port.
- ▶ Mode: `Command is in all modes available.`
- ▶ Privilege Level: `Guest`
- ▶ Format: `show lldp med interface [<P-1>]`

Paramete r	Value	Meaning
`P-1`	slot no./port no.	

35.3.3 show lldp med local-device

Display detailed information about the LLDP-MED data
- ▶ Mode: `Command is in all modes available.`
- ▶ Privilege Level: `Guest`
- ▶ Format: `show lldp med local-device <P-1>`

Paramete r	Value	Meaning
`P-1`	slot no./port no.	

35.3.4   show lldp med remote-device detail

Display LLDP-MED detail configuration for a remote device.
- ▶ Mode: `Command is in all modes available.`
- ▶ Privilege Level: `Guest`
- ▶ Format: `show lldp med remote-device detail <P-1>`

Parameter	Value	Meaning
P-1	slot no./port no.	

35.3.5   show lldp med remote-device summary

Display LLDP-MED summary configuration for a remote device.
- ▶ Mode: `Command is in all modes available.`
- ▶ Privilege Level: `Guest`
- ▶ Format: `show lldp med remote-device summary [<P-1>]`

Parameter	Value	Meaning
P-1	slot no./port no.	

36 Logging

36.1   logging

Logging configuration.

36.1.1   logging audit-trail

Add a comment for the audit trail.
▶ Mode: `Global Config Mode`
▶ Privilege Level: `Administrator`
▶ Format: `logging audit-trail <P-1>`

Paramete r	Value	Meaning
P-1	string	Enter a user-defined text, max. 80 characters.

36.1.2   logging buffered severity

Configure the minimum severity level to be logged to the high priority buffer.
▶ Mode: `Global Config Mode`
▶ Privilege Level: `Administrator`
▶ Format: `logging buffered severity <P-1>`

Paramete r	Value	Meaning
P-1	emergency	System is unusable. System failure has occurred.
	alert	Action must be taken immediately. Unrecoverable failure of a component. System failure likely.
	critical	Recoverable failure of a component that may lead to system failure.
	error	Error conditions. Recoverable failure of a component.
	warning	Minor failure, e.g. misconfiguration of a component.
	notice	Normal but significant conditions.
	informational	Informational messages.
	debug	Debug-level messages.
	0	Same as emergency
	1	Same as alert
	2	Same as critical
	3	Same as error
	4	Same as warning
	5	Same as notice
	6	Same as informational
	7	Same as debug

36.1.3 logging host add

Add a new logging host.
- ▶ Mode: `Global Config Mode`
- ▶ Privilege Level: `Administrator`
- ▶ Format: `logging host add <P-1> addr <P-2> <P-3> [transport <P-4>] [port <P-5>] [severity <P-6>] [type <P-7>]`

`addr`: Enter the IP address of the server.
`[transport]`: Configure the type of transport used for syslog server transmission.
`[port]`: Enter the port used for syslog server transmission.
`[severity]`: Configure the minimum severity level to be sent to this syslog server.
`[type]`: Configure the type of log messages to be sent to the syslog server.

Parameter	Value	Meaning
P-1	1..8	`Syslog server entry index`
P-2	string	Hostname or IP address.
P-3	a.b.c.d	IP address.
P-4	udp	`The UDP-based transmission.`
	tls	`The TLS-based transmission.`
P-5	1..65535	`Port number to be used`
P-6	emergency	`System is unusable. System failure has occurred.`
	alert	`Action must be taken immediately. Unrecoverable failure of a component. System failure likely.`
	critical	`Recoverable failure of a component that may lead to system failure.`
	error	`Error conditions. Recoverable failure of a component.`
	warning	`Minor failure, e.g. misconfiguration of a component.`
	notice	`Normal but significant conditions.`
	informational	`Informational messages.`
	debug	`Debug-level messages.`
	0	`Same as emergency`
	1	`Same as alert`
	2	`Same as critical`
	3	`Same as error`
	4	`Same as warning`
	5	`Same as notice`
	6	`Same as informational`
	7	`Same as debug`
P-7	systemlog	`the system event log entries`
	audittrail	`the audit trail log entries`

36.1.4 logging host delete

Delete a logging host.
- ▶ Mode: `Global Config Mode`
- ▶ Privilege Level: `Administrator`
- ▶ Format: `logging host delete <P-1>`

Parameter	Value	Meaning
P-1	1..8	`Syslog server entry index`

36.1.5 logging host enable

Enable a logging host.
▶ Mode: `Global Config Mode`
▶ Privilege Level: `Administrator`
▶ Format: `logging host enable <P-1>`

Parameter	Value	Meaning
P-1	1..8	Syslog server entry index

36.1.6 logging host disable

Disable a logging host.
▶ Mode: `Global Config Mode`
▶ Privilege Level: `Administrator`
▶ Format: `logging host disable <P-1>`

Parameter	Value	Meaning
P-1	1..8	Syslog server entry index

36.1.7 logging host modify

Modify an existing logging host.
▶ Mode: `Global Config Mode`
▶ Privilege Level: `Administrator`
▶ Format: `logging host modify <P-1> [addr <P-2> <P-3>] [transport <P-4>] [port <P-5>] [severity <P-6>] [type <P-7>]`
`[addr]`: Enter the IP address of the server.
`[transport]`: Configure the type of transport used for syslog server transmission.
`[port]`: Enter the port used for syslog server transmission.
`[severity]`: Configure the minimum severity level to be sent to this syslog server.
`[type]`: Configure the type of log messages to be sent to the syslog server.

Parameter	Value	Meaning
P-1	1..8	Syslog server entry index
P-2	string	Hostname or IP address.
P-3	a.b.c.d	IP address.
P-4	udp	The UDP-based transmission.
	tls	The TLS-based transmission.
P-5	1..65535	Port number to be used

Paramete r	Value	Meaning
P-6	emergency	System is unusable. System failure has occurred.
	alert	Action must be taken immediately. Unrecoverable failure of a component. System failure likely.
	critical	Recoverable failure of a component that may lead to system failure.
	error	Error conditions. Recoverable failure of a component.
	warning	Minor failure, e.g. misconfiguration of a component.
	notice	Normal but significant conditions.
	informational	Informational messages.
	debug	Debug-level messages.
	0	Same as emergency
	1	Same as alert
	2	Same as critical
	3	Same as error
	4	Same as warning
	5	Same as notice
	6	Same as informational
	7	Same as debug
P-7	systemlog	the system event log entries
	audittrail	the audit trail log entries

36.1.8 logging syslog operation

Enable or disable the syslog client.
▶ Mode: `Global Config Mode`
▶ Privilege Level: `Administrator`
▶ Format: `logging syslog operation`

■ **no logging syslog operation**
Disable the option
  ▶ Mode: `Global Config Mode`
  ▶ Privilege Level: `Administrator`
  ▶ Format: `no logging syslog operation`

36.1.9 logging current-console operation

Enable or disable logging messages to the current remote console.
▶ Mode: `Global Config Mode`
▶ Privilege Level: `Administrator`
▶ Format: `logging current-console operation`

■ **no logging current-console operation**
   Disable the option
   ▶ Mode: `Global Config Mode`
   ▶ Privilege Level: `Administrator`
   ▶ Format: `no logging current-console operation`

36.1.10 logging current-console severity

Configure the minimum severity level to be sent to the current remote console.
▶ Mode: `Global Config Mode`
▶ Privilege Level: `Administrator`
▶ Format: `logging current-console severity <P-1>`

Parameter	Value	Meaning
P-1	emergency	`System is unusable. System failure has occurred.`
	alert	`Action must be taken immediately. Unrecoverable failure of a component. System failure likely.`
	critical	`Recoverable failure of a component that may lead to system failure.`
	error	`Error conditions. Recoverable failure of a component.`
	warning	`Minor failure, e.g. misconfiguration of a component.`
	notice	`Normal but significant conditions.`
	informational	`Informational messages.`
	debug	`Debug-level messages.`
	0	`Same as emergency`
	1	`Same as alert`
	2	`Same as critical`
	3	`Same as error`
	4	`Same as warning`
	5	`Same as notice`
	6	`Same as informational`
	7	`Same as debug`

36.1.11 logging console operation

Enable or disable logging to the local V.24 console.
▶ Mode: `Global Config Mode`
▶ Privilege Level: `Administrator`
▶ Format: `logging console operation`

■ **no logging console operation**
Disable the option
▶ Mode: `Global Config Mode`
▶ Privilege Level: `Administrator`
▶ Format: `no logging console operation`

36.1.12 logging console severity

Configure the minimum severity level to be logged to the V.24 console.
▶ Mode: `Global Config Mode`
▶ Privilege Level: `Administrator`
▶ Format: `logging console severity <P-1>`

Parameter	Value	Meaning
P-1	emergency	`System is unusable. System failure has occurred.`
	alert	`Action must be taken immediately. Unrecoverable failure of a component. System failure likely.`
	critical	`Recoverable failure of a component that may lead to system failure.`
	error	`Error conditions. Recoverable failure of a component.`
	warning	`Minor failure, e.g. misconfiguration of a component.`
	notice	`Normal but significant conditions.`
	informational	`Informational messages.`
	debug	`Debug-level messages.`
	0	`Same as emergency`
	1	`Same as alert`
	2	`Same as critical`
	3	`Same as error`
	4	`Same as warning`
	5	`Same as notice`
	6	`Same as informational`
	7	`Same as debug`

36.1.13 logging persistent operation

Enable or disable persistent logging. This feature is only available when an ENVM is connected to the device. The logging information is saved on the selected ENVM.
▶ Mode: `Global Config Mode`
▶ Privilege Level: `Administrator`
▶ Format: `logging persistent operation`

■ **no logging persistent operation**
Disable the option
▶ Mode: `Global Config Mode`
▶ Privilege Level: `Administrator`
▶ Format: `no logging persistent operation`

36.1.14 logging persistent numfiles

Enter the maximum number of log files.
▶ Mode: `Global Config Mode`
▶ Privilege Level: `Administrator`
▶ Format: `logging persistent numfiles <P-1>`

Paramete r	Value	Meaning
P-1	0..25	number of logfiles

36.1.15 logging persistent filesize

Enter the maximum size of a log file.
▶ Mode: `Global Config Mode`
▶ Privilege Level: `Administrator`
▶ Format: `logging persistent filesize <P-1>`

Paramete r	Value	Meaning
P-1	0..4096	Maximum persistent logfile size on the non-volatile memory in kBytes

36.1.16 logging persistent severity-level

Configure the minimum severity level to be logged into files.
▶ Mode: `Global Config Mode`
▶ Privilege Level: `Administrator`
▶ Format: `logging persistent severity-level <P-1>`

Paramete r	Value	Meaning
P-1	emergency	System is unusable. System failure has occurred.
	alert	Action must be taken immediately. Unrecoverable failure of a component. System failure likely.
	critical	Recoverable failure of a component that may lead to system failure.
	error	Error conditions. Recoverable failure of a component.
	warning	Minor failure, e.g. misconfiguration of a component.
	notice	Normal but significant conditions.
	informational	Informational messages.
	debug	Debug-level messages.
	0	Same as emergency
	1	Same as alert
	2	Same as critical
	3	Same as error
	4	Same as warning
	5	Same as notice
	6	Same as informational
	7	Same as debug

36.1.17 logging email operation

Enable or disable logging email-alert globally.
▶ Mode: `Global Config Mode`
▶ Privilege Level: `Administrator`
▶ Format: `logging email operation`

■ no logging email operation
Disable the option
▶ Mode: `Global Config Mode`
▶ Privilege Level: `Administrator`
▶ Format: `no logging email operation`

36.1.18 logging email from-addr

Configure mail address used by device to send email-alert.
▶ Mode: `Global Config Mode`
▶ Privilege Level: `Administrator`
▶ Format: `logging email from-addr <P-1>`

Paramete r	Value	Meaning
P-1	string	Enter a valid email address

36.1.19 logging email duration

Periodic timer (in minutes) to send an non-critical logs in mail.
▶ Mode: Global Config Mode
▶ Privilege Level: Administrator
▶ Format: logging email duration <P-1>

Paramete r	Value	Meaning
P-1	30..1440	Time duration in minutes

36.1.20 logging email severity urgent

Urgent severity level
▶ Mode: Global Config Mode
▶ Privilege Level: Administrator
▶ Format: logging email severity urgent <P-1>

Paramete r	Value	Meaning
P-1	emergency	System is unusable. System failure has occurred.
	alert	Action must be taken immediately. Unrecoverable failure of a component. System failure likely.
	critical	Recoverable failure of a component that may lead to system failure.
	error	Error conditions. Recoverable failure of a component.
	warning	Minor failure, e.g. misconfiguration of a component.
	notice	Normal but significant conditions.
	informational	Informational messages.
	debug	Debug-level messages.
	0	Same as emergency
	1	Same as alert
	2	Same as critical
	3	Same as error
	4	Same as warning
	5	Same as notice
	6	Same as informational
	7	Same as debug

36.1.21 logging email severity non-urgent

Non-urgent severity level
▶ Mode: `Global Config Mode`
▶ Privilege Level: `Administrator`
▶ Format: `logging email severity non-urgent <P-1>`

Parameter	Value	Meaning
P-1	emergency	System is unusable. System failure has occurred.
	alert	Action must be taken immediately. Unrecoverable failure of a component. System failure likely.
	critical	Recoverable failure of a component that may lead to system failure.
	error	Error conditions. Recoverable failure of a component.
	warning	Minor failure, e.g. misconfiguration of a component.
	notice	Normal but significant conditions.
	informational	Informational messages.
	debug	Debug-level messages.
	0	Same as emergency
	1	Same as alert
	2	Same as critical
	3	Same as error
	4	Same as warning
	5	Same as notice
	6	Same as informational
	7	Same as debug

36.1.22 logging email to-addr add

Create a destination address entry with default values
▶ Mode: `Global Config Mode`
▶ Privilege Level: `Administrator`
▶ Format: `logging email to-addr add <P-1> [addr <P-2>] [msgtype <P-3>]`
`[addr]`: Create an entry with specified address
`[msgtype]`: Create an entry with specified message type

Parameter	Value	Meaning
P-1	1..10	Destination address entry index
P-2	string	Enter a valid email address
P-3	urgent	Urgent message type
	non-urgent	Non-urgent message type

36.1.23 logging email to-addr delete

Delete a destination address
▶ **Mode:** `Global Config Mode`
▶ **Privilege Level:** `Administrator`
▶ **Format:** `logging email to-addr delete <P-1>`

Paramete r	Value	Meaning
P-1	1..10	Destination address entry index

36.1.24 logging email to-addr modify

Modify a destination address
▶ **Mode:** `Global Config Mode`
▶ **Privilege Level:** `Administrator`
▶ **Format:** `logging email to-addr modify <P-1> [addr <P-2>] [msgtype <P-3>]`
`[addr]`: Modify the destination address
`[msgtype]`: Modify the message type

Paramete r	Value	Meaning
P-1	1..10	Destination address entry index
P-2	string	Enter a valid email address
P-3	urgent	Urgent message type
	non-urgent	Non-urgent message type

36.1.25 logging email mail-server add

Add a server entry to SMTP address table
▶ **Mode:** `Global Config Mode`
▶ **Privilege Level:** `Administrator`
▶ **Format:** `logging email mail-server add <P-1> [addr <P-2>] [security <P-3>] [username <P-4>] [password <P-5>] [port <P-6>] [timeout <P-7>] [description <P-8>]`
`[addr]`: SMTP server address
`[security]`: Security mode used in SMTP server.
`[username]`: Login ID to access SMTP server.
`[password]`: Password to access SMTP server.
`[port]`: SMTP server port number.
`[timeout]`: SMTP server connection timeout
`[description]`: SMTP server description

Paramete r	Value	Meaning
P-1	1..5	SMTP server index
P-2	string	Hostname or IP address.
P-3	none	Security mode none
	tlsv1	Security mode TLSv1
P-4	string	Enter a user-defined text, max. 32 characters.
P-5	string	Enter a user-defined text, max. 32 characters.
P-6	1..65535	Port number to be used
P-7	1..15	SMTP server timeout range
P-8	string	Enter a user-defined text, max. 1024 characters (allowed characters are from ASCII 32 to 127).

36.1.26 logging email mail-server delete

Delete a server entry from SMTP address table
▶ Mode: `Global Config Mode`
▶ Privilege Level: `Administrator`
▶ Format: `logging email mail-server delete <P-1>`

Paramete r	Value	Meaning
P-1	1..5	SMTP server index

36.1.27 logging email mail-server modify

Modify an SMTP server entry
▶ Mode: `Global Config Mode`
▶ Privilege Level: `Administrator`
▶ Format: `logging email mail-server modify <P-1> [addr <P-2>] [security <P-3>] [username <P-4>] [password <P-5>] [port <P-6>] [timeout <P-7>] [description <P-8>]`

`[addr]`: SMTP server address
`[security]`: Security mode used in SMTP server.
`[username]`: Login ID to access SMTP server.
`[password]`: Password to access SMTP server.
`[port]`: SMTP server port number.
`[timeout]`: SMTP Timeout
`[description]`: SMTP server description

Paramete r	Value	Meaning
P-1	1..5	SMTP server index
P-2	string	Hostname or IP address.

Paramete r	Value	Meaning
P-3	none	Security mode none
	tlsv1	Security mode TLSv1
P-4	string	Enter a user-defined text, max. 32 characters.
P-5	string	Enter a user-defined text, max. 32 characters.
P-6	1..65535	Port number to be used
P-7	1..15	SMTP server timeout range
P-8	string	Enter a user-defined text, max. 1024 characters (allowed characters are from ASCII 32 to 127).

36.1.28 logging email subject add

Create an email subject entry
▶ Mode: Global Config Mode
▶ Privilege Level: Administrator
▶ Format: logging email subject add <P-1> [<P-2>]

Paramete r	Value	Meaning
P-1	urgent	Urgent message type
	non-urgent	Non-urgent message type
P-2	string	<string> Enter the email subject (Within double quotations if subject includes space)

36.1.29 logging email subject delete

Delete an email subject entry
▶ Mode: Global Config Mode
▶ Privilege Level: Administrator
▶ Format: logging email subject delete <P-1>

Paramete r	Value	Meaning
P-1	urgent	Urgent message type
	non-urgent	Non-urgent message type

36.1.30 logging email subject modify

Modify an email subject entry
▶ Mode: `Global Config Mode`
▶ Privilege Level: `Administrator`
▶ Format: `logging email subject modify <P-1> <P-2>`

Parameter	Value	Meaning
P-1	urgent	`Urgent message type`
	non-urgent	`Non-urgent message type`
P-2	string	`<string> Enter the email subject (Within double quotations if subject includes space)`

36.1.31 logging email test msgtype

Configure the message type for test mail.
▶ Mode: `Global Config Mode`
▶ Privilege Level: `Administrator`
▶ Format: `logging email test msgtype <P-1> <P-2>`

Parameter	Value	Meaning
P-1	urgent	`Urgent message type`
	non-urgent	`Non-urgent message type`
P-2	string	`Enter a user-defined text, max. 255 characters.`

36.2 show

Display device options and settings.

36.2.1 show logging buffered

Display buffered (in-memory) log entries.
- ▶ Mode: `Command is in all modes available.`
- ▶ Privilege Level: `Guest`
- ▶ Format: `show logging buffered [<P-1>]`

Parameter	Value	Meaning
P-1	string	`<filter>` Enter a comma separated list of severity ranges, numbers or enum strings are allowed. Example: 0-1,informational-debug

36.2.2 show logging traplogs

Display trap log entries.
- ▶ Mode: `Command is in all modes available.`
- ▶ Privilege Level: `Guest`
- ▶ Format: `show logging traplogs`

36.2.3 show logging console

Display console logging configurations.
- ▶ Mode: `Command is in all modes available.`
- ▶ Privilege Level: `Guest`
- ▶ Format: `show logging console`

36.2.4 show logging persistent

Display persistent logging configurations.
- ▶ Mode: `Command is in all modes available.`
- ▶ Privilege Level: `Guest`
- ▶ Format: `show logging persistent [logfiles]`

`[logfiles]`: List the persistent log files.

36.2.5 show logging syslog

Display current syslog operational setting.
- ▶ Mode: `Command is in all modes available.`
- ▶ Privilege Level: `Guest`
- ▶ Format: `show logging syslog`

36.2.6 show logging host

Display a list of logging hosts currently configured.
- ▶ Mode: `Command is in all modes available.`
- ▶ Privilege Level: `Guest`
- ▶ Format: `show logging host`

36.2.7 show logging email statistics

Display the statistics of email logging.
- ▶ Mode: `Command is in all modes available.`
- ▶ Privilege Level: `Guest`
- ▶ Format: `show logging email statistics`

36.2.8 show logging email global

Display global settings of email logging feature.
▶ Mode: `Command is in all modes available.`
▶ Privilege Level: `Guest`
▶ Format: `show logging email global`

36.2.9 show logging email to-addr

Display list of destination addresses configured.
▶ Mode: `Command is in all modes available.`
▶ Privilege Level: `Guest`
▶ Format: `show logging email to-addr [<P-1>]`

Parameter	Value	Meaning
P-1	1..10	Destination address entry index

36.2.10 show logging email subject

Display the subject entries configured.
▶ Mode: `Command is in all modes available.`
▶ Privilege Level: `Guest`
▶ Format: `show logging email subject [<P-1>]`

Parameter	Value	Meaning
P-1	urgent	Urgent message type
	non-urgent	Non-urgent message type

36.2.11 show logging email mail-server

Display SMTP server settings.
▶ Mode: `Command is in all modes available.`
▶ Privilege Level: `Guest`
▶ Format: `show logging email mail-server [<P-1>]`

Paramete r	Value	Meaning
P-1	1..5	SMTP server index

36.3 copy

Copy different kinds of items.

36.3.1 copy eventlog buffered envm

Copy a buffered log from the device to external non-volatile memory.
- ▶ Mode: `Privileged Exec Mode`
- ▶ Privilege Level: `Operator`
- ▶ Format: `copy eventlog buffered envm <P-1>`

Parameter	Value	Meaning
P-1	string	Enter a user-defined text, max. 32 characters.

36.3.2 copy eventlog buffered remote

Copy a buffered log from the device to a file server.
- ▶ Mode: `Privileged Exec Mode`
- ▶ Privilege Level: `Operator`
- ▶ Format: `copy eventlog buffered remote <P-1>`

Parameter	Value	Meaning
P-1	string	Enter a user-defined text, max. 128 characters.

36.3.3 copy eventlog persistent

Copy the persistent logs from the device to an envm or a file server.
- ▶ Mode: `Privileged Exec Mode`
- ▶ Privilege Level: `Operator`
- ▶ Format: `copy eventlog persistent <P-1> envm <P-2> remote <P-3>`

`envm`: Copy the persistent log from the device to external non-volatile memory.
`remote`: Copy the persistent logs from the device to a file server.

Paramete r	Value	Meaning
P-1	string	Enter a user-defined text, max. 32 characters.
P-2	string	Enter a user-defined text, max. 32 characters.
P-3	string	Enter a user-defined text, max. 128 characters.

36.3.4   copy traplog system envm

Copy the traplog from the device to external non-volatile memory.
▶ Mode: Privileged Exec Mode
▶ Privilege Level: Operator
▶ Format: copy traplog system envm <P-1>

Paramete r	Value	Meaning
P-1	string	Enter a user-defined text, max. 32 characters.

36.3.5   copy traplog system remote

Copy the traplog from the device to a file server
▶ Mode: Privileged Exec Mode
▶ Privilege Level: Operator
▶ Format: copy traplog system remote <P-1>

Paramete r	Value	Meaning
P-1	string	Enter a user-defined text, max. 128 characters.

36.3.6   copy audittrail system envm

Copy the audit trail from the device to external non-volatile memory.
▶ Mode: Privileged Exec Mode
▶ Privilege Level: Operator, Auditor
▶ Format: copy audittrail system envm <P-1>

Paramete r	Value	Meaning
P-1	string	Enter a user-defined text, max. 32 characters.

36.3.7 copy audittrail system remote

Copy the audit trail from the device to a file server.
▶ Mode: `Privileged Exec Mode`
▶ Privilege Level: `Operator, Auditor`
▶ Format: `copy audittrail system remote <P-1>`

Paramete r	Value	Meaning
P-1	string	Enter a user-defined text, max. 128 characters.

36.3.8 copy mailcacert remote

Copy CA certificate file (*.pem) from the remote AD server to the specified destination.
▶ Mode: `Privileged Exec Mode`
▶ Privilege Level: `Administrator`
▶ Format: `copy mailcacert remote <P-1> nvm [<P-2>]`
`nvm`: Copy CA certificate file (*.pem) from the remote AD server to the device.

Paramete r	Value	Meaning
P-1	string	Enter a user-defined text, max. 128 characters.
P-2	string	Enter a user-defined text, max. 100 characters.

36.3.9 copy mailcacert envm

Copy CA certificate file (*.pem) from external non-volatile memory to the specified destination.
▶ Mode: `Privileged Exec Mode`
▶ Privilege Level: `Administrator`
▶ Format: `copy mailcacert envm <P-1> nvm [<P-2>]`
`nvm`: Copy CA certificate file (*.pem) from external non-volatile memory to the device.

Paramete r	Value	Meaning
P-1	string	Enter a user-defined text, max. 128 characters.
P-2	string	Enter a user-defined text, max. 100 characters.

36.3.10 copy syslogcacert remote

Copy CA certificate file (*.pem) from the remote AD server to the specified destination.
▶ Mode: `Privileged Exec Mode`
▶ Privilege Level: `Administrator`
▶ Format: `copy syslogcacert remote <P-1> nvm [<P-2>]`
`nvm`: Copy CA certificate file (*.pem) from the remote AD server to the device.

Parameter	Value	Meaning
P-1	string	Enter a user-defined text, max. 128 characters.
P-2	string	Enter a user-defined text, max. 100 characters.

36.3.11 copy syslogcacert envm

Copy CA certificate file (*.pem) from external non-volatile memory to the specified destination.
▶ Mode: `Privileged Exec Mode`
▶ Privilege Level: `Administrator`
▶ Format: `copy syslogcacert envm <P-1> nvm [<P-2>]`
`nvm`: Copy CA certificate file (*.pem) from external non-volatile memory to the device.

Parameter	Value	Meaning
P-1	string	Enter a user-defined text, max. 128 characters.
P-2	string	Enter a user-defined text, max. 100 characters.

36.4 clear

Clear several items.

36.4.1 clear logging buffered

Clear buffered log from memory.
▶ Mode: `Privileged Exec Mode`
▶ Privilege Level: `Administrator`
▶ Format: `clear logging buffered`

36.4.2 clear logging persistent

Clear persistent log from memory.
▶ Mode: `Privileged Exec Mode`
▶ Privilege Level: `Administrator`
▶ Format: `clear logging persistent`

36.4.3 clear logging email statistics

Clear email statistics
▶ Mode: `Privileged Exec Mode`
▶ Privilege Level: `Administrator`
▶ Format: `clear logging email statistics`

36.4.4 clear eventlog

Clear the event log entries from memory.
- ▶ Mode: `Privileged Exec Mode`
- ▶ Privilege Level: `Administrator`
- ▶ Format: `clear eventlog`

37 Management Access

37.1 network

Configure the inband and outband connectivity.

37.1.1 network management access web timeout

Set the web interface idle timeout.
▶ **Mode:** `Privileged Exec Mode`
▶ **Privilege Level:** `Administrator`
▶ **Format:** `network management access web timeout <P-1>`

Paramete r	Value	Meaning
P-1	0..160	Idle timeout of a session in minutes (default: 5).

37.1.2 network management access add

Add a new entry with index.
▶ **Mode:** `Privileged Exec Mode`
▶ **Privilege Level:** `Administrator`
▶ **Format:** `network management access add <P-1> [ip <P-2>] [mask <P-3>] [http <P-4>] [https <P-5>] [snmp <P-6>] [telnet <P-7>] [iec61850-mms <P-8>] [modbus-tcp <P-9>] [ssh <P-10>] [ethernet-ip <P-11>] [profinet-io <P-12>]`
`[ip]:` Configure IP address which should have access to management.
`[mask]:` Configure network mask to allow a subnet for management access.
`[http]:` Configure if HTTP is allowed to have management access.
`[https]:` Configure if HTTPS is allowed to have management access.
`[snmp]:` Configure if SNMP is allowed to have management access.
`[telnet]:` Configure if TELNET is allowed to have management access.
`[iec61850-mms]:` Configure if IEC61850-MMS is allowed to have management access.
`[modbus-tcp]:` Configure if Modbus TCP/IP is allowed to have management access.
`[ssh]:` Configure if SSH is allowed to have management access.
`[ethernet-ip]:` Configure if EtherNet/IP is allowed to have management access.
`[profinet-io]:` Configure if PROFINET is allowed to have management access.

Paramete r	Value	Meaning
P-1	1..16	Pool entry index.
P-2	a.b.c.d	IP address.
P-3	0..32	Prefix length netmask.
P-4	enable	Enable the option.
	disable	Disable the option.

Paramete r	Value	Meaning
P-5	enable	Enable the option.
	disable	Disable the option.
P-6	enable	Enable the option.
	disable	Disable the option.
P-7	enable	Enable the option.
	disable	Disable the option.
P-8	enable	Enable the option.
	disable	Disable the option.
P-9	enable	Enable the option.
	disable	Disable the option.
P-10	enable	Enable the option.
	disable	Disable the option.
P-11	enable	Enable the option.
	disable	Disable the option.
P-12	enable	Enable the option.
	disable	Disable the option.

37.1.3 network management access delete

Delete an entry with index.
▶ Mode: `Privileged Exec Mode`
▶ Privilege Level: `Administrator`
▶ Format: `network management access delete <P-1>`

Paramete r	Value	Meaning
P-1	1..16	Pool entry index.

37.1.4 network management access modify

Modify an entry with index.
▶ Mode: `Privileged Exec Mode`
▶ Privilege Level: `Administrator`
▶ Format: `network management access modify <P-1> ip <P-2> mask <P-3> http <P-4> https <P-5> snmp <P-6> telnet <P-7> iec61850-mms <P-8> modbus-tcp <P-9> ssh <P-10> ethernet-ip <P-11> profinet-io <P-12>`

`ip`: Configure ip-address which should have access to management.
`mask`: Configure network mask to allow a subnet for management access.
`http`: Configure if HTTP is allowed to have management access.
`https`: Configure if HTTPS is allowed to have management access.
`snmp`: Configure if SNMP is allowed to have management access.
`telnet`: Configure if TELNET is allowed to have management access.

`iec61850-mms`: Configure if IEC61850-MMS is allowed to have management access.
`modbus-tcp`: Configure if Modbus TCP/IP is allowed to have management access.
`ssh`: Configure if SSH is allowed to have management access.
`ethernet-ip`: Configure if EtherNet/IP is allowed to have management access.
`profinet-io`: Configure if PROFINET is allowed to have management access.

Parameter	Value	Meaning
P-1	1..16	Pool entry index.
P-2	a.b.c.d	IP address.
P-3	0..32	Prefix length netmask.
P-4	enable	Enable the option.
	disable	Disable the option.
P-5	enable	Enable the option.
	disable	Disable the option.
P-6	enable	Enable the option.
	disable	Disable the option.
P-7	enable	Enable the option.
	disable	Disable the option.
P-8	enable	Enable the option.
	disable	Disable the option.
P-9	enable	Enable the option.
	disable	Disable the option.
P-10	enable	Enable the option.
	disable	Disable the option.
P-11	enable	Enable the option.
	disable	Disable the option.
P-12	enable	Enable the option.
	disable	Disable the option.

37.1.5   network management access operation

Enable/Disable operation for RMA.
▶ Mode: `Privileged Exec Mode`
▶ Privilege Level: `Administrator`
▶ Format: `network management access operation`

■ **no network management access operation**
Disable the option
▶ Mode: `Privileged Exec Mode`
▶ Privilege Level: `Administrator`
▶ Format: `no network management access operation`

37.1.6   network management access status

Activate/Deactivate an entry.
▶ Mode: `Privileged Exec Mode`
▶ Privilege Level: `Administrator`
▶ Format: `network management access status <P-1>`

Paramete r	Value	Meaning
P-1	1..16	Pool entry index.

■ **no network management access status**
Disable the option
▶ Mode: `Privileged Exec Mode`
▶ Privilege Level: `Administrator`
▶ Format: `no network management access status <P-1>`

37.2 show

Display device options and settings.

37.2.1 show network management access global

Show global restricted management access preferences.
- ▶ Mode: `Command is in all modes available.`
- ▶ Privilege Level: `Guest`
- ▶ Format: `show network management access global`

37.2.2 show network management access rules

Show restricted management access rules.
- ▶ Mode: `Command is in all modes available.`
- ▶ Privilege Level: `Guest`
- ▶ Format: `show network management access rules [<P-1>]`

Parameter	Value	Meaning
P-1	1..16	Pool entry index.

38 Management Address

38.1 network

Configure the inband and outband connectivity.

38.1.1 network management mac

Configure the locally administered MAC address.
- ▶ Mode: `Privileged Exec Mode`
- ▶ Privilege Level: `Operator`
- ▶ Format: `network management mac [local-address <P-1>]`

`[local-address]:` Enter the local admin MAC address (xx:xx:xx:xx:xx:xx).If the local address is nonzero, the device starts with this MAC address at the next boot. If the MAC address is changed, they must be stored by the configuration manager. A MAC address with a set multicast bit will not be accepted

Parameter	Value	Meaning
P-1	aa:bb:cc:dd:ee:ff	MAC address.

38.1.2 network management port

Configure management access per port. Setting to 'all' will allowed access from all ports.
- ▶ Mode: `Privileged Exec Mode`
- ▶ Privilege Level: `Operator`
- ▶ Format: `network management port <P-1>`

Parameter	Value	Meaning
P-1	all or slot no./port no.	

38.2 show

Display device options and settings.

38.2.1 show network management mac

Displays the MAC address settings.
▶ **Mode:** `Command is in all modes available.`
▶ **Privilege Level:** `Guest`
▶ **Format:** `show network management mac`

38.2.2 show network management port

Show the management access port.
▶ **Mode:** `Command is in all modes available.`
▶ **Privilege Level:** `Guest`
▶ **Format:** `show network management port`

39 Modbus

39.1 modbus-tcp

Configure Modbus TCP/IP server settings.

39.1.1 modbus-tcp operation

Enable or disable the Modbus TCP/IP server.
▶ **Mode:** `Global Config Mode`
▶ **Privilege Level:** `Operator`
▶ **Format:** `modbus-tcp operation`

■ no modbus-tcp operation
Disable the option
▶ **Mode:** `Global Config Mode`
▶ **Privilege Level:** `Operator`
▶ **Format:** `no modbus-tcp operation`

39.1.2 modbus-tcp write-access

Enable or disable the write-access on Modbus TCP/IP registers. - Possible security risk, as Modbus TCP/IP communication is not authenticated - .
▶ **Mode:** `Global Config Mode`
▶ **Privilege Level:** `Operator`
▶ **Format:** `modbus-tcp write-access`

■ no modbus-tcp write-access
Disable the option
▶ **Mode:** `Global Config Mode`
▶ **Privilege Level:** `Operator`
▶ **Format:** `no modbus-tcp write-access`

39.1.3   modbus-tcp port

Defines the port number of the Modbus TCP/IP server (default: 502).
▶ **Mode:** `Global Config Mode`
▶ **Privilege Level:** `Operator`
▶ **Format:** `modbus-tcp port <P-1>`

Paramete r	Value	Meaning
P-1	1..65535	Enter port number between 1 and 65535

39.1.4   modbus-tcp max-sessions

Defines the maximum number of concurrent Modbus TCP/IP sessions (default: 5).
▶ **Mode:** `Global Config Mode`
▶ **Privilege Level:** `Operator`
▶ **Format:** `modbus-tcp max-sessions <P-1>`

Paramete r	Value	Meaning
P-1	1..5	Maximum number of concurrent Modbus TCP/IP server sessions (default: 5).

39.2 show

Display device options and settings.

39.2.1 show modbus-tcp

Show the Modbus TCP/IP server settings.
- ▶ **Mode:** `Command is in all modes available.`
- ▶ **Privilege Level:** `Guest`
- ▶ **Format:** `show modbus-tcp`

40 Media Redundancy Protocol (MRP)

40.1 mrp

Configure the MRP settings.

40.1.1 mrp domain modify advanced-mode

Configure the MRM Advanced Mode.
▶ **Mode:** `Global Config Mode`
▶ **Privilege Level:** `Operator`
▶ **Format:** `mrp domain modify advanced-mode <P-1>`

Paramete r	Value	Meaning
P-1	enable	Enable the option.
	disable	Disable the option.

40.1.2 mrp domain modify manager-priority

Configure the MRM priority.
▶ **Mode:** `Global Config Mode`
▶ **Privilege Level:** `Operator`
▶ **Format:** `mrp domain modify manager-priority <P-1>`

Paramete r	Value	Meaning
P-1	0..65535	Enter the MRM priority (default: 32768).

40.1.3 mrp domain modify mode

Configure the role of the MRP device.
▶ **Mode:** `Global Config Mode`
▶ **Privilege Level:** `Operator`
▶ **Format:** `mrp domain modify mode <P-1>`

Paramete r	Value	Meaning
P-1	client	The device will be in the role of a ring client (MRC).
	manager	The device will be in the role of a ring manager (MRM).

40.1.4   mrp domain modify name

Configure the logical name of the MRP domain.
▶ Mode: `Global Config Mode`
▶ Privilege Level: `Operator`
▶ Format: `mrp domain modify name <P-1>`

Paramete r	Value	Meaning
P-1	string	Enter a user-defined text, max. 255 characters.

40.1.5   mrp domain modify operation

Enable or disable the MRP function.
▶ Mode: `Global Config Mode`
▶ Privilege Level: `Operator`
▶ Format: `mrp domain modify operation <P-1>`

Paramete r	Value	Meaning
P-1	enable	Enable the option.
	disable	Disable the option.

40.1.6   mrp domain modify port primary

Configure the primary ringport.
▶ Mode: `Global Config Mode`
▶ Privilege Level: `Operator`
▶ Format: `mrp domain modify port primary <P-1>`

Paramete r	Value	Meaning
P-1	slot no./port no.	

40.1.7 mrp domain modify port secondary

Configure the secondary ringport.
▶ Mode: `Global Config Mode`
▶ Privilege Level: `Operator`
▶ Format: `mrp domain modify port secondary <P-1> [fixed-backup <P-2>]`
`[fixed-backup]`: Enable or disable the secondary ringport of the manager to be the backup port permanently.

Parameter	Value	Meaning
P-1	slot no./port no.	
P-2	enable	Enable the option.
	disable	Disable the option.

40.1.8 mrp domain modify recovery-delay

Configure the MRM Recovery Delay.
▶ Mode: `Global Config Mode`
▶ Privilege Level: `Operator`
▶ Format: `mrp domain modify recovery-delay <P-1>`

Parameter	Value	Meaning
P-1	500ms	Maximum recovery delay of 500ms in the MRP domain.
	200ms	Maximum recovery delay of 200ms in the MRP domain.
	30ms	Maximum recovery delay of 30ms in the MRP domain.
	10ms	Maximum recovery delay of 10ms in the MRP domain.

40.1.9 mrp domain modify round-trip-delay

Configure the round-trip-delay counters.
▶ Mode: `Global Config Mode`
▶ Privilege Level: `Operator`
▶ Format: `mrp domain modify round-trip-delay <P-1>`

Parameter	Value	Meaning
P-1	reset	Reset the round-trip-delay counters.

40.1.10 mrp domain modify vlan

Configure the VLAN identifier of the MRP domain.\n(VLAN ID 0 means that no VLAN is used).
- ▶ Mode: `Global Config Mode`
- ▶ Privilege Level: `Operator`
- ▶ Format: `mrp domain modify vlan <P-1>`

Paramete r	Value	Meaning
P-1	0..4042	VLAN identifier of the MRP domain.\n(VLAN ID 0 means that no VLAN is used).

40.1.11 mrp domain add default-domain

Default MRP domain ID.
- ▶ Mode: `Global Config Mode`
- ▶ Privilege Level: `Operator`
- ▶ Format: `mrp domain add default-domain`

40.1.12 mrp domain add domain-id

MRP domain ID. Format: 16 bytes in decimal notation.\n(Example:
1.2.3.4.5.6.7.8.9.10.11.12.13.14.15.16).
- ▶ Mode: `Global Config Mode`
- ▶ Privilege Level: `Operator`
- ▶ Format: `mrp domain add domain-id <P-1>`

Paramete r	Value	Meaning
P-1	string	<domain id> MRP domain ID. Format: 16 bytes in decimal notation.\n(Example: 1.2.3.4.5.6.7.8.9.10.11.12.13.14.15.16).

40.1.13 mrp domain delete

Delete the current MRP domain.
- ▶ Mode: `Global Config Mode`
- ▶ Privilege Level: `Operator`
- ▶ Format: `mrp domain delete`

40.1.14 mrp operation

Enable or disable MRP.
- ▶ Mode: `Global Config Mode`
- ▶ Privilege Level: `Operator`
- ▶ Format: `mrp operation`

■ no mrp operation
Disable the option
- ▶ Mode: `Global Config Mode`
- ▶ Privilege Level: `Operator`
- ▶ Format: `no mrp operation`

40.2 show

Display device options and settings.

40.2.1 show mrp

Show MRP settings.
- ▶ **Mode:** `Command is in all modes available.`
- ▶ **Privilege Level:** `Guest`
- ▶ **Format:** `show mrp`

41   MRP IEEE

41.1 mrp-ieee

Configure IEEE MRP parameters and protocols, MVRP for dynamic VLAN registration and MMRP for dynamic MAC registration on a port.

41.1.1 mrp-ieee global join-time

Set the IEEE multiple registration protocol join time-interval. The join timer controls the interval between join message transmissions sent to applicant state machines. An instance of this timer is required on a per-Port, per-MRP participant basis.
- ▶ Mode: `Interface Range Mode`
- ▶ Privilege Level: `Operator`
- ▶ Format: `mrp-ieee global join-time <P-1>`

Parameter	Value	Meaning
P-1	10..100	Join time-interval in centi-seconds.

41.1.2 mrp-ieee global leave-time

Set the IEEE multiple registration protocol leave time-interval. The leave timer controls the period of time that the registrar state machine waits in the leave state before transiting to the empty state. An instance of the timer is required for each state machine in the leave state.
- ▶ Mode: `Interface Range Mode`
- ▶ Privilege Level: `Operator`
- ▶ Format: `mrp-ieee global leave-time <P-1>`

Parameter	Value	Meaning
P-1	20..600	Leave time-interval in centi-seconds.

41.1.3 mrp-ieee global leave-all-time

Set the IEEE multiple registration protocol leave-all time-interval. The leave all timer controls the frequency with which the leaveall state machine generates leaveall PDUs. The timer is required on a per-Port, per-MRP Participant basis.

▶ Mode: `Interface Range Mode`
▶ Privilege Level: `Operator`
▶ Format: `mrp-ieee global leave-all-time <P-1>`

Parameter	Value	Meaning
P-1	200..6000	Leave-All time-interval in centi-seconds.

41.2 show

Display device options and settings.

41.2.1 show mrp-ieee global interface

Show the global configuration of IEEE multiple registration protocol per interface.
- ▶ Mode: `Command is in all modes available.`
- ▶ Privilege Level: `Guest`
- ▶ Format: `show mrp-ieee global interface [<P-1>]`

Parameter	Value	Meaning
P-1	slot no./port no.	

42 MRP IEEE MMRP

42.1 mrp-ieee

Configure IEEE MRP protocols.

42.1.1 mrp-ieee mmrp vlan-id

Configure the VLAN parameters.
- ▶ Mode: `VLAN Database Mode`
- ▶ Privilege Level: `Operator`
- ▶ Format: `mrp-ieee mmrp vlan-id <P-1> forward-all <P-2> forbidden-servicereq <P-3>`

`forward-all`: Enable or disable 'Forward All Groups' in a given Vlan for a given interface.
`forbidden-servicereq`: Enable or disable the mmrp feature 'Forbidden Service Requirement' in a given Vlan for a given interface.

Parameter	Value	Meaning
P-1	1..4042	Enter the VLAN ID.
P-2	slot no./port no.	
P-3	slot no./port no.	

■ no mrp-ieee mmrp vlan-id
Disable the option
- ▶ Mode: `VLAN Database Mode`
- ▶ Privilege Level: `Operator`
- ▶ Format: `no mrp-ieee mmrp vlan-id <P-1> forward-all <P-2> forbidden-servicereq <P-3>`

42.2 show

Display device options and settings.

42.2.1 show mrp-ieee mmrp global

Display the IEEE MMRP global configuration.
- ▶ Mode: `Command is in all modes available.`
- ▶ Privilege Level: `Guest`
- ▶ Format: `show mrp-ieee mmrp global`

42.2.2 show mrp-ieee mmrp interface

Display the IEEE MMRP interface configuration.
- ▶ Mode: `Command is in all modes available.`
- ▶ Privilege Level: `Guest`
- ▶ Format: `show mrp-ieee mmrp interface [<P-1>]`

Parameter	Value	Meaning
`P-1`	slot no./port no.	

42.2.3 show mrp-ieee mmrp statistics global

Display the IEEE MMRP global statistics.
- ▶ Mode: `Command is in all modes available.`
- ▶ Privilege Level: `Guest`
- ▶ Format: `show mrp-ieee mmrp statistics global`

42.2.4   show mrp-ieee mmrp statistics interface

Display the IEEE MMRP interface statistics.
- ▶ Mode: `Command is in all modes available.`
- ▶ Privilege Level: `Guest`
- ▶ Format: `show mrp-ieee mmrp statistics interface [<P-1>]`

Parameter	Value	Meaning
P-1	slot no./port no.	

42.2.5   show mrp-ieee mmrp service-requirement forward-all vlan

Show Forward-All setting for port in given VLAN.
- ▶ Mode: `Command is in all modes available.`
- ▶ Privilege Level: `Guest`
- ▶ Format: `show mrp-ieee mmrp service-requirement forward-all vlan [<P-1>]`

Parameter	Value	Meaning
P-1	1..4042	Enter the VLAN ID.

42.2.6   show mrp-ieee mmrp service-requirement forbidden vlan

Show Forward-All setting for port in given VLAN.
- ▶ Mode: `Command is in all modes available.`
- ▶ Privilege Level: `Guest`
- ▶ Format: `show mrp-ieee mmrp service-requirement forbidden vlan [<P-1>]`

Parameter	Value	Meaning
P-1	1..4042	Enter the VLAN ID.

42.3 mrp-ieee

Configure IEEE MRP protocols, MVRP for dynamic VLAN registration and MMRP for dynamic MAC registration.

42.3.1 mrp-ieee mmrp operation

Enable or disable MMRP globally. Devices use MMRP information for dynamic registration of group membership and individual MAC addresses with end devices and switches that support extended filtering services, within the connected LAN.
- ▶ Mode: `Global Config Mode`
- ▶ Privilege Level: `Operator`
- ▶ Format: `mrp-ieee mmrp operation`

■ **no mrp-ieee mmrp operation**
  Disable the option
  - ▶ Mode: `Global Config Mode`
  - ▶ Privilege Level: `Operator`
  - ▶ Format: `no mrp-ieee mmrp operation`

42.3.2 mrp-ieee mmrp periodic-machine

Enable or disable MMRP periodic state machine globally. When enabled, the periodic state machine sends extra MMRP messages when the periodic timer expires.
- ▶ Mode: `Global Config Mode`
- ▶ Privilege Level: `Operator`
- ▶ Format: `mrp-ieee mmrp periodic-machine`

■ **no mrp-ieee mmrp periodic-machine**
  Disable the option
  - ▶ Mode: `Global Config Mode`
  - ▶ Privilege Level: `Operator`
  - ▶ Format: `no mrp-ieee mmrp periodic-machine`

42.4   clear

Clear several items.

42.4.1   clear mrp-ieee mmrp

Clear the IEEE MMRP global and port statistic tables.
- ▶ Mode: `Privileged Exec Mode`
- ▶ Privilege Level: `Operator`
- ▶ Format: `clear mrp-ieee mmrp`

42.5   mrp-ieee

Configure IEEE MRP parameters and protocols, MVRP for dynamic VLAN registration and MMRP for dynamic MAC registration on a port.

42.5.1   mrp-ieee mmrp operation

Enable or disable MMRP on the interface, with MMRP enabled globally and on this interface, the device sends and receives MMRP messages on this port.
- ▶ Mode: `Interface Range Mode`
- ▶ Privilege Level: `Operator`
- ▶ Format: `mrp-ieee mmrp operation`

■ no mrp-ieee mmrp operation
Disable the option
- ▶ Mode: `Interface Range Mode`
- ▶ Privilege Level: `Operator`
- ▶ Format: `no mrp-ieee mmrp operation`

42.5.2   mrp-ieee mmrp restrict-register

Enable or disable restriction of dynamic mac address registration using IEEE MMRP on the port. When enabled, the dynamic registration of mac address attributes is allowed only if the attribute has already been statically registered on the device.
- ▶ Mode: `Interface Range Mode`
- ▶ Privilege Level: `Operator`
- ▶ Format: `mrp-ieee mmrp restrict-register`

■ no mrp-ieee mmrp restrict-register
Disable the option
- ▶ Mode: `Interface Range Mode`
- ▶ Privilege Level: `Operator`
- ▶ Format: `no mrp-ieee mmrp restrict-register`

42.6 show

Display device options and settings.

42.6.1 show mac-filter-table mmrp

Display MMRP entries in the MFDB table.
- ▶ **Mode:** `Command is in all modes available.`
- ▶ **Privilege Level:** `Guest`
- ▶ **Format:** `show mac-filter-table mmrp`

43   MRP IEEE MVRP

43.1 mrp-ieee

Configure IEEE MRP protocols, MVRP for dynamic VLAN registration and MMRP for dynamic MAC registration.

43.1.1 mrp-ieee mvrp operation

Enable or disable IEEE MVRP globally. When enabled, the device distributes VLAN membership information on MVRP enable active ports. MVRP-aware devices use the information to dynamically create VLAN members and update the local VLAN member database.
- ▶ Mode: `Global Config Mode`
- ▶ Privilege Level: `Operator`
- ▶ Format: `mrp-ieee mvrp operation`

■ no mrp-ieee mvrp operation
Disable the option
- ▶ Mode: `Global Config Mode`
- ▶ Privilege Level: `Operator`
- ▶ Format: `no mrp-ieee mvrp operation`

43.1.2 mrp-ieee mvrp periodic-machine

Enable or disable IEEE MVRP periodic state machine globally. When enabled, the device sends MVRP messages to the connected MVRP-aware devices when the periodic timer expires.
- ▶ Mode: `Global Config Mode`
- ▶ Privilege Level: `Operator`
- ▶ Format: `mrp-ieee mvrp periodic-machine`

■ no mrp-ieee mvrp periodic-machine
Disable the option
- ▶ Mode: `Global Config Mode`
- ▶ Privilege Level: `Operator`
- ▶ Format: `no mrp-ieee mvrp periodic-machine`

43.2 mrp-ieee

Configure IEEE MRP parameters and protocols, MVRP for dynamic VLAN registration and MMRP for dynamic MAC registration on a port.

43.2.1 mrp-ieee mvrp operation

Enable or disable IEEE MVRP on the port. When enabled, globally and on this port, the device distributes VLAN membership information to MVRP aware devices connected to this port.
▶ Mode: `Interface Range Mode`
▶ Privilege Level: `Operator`
▶ Format: `mrp-ieee mvrp operation`

■ **no mrp-ieee mvrp operation**
  Disable the option
  ▶ Mode: `Interface Range Mode`
  ▶ Privilege Level: `Operator`
  ▶ Format: `no mrp-ieee mvrp operation`

43.2.2 mrp-ieee mvrp restrict-register

Enable or disable restriction of dynamic VLAN registration using IEEE MVRP on the port. When enabled, the dynamic registration of VLAN attributes is allowed only if the attribute has already been statically registered on the device.
▶ Mode: `Interface Range Mode`
▶ Privilege Level: `Operator`
▶ Format: `mrp-ieee mvrp restrict-register`

■ **no mrp-ieee mvrp restrict-register**
  Disable the option
  ▶ Mode: `Interface Range Mode`
  ▶ Privilege Level: `Operator`
  ▶ Format: `no mrp-ieee mvrp restrict-register`

43.3 show

Display device options and settings.

43.3.1 show mrp-ieee mvrp global

Display the IEEE MVRP global configuration.
- ▶ Mode: `Command is in all modes available.`
- ▶ Privilege Level: `Guest`
- ▶ Format: `show mrp-ieee mvrp global`

43.3.2 show mrp-ieee mvrp interface

Display the IEEE MVRP interface configuration.
- ▶ Mode: `Command is in all modes available.`
- ▶ Privilege Level: `Guest`
- ▶ Format: `show mrp-ieee mvrp interface [<P-1>]`

Paramete r	Value	Meaning
`P-1`	slot no./port no.	

43.3.3 show mrp-ieee mvrp statistics global

Display the IEEE MVRP global statistics.
- ▶ Mode: `Command is in all modes available.`
- ▶ Privilege Level: `Guest`
- ▶ Format: `show mrp-ieee mvrp statistics global`

43.3.4   show mrp-ieee mvrp statistics interface

Display the IEEE MVRP interface statistics.
▶ Mode: `Command is in all modes available.`
▶ Privilege Level: `Guest`
▶ Format: `show mrp-ieee mvrp statistics interface [<P-1>]`

Parameter	Value	Meaning
`P-1`	slot no./port no.	

43.4 clear

Clear several items.

43.4.1 clear mrp-ieee mvrp

Clear the IEEE MVRP global and port statistic tables.
- ▶ Mode: `Privileged Exec Mode`
- ▶ Privilege Level: `Operator`
- ▶ Format: `clear mrp-ieee mvrp`

44 Out-of-band Management

44.1   network

Configure the inband and outband connectivity.

44.1.1   network out-of-band operation

Enable or disable the out-of-band management.
▶ **Mode:** `Privileged Exec Mode`
▶ **Privilege Level:** `Operator`
▶ **Format:** `network out-of-band operation`

■ **no network out-of-band operation**
   Disable the option
   ▶ **Mode:** `Privileged Exec Mode`
   ▶ **Privilege Level:** `Operator`
   ▶ **Format:** `no network out-of-band operation`

44.1.2   network out-of-band protocol

Select DHCP or none as the out-of-band configuration protocol.
▶ **Mode:** `Privileged Exec Mode`
▶ **Privilege Level:** `Operator`
▶ **Format:** `network out-of-band protocol <P-1>`

Parameter	Value	Meaning
P-1	none	`No out-of-band config protocol.`
	dhcp	`DHCP`

44.1.3 network out-of-band parms

Set out-of-band IP address, subnet mask and gateway.

▶ Mode: `Privileged Exec Mode`
▶ Privilege Level: `Operator`
▶ Format: `network out-of-band parms <P-1> <P-2> [<P-3>]`

Parameter	Value	Meaning
P-1	A.B.C.D	IP address.
P-2	A.B.C.D	IP address.
P-3	A.B.C.D	IP address.

44.2　show

Display device options and settings.

45   Protocol Based VLAN

45.1 vlan

Creation and configuration of VLANS.

45.1.1 vlan protocol group add

Add a new group or add protocols to an existing group.
▶ Mode: `VLAN Database Mode`
▶ Privilege Level: `Operator`
▶ Format: `vlan protocol group add <P-1> name <P-2> vlan-id <P-3> ethertype <P-4>`

`name`: Assign a group name .
`vlan-id`: Associate a VLAN ID to a group.
`ethertype`: Add protocols to an existing group. Before adding protocols to a group please create one.

Parameter	Value	Meaning
P-1	1..128	Protocol based VLANs group index.
P-2	string	Enter a user-defined text, max. 256 characters.
P-3	1..4042	Enter the VLAN ID.
P-4	string	<protocol-list> Enter a comma-separated list of mnemonics or values, max. 256 chars (eg.: 1536-65535, ip, arp, ipx). Hexadecimal values are entered with a leading \'0x\', eg. 0x600-0xffff.

■ **no vlan protocol group add**
Disable the option
▶ Mode: `VLAN Database Mode`
▶ Privilege Level: `Operator`
▶ Format: `no vlan protocol group add name vlan-id ethertype <P-4>`

45.1.2 vlan protocol group modify

Modify a protocol group.
▶ Mode: `VLAN Database Mode`
▶ Privilege Level: `Operator`
▶ Format: `vlan protocol group modify <P-1> [name <P-2>] [vlan-id <P-3>] [ethertype <P-4>]`

`[name]`: Modify the group name.
`[vlan-id]`: Modify the VLAN ID of a group.

[ethertype]: Modify ethertypes from a protocol group.

Paramete r	Value	Meaning
P-1	1..128	Protocol based VLANs group index.
P-2	string	Enter a user-defined text, max. 256 characters.
P-3	1..4042	Enter the VLAN ID.
P-4	string	<protocol-list> Enter a comma-separated list of mnemonics or values, max. 256 chars (eg.: 1536-65535, ip, arp, ipx). Hexadecimal values are entered with a leading \'0x\', eg. 0x600-0xffff.

45.1.3   vlan protocol group delete

Delete a protocol group.
▶ Mode: VLAN Database Mode
▶ Privilege Level: Operator
▶ Format: vlan protocol group delete <P-1> [ethertype <P-2>]
[ethertype]: Remove ethertypes from a protocol group.

Paramete r	Value	Meaning
P-1	1..128	Protocol based VLANs group index.
P-2	string	<protocol-list> Enter a comma-separated list of mnemonics or values, max. 256 chars (eg.: 1536-65535, ip, arp, ipx). Hexadecimal values are entered with a leading \'0x\', eg. 0x600-0xffff.

45.2 vlan

Configure 802.1Q port parameters for VLANs.

45.2.1 vlan protocol group add

Add this interface to a group.
▶ Mode: `Interface Range Mode`
▶ Privilege Level: `Operator`
▶ Format: `vlan protocol group add <P-1>`

Parameter	Value	Meaning
P-1	1..128	Protocol based VLANs group index.

45.2.2 vlan protocol group delete

Remove this interface from a group.
▶ Mode: `Interface Range Mode`
▶ Privilege Level: `Operator`
▶ Format: `vlan protocol group delete <P-1>`

Parameter	Value	Meaning
P-1	1..128	Protocol based VLANs group index.

45.3 show

Display device options and settings.

46 Port Monitor

46.1 port-monitor

Configure the Port Monitor condition settings.

46.1.1 port-monitor operation

Enable or disable the port monitor.
▶ Mode: `Global Config Mode`
▶ Privilege Level: `Operator`
▶ Format: `port-monitor operation`

■ **no port-monitor operation**
   Disable the option
   ▶ Mode: `Global Config Mode`
   ▶ Privilege Level: `Operator`
   ▶ Format: `no port-monitor operation`

46.2 port-monitor

Configure the Port Monitor condition settings.

46.2.1 port-monitor condition crc-fragments interval

Configure the measure interval in seconds (5-180s) for CRC-Fragment detection. Default 10.
- ▶ Mode: `Interface Range Mode`
- ▶ Privilege Level: `Operator`
- ▶ Format: `port-monitor condition crc-fragments interval <P-1>`

Parameter	Value	Meaning
P-1	5..180	Enter a number in the given range.

46.2.2 port-monitor condition crc-fragments count

Configure the CRC-Fragment counter in parts per million (1-1000000 [ppm]). Default 1000 [ppm].
- ▶ Mode: `Interface Range Mode`
- ▶ Privilege Level: `Operator`
- ▶ Format: `port-monitor condition crc-fragments count <P-1>`

Parameter	Value	Meaning
P-1	1..1000000	Enter a number in the given range.

46.2.3 port-monitor condition crc-fragments mode

Enable or disable CRC-Fragments condition to trigger an action.
- ▶ Mode: `Interface Range Mode`
- ▶ Privilege Level: `Operator`
- ▶ Format: `port-monitor condition crc-fragments mode`

■ **no port-monitor condition crc-fragments mode**
Disable the option
▶ Mode: `Interface Range Mode`
▶ Privilege Level: `Operator`
▶ Format: `no port-monitor condition crc-fragments mode`

46.2.4 port-monitor condition link-flap interval

Configure the measure interval in seconds (1-180s) for Link Flap detection. Default 10.
▶ Mode: `Interface Range Mode`
▶ Privilege Level: `Operator`
▶ Format: `port-monitor condition link-flap interval <P-1>`

Paramete r	Value	Meaning
P-1	1..180	Enter a number in the given range.

46.2.5 port-monitor condition link-flap count

Configure the Link Flap counter (1-100). Default 5.
▶ Mode: `Interface Range Mode`
▶ Privilege Level: `Operator`
▶ Format: `port-monitor condition link-flap count <P-1>`

Paramete r	Value	Meaning
P-1	1..100	Enter a number in the given range.

46.2.6 port-monitor condition link-flap mode

Enable or disable link-flap condition to trigger an action.
▶ Mode: `Interface Range Mode`
▶ Privilege Level: `Operator`
▶ Format: `port-monitor condition link-flap mode`

■ **no port-monitor condition link-flap mode**
Disable the option
▶ Mode: `Interface Range Mode`
▶ Privilege Level: `Operator`
▶ Format: `no port-monitor condition link-flap mode`

46.2.7 port-monitor condition duplex-mismatch mode

Enable or disable duplex mismatch detection condition to trigger an action.
▶ Mode: `Interface Range Mode`
▶ Privilege Level: `Operator`
▶ Format: `port-monitor condition duplex-mismatch mode`

■ **no port-monitor condition duplex-mismatch mode**
Disable the option
▶ Mode: `Interface Range Mode`
▶ Privilege Level: `Operator`
▶ Format: `no port-monitor condition duplex-mismatch mode`

46.2.8 port-monitor condition overload-detection traffic-type

Configure Overload detection condition traffic type.
▶ Mode: `Interface Range Mode`
▶ Privilege Level: `Operator`
▶ Format: `port-monitor condition overload-detection traffic-type <P-1>`

Parameter	Value	Meaning
P-1	all	All packets.
	bc	Broadcast packets.
	bc-mc	Broadcast and multicast packets.

46.2.9   port-monitor condition overload-detection unit

Configure Overload detection condition threshold type.
▶ Mode: `Interface Range Mode`
▶ Privilege Level: `Operator`
▶ Format: `port-monitor condition overload-detection unit <P-1>`

Paramete r	Value	Meaning
P-1	pps	Packets per second.
	kbps	Kilobits per second.

46.2.10   port-monitor condition overload-detection upper-threshold

Configure Overload detection condition threshold type upper-threshold.
▶ Mode: `Interface Range Mode`
▶ Privilege Level: `Operator`
▶ Format: `port-monitor condition overload-detection upper-threshold <P-1>`

Paramete r	Value	Meaning
P-1	0..10000000	Enter a number in the given range.

46.2.11   port-monitor condition overload-detection lower-threshold

Configure Overload detection condition threshold type lower-threshold.
▶ Mode: `Interface Range Mode`
▶ Privilege Level: `Operator`
▶ Format: `port-monitor condition overload-detection lower-threshold <P-1>`

Paramete r	Value	Meaning
P-1	0..10000000	Enter a number in the given range.

46.2.12 port-monitor condition overload-detection polling-interval

Configure Overload detection condition detection interval.
- ▶ Mode: `Interface Range Mode`
- ▶ Privilege Level: `Operator`
- ▶ Format: `port-monitor condition overload-detection polling-interval <P-1>`

Parameter	Value	Meaning
P-1	1..20	Enter a number in the given range.

46.2.13 port-monitor condition overload-detection mode

Enable or disable Overload-Detection condition to trigger an action.
- ▶ Mode: `Interface Range Mode`
- ▶ Privilege Level: `Operator`
- ▶ Format: `port-monitor condition overload-detection mode`

■ **no port-monitor condition overload-detection mode**
   Disable the option
- ▶ Mode: `Interface Range Mode`
- ▶ Privilege Level: `Operator`
- ▶ Format: `no port-monitor condition overload-detection mode`

46.2.14 port-monitor condition speed-duplex mode

Enable or disable link speed and duplex condition to trigger an action.
- ▶ Mode: `Interface Range Mode`
- ▶ Privilege Level: `Operator`
- ▶ Format: `port-monitor condition speed-duplex mode`

■ **no port-monitor condition speed-duplex mode**
   Disable the option
- ▶ Mode: `Interface Range Mode`
- ▶ Privilege Level: `Operator`
- ▶ Format: `no port-monitor condition speed-duplex mode`

46.2.15 port-monitor condition speed-duplex speed

Set speed-duplex combination.
▶ Mode: `Interface Range Mode`
▶ Privilege Level: `Operator`
▶ Format: `port-monitor condition speed-duplex speed [<P-1>] [<P-2>] [<P-3>] [<P-4>] [<P-5>] [<P-6>] [<P-7>]`

Parameter	Value	Meaning
P-1	[hdx10]	10 Mbit/s - half duplex
P-2	[fdx10]	10 Mbit/s - full duplex
P-3	[hdx100]	100 Mbit/s - half duplex
P-4	[fdx100]	100 Mbit/s - full duplex
P-5	[hdx-1000]	1000 Mbit/s - half duplex
P-6	[fdx-1000]	1000 Mbit/s - full duplex
P-7	[fdx-2500]	2500 Mbit/s - full duplex

46.2.16 port-monitor condition speed-duplex clear

Clear the allowed speed-duplex combination list.
▶ Mode: `Interface Range Mode`
▶ Privilege Level: `Operator`
▶ Format: `port-monitor condition speed-duplex clear`

46.2.17 port-monitor action

Enable or disable interface on port condition.
▶ Mode: `Interface Range Mode`
▶ Privilege Level: `Operator`
▶ Format: `port-monitor action <P-1>`

Parameter	Value	Meaning
P-1	port-disable	`Disable interface on port condition.`
	trap-only	`Send only a trap.`
	auto-disable	`Enable or disable interface on port condition by AUTODIS.`

46.2.18 port-monitor reset

Reset the port monitor.
▶ Mode: `Interface Range Mode`
▶ Privilege Level: `Operator`
▶ Format: `port-monitor reset [<P-1>]`

Paramete r	Value	Meaning
P-1	port	Press Enter to execute the command.

■ **no port-monitor reset**

Disable the option
▶ Mode: `Interface Range Mode`
▶ Privilege Level: `Operator`
▶ Format: `no port-monitor reset [<P-1>]`

46.3　show

Display device options and settings.

46.3.1　show port-monitor operation

Display the Port Monitor operation.
▶ Mode: `Command is in all modes available.`
▶ Privilege Level: `Guest`
▶ Format: `show port-monitor operation`

46.3.2　show port-monitor brief

Display the Port Monitor summary.
▶ Mode: `Command is in all modes available.`
▶ Privilege Level: `Guest`
▶ Format: `show port-monitor brief`

46.3.3　show port-monitor overload-detection counters

Display the overload-detection counters of last interval.
▶ Mode: `Command is in all modes available.`
▶ Privilege Level: `Guest`
▶ Format: `show port-monitor overload-detection counters`

46.3.4　show port-monitor overload-detection port

Display the Port Monitor overload detection interface details.
- ▶ Mode: `Command is in all modes available.`
- ▶ Privilege Level: `Guest`
- ▶ Format: `show port-monitor overload-detection port [<P-1>]`

Parameter	Value	Meaning
P-1	slot no./port no.	

46.3.5　show port-monitor speed-duplex

Display the Port Monitor link speed and duplex interface settings.
- ▶ Mode: `Command is in all modes available.`
- ▶ Privilege Level: `Guest`
- ▶ Format: `show port-monitor speed-duplex [<P-1>]`

Parameter	Value	Meaning
P-1	slot no./port no.	

46.3.6　show port-monitor port

Display the Port Monitor interface details.
- ▶ Mode: `Command is in all modes available.`
- ▶ Privilege Level: `Guest`
- ▶ Format: `show port-monitor port <P-1>`

Parameter	Value	Meaning
P-1	slot no./port no.	

46.3.7　show port-monitor link-flap

Display the link-flaps counts for a specific interface.
- ▶ Mode: `Command is in all modes available.`
- ▶ Privilege Level: `Guest`
- ▶ Format: `show port-monitor link-flap <P-1>`

Paramete r	Value	Meaning
P-1	slot no./port no.	

46.3.8 show port-monitor crc-fragments

Display CRC-Fragments counts for a specific interface.
- ▶ Mode: `Command is in all modes available.`
- ▶ Privilege Level: `Guest`
- ▶ Format: `show port-monitor crc-fragments <P-1>`

Paramete r	Value	Meaning
P-1	slot no./port no.	

47 Port Security

47.1 port-security

Port MAC locking/security

47.1.1 port-security operation

Enable/Disable Port MAC locking/security
- ▶ Mode: `Global Config Mode`
- ▶ Privilege Level: `Operator`
- ▶ Format: `port-security operation`

■ **no port-security operation**
Disable the option
- ▶ Mode: `Global Config Mode`
- ▶ Privilege Level: `Operator`
- ▶ Format: `no port-security operation`

47.2 port-security

Port MAC locking/security

47.2.1 port-security operation

Enable/Disable Port MAC locking/security for the interface.
- ▶ Mode: `Interface Range Mode`
- ▶ Privilege Level: `Operator`
- ▶ Format: `port-security operation`

■ **no port-security operation**
  Disable the option
  - ▶ Mode: `Interface Range Mode`
  - ▶ Privilege Level: `Operator`
  - ▶ Format: `no port-security operation`

47.2.2 port-security max-dynamic

Set dynamic limit for the interface.
- ▶ Mode: `Interface Range Mode`
- ▶ Privilege Level: `Operator`
- ▶ Format: `port-security max-dynamic <P-1>`

Paramete r	Value	Meaning
P-1	0..600	maximum number of dynamically locked MAC addresses allowed

47.2.3 port-security max-static

Set Static Limit for the interface.
▶ Mode: `Interface Range Mode`
▶ Privilege Level: `Operator`
▶ Format: `port-security max-static <P-1>`

Paramete r	Value	Meaning
P-1	0..64	maximum number of statically locked MAC addresses allowed

47.2.4 port-security mac-address add

Add Static MAC address to the interface.
▶ Mode: `Interface Range Mode`
▶ Privilege Level: `Operator`
▶ Format: `port-security mac-address add <P-1> <P-2>`

Paramete r	Value	Meaning
P-1	aa:bb:cc:dd:ee:ff	MAC address.
P-2	1..4042	VLAN ID

47.2.5 port-security mac-address move

Make dynamic MAC addresses static for the interface.
▶ Mode: `Interface Range Mode`
▶ Privilege Level: `Operator`
▶ Format: `port-security mac-address move`

47.2.6 port-security mac-address delete

Remove Static MAC address from the interface.
▶ Mode: `Interface Range Mode`
▶ Privilege Level: `Operator`
▶ Format: `port-security mac-address delete <P-1> <P-2>`

Paramete r	Value	Meaning
P-1	aa:bb:cc:dd:ee:ff	MAC address.
P-2	1..4042	VLAN ID

47.2.7 port-security violation-traps

SNMP violation traps for the interface.
▶ Mode: `Interface Range Mode`
▶ Privilege Level: `Operator`
▶ Format: `port-security violation-traps operation [frequency <P-1>]`
`operation`: Enable/Disable SNMP violation traps for the interface.
`[frequency]`: The minimum seconds between two successive violation traps on this port.

Paramete r	Value	Meaning
P-1	0..3600	time in seconds

■ no port-security violation-traps
Disable the option
▶ Mode: `Interface Range Mode`
▶ Privilege Level: `Operator`
▶ Format: `no port-security violation-traps operation [frequency]`

47.3 show

Display device options and settings.

47.3.1 show port-security global

Port Security global status
▶ Mode: `Command is in all modes available.`
▶ Privilege Level: `Guest`
▶ Format: `show port-security global`

47.3.2 show port-security interface

Display port-security (port MAC locking) information for system.
▶ Mode: `Command is in all modes available.`
▶ Privilege Level: `Guest`
▶ Format: `show port-security interface [<P-1>]`

Paramete r	Value	Meaning
`P-1`	slot no./port no.	

47.3.3 show port-security dynamic

Display dynamically learned MAC addresses
▶ Mode: `Command is in all modes available.`
▶ Privilege Level: `Guest`
▶ Format: `show port-security dynamic <P-1>`

Paramete r	Value	Meaning
`P-1`	slot no./port no.	

47.3.4   show port-security static

Display statically locked MAC addresses
▶ Mode: `Command is in all modes available.`
▶ Privilege Level: `Guest`
▶ Format: `show port-security static <P-1>`

Paramete r	Value	Meaning
`P-1`	slot no./port no.	

47.3.5   show port-security violation

Display port security violation information.
▶ Mode: `Command is in all modes available.`
▶ Privilege Level: `Guest`
▶ Format: `show port-security violation <P-1>`

Paramete r	Value	Meaning
`P-1`	slot no./port no.	

48 Password Management

48.1 passwords

Manage password policies and options.

48.1.1 passwords min-length

Set minimum password length for user passwords.
▶ Mode: `Global Config Mode`
▶ Privilege Level: `Administrator`
▶ Format: `passwords min-length <P-1>`

Parameter	Value	Meaning
P-1	1..64	Enter a number in the given range.

48.1.2 passwords max-login-attempts

Set maximum login attempts for the users.
▶ Mode: `Global Config Mode`
▶ Privilege Level: `Administrator`
▶ Format: `passwords max-login-attempts <P-1>`

Parameter	Value	Meaning
P-1	0..5	Enter a number in the given range.

48.1.3 passwords min-uppercase-chars

Set minimum upper case characters for user passwords.
▶ Mode: `Global Config Mode`
▶ Privilege Level: `Administrator`
▶ Format: `passwords min-uppercase-chars <P-1>`

Parameter	Value	Meaning
P-1	0..16	Enter a number in the given range.

48.1.4   passwords min-lowercase-chars

Set minimum lower case characters for user passwords.
▶ Mode: `Global Config Mode`
▶ Privilege Level: `Administrator`
▶ Format: `passwords min-lowercase-chars <P-1>`

Parameter	Value	Meaning
P-1	0..16	Enter a number in the given range.

48.1.5   passwords min-numeric-chars

Set minimum numeric characters for user passwords.
▶ Mode: `Global Config Mode`
▶ Privilege Level: `Administrator`
▶ Format: `passwords min-numeric-chars <P-1>`

Parameter	Value	Meaning
P-1	0..16	Enter a number in the given range.

48.1.6   passwords min-special-chars

Set minimum special characters for user passwords.
▶ Mode: `Global Config Mode`
▶ Privilege Level: `Administrator`
▶ Format: `passwords min-special-chars <P-1>`

Parameter	Value	Meaning
P-1	0..16	Enter a number in the given range.

48.2 show

Display device options and settings.

48.2.1 show passwords

Display password policies and options.
▶ **Mode:** `Command is in all modes available.`
▶ **Privilege Level:** `Administrator`
▶ **Format:** `show passwords`

49 Radius

49.1   authorization

Configure authorization parameters.

49.1.1   authorization network radius

Enable or disable the switch to accept VLAN assignment by the RADIUS server.
▶ **Mode:** `Global Config Mode`
▶ **Privilege Level:** `Administrator`
▶ **Format:** `authorization network radius`

■ **no authorization network radius**
   Disable the option
   ▶ **Mode:** `Global Config Mode`
   ▶ **Privilege Level:** `Administrator`
   ▶ **Format:** `no authorization network radius`

49.2 radius

Configure RADIUS parameters.

49.2.1 radius accounting mode

Enable or disable RADIUS accounting function.
- ▶ Mode: `Global Config Mode`
- ▶ Privilege Level: `Administrator`
- ▶ Format: `radius accounting mode`

■ **no radius accounting mode**
 Disable the option
 - ▶ Mode: `Global Config Mode`
 - ▶ Privilege Level: `Administrator`
 - ▶ Format: `no radius accounting mode`

49.2.2 radius server attribute 4

Specifies the RADIUS client to use the NAS-IP Address attribute in the RADIUS requests.
- ▶ Mode: `Global Config Mode`
- ▶ Privilege Level: `Administrator`
- ▶ Format: `radius server attribute 4 <P-1>`

Paramete r	Value	Meaning
P-1	A.B.C.D	IP address.

49.2.3 radius server acct add

Add a RADIUS accounting server.
▶ Mode: `Global Config Mode`
▶ Privilege Level: `Administrator`
▶ Format: `radius server acct add <P-1> ip <P-2> [name <P-3>] [port <P-4>]`
`ip`: RADIUS accounting server IP address.
`[name]`: RADIUS accounting server name.
`[port]`: RADIUS accounting server port (default: 1813).

Parameter	Value	Meaning
P-1	1..8	Next RADIUS server valid index (it can be seen with '#show radius global' command).
P-2	string	Hostname or IP address.
P-3	string	Enter a user-defined text, max. 32 characters.
P-4	1..65535	Enter port number between 1 and 65535

49.2.4 radius server acct delete

Delete a RADIUS accounting server.
▶ Mode: `Global Config Mode`
▶ Privilege Level: `Administrator`
▶ Format: `radius server acct delete <P-1>`

Parameter	Value	Meaning
P-1	1..8	RADIUS server index.

49.2.5 radius server acct modify

Change a RADIUS accounting server parameters.
▶ Mode: `Global Config Mode`
▶ Privilege Level: `Administrator`
▶ Format: `radius server acct modify <P-1> [name <P-2>] [port <P-3>] [status <P-4>] [secret [<P-5>]] [encrypted <P-6>]`
`[name]`: RADIUS accounting server name.
`[port]`: RADIUS accounting server port (default: 1813).
`[status]`: Enable or disable a RADIUS accounting server entry.
`[secret]`: Configure the shared secret for the RADIUS accounting server.
`[encrypted]`: Configure the encrypted shared secret.

Parameter	Value	Meaning
P-1	1..8	RADIUS server index.
P-2	string	Enter a user-defined text, max. 32 characters.

Parameter	Value	Meaning
P-3	1..65535	Enter port number between 1 and 65535
P-4	enable	Enable the option.
	disable	Disable the option.
P-5	string	Enter a user-defined text, max. 128 characters.
P-6	string	Enter a user-defined text, max. 128 characters.

49.2.6   radius server auth add

Add a RADIUS authentication server.
▶ Mode: Global Config Mode
▶ Privilege Level: Administrator
▶ Format: radius server auth add <P-1> ip <P-2> [name <P-3>] [port <P-4>]
ip: RADIUS authentication server IP address.
[name]: RADIUS authentication server name.
[port]: RADIUS authentication server port (default: 1812).

Parameter	Value	Meaning
P-1	1..8	Next RADIUS server valid index (it can be seen with '#show radius global' command).
P-2	string	Hostname or IP address.
P-3	string	Enter a user-defined text, max. 32 characters.
P-4	1..65535	Enter port number between 1 and 65535

49.2.7   radius server auth delete

Delete a RADIUS authentication server.
▶ Mode: Global Config Mode
▶ Privilege Level: Administrator
▶ Format: radius server auth delete <P-1>

Parameter	Value	Meaning
P-1	1..8	RADIUS server index.

49.2.8   radius server auth modify

Change a RADIUS authentication server parameters.
▶ Mode: `Global Config Mode`
▶ Privilege Level: `Administrator`
▶ Format: `radius server auth modify <P-1> [name <P-2>] [port <P-3>] [msgauth <P-4>] [primary <P-5>] [status <P-6>] [secret [<P-7>]] [encrypted <P-8>]`

`[name]`: RADIUS authentication server name.
`[port]`: RADIUS authentication server port (default: 1812).
`[msgauth]`: Enable or disable the message authenticator attribute for this server.
`[primary]`: Configure the primary RADIUS server.
`[status]`: Enable or disable a RADIUS authentication server entry.
`[secret]`: Configure the shared secret for the RADIUS authentication server.
`[encrypted]`: Configure the encrypted shared secret.

Parameter	Value	Meaning
P-1	1..8	RADIUS server index.
P-2	string	Enter a user-defined text, max. 32 characters.
P-3	1..65535	Enter port number between 1 and 65535
P-4	enable	Enable the option.
	disable	Disable the option.
P-5	enable	Enable the option.
	disable	Disable the option.
P-6	enable	Enable the option.
	disable	Disable the option.
P-7	string	Enter a user-defined text, max. 128 characters.
P-8	string	Enter a user-defined text, max. 128 characters.

49.2.9   radius server retransmit

Configure the retransmit value for the RADIUS server.
▶ Mode: `Global Config Mode`
▶ Privilege Level: `Administrator`
▶ Format: `radius server retransmit <P-1>`

Parameter	Value	Meaning
P-1	1..15	Maximum number of retransmissions (default: 4).

49.2.10 radius server timeout

Configure the RADIUS server timeout value.
▶ **Mode:** `Global Config Mode`
▶ **Privilege Level:** `Administrator`
▶ **Format:** `radius server timeout <P-1>`

Parameter	Value	Meaning
P-1	1..30	Timeout in seconds (default: 5).

49.3 show

Display device options and settings.

49.3.1 show radius global

Display global RADIUS configuration.
- ▶ Mode: `Command is in all modes available.`
- ▶ Privilege Level: `Guest`
- ▶ Format: `show radius global`

49.3.2 show radius auth servers

Display all configured RADIUS authentication servers.
- ▶ Mode: `Command is in all modes available.`
- ▶ Privilege Level: `Guest`
- ▶ Format: `show radius auth servers [<P-1>]`

Paramete r	Value	Meaning
P-1	1..8	RADIUS server index.

49.3.3 show radius auth statistics

Display RADIUS authentication server statistics.
- ▶ Mode: `Command is in all modes available.`
- ▶ Privilege Level: `Guest`
- ▶ Format: `show radius auth statistics <P-1>`

Paramete r	Value	Meaning
P-1	1..8	RADIUS server index.

49.3.4   show radius acct statistics

Display RADIUS accounting server statistics.
▶ Mode: `Command is in all modes available.`
▶ Privilege Level: `Guest`
▶ Format: `show radius acct statistics <P-1>`

Paramete r	Value	Meaning
P-1	1..8	RADIUS server index.

49.3.5   show radius acct servers

Display all configured RADIUS accounting servers.
▶ Mode: `Command is in all modes available.`
▶ Privilege Level: `Guest`
▶ Format: `show radius acct servers [<P-1>]`

Paramete r	Value	Meaning
P-1	1..8	RADIUS server index.

49.4 clear

Clear several items.

49.4.1 clear radius

Clear the RADIUS statistics.
▶ Mode: `Privileged Exec Mode`
▶ Privilege Level: `Administrator`
▶ Format: `clear radius <P-1>`

Paramete r	Value	Meaning
P-1	statistics	Clear the RADIUS statistics.

50 Remote Monitoring (RMON)

50.1 rmon-alarm

Create a RMON alarm action.

50.1.1 rmon-alarm add

Add RMON alarm.
- ▶ Mode: `Global Config Mode`
- ▶ Privilege Level: `Operator`
- ▶ Format: `rmon-alarm add <P-1> [mib-variable <P-2>] [rising-threshold <P-3>] [falling-threshold <P-4>]`

`[mib-variable]`: MIB variable
`[rising-threshold]`: Rising threshold
`[falling-threshold]`: Falling threshold

Paramete r	Value	Meaning
P-1	1..150	Enter an index that uniquely identifies an entry in the alarm table.
P-2	string	Enter an object identifier of the particular variable to be sampled, max. 32 characters.
P-3	1..2147483647	Enter the rising threshold for the sampled statistic.
P-4	1..2147483647	Enter the falling threshold for the sampled statistic.

50.1.2 rmon-alarm enable

Enable RMON alarm.
- ▶ Mode: `Global Config Mode`
- ▶ Privilege Level: `Operator`
- ▶ Format: `rmon-alarm enable <P-1>`

Paramete r	Value	Meaning
P-1	1..150	Enter an index that uniquely identifies an entry in the alarm table.

50.1.3 rmon-alarm disable

Disable RMON alarm.
▶ Mode: `Global Config Mode`
▶ Privilege Level: `Operator`
▶ Format: `rmon-alarm disable <P-1>`

Parameter	Value	Meaning
P-1	1..150	Enter an index that uniquely identifies an entry in the alarm table.

50.1.4 rmon-alarm delete

Delete RMON alarm.
▶ Mode: `Global Config Mode`
▶ Privilege Level: `Operator`
▶ Format: `rmon-alarm delete <P-1>`

Parameter	Value	Meaning
P-1	1..150	Enter an index that uniquely identifies an entry in the alarm table.

50.1.5 rmon-alarm modify

Modify RMON alarm parameters.
▶ Mode: `Global Config Mode`
▶ Privilege Level: `Operator`
▶ Format: `rmon-alarm modify <P-1> [mib-variable <P-2>] [rising-threshold <P-3>] [falling-threshold <P-4>] [interval <P-5>] [sample-type <P-6>] [startup-alarm <P-7>] [rising-event <P-8>] [falling-event <P-9>]`
`[mib-variable]`: Enter the alarm mib variable.
`[rising-threshold]`: Enter the alarm rising threshold.
`[falling-threshold]`: Enter the alarm falling-threshold.
`[interval]`: Enter the alarm interval in seconds over which the data is sampled.
`[sample-type]`: Enter the alarm method of sampling the selected variable.
`[startup-alarm]`: Enter the alarm type.
`[rising-event]`: Enter the alarm rising-event index.
`[falling-event]`: Enter the alarm falling-event index.

Parameter	Value	Meaning
P-1	1..150	Enter an index that uniquely identifies an entry in the alarm table.

Paramete r	Value	Meaning
P-2	string	Enter an object identifier of the particular variable to be sampled, max. 32 characters.
P-3	1..2147483647	Enter the rising threshold for the sampled statistic.
P-4	1..2147483647	Enter the falling threshold for the sampled statistic.
P-5	1..2147483647	Enter the interval in seconds over which the data is sampled and compared with the rising and falling thresholds.
P-6	absoluteValue	Variable is compared directly with the thresholds.
	deltaValue	Variable is subtracted from the current value and the difference compared with the thresholds.
P-7	risingAlarm	Single rising alarm generated when the sample is greater than or equal to the rising threshold.
	fallingAlarm	Single falling alarm generated when the sample is less than or equal to the falling threshold.
	risingOrFallingAlarm	Single Rising alarm generated when the sample is greater than or equal to risingThreshold and single falling alarm generated when the sample is less than or equal to fallingThreshold.
P-8	1..65535	Enter the index of the eventEntry that is used when a rising threshold is crossed.
P-9	1..65535	Enter the index of the eventEntry that is used when a falling threshold is crossed.

50.2   show

Display device options and settings.

50.2.1   show rmon statistics

Show RMON statistics configuration.
▶ **Mode:** `Command is in all modes available.`
▶ **Privilege Level:** `Guest`
▶ **Format:** `show rmon statistics [<P-1>]`

Paramete r	Value	Meaning
`P-1`	slot no./port no.	

50.2.2   show rmon alarm

Display configuration on RMON alarms.
▶ **Mode:** `Command is in all modes available.`
▶ **Privilege Level:** `Guest`
▶ **Format:** `show rmon alarm`

51   Script File

51.1 script

CLI Script File.

51.1.1 script apply

Executes the CLI script file available in the device.
▶ Mode: `Privileged Exec Mode`
▶ Privilege Level: `Administrator`
▶ Format: `script apply <P-1>`

Paramete r	Value	Meaning
`P-1`	string	Filename.

51.1.2 script validate

Only validates the CLI script file available in the device.
▶ Mode: `Privileged Exec Mode`
▶ Privilege Level: `Administrator`
▶ Format: `script validate <P-1>`

Paramete r	Value	Meaning
`P-1`	string	Filename.

51.1.3 script list system

List all the script files available in the device memory.
▶ Mode: `Privileged Exec Mode`
▶ Privilege Level: `Administrator`
▶ Format: `script list system`

51.1.4 script list envm

List all the script files available in external non-volatile memory.
▶ Mode: `Privileged Exec Mode`
▶ Privilege Level: `Administrator`
▶ Format: `script list envm`

51.1.5 script delete

Delete the CLI script files.
▶ Mode: `Privileged Exec Mode`
▶ Privilege Level: `Administrator`
▶ Format: `script delete [<P-1>]`

Paramete r	Value	Meaning
P-1	string	Filename.

51.2 copy

Copy different kinds of items.

51.2.1 copy script envm

Copy script file from external non-volatile memory to specified destination.
▶ Mode: `Privileged Exec Mode`
▶ Privilege Level: `Administrator`
▶ Format: `copy script envm <P-1> running-config nvm <P-2>`
`running-config`: Copy script file from external non-volatile memory to the running-config.
`nvm`: Copy script file from external non-volatile memory to the non-volatile memory.

Paramete r	Value	Meaning
`P-1`	string	Filename.
`P-2`	string	`Enter a user-defined text, max. 32 characters.`

51.2.2 copy script remote

Copy script file from server to specified destination.
▶ Mode: `Privileged Exec Mode`
▶ Privilege Level: `Administrator`
▶ Format: `copy script remote <P-1> running-config nvm <P-2>`
`running-config`: Copy script file from file server to running-config.
`nvm`: Copy script file to non-volatile memory.

Paramete r	Value	Meaning
`P-1`	string	`Enter a user-defined text, max. 128 characters.`
`P-2`	string	`Enter a user-defined text, max. 32 characters.`

51.2.3 copy script nvm

Copy Script file from non-volatile memory to the specified destination.
▶ Mode: `Privileged Exec Mode`
▶ Privilege Level: `Administrator`
▶ Format: `copy script nvm <P-1> running-config envm <P-2> remote <P-3>`
`running-config`: Copy Script file from non-volatile system memory to running-config.
`envm`: Copy Script file to external non-volatile memory device.
`remote`: Copy Script file to file server.

Paramete r	Value	Meaning
P-1	string	Filename.
P-2	string	Enter a user-defined text, max. 32 characters.
P-3	string	Enter a user-defined text, max. 128 characters.

51.2.4 copy script running-config nvm

Copy running configuration to non-volatile memory.
▶ Mode: `Privileged Exec Mode`
▶ Privilege Level: `Administrator`
▶ Format: `copy script running-config nvm <P-1> [all]`
`[all]`: Copy all running configuration to non-volatile memory.

Paramete r	Value	Meaning
P-1	string	Enter a user-defined text, max. 32 characters.

51.2.5 copy script running-config envm

Copy running configuration to external non-volatile memory device.
▶ Mode: `Privileged Exec Mode`
▶ Privilege Level: `Administrator`
▶ Format: `copy script running-config envm <P-1> [all]`
`[all]`: Copy all running configuration to external non-volatile memory.

Paramete r	Value	Meaning
P-1	string	Enter a user-defined text, max. 32 characters.

51.2.6   copy script running-config remote

Copy running configuration to a file server.
- ▶ Mode: `Privileged Exec Mode`
- ▶ Privilege Level: `Administrator`
- ▶ Format: `copy script running-config remote <P-1> [all]`

`[all]`: Copy all running configuration to file server.

Parameter	Value	Meaning
P-1	string	Enter a user-defined text, max. 128 characters.

51.3 show

Display device options and settings.

51.3.1 show script envm

Displays the content of the CLI script file present in the envm.
▶ Mode: `Command is in all modes available.`
▶ Privilege Level: `Administrator`
▶ Format: `show script envm <P-1>`

Paramete r	Value	Meaning
`P-1`	string	Filename.

51.3.2 show script system

Displays the content of the CLI script file present in the device.
▶ Mode: `Command is in all modes available.`
▶ Privilege Level: `Administrator`
▶ Format: `show script system <P-1>`

Paramete r	Value	Meaning
`P-1`	string	Filename.

52 Selftest

52.1 selftest

Configure the selftest settings.

52.1.1 selftest action

Configure the action that a selftest component should take.
▶ Mode: `Global Config Mode`
▶ Privilege Level: `Administrator`
▶ Format: `selftest action <P-1> <P-2>`

Parameter	Value	Meaning
P-1	task	Configure the action for task errors.
	resource	Configure the action for lack of resources.
	software	Configure the action for broken software integrity.
	hardware	Configure the action for detected hardware errors.
P-2	log-only	Write a message to the logging file.
	send-trap	Send a trap to the management station.
	reboot	Reboot the device.

52.1.2 selftest ramtest

Enable or disable the RAM selftest on cold start of the device. When disabled the device booting time is reduced.
▶ Mode: `Global Config Mode`
▶ Privilege Level: `Administrator`
▶ Format: `selftest ramtest`

■ no selftest ramtest
Disable the option
▶ Mode: `Global Config Mode`
▶ Privilege Level: `Administrator`
▶ Format: `no selftest ramtest`

52.1.3 selftest system-monitor

Enable or disable the System Monitor 1 access during the boot phase. Please note: If the System Monitor is disabled it is possible to loose access to the device permanently in case of loosing administrator password or mis-configuration.
▶ Mode: `Global Config Mode`
▶ Privilege Level: `Administrator`
▶ Format: `selftest system-monitor`

■ **no selftest system-monitor**
Disable the option
▶ Mode: `Global Config Mode`
▶ Privilege Level: `Administrator`
▶ Format: `no selftest system-monitor`

52.1.4 selftest boot-default-on-error

Enable or disable loading of the default configuration in case there is any error loading the configuration during boot phase. If disabled the system will be halted.
▶ Mode: `Global Config Mode`
▶ Privilege Level: `Administrator`
▶ Format: `selftest boot-default-on-error`

■ **no selftest boot-default-on-error**
Disable the option
▶ Mode: `Global Config Mode`
▶ Privilege Level: `Administrator`
▶ Format: `no selftest boot-default-on-error`

52.2   show

Display device options and settings.

52.2.1   show selftest action

Displays the actions of the device takes if an error occurs.
▶ Mode: `Command is in all modes available.`
▶ Privilege Level: `Guest`
▶ Format: `show selftest action`

52.2.2   show selftest settings

Displays the selftest settings.
▶ Mode: `Command is in all modes available.`
▶ Privilege Level: `Guest`
▶ Format: `show selftest settings`

53 Small Form-factor Pluggable (SFP)

53.1 show

Display device options and settings.

53.1.1 show sfp

Show info about plugged in SFP modules
▶ Mode: `Command is in all modes available.`
▶ Privilege Level: `Guest`
▶ Format: `show sfp [<P-1>]`

Paramete r	Value	Meaning
P-1	slot no./port no.	

54 Signal Contact

54.1   signal-contact

Configure the signal contact settings.

54.1.1   signal-contact mode

Configure the Signal Contact mode setting.
▶ Mode: `Global Config Mode`
▶ Privilege Level: `Administrator`
▶ Format: `signal-contact <P-1> mode <P-2>`

Parameter	Value	Meaning
`P-1`	signal contact no.	
`P-2`	manual	The signal contact's status is determined by the\nassociated manual setting (subcommand 'state').
	monitor	The signal contact's status is determined by the\nassociated monitor settings.
	device-status	The signal contact's status is determined by the\ndevice status.
	security-status	The signal contact's status is determined by the\nsecurity status.
	dev-sec-status	The signal contact's status is determined by the\ndevice status and security status.

54.1.2   signal-contact monitor link-failure

Sets the monitoring of the network connection(s).
▶ Mode: `Global Config Mode`
▶ Privilege Level: `Administrator`
▶ Format: `signal-contact <P-1> monitor link-failure`

Parameter	Value	Meaning
`P-1`	signal contact no.	

■ **no signal-contact monitor link-failure**
   Disable the option
   ▶ Mode: `Global Config Mode`
   ▶ Privilege Level: `Administrator`
   ▶ Format: `no signal-contact <P-1> monitor link-failure`

54.1.3 signal-contact monitor envm-not-in-sync

Sets the monitoring whether the external non-volatile memory device\nis in sync with the running configuration.
- ▶ Mode: `Global Config Mode`
- ▶ Privilege Level: `Administrator`
- ▶ Format: `signal-contact <P-1> monitor envm-not-in-sync`

Paramete r	Value	Meaning
`P-1`		signal contact no.

■ no signal-contact monitor envm-not-in-sync
Disable the option
- ▶ Mode: `Global Config Mode`
- ▶ Privilege Level: `Administrator`
- ▶ Format: `no signal-contact <P-1> monitor envm-not-in-sync`

54.1.4 signal-contact monitor envm-removal

Sets the monitoring of the external non-volatile memory device removal.
- ▶ Mode: `Global Config Mode`
- ▶ Privilege Level: `Administrator`
- ▶ Format: `signal-contact <P-1> monitor envm-removal`

Paramete r	Value	Meaning
`P-1`		signal contact no.

■ no signal-contact monitor envm-removal
Disable the option
- ▶ Mode: `Global Config Mode`
- ▶ Privilege Level: `Administrator`
- ▶ Format: `no signal-contact <P-1> monitor envm-removal`

54.1.5   signal-contact monitor temperature

Sets the monitoring of the device temperature.
▶ Mode: `Global Config Mode`
▶ Privilege Level: `Administrator`
▶ Format: `signal-contact <P-1> monitor temperature`

Parameter	Value	Meaning
`P-1`		signal contact no.

■ **no signal-contact monitor temperature**
Disable the option
▶ Mode: `Global Config Mode`
▶ Privilege Level: `Administrator`
▶ Format: `no signal-contact <P-1> monitor temperature`

54.1.6   signal-contact monitor ring-redundancy

Sets the monitoring of the ring-redundancy.
▶ Mode: `Global Config Mode`
▶ Privilege Level: `Administrator`
▶ Format: `signal-contact <P-1> monitor ring-redundancy`

Parameter	Value	Meaning
`P-1`		signal contact no.

■ **no signal-contact monitor ring-redundancy**
Disable the option
▶ Mode: `Global Config Mode`
▶ Privilege Level: `Administrator`
▶ Format: `no signal-contact <P-1> monitor ring-redundancy`

54.1.7   signal-contact state

Configure the Signal Contact manual state (only takes\nimmediate effect in manual mode).
▶ Mode: `Global Config Mode`
▶ Privilege Level: `Administrator`
▶ Format: `signal-contact <P-1> state <P-2>`

Paramete r	Value	Meaning
P-1	signal contact no.	
P-2	open	Open the signal contact (only takes effect\nin the manual mode).
	close	Close the signal contact (only takes effect\nin the manual mode).

54.1.8   signal-contact trap

Configure if a trap is sent when the Signal Contact\nchanges state (in monitor mode).
▶ Mode: `Global Config Mode`
▶ Privilege Level: `Administrator`
▶ Format: `signal-contact <P-1> trap`

Paramete r	Value	Meaning
P-1	signal contact no.	

■ **no signal-contact trap**
  Disable the option
   ▶ Mode: `Global Config Mode`
   ▶ Privilege Level: `Administrator`
   ▶ Format: `no signal-contact <P-1> trap`

54.2 signal-contact

Configure the signal contact interface settings.

54.2.1 signal-contact link-alarm

Configure the monitoring of the specific network ports.
▶ Mode: `Interface Range Mode`
▶ Privilege Level: `Administrator`
▶ Format: `signal-contact <P-1> link-alarm`

Parameter	Value	Meaning
P-1		signal contact no.

■ no signal-contact link-alarm
Disable the option
▶ Mode: `Interface Range Mode`
▶ Privilege Level: `Administrator`
▶ Format: `no signal-contact <P-1> link-alarm`

54.3 show

Display device options and settings.

54.3.1 show signal-contact

Display signal contact settings.
- ▶ Mode: `Command is in all modes available.`
- ▶ Privilege Level: `Guest`
- ▶ Format: `show signal-contact <P-1> mode monitor state trap link-alarm module events all`

`mode`: Display the signal contact mode.

`monitor`: Display the signal contact monitor settings.

`state`: Display the signal contact state (open/close).\nNote: This covers the signal contact`s administrative\nsetting as well as its actual state.

`trap`: Display the signal contact trap information and settings.

`link-alarm`: Display the settings of the monitoring of the specific\nnetwork ports.

`module`: Display the settings of the monitoring of the specific\nmodules.

`events`: Display occurred device status events.

`all`: Display all signal contact settings for the specified\nsignal contact.

Parameter	Value	Meaning
P-1	signal contact no.	

55 Switched Monitoring (SMON)

55.1   monitor

Configure port mirroring.

55.1.1   monitor session

Configure port mirroring.
▶ **Mode:** `Global Config Mode`
▶ **Privilege Level:** `Operator`
▶ **Format:** `monitor session <P-1> destination interface <P-2> remote vlan <P-3>`
  `source interface <P-4> direction <P-5> operation vlan <P-6> remote vlan <P-`
  `7> mode`

`destination`: Configure the probe interface.
`interface`: Configure interface.
`remote`: Destination RSPAN configuration.
`vlan`: Set the destination RSPAN VLAN used to tag the mirrored frames.
`source`: Configure the source interface.
`interface`: Configure interface
`direction`: Select interface.
`operation`: Enable/disable mirroring on an interface.
`vlan`: Set the VLAN to mirror.
`remote`: Source RSPAN configuration.
`vlan`: Set the source RSPAN VLAN on which mirrored frames are expected.
`mode`: Enable/Disable port mirroring session. Note: does\nnot affect the source or destination interfaces.

Paramete r	Value	Meaning
P-1	1	Monitor session index.
P-2	slot no./port no.	
P-3	integer	VLAN Mirror Remote VLAN ID List.
P-4	slot no./port no.	
P-5	none	None.
	tx	Packets that are transmitted on the source interfaces are copied to the destination interface.
	rx	Packets that are received on the source interfaces are copied to the destination interface.
	txrx	Packets that are transmitted or received on the source interfaces are copied to the destination interface.
P-6	0..4042	Enter the VLAN ID. Entering of ID 0 disables the feature.
P-7	integer	VLAN Mirror Remote VLAN ID List.

■ **no monitor session**

Disable the option

▶ Mode: `Global Config Mode`
▶ Privilege Level: `Operator`
▶ Format: `no monitor session <P-1> destination interface remote vlan source interface <P-4> direction operation vlan remote vlan mode`

55.2 show

Display device options and settings.

55.2.1 show monitor session

Display port monitor session settings.
▶ Mode: `Command is in all modes available.`
▶ Privilege Level: `Guest`
▶ Format: `show monitor session <P-1>`

Paramete r	Value	Meaning
P-1	1	Monitor session index.

55.3 clear

Clear several items.

55.3.1 clear monitor session

Delete configuration for this session.
- ▶ Mode: `Privileged Exec Mode`
- ▶ Privilege Level: `Operator`
- ▶ Format: `clear monitor session <P-1>`

Parameter	Value	Meaning
P-1	1	Monitor session index.

56 Simple Network Management Protocol (SNMP)

56.1 snmp

Configure of SNMP versions and traps.

56.1.1 snmp access version v1

Enable or disable SNMP version V1.
▶ **Mode:** `Global Config Mode`
▶ **Privilege Level:** `Administrator`
▶ **Format:** `snmp access version v1`

■ no snmp access version v1
Disable the option
▶ **Mode:** `Global Config Mode`
▶ **Privilege Level:** `Administrator`
▶ **Format:** `no snmp access version v1`

56.1.2 snmp access version v2

Enable or disable SNMP version V2.
▶ **Mode:** `Global Config Mode`
▶ **Privilege Level:** `Administrator`
▶ **Format:** `snmp access version v2`

■ no snmp access version v2
Disable the option
▶ **Mode:** `Global Config Mode`
▶ **Privilege Level:** `Administrator`
▶ **Format:** `no snmp access version v2`

56.1.3   snmp access version v3

Enable or disable SNMP version V3.
- ▶ Mode: `Global Config Mode`
- ▶ Privilege Level: `Administrator`
- ▶ Format: `snmp access version v3`

■ no snmp access version v3
Disable the option
- ▶ Mode: `Global Config Mode`
- ▶ Privilege Level: `Administrator`
- ▶ Format: `no snmp access version v3`

56.1.4   snmp access port

Configure the SNMP access port.
- ▶ Mode: `Global Config Mode`
- ▶ Privilege Level: `Administrator`
- ▶ Format: `snmp access port <P-1>`

Paramete r	Value	Meaning
P-1	1..65535	Port number of the SNMP server (default: 161).

56.1.5   snmp access snmp-over-802

Configure SNMPover802.
- ▶ Mode: `Global Config Mode`
- ▶ Privilege Level: `Administrator`
- ▶ Format: `snmp access snmp-over-802`

■ no snmp access snmp-over-802
Disable the option
- ▶ Mode: `Global Config Mode`
- ▶ Privilege Level: `Administrator`
- ▶ Format: `no snmp access snmp-over-802`

56.2   show

Display device options and settings.

56.2.1   show snmp access

Show SNMP access configuration settings.
- ▶ **Mode:** `Command is in all modes available.`
- ▶ **Privilege Level:** `Guest`
- ▶ **Format:** `show snmp access`

57 SNMP Community

57.1 snmp

Configure of SNMP versions and traps.

57.1.1 snmp community ro

SNMP v1/v2 read-only community.
▶ Mode: `Global Config Mode`
▶ Privilege Level: `Administrator`
▶ Format: `snmp community ro`

57.1.2 snmp community rw

SNMP v1/v2 read-write community.
▶ Mode: `Global Config Mode`
▶ Privilege Level: `Administrator`
▶ Format: `snmp community rw`

57.2 show

Display device options and settings.

57.2.1 show snmp community

Display SNMP v1/2 community.
- ▶ Mode: `Command is in all modes available.`
- ▶ Privilege Level: `Administrator`
- ▶ Format: `show snmp community`

58 SNMP Logging

58.1 logging

Logging configuration.

58.1.1 logging snmp-request get operation

Enable or disable logging of SNMP GET or SET requests.
▶ Mode: `Global Config Mode`
▶ Privilege Level: `Administrator`
▶ Format: `logging snmp-request get operation <P-1>`

Parameter	Value	Meaning
P-1	enable	Enable logging of SNMP GET or SET requests.
	disable	Disable logging of SNMP GET or SET requests.

■ **no logging snmp-request get operation**
Disable the option
▶ Mode: `Global Config Mode`
▶ Privilege Level: `Administrator`
▶ Format: `no logging snmp-request get operation <P-1>`

58.1.2 logging snmp-request get severity

Define severity level.
▶ Mode: `Global Config Mode`
▶ Privilege Level: `Administrator`
▶ Format: `logging snmp-request get severity <P-1>`

Paramete r	Value	Meaning
P-1	emergency	System is unusable. System failure has occurred.
	alert	Action must be taken immediately. Unrecoverable failure of a component. System failure likely.
	critical	Recoverable failure of a component that may lead to system failure.
	error	Error conditions. Recoverable failure of a component.
	warning	Minor failure, e.g. misconfiguration of a component.
	notice	Normal but significant conditions.
	informational	Informational messages.
	debug	Debug-level messages.
	0	Same as emergency
	1	Same as alert
	2	Same as critical
	3	Same as error
	4	Same as warning
	5	Same as notice
	6	Same as informational
	7	Same as debug

58.1.3 logging snmp-request set operation

Enable or disable logging of SNMP GET or SET requests.
▶ Mode: Global Config Mode
▶ Privilege Level: Administrator
▶ Format: logging snmp-request set operation <P-1>

Paramete r	Value	Meaning
P-1	enable	Enable logging of SNMP GET or SET requests.
	disable	Disable logging of SNMP GET or SET requests.

■ no logging snmp-request set operation
Disable the option
▶ Mode: Global Config Mode
▶ Privilege Level: Administrator
▶ Format: no logging snmp-request set operation <P-1>

58.1.4 logging snmp-request set severity

Define severity level.
▶ Mode: `Global Config Mode`
▶ Privilege Level: `Administrator`
▶ Format: `logging snmp-request set severity <P-1>`

Parameter	Value	Meaning
P-1	emergency	System is unusable. System failure has occurred.
	alert	Action must be taken immediately. Unrecoverable failure of a component. System failure likely.
	critical	Recoverable failure of a component that may lead to system failure.
	error	Error conditions. Recoverable failure of a component.
	warning	Minor failure, e.g. misconfiguration of a component.
	notice	Normal but significant conditions.
	informational	Informational messages.
	debug	Debug-level messages.
	0	Same as emergency
	1	Same as alert
	2	Same as critical
	3	Same as error
	4	Same as warning
	5	Same as notice
	6	Same as informational
	7	Same as debug

58.2   show

Display device options and settings.

58.2.1   show logging snmp

Show the SNMP logging settings.
▶ Mode: `Command is in all modes available.`
▶ Privilege Level: `Guest`
▶ Format: `show logging snmp`

59 Simple Network Time Protocol (SNTP)

59.1 sntp

Configure SNTP settings.

59.1.1 sntp client operation

Enable or disable the SNTP client
▶ Mode: `Global Config Mode`
▶ Privilege Level: `Administrator`
▶ Format: `sntp client operation`

■ **no sntp client operation**
Disable the option
▶ Mode: `Global Config Mode`
▶ Privilege Level: `Administrator`
▶ Format: `no sntp client operation`

59.1.2 sntp client operating-mode

Set the operating mode of the SNTP client. \nIn unicast-mode, the client sends a request to the SNTP Server. \nIn broadcast-mode, the client waits for a broadcast message from the SNTP Server.
▶ Mode: `Global Config Mode`
▶ Privilege Level: `Administrator`
▶ Format: `sntp client operating-mode <P-1>`

Parameter	Value	Meaning
P-1	unicast	Set the operating mode to unicast.
	broadcast	Set the operating mode to broadcast.

59.1.3 sntp client request-interval

Set the SNTP client request interval in seconds. \nThe request-interval is only used in the operating-mode unicast.
- ▶ **Mode:** `Global Config Mode`
- ▶ **Privilege Level:** `Administrator`
- ▶ **Format:** `sntp client request-interval <P-1>`

Parameter	Value	Meaning
P-1	5..3600	Enter a number in the given range.

59.1.4 sntp client broadcast-rcv-timeout

Set the SNTP client broadcast receive timeout in seconds. \nThe broadcast receive timeout is only used in the operating-mode broadcast.
- ▶ **Mode:** `Global Config Mode`
- ▶ **Privilege Level:** `Administrator`
- ▶ **Format:** `sntp client broadcast-rcv-timeout <P-1>`

Parameter	Value	Meaning
P-1	128..2048	Enter a number in the given range.

59.1.5 sntp client disable-after-sync

If this option is activated, the SNTP client disables itself \nonce it is synchronized to a SNTP server.
- ▶ **Mode:** `Global Config Mode`
- ▶ **Privilege Level:** `Administrator`
- ▶ **Format:** `sntp client disable-after-sync`

■ **no sntp client disable-after-sync**
Disable the option
- ▶ **Mode:** `Global Config Mode`
- ▶ **Privilege Level:** `Administrator`
- ▶ **Format:** `no sntp client disable-after-sync`

59.1.6   sntp client server add

Add a SNTP client server connection
▶ Mode: `Global Config Mode`
▶ Privilege Level: `Administrator`
▶ Format: `sntp client server add <P-1> <P-2> [port <P-3>] [description <P-4>]`
`[port]`: Set the port number of the external time server.
`[description]`: Description of the external time server

Parameter	Value	Meaning
P-1	1..4	Enter a number in the given range.
P-2	string	Hostname or IP address.
P-3	1..65535	Port number of SNTP Server (default 123).
P-4	string	Enter a user-defined text, max. 32 characters.

59.1.7   sntp client server delete

delete a SNTP client server connection
▶ Mode: `Global Config Mode`
▶ Privilege Level: `Administrator`
▶ Format: `sntp client server delete <P-1>`

Parameter	Value	Meaning
P-1	1..4	Enter a number in the given range.

59.1.8   sntp client server mode

Enable or disable a SNTP client server connection
▶ Mode: `Global Config Mode`
▶ Privilege Level: `Administrator`
▶ Format: `sntp client server mode <P-1>`

Parameter	Value	Meaning
P-1	1..4	Enter a number in the given range.

■ **no sntp client server mode**
  Disable the option
  ▶ Mode: `Global Config Mode`
  ▶ Privilege Level: `Administrator`
  ▶ Format: `no sntp client server mode <P-1>`

59.1.9 sntp server operation

Enable or disable the SNTP server
▶ Mode: `Global Config Mode`
▶ Privilege Level: `Administrator`
▶ Format: `sntp server operation`

■ no sntp server operation
Disable the option
▶ Mode: `Global Config Mode`
▶ Privilege Level: `Administrator`
▶ Format: `no sntp server operation`

59.1.10 sntp server port

Set the local socket port number used to listen for client requests.
▶ Mode: `Global Config Mode`
▶ Privilege Level: `Administrator`
▶ Format: `sntp server port <P-1>`

Parameter	Value	Meaning
P-1	1..65535	Port number of SNTP Server (default 123).

59.1.11 sntp server only-if-synchronized

Set the disabling of the SNTP server function,\nif it is not synchronized to another external time reference
▶ Mode: `Global Config Mode`
▶ Privilege Level: `Administrator`
▶ Format: `sntp server only-if-synchronized`

■ no sntp server only-if-synchronized
Disable the option
▶ Mode: `Global Config Mode`
▶ Privilege Level: `Administrator`
▶ Format: `no sntp server only-if-synchronized`

59.1.12 sntp server broadcast operation

Enable or disable the SNTP server broadcast mode
- ▶ **Mode:** `Global Config Mode`
- ▶ **Privilege Level:** `Administrator`
- ▶ **Format:** `sntp server broadcast operation`

■ **no sntp server broadcast operation**
  Disable the option
  - ▶ **Mode:** `Global Config Mode`
  - ▶ **Privilege Level:** `Administrator`
  - ▶ **Format:** `no sntp server broadcast operation`

59.1.13 sntp server broadcast address

Set the SNTP server's broadcast or multicast IP address\n(default: 0.0.0.0 (none)).
- ▶ **Mode:** `Global Config Mode`
- ▶ **Privilege Level:** `Administrator`
- ▶ **Format:** `sntp server broadcast address <P-1>`

Paramete r	Value	Meaning
`P-1`	a.b.c.d	IP address.

59.1.14 sntp server broadcast port

Set the destination socket port number used to send\nbroadcast or multicast messages to the client.
- ▶ **Mode:** `Global Config Mode`
- ▶ **Privilege Level:** `Administrator`
- ▶ **Format:** `sntp server broadcast port <P-1>`

Paramete r	Value	Meaning
`P-1`	1..65535	`Port number of SNTP Server (default 123).`

59.1.15 sntp server broadcast interval

Set the SNTP server's interval in seconds for sending\nbroadcast or multicast messages.
▶ Mode: `Global Config Mode`
▶ Privilege Level: `Administrator`
▶ Format: `sntp server broadcast interval <P-1>`

Parameter	Value	Meaning
P-1	64..1024	Enter a number in the given range.

59.1.16 sntp server broadcast vlan

Set the SNTP server's broadcast VLAN ID used for sending\nbroadcast or multicast messages.
▶ Mode: `Global Config Mode`
▶ Privilege Level: `Administrator`
▶ Format: `sntp server broadcast vlan <P-1>`

Parameter	Value	Meaning
P-1	0..4042	Enter the VLAN ID. Entering of ID 0 uses the management VLAN ID.

59.2 show

Display device options and settings.

59.2.1 show sntp global

Show SNTP configuration parameters and information.
▶ Mode: `Command is in all modes available.`
▶ Privilege Level: `Guest`
▶ Format: `show sntp global`

59.2.2 show sntp client status

Show SNTP client status.
▶ Mode: `Command is in all modes available.`
▶ Privilege Level: `Guest`
▶ Format: `show sntp client status`

59.2.3 show sntp client server

Show SNTP client server connections.
▶ Mode: `Command is in all modes available.`
▶ Privilege Level: `Guest`
▶ Format: `show sntp client server [<P-1>]`

Parameter	Value	Meaning
P-1	1..4	Enter a number in the given range.

59.2.4 show sntp server status

Show SNTP server configuration parameters and information.
- ▶ Mode: `Command is in all modes available.`
- ▶ Privilege Level: `Guest`
- ▶ Format: `show sntp server status`

59.2.5 show sntp server broadcast

Show SNTP server broadcast configuration parameters.
- ▶ Mode: `Command is in all modes available.`
- ▶ Privilege Level: `Guest`
- ▶ Format: `show sntp server broadcast`

60 Spanning Tree

60.1 spanning-tree

Enable or disable the Spanning Tree protocol.

60.1.1 spanning-tree operation

Enable or disable the function.
- ▶ Mode: `Global Config Mode`
- ▶ Privilege Level: `Operator`
- ▶ Format: `spanning-tree operation`

■ **no spanning-tree operation**
Disable the option
- ▶ Mode: `Global Config Mode`
- ▶ Privilege Level: `Operator`
- ▶ Format: `no spanning-tree operation`

60.1.2 spanning-tree bpdu-filter

Enable or disable the BPDU filter on the edge ports.
- ▶ Mode: `Global Config Mode`
- ▶ Privilege Level: `Operator`
- ▶ Format: `spanning-tree bpdu-filter`

■ **no spanning-tree bpdu-filter**
Disable the option
- ▶ Mode: `Global Config Mode`
- ▶ Privilege Level: `Operator`
- ▶ Format: `no spanning-tree bpdu-filter`

60.1.3 spanning-tree bpdu-guard

Enable or disable the BPDU guard on the edge ports.
▶ Mode: `Global Config Mode`
▶ Privilege Level: `Operator`
▶ Format: `spanning-tree bpdu-guard`

■ **no spanning-tree bpdu-guard**
  Disable the option
  ▶ Mode: `Global Config Mode`
  ▶ Privilege Level: `Operator`
  ▶ Format: `no spanning-tree bpdu-guard`

60.1.4 spanning-tree bpdu-migration-check

Force the specified port to transmit RST or MST BPDUs.
▶ Mode: `Global Config Mode`
▶ Privilege Level: `Operator`
▶ Format: `spanning-tree bpdu-migration-check <P-1>`

Parameter	Value	Meaning
`P-1`	slot no./port no.	

60.1.5 spanning-tree forceversion

Set the force protocol version parameter.
▶ Mode: `Global Config Mode`
▶ Privilege Level: `Operator`
▶ Format: `spanning-tree forceversion <P-1>`

Parameter	Value	Meaning
`P-1`	stp	`Spanning Tree Protocol (STP).`
	rstp	`Rapid Spanning Tree Protocol (RSTP).`

60.1.6   spanning-tree forward-time

Set the Bridge Forward Delay parameter [s].
▶ Mode: `Global Config Mode`
▶ Privilege Level: `Operator`
▶ Format: `spanning-tree forward-time <P-1>`

Paramete r	Value	Meaning
P-1	4..30	Enter the bridge forward delay as an integer.

60.1.7   spanning-tree hello-time

Set the Hello Time parameter [s].
▶ Mode: `Global Config Mode`
▶ Privilege Level: `Operator`
▶ Format: `spanning-tree hello-time <P-1>`

Paramete r	Value	Meaning
P-1	1..2	Set the Hello Time parameter (unit: seconds).

60.1.8   spanning-tree hold-count

Set the bridge hold count parameter.
▶ Mode: `Global Config Mode`
▶ Privilege Level: `Operator`
▶ Format: `spanning-tree hold-count <P-1>`

Paramete r	Value	Meaning
P-1	1..40	Set bridge hold count parameter.

60.1.9   spanning-tree max-age

Set the bridge Max Age parameter.
▶ Mode: `Global Config Mode`
▶ Privilege Level: `Operator`
▶ Format: `spanning-tree max-age <P-1>`

Paramete r	Value	Meaning
P-1	6..40	Set the bridge Max Age parameter.

60.1.10 spanning-tree ring-only-mode operation

Enable or disable the RSTP Ring Only Mode.
▶ Mode: `Global Config Mode`
▶ Privilege Level: `Operator`
▶ Format: `spanning-tree ring-only-mode operation`

■ **no spanning-tree ring-only-mode operation**
Disable the option
▶ Mode: `Global Config Mode`
▶ Privilege Level: `Operator`
▶ Format: `no spanning-tree ring-only-mode operation`

60.1.11 spanning-tree ring-only-mode first-port

Configure the first ring port.
▶ Mode: `Global Config Mode`
▶ Privilege Level: `Operator`
▶ Format: `spanning-tree ring-only-mode first-port <P-1>`

Paramete r	Value	Meaning
P-1	slot no./port no.	

60.1.12 spanning-tree ring-only-mode second-port

Configure the second ring port.
▶ Mode: `Global Config Mode`
▶ Privilege Level: `Operator`
▶ Format: `spanning-tree ring-only-mode second-port <P-1>`

Paramete r	Value	Meaning
P-1	slot no./port no.	

60.1.13 spanning-tree mst

MST instance related configuration.
▶ **Mode:** `Global Config Mode`
▶ **Privilege Level:** `Operator`
▶ **Format:** `spanning-tree mst`

60.2 spanning-tree

Enable or disable the Spanning Tree protocol on a port.

60.2.1 spanning-tree mode

Enable or disable the function.
▶ Mode: `Interface Range Mode`
▶ Privilege Level: `Operator`
▶ Format: `spanning-tree mode`

■ **no spanning-tree mode**
Disable the option
▶ Mode: `Interface Range Mode`
▶ Privilege Level: `Operator`
▶ Format: `no spanning-tree mode`

60.2.2 spanning-tree bpdu-flood

Enable or disable BPDU flooding on a port.
▶ Mode: `Interface Range Mode`
▶ Privilege Level: `Operator`
▶ Format: `spanning-tree bpdu-flood`

■ **no spanning-tree bpdu-flood**
Disable the option
▶ Mode: `Interface Range Mode`
▶ Privilege Level: `Operator`
▶ Format: `no spanning-tree bpdu-flood`

60.2.3 spanning-tree edge-auto

Enable or disable auto edge detection on a port.
▶ Mode: `Interface Range Mode`
▶ Privilege Level: `Operator`
▶ Format: `spanning-tree edge-auto`

■ **no spanning-tree edge-auto**
Disable the option
   ▶ Mode: `Interface Range Mode`
   ▶ Privilege Level: `Operator`
   ▶ Format: `no spanning-tree edge-auto`

60.2.4 spanning-tree edge-port

Enable or disable edge port usage on a port.
▶ Mode: `Interface Range Mode`
▶ Privilege Level: `Operator`
▶ Format: `spanning-tree edge-port`

■ **no spanning-tree edge-port**
Disable the option
   ▶ Mode: `Interface Range Mode`
   ▶ Privilege Level: `Operator`
   ▶ Format: `no spanning-tree edge-port`

60.2.5 spanning-tree guard-loop

Enable or disable the loop guard on a port.
▶ Mode: `Interface Range Mode`
▶ Privilege Level: `Operator`
▶ Format: `spanning-tree guard-loop`

■ **no spanning-tree guard-loop**
Disable the option
▶ Mode: `Interface Range Mode`
▶ Privilege Level: `Operator`
▶ Format: `no spanning-tree guard-loop`

60.2.6   spanning-tree guard-root

Enable or disable the root guard on a port.
▶ Mode: `Interface Range Mode`
▶ Privilege Level: `Operator`
▶ Format: `spanning-tree guard-root`

■ **no spanning-tree guard-root**
Disable the option
▶ Mode: `Interface Range Mode`
▶ Privilege Level: `Operator`
▶ Format: `no spanning-tree guard-root`

60.2.7   spanning-tree guard-tcn

Enable or disable the TCN guard on a port.
▶ Mode: `Interface Range Mode`
▶ Privilege Level: `Operator`
▶ Format: `spanning-tree guard-tcn`

■ **no spanning-tree guard-tcn**
Disable the option
▶ Mode: `Interface Range Mode`
▶ Privilege Level: `Operator`
▶ Format: `no spanning-tree guard-tcn`

60.2.8 spanning-tree cost

Specify the port path cost for STP, RSTP and CIST.
▶ Mode: `Interface Range Mode`
▶ Privilege Level: `Operator`
▶ Format: `spanning-tree cost <P-1>`

Parameter	Value	Meaning
P-1	0..200000000	Specify the port path cost.

60.2.9 spanning-tree priority

Specify the port priority for STP, RSTP and CIST.
▶ Mode: `Interface Range Mode`
▶ Privilege Level: `Operator`
▶ Format: `spanning-tree priority <P-1>`

Parameter	Value	Meaning
P-1	0..240	Specify the port priority.

60.3 show

Display device options and settings.

60.3.1 show spanning-tree global

Display the Common and Internal Spanning Tree information and settings.
- ▶ Mode: `Command is in all modes available.`
- ▶ Privilege Level: `Guest`
- ▶ Format: `show spanning-tree global`

60.3.2 show spanning-tree mst instance

Display summarized information and settings for all ports in an MST instance.
- ▶ Mode: `Command is in all modes available.`
- ▶ Privilege Level: `Guest`
- ▶ Format: `show spanning-tree mst instance`

60.3.3 show spanning-tree mst port

Display summarized information and settings for all ports in an MST instance.
- ▶ Mode: `Command is in all modes available.`
- ▶ Privilege Level: `Guest`
- ▶ Format: `show spanning-tree mst port [<P-1>]`

Parameter	Value	Meaning
`P-1`	slot no./port no.	

60.3.4 show spanning-tree port

Spanning Tree information and settings for an interface.
- ▶ Mode: `Command is in all modes available.`
- ▶ Privilege Level: `Guest`
- ▶ Format: `show spanning-tree port <P-1>`

Parameter	Value	Meaning
P-1	slot no./port no.	

61 Secure Shell (SSH)

61.1 ssh

Set SSH parameters.

61.1.1 ssh server

Enable or disable the SSH server.
▶ **Mode:** `Global Config Mode`
▶ **Privilege Level:** `Administrator`
▶ **Format:** `ssh server`

■ **no ssh server**
Disable the option
   ▶ **Mode:** `Global Config Mode`
   ▶ **Privilege Level:** `Administrator`
   ▶ **Format:** `no ssh server`

61.1.2 ssh timeout

Set the SSH connection idle timeout in minutes (default: 5).
▶ **Mode:** `Global Config Mode`
▶ **Privilege Level:** `Administrator`
▶ **Format:** `ssh timeout <P-1>`

Parameter	Value	Meaning
P-1	0..160	Idle timeout of a session in minutes (default: 5).

61.1.3 ssh port

Set the SSH server port number (default: 22).
▶ Mode: `Global Config Mode`
▶ Privilege Level: `Administrator`
▶ Format: `ssh port <P-1>`

Parameter	Value	Meaning
P-1	1..65535	Port number of the SSH server (default: 22).

61.1.4 ssh max-sessions

Set the maximum number of concurrent SSH sessions (default: 5).
▶ Mode: `Global Config Mode`
▶ Privilege Level: `Administrator`
▶ Format: `ssh max-sessions <P-1>`

Parameter	Value	Meaning
P-1	1..5	Maximum number of concurrent SSH sessions.

61.1.5 ssh outbound max-sessions

Set the maximum number of concurrent outbound SSH sessions (default: 5).
▶ Mode: `Global Config Mode`
▶ Privilege Level: `Administrator`
▶ Format: `ssh outbound max-sessions <P-1>`

Parameter	Value	Meaning
P-1	1..5	Maximum number of concurrent SSH sessions.

61.1.6 ssh outbound timeout

Set the SSH connection idle timeout in minutes (default: 5).
▶ Mode: `Global Config Mode`
▶ Privilege Level: `Administrator`
▶ Format: `ssh outbound timeout <P-1>`

Paramete r	Value	Meaning
P-1	0..160	Idle timeout of a session in minutes (default: 5).

61.1.7   ssh key rsa

Generate or delete RSA key
▶ Mode: `Global Config Mode`
▶ Privilege Level: `Administrator`
▶ Format: `ssh key rsa <P-1>`

Paramete r	Value	Meaning
P-1	generate	Generates the item
	delete	Deletes the item

61.1.8   ssh key dsa

Generate or delete DSA key
▶ Mode: `Global Config Mode`
▶ Privilege Level: `Administrator`
▶ Format: `ssh key dsa <P-1>`

Paramete r	Value	Meaning
P-1	generate	Generates the item
	delete	Deletes the item

61.2   copy

Copy different kinds of items.

61.2.1   copy sshkey remote

Copy the SSH key from a server to the specified destination.
▶ Mode: `Privileged Exec Mode`
▶ Privilege Level: `Administrator`
▶ Format: `copy sshkey remote <P-1> nvm`
`nvm`: Copy the SSH key from a server to non-volatile memory.

Paramete r	Value	Meaning
P-1	string	Enter a user-defined text, max. 128 characters.

61.2.2   copy sshkey envm

Copy the SSH key from external non-volatile memory to the specified destination.
▶ Mode: `Privileged Exec Mode`
▶ Privilege Level: `Administrator`
▶ Format: `copy sshkey envm <P-1> nvm`
`nvm`: Copy the SSH key from external non-volatile memory to non-volatile memory.

Paramete r	Value	Meaning
P-1	string	Enter a user-defined text, max. 128 characters.

61.3   show

Display device options and settings.

61.3.1   show ssh

Show SSH server and client information.
- ▶ **Mode:** `Command is in all modes available.`
- ▶ **Privilege Level:** `Guest`
- ▶ **Format:** `show ssh`

62 Storm Control

62.1 storm-control

Configure the global storm-control settings.

62.1.1 storm-control flow-control

Enable or disable flow control globally.
▶ Mode: `Global Config Mode`
▶ Privilege Level: `Operator`
▶ Format: `storm-control flow-control`

■ **no storm-control flow-control**
Disable the option
▶ Mode: `Global Config Mode`
▶ Privilege Level: `Operator`
▶ Format: `no storm-control flow-control`

62.2 traffic-shape

Traffic shape commands.

62.2.1 traffic-shape bw

Set threshold value
▶ Mode: `Interface Range Mode`
▶ Privilege Level: `Operator`
▶ Format: `traffic-shape bw <P-1>`

Parameter	Value	Meaning
P-1	0..100	Enter a number in the given range.

62.3 mtu

62.3.1 mtu

Set the MTU size (without VLAN tag size, because the VLAN tag is ignored for size calculation).
▶ Mode: `Interface Range Mode`
▶ Privilege Level: `Operator`
▶ Format: `mtu <P-1>`

Parameter	Value	Meaning
P-1	1518..12288	Enter a number in the given range.

62.4 mtu

62.4.1 mtu

Set the MTU size (without VLAN tag size, because the VLAN tag is ignored for size calculation).
- ▶ Mode: `Interface Range Mode`
- ▶ Privilege Level: `Operator`
- ▶ Format: `mtu <P-1>`

Parameter	Value	Meaning
P-1	1518..12288	Enter a number in the given range.

62.5 storm-control

Storm control commands

62.5.1 storm-control flow-control

Enable or disable flow control (802.3x) for this port.
▶ Mode: `Interface Range Mode`
▶ Privilege Level: `Operator`
▶ Format: `storm-control flow-control`

■ no storm-control flow-control
Disable the option
▶ Mode: `Interface Range Mode`
▶ Privilege Level: `Operator`
▶ Format: `no storm-control flow-control`

62.5.2 storm-control ingress unit

Set unit.
▶ Mode: `Interface Range Mode`
▶ Privilege Level: `Operator`
▶ Format: `storm-control ingress unit <P-1>`

Parameter	Value	Meaning
P-1	percent	Metering unit expressed in percentage of bandwidth.
	pps	Metering unit expressed in packets per second.

62.5.3 storm-control ingress threshold

Set threshold value. The rate limiter function calculates the threshold based on data packets sized 512 bytes. When the unit is set to pps, the maximum value is 24414 for 100Mb/s and 244140 for 1000Mb/s.
▶ Mode: `Interface Range Mode`
▶ Privilege Level: `Operator`
▶ Format: `storm-control ingress threshold <P-1>`

Parameter	Value	Meaning
P-1	0..14880000	Enter a number in the given range. If the configured unit is percent enter a number in (0..100) range.

62.5.4 storm-control ingress unicast operation

Enable/disable ingress unicast storm control.
▶ Mode: `Interface Range Mode`
▶ Privilege Level: `Operator`
▶ Format: `storm-control ingress unicast operation`

■ **no storm-control ingress unicast operation**
Disable the option
▶ Mode: `Interface Range Mode`
▶ Privilege Level: `Operator`
▶ Format: `no storm-control ingress unicast operation`

62.5.5 storm-control ingress multicast operation

enable/disable ingress multicast storm control.
▶ Mode: `Interface Range Mode`
▶ Privilege Level: `Operator`
▶ Format: `storm-control ingress multicast operation`

■ **no storm-control ingress multicast operation**
Disable the option
▶ Mode: `Interface Range Mode`
▶ Privilege Level: `Operator`
▶ Format: `no storm-control ingress multicast operation`

62.5.6   storm-control ingress broadcast operation

Enable/disable ingress broadcast storm control.
▶ Mode: `Interface Range Mode`
▶ Privilege Level: `Operator`
▶ Format: `storm-control ingress broadcast operation`

■ **no storm-control ingress broadcast operation**
Disable the option
▶ Mode: `Interface Range Mode`
▶ Privilege Level: `Operator`
▶ Format: `no storm-control ingress broadcast operation`

62.6 show

Display device options and settings.

62.6.1 show storm-control flow-control

Global flow control status.
- ▶ Mode: `Command is in all modes available.`
- ▶ Privilege Level: `Guest`
- ▶ Format: `show storm-control flow-control`

62.6.2 show storm-control ingress

Show storm control ingress parameters.
- ▶ Mode: `Command is in all modes available.`
- ▶ Privilege Level: `Guest`
- ▶ Format: `show storm-control ingress [<P-1>]`

Paramete r	Value	Meaning
`P-1`	slot no./port no.	

62.6.3 show traffic-shape

Show Traffic Shape Parameters.
- ▶ Mode: `Command is in all modes available.`
- ▶ Privilege Level: `Guest`
- ▶ Format: `show traffic-shape`

62.6.4 show mtu

Show mtu Parameters.
- ▶ Mode: `Command is in all modes available.`
- ▶ Privilege Level: `Guest`
- ▶ Format: `show mtu`

63   System

63.1 system

Set system related values e.g. name of the device, location of the device, contact data for the person responsible for the device, and pre-login banner text.

63.1.1 system name

Edit the name of the device. The system name consists of an alphanumeric ASCII character string with 0..255 characters.
▶ Mode: `Global Config Mode`
▶ Privilege Level: `Operator`
▶ Format: `system name <P-1>`

Paramete r	Value	Meaning
P-1	string	Enter a user-defined text, max. 255 characters.

63.1.2 system location

Edit the location of the device. The system location consists of an alphanumeric ASCII character string with 0..255 characters.
▶ Mode: `Global Config Mode`
▶ Privilege Level: `Operator`
▶ Format: `system location <P-1>`

Paramete r	Value	Meaning
P-1	string	Enter a user-defined text, max. 255 characters.

63.1.3 system contact

Edit the contact information for the person responsible for the device. The contact data consists of an alphanumeric ASCII character string with 0..255 characters.
▶ Mode: `Global Config Mode`
▶ Privilege Level: `Operator`
▶ Format: `system contact <P-1>`

Paramete r	Value	Meaning
P-1	string	Enter a user-defined text, max. 255 characters.

63.1.4 system pre-login-banner operation

Enable or disable the pre-login banner. You use the pre-login banner to display a greeting or information to users before they login to the device.
- ▶ Mode: `Global Config Mode`
- ▶ Privilege Level: `Administrator`
- ▶ Format: `system pre-login-banner operation`

■ **no system pre-login-banner operation**
Disable the option
- ▶ Mode: `Global Config Mode`
- ▶ Privilege Level: `Administrator`
- ▶ Format: `no system pre-login-banner operation`

63.1.5 system pre-login-banner text

Edit the text for the pre-login banner (C printf format syntax allowed: \\n\\t) The device allows you to edit an alphanumeric ASCII character string with up to 512 characters.
- ▶ Mode: `Global Config Mode`
- ▶ Privilege Level: `Administrator`
- ▶ Format: `system pre-login-banner text <P-1>`

Paramete r	Value	Meaning
P-1	string	Enter a user-defined text, max. 512 characters (allowed characters are from ASCII 32 to 127).

63.1.6   system resources operation

Enable or disable the measurement operation.
- ▶ Mode: `Global Config Mode`
- ▶ Privilege Level: `Administrator`
- ▶ Format: `system resources operation`

■ no system resources operation
Disable the option
- ▶ Mode: `Global Config Mode`
- ▶ Privilege Level: `Administrator`
- ▶ Format: `no system resources operation`

63.2 temperature

Configure the upper and lower temperature limits of the device. The device allows you to set the threshold as an integer from -99 through 99. You configure the temperatures in degrees Celsius.

63.2.1 temperature upper-limit

Configure the upper temperature limit.
▶ Mode: `Global Config Mode`
▶ Privilege Level: `Administrator`
▶ Format: `temperature upper-limit <P-1>`

Parameter	Value	Meaning
P-1	-99..99	Upper temperature threshold ([C], default 70).

63.2.2 temperature lower-limit

Configure the lower temperature limit.
▶ Mode: `Global Config Mode`
▶ Privilege Level: `Administrator`
▶ Format: `temperature lower-limit <P-1>`

Parameter	Value	Meaning
P-1	-99..99	Lower temperature threshold ([C], default 0).

63.3 show

Display device options and settings.

63.3.1 show eventlog

Show event log notice and warning entries with time stamp.
▶ Mode: `Command is in all modes available.`
▶ Privilege Level: `Guest`
▶ Format: `show eventlog`

63.3.2 show system info

Show system related information.
▶ Mode: `Command is in all modes available.`
▶ Privilege Level: `Guest`
▶ Format: `show system info`

63.3.3 show system pre-login-banner

Show pre-login banner status and text.
▶ Mode: `Command is in all modes available.`
▶ Privilege Level: `Guest`
▶ Format: `show system pre-login-banner`

63.3.4   show system flash-status

Show the flash memory statistics of the device.
▶ Mode: `Command is in all modes available.`
▶ Privilege Level: `Guest`
▶ Format: `show system flash-status`

63.3.5   show system temperature limits

Show temperature limits.
▶ Mode: `Command is in all modes available.`
▶ Privilege Level: `Guest`
▶ Format: `show system temperature limits`

63.3.6   show system temperature extremes

Show minimum and maximum recorded temperature.
▶ Mode: `Command is in all modes available.`
▶ Privilege Level: `Guest`
▶ Format: `show system temperature extremes`

63.3.7   show system temperature histogram

Show the temperature histogram of the device.
▶ Mode: `Command is in all modes available.`
▶ Privilege Level: `Guest`
▶ Format: `show system temperature histogram`

63.3.8   show system temperature counters

Display number of 20 centigrade C variations in maximum one hour period.
- ▶ Mode: `Command is in all modes available.`
- ▶ Privilege Level: `Guest`
- ▶ Format: `show system temperature counters`

63.3.9   show system resources

Display the system resources information (cpu utilization, memory and network cpu utilization).
- ▶ Mode: `Command is in all modes available.`
- ▶ Privilege Level: `Guest`
- ▶ Format: `show system resources`

63.3.10 show psu slot

Display power supply slots
- ▶ Mode: `Command is in all modes available.`
- ▶ Privilege Level: `Guest`
- ▶ Format: `show psu slot`

63.3.11 show psu unit

Display information for power supply units.
- ▶ Mode: `Command is in all modes available.`
- ▶ Privilege Level: `Guest`
- ▶ Format: `show psu unit`

64 Telnet

64.1 telnet

Set Telnet parameters.

64.1.1 telnet server

Enable or disable the telnet server.
- ▶ Mode: `Global Config Mode`
- ▶ Privilege Level: `Administrator`
- ▶ Format: `telnet server`

■ no telnet server
Disable the option
- ▶ Mode: `Global Config Mode`
- ▶ Privilege Level: `Administrator`
- ▶ Format: `no telnet server`

64.1.2 telnet timeout

Set the idle timeout for a telnet connection in minutes.
- ▶ Mode: `Global Config Mode`
- ▶ Privilege Level: `Administrator`
- ▶ Format: `telnet timeout <P-1>`

Parameter	Value	Meaning
P-1	0..160	Idle timeout of a session in minutes (default: 5).

64.1.3   telnet port

Set the listening port for the telnet server.
▶ Mode: `Global Config Mode`
▶ Privilege Level: `Administrator`
▶ Format: `telnet port <P-1>`

Paramete r	Value	Meaning
P-1	1..65535	Set the listening port for the telnet server.

64.1.4   telnet max-sessions

Set the maximum number of sessions for the telnet server.
▶ Mode: `Global Config Mode`
▶ Privilege Level: `Administrator`
▶ Format: `telnet max-sessions <P-1>`

Paramete r	Value	Meaning
P-1	1..5	Set the maximum number of connections for the telnet server.

64.2   show

Display device options and settings.

64.2.1   show telnet

Show telnet server information.
▶ Mode: `Command is in all modes available.`
▶ Privilege Level: `Guest`
▶ Format: `show telnet`

65 Traps

65.1 snmp

Configure of SNMP versions and traps.

65.1.1 snmp trap operation

Global enable/disable SNMP trap.
- ▶ Mode: `Global Config Mode`
- ▶ Privilege Level: `Administrator`
- ▶ Format: `snmp trap operation`

■ no snmp trap operation
Disable the option
- ▶ Mode: `Global Config Mode`
- ▶ Privilege Level: `Administrator`
- ▶ Format: `no snmp trap operation`

65.1.2 snmp trap mode

Enable/disable SNMP trap entry.
- ▶ Mode: `Global Config Mode`
- ▶ Privilege Level: `Administrator`
- ▶ Format: `snmp trap mode <P-1>`

Paramete r	Value	Meaning
P-1	string	`<name> Trap name (1 to 32 characters)`

■ no snmp trap mode
Disable the option
- ▶ Mode: `Global Config Mode`
- ▶ Privilege Level: `Administrator`
- ▶ Format: `no snmp trap mode <P-1>`

65.1.3 snmp trap delete

Delete SNMP trap entry.
▶ Mode: `Global Config Mode`
▶ Privilege Level: `Administrator`
▶ Format: `snmp trap delete <P-1>`

Parameter	Value	Meaning
P-1	string	`<name> Trap name (1 to 32 characters)`

65.1.4 snmp trap add

Add SNMP trap entry.
▶ Mode: `Global Config Mode`
▶ Privilege Level: `Administrator`
▶ Format: `snmp trap add <P-1> <P-2>`

Parameter	Value	Meaning
P-1	string	`<name> Trap name (1 to 32 characters)`
P-2	<a.b.c.d>	`a.b.c.d  Single IP address.`
	a.b.c.d:n	`a.b.c.d:n  Address with port.`

65.2 show

Display device options and settings.

65.2.1 show snmp traps

Display SNMP traps.
- ▶ **Mode:** `Command is in all modes available.`
- ▶ **Privilege Level:** `Guest`
- ▶ **Format:** `show snmp traps`

66 User Management

66.1 show

Display device options and settings.

66.1.1 show custom-role global

Display the common information of custom role.
▶ Mode: `Command is in all modes available.`
▶ Privilege Level: `Guest`
▶ Format: `show custom-role global [<P-1>]`

Paramete r	Value	Meaning
P-1	slot no./port no.	

66.1.2 show custom-role commands

Display the included and excluded commands.
▶ Mode: `Command is in all modes available.`
▶ Privilege Level: `Guest`
▶ Format: `show custom-role commands [<P-1>]`

Paramete r	Value	Meaning
P-1	slot no./port no.	

67 Users

67.1 users

Manage Users and User Accounts.

67.1.1 users add

Add a new user.
▶ Mode: `Global Config Mode`
▶ Privilege Level: `Administrator`
▶ Format: `users add <P-1>`

Parameter	Value	Meaning
`P-1`	string	`<user>` User name (up to 32 characters).

67.1.2 users delete

Delete an existing user.
▶ Mode: `Global Config Mode`
▶ Privilege Level: `Administrator`
▶ Format: `users delete <P-1>`

Parameter	Value	Meaning
`P-1`	string	`<user>` User name (up to 32 characters).

67.1.3 users enable

Enable user.
▶ Mode: `Global Config Mode`
▶ Privilege Level: `Administrator`
▶ Format: `users enable <P-1>`

Parameter	Value	Meaning
`P-1`	string	`<user>` User name (up to 32 characters).

67.1.4   users disable

Disable user.
▶ **Mode:** `Global Config Mode`
▶ **Privilege Level:** `Administrator`
▶ **Format:** `users disable <P-1>`

Parameter	Value	Meaning
P-1	string	`<user> User name (up to 32 characters).`

67.1.5   users password

Change user password.
▶ **Mode:** `Global Config Mode`
▶ **Privilege Level:** `Administrator`
▶ **Format:** `users password <P-1> [<P-2>]`

Parameter	Value	Meaning
P-1	string	`<user> User name (up to 32 characters).`
P-2	string	`Enter a user-defined text, max. 64 characters.`

67.1.6   users snmpv3 authentication

Specify authentication setting for a user.
▶ **Mode:** `Global Config Mode`
▶ **Privilege Level:** `Administrator`
▶ **Format:** `users snmpv3 authentication <P-1> <P-2>`

Parameter	Value	Meaning
P-1	string	`<user> User name (up to 32 characters).`
P-2	md5	`MD5 as SNMPv3 user authentication mode.`
	sha1	`SHA1 as SNMPv3 user authentication mode.`

67.1.7 users snmpv3 encryption

Specify encryption settings for a user.
- ▶ Mode: `Global Config Mode`
- ▶ Privilege Level: `Administrator`
- ▶ Format: `users snmpv3 encryption <P-1> <P-2>`

Parameter	Value	Meaning
P-1	string	`<user> User name (up to 32 characters).`
P-2	none	`SNMPv3 encryption method is none.`
	des	`DES as SNMPv3 encryption method.`
	aescfb128	`AES-128 as SNMPv3 encryption method.`

67.1.8 users access-role

Specify snmpv3 access role for a user.
- ▶ Mode: `Global Config Mode`
- ▶ Privilege Level: `Administrator`
- ▶ Format: `users access-role <P-1> <P-2>`

Parameter	Value	Meaning
P-1	string	`<user> User name (up to 32 characters).`
P-2	slot no./port no.	

67.1.9 users lock-status

Set the lockout status of a specified user.
- ▶ Mode: `Global Config Mode`
- ▶ Privilege Level: `Administrator`
- ▶ Format: `users lock-status <P-1> <P-2>`

Parameter	Value	Meaning
P-1	string	`<user> User name (up to 32 characters).`
P-2	unlock	`Unlock specific user. User can login again.`

67.1.10 users password-policy-check

Set password policy check option. The device checks the "minimum password length", regardless of the setting for this option.

▶ **Mode:** `Global Config Mode`
▶ **Privilege Level:** `Administrator`
▶ **Format:** `users password-policy-check <P-1> <P-2>`

Parameter	Value	Meaning
P-1	string	`<user> User name (up to 32 characters).`
P-2	enable	`Enable the option.`
	disable	`Disable the option.`

67.2 show

Display device options and settings.

67.2.1 show users

Display users and user accounts information.
▶ **Mode:** `Command is in all modes available.`
▶ **Privilege Level:** `Administrator`
▶ **Format:** `show users`

68 Virtual LAN (VLAN)

68.1 name

68.1.1 name

Assign a name to a VLAN
► **Mode:** VLAN Database Mode
► **Privilege Level:** Operator
► **Format:** name <P-1> <P-2>

Parameter	Value	Meaning
P-1	1..4042	Enter the VLAN ID.
P-2	string	Enter a user-defined text, max. 32 characters.

68.2 vlan-unaware-mode

68.2.1 vlan-unaware-mode

Enable or disable VLAN unaware mode.
- ▶ Mode: `VLAN Database Mode`
- ▶ Privilege Level: `Operator`
- ▶ Format: `vlan-unaware-mode`

■ **no vlan-unaware-mode**

Disable the option
- ▶ Mode: `VLAN Database Mode`
- ▶ Privilege Level: `Operator`
- ▶ Format: `no vlan-unaware-mode`

68.3 vlan

Creation and configuration of VLANS.

68.3.1 vlan add

Create a VLAN
- ▶ Mode: `VLAN Database Mode`
- ▶ Privilege Level: `Operator`
- ▶ Format: `vlan add <P-1>`

Parameter	Value	Meaning
P-1	1..4042	Enter the VLAN ID.

68.3.2 vlan delete

Delete a VLAN
- ▶ Mode: `VLAN Database Mode`
- ▶ Privilege Level: `Operator`
- ▶ Format: `vlan delete <P-1>`

Parameter	Value	Meaning
P-1	2..4042	Enter VLAN ID. VLAN ID 1 can not be deleted or created

68.4 vlan

Configure 802.1Q port parameters for VLANs.

68.4.1 vlan acceptframe

Configure how to handle tagged/untagged frames received.
▶ Mode: `Interface Range Mode`
▶ Privilege Level: `Operator`
▶ Format: `vlan acceptframe <P-1>`

Parameter	Value	Meaning
P-1	all	Untagged frames or priority frames received on this interface are accepted and \n assigned the value of the interface VLAN ID for this port.
	vlanonly	Only frames received with a VLAN tag will be forwarded. All other frames will be dropped.

68.4.2 vlan ingressfilter

Enable/Disable application of Ingress Filtering Rules.
▶ Mode: `Interface Range Mode`
▶ Privilege Level: `Operator`
▶ Format: `vlan ingressfilter`

■ **no vlan ingressfilter**
Disable the option
  ▶ Mode: `Interface Range Mode`
  ▶ Privilege Level: `Operator`
  ▶ Format: `no vlan ingressfilter`

68.4.3   vlan priority

Configure the priority for untagged frames.
▶ Mode: `Interface Range Mode`
▶ Privilege Level: `Operator`
▶ Format: `vlan priority <P-1>`

Parameter	Value	Meaning
P-1	0..7	Enter a number in the given range.

68.4.4   vlan pvid

Configure the VLAN id for a specific port.
▶ Mode: `Interface Range Mode`
▶ Privilege Level: `Operator`
▶ Format: `vlan pvid <P-1>`

Parameter	Value	Meaning
P-1	1..4042	Enter the VLAN ID.

68.4.5   vlan tagging

Enable or disable tagging for a specific VLAN port.
▶ Mode: `Interface Range Mode`
▶ Privilege Level: `Operator`
▶ Format: `vlan tagging <P-1>`

Parameter	Value	Meaning
P-1	1..4042	Enter the VLAN ID.

■ **no vlan tagging**
Disable the option
▶ Mode: `Interface Range Mode`
▶ Privilege Level: `Operator`
▶ Format: `no vlan tagging <P-1>`

68.4.6   vlan participation include

vlan participation to include
▶ Mode: `Interface Range Mode`
▶ Privilege Level: `Operator`
▶ Format: `vlan participation include <P-1>`

Parameter	Value	Meaning
P-1	1..4042	Enter the VLAN ID.

68.4.7   vlan participation exclude

vlan participation to exclude
▶ Mode: `Interface Range Mode`
▶ Privilege Level: `Operator`
▶ Format: `vlan participation exclude <P-1>`

Parameter	Value	Meaning
P-1	1..4042	Enter the VLAN ID.

68.4.8   vlan participation auto

vlan participation to auto
▶ Mode: `Interface Range Mode`
▶ Privilege Level: `Operator`
▶ Format: `vlan participation auto <P-1>`

Parameter	Value	Meaning
P-1	1..4042	Enter the VLAN ID.

68.5   show

Display device options and settings.

68.5.1   show vlan id

Display configuration of a single specified VLAN.
▶ **Mode:** `Command is in all modes available.`
▶ **Privilege Level:** `Guest`
▶ **Format:** `show vlan id <P-1>`

Paramete r	Value	Meaning
P-1	1..4042	Enter the VLAN ID.

68.5.2   show vlan brief

Show general VLAN parameters.
▶ **Mode:** `Command is in all modes available.`
▶ **Privilege Level:** `Guest`
▶ **Format:** `show vlan brief`

68.5.3   show vlan port

Show VLAN configuration of a single port.
▶ **Mode:** `Command is in all modes available.`
▶ **Privilege Level:** `Guest`
▶ **Format:** `show vlan port [<P-1>]`

Paramete r	Value	Meaning
P-1	slot no./port no.	

68.5.4   show vlan member current

Show membership of ports in static VLAN or dynamically created.
- ▶ **Mode:** `Command is in all modes available.`
- ▶ **Privilege Level:** `Guest`
- ▶ **Format:** `show vlan member current`

68.5.5   show vlan member static

Show membership of ports in static VLAN.
- ▶ **Mode:** `Command is in all modes available.`
- ▶ **Privilege Level:** `Guest`
- ▶ **Format:** `show vlan member static`

68.6 network

Configure the inband and outband connectivity.

68.6.1 network management vlan

Configure the management VLAN ID of the switch.
▶ Mode: `Privileged Exec Mode`
▶ Privilege Level: `Operator`
▶ Format: `network management vlan <P-1>`

Parameter	Value	Meaning
P-1	1..4042	Enter the VLAN ID.

68.6.2 network management priority dot1p

Configure the management VLAN priority of the switch.
▶ Mode: `Privileged Exec Mode`
▶ Privilege Level: `Operator`
▶ Format: `network management priority dot1p <P-1>`

Parameter	Value	Meaning
P-1	0..7	Enter a number in the given range.

68.6.3 network management priority ip-dscp

Configure the management VLAN ip-dscp priority of the switch.
▶ Mode: `Privileged Exec Mode`
▶ Privilege Level: `Operator`
▶ Format: `network management priority ip-dscp <P-1>`

Parameter	Value	Meaning
P-1	0..63	Enter a number in the given range.

A Further Support

■ Technical Questions

For technical questions, please contact any Hirschmann dealer in your area or Hirschmann directly.

You will find the addresses of our partners on the Internet at
http://www.hirschmann.com

Contact our support at
https://hirschmann-support.belden.eu.com

You can contact us

in the EMEA region at
▶ Tel.: +49 (0)1805 14-1538
▶ E-mail: hac.support@belden.com

in the America region at
▶ Tel.: +1 (717) 217-2270
▶ E-mail: inet-support.us@belden.com

in the Asia-Pacific region at
▶ Tel.: +65 6854 9860
▶ E-mail: inet-ap@belden.com

■ Hirschmann Competence Center

The Hirschmann Competence Center is ahead of its competitors:
▶ 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.
The current technology and product training courses can be found at http://www.hicomcenter.com
▶ Support ranges from the first installation through the standby service to maintenance concepts.

With the Hirschmann Competence Center, you have decided against making any compromises. Our client-customized package leaves you free to choose the service components you want to use.
Internet:
http://www.hicomcenter.com

User Manual

Configuration
Embedded Ethernet Switch eXtend
HiOS-2E

Contents

Contents

Contents

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 "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 "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 "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 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 an important 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

Key

Introduction

The device has been developed for use in a harsh industrial environment. Accordingly, the installation process has been kept simple. Thanks to the selected default settings, you only have to enter a few settings before starting to operate the device.

1 User interfaces

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

User interface	Can be reached through …	Prerequisite
Graphical User Interface (GUI)	Ethernet (In-Band)	Web browser
Command Line Interface (CLI)	Ethernet (In-Band) V.24 (Out-of-Band)	Terminal emulation software
System monitor	V.24 (Out-of-Band)	Terminal emulation software

Table 1: User interfaces for accessing the management of the device

1.1 Graphical user interface

■ System requirements

To open the graphical user interface, you need the desktop version of a web browser with HTML5 and JavaScript support.

Note: Third-party software such as web browsers validate certificates based on criteria such as their expiration date and current cryptographic parameter recommendations. Old certificates can cause errors, for example, when they expire or cryptographic recommendations change. Upload your own, up-to-date certificate or regenerate the certificate with the latest firmware to solve validation conflicts with third-party software.

■ Starting the graphical user interface

The prerequisite for starting the graphical user interface is that the IP parameters are configured in the device.

☐ Start your web browser.

☐ Write the IP address of the device in the address field of the web browser.
   Use the following form: `https://xxx.xxx.xxx.xxx`
   The web browser sets up the connection to the device and displays the Login page.

☐ If you want to change the language of the graphical user interface, click the appropriate link in the top right corner of the Login page.

☐ Enter the user name.

☐ Enter the password.

☐ Click the *Login* button.
   The web browser displays the graphical user interface.

1.2 Command line interface

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

The Command Line Interface provides IT specialists with a familiar environment for configuring IT devices. As an experienced user or administrator, you have knowledge about the basics and about using Hirschmann devices.

1.2.1 Preparing the data connection

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

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

You can access the user interface of the Command Line Interface for example, with the freeware program *PuTTY*. This program is provided on the product CD.
☐ Install the *PuTTY* program on your computer.

1.2.2 CLI access using Telnet

■ Telnet connection using Windows

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

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

☐ Enter the command `telnet <IP_address>`.


```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

h:\>telnet 10.100.10.100
```
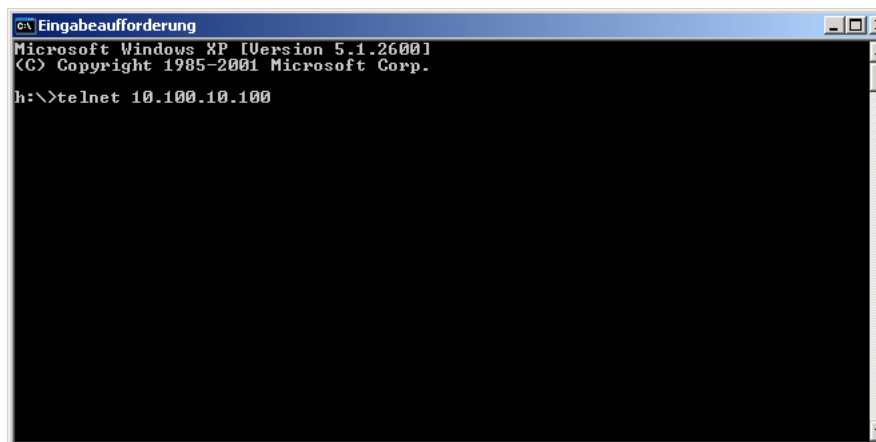
Figure 1: Command Prompt : Setting up the Telnet connection to the device

■ Telnet connection using PuTTY

☐ Start the *PuTTY* program on your computer.
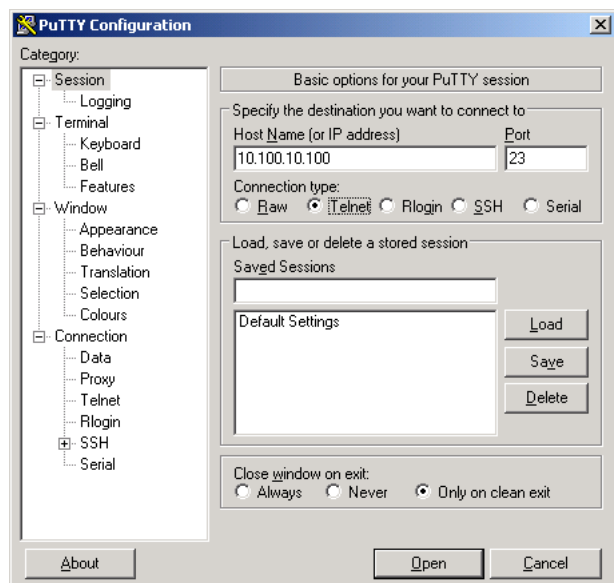
Figure 2: PuTTY input screen

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

☐ To select the connection type, select the *Telnet* radio button in the *Connection type* range.

☐ 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 2 users to have access to the Command Line Interface at the same time.

```
User: admin
Password:*******
```

Figure 3: Login screen of the Command Line Interface

Note: Change the password during the first startup procedure.
☐ Enter the user name. The default user name is admin. Press the <Enter> key.
☐ Enter the password. The default password is private. Press the <Enter> key. The device offers the possibility to change the user name and the password later in the Command Line Interface. These entries are case-sensitive.

The device displays the Command Line Interface start screen with the command prompt:
```
EESX >
```
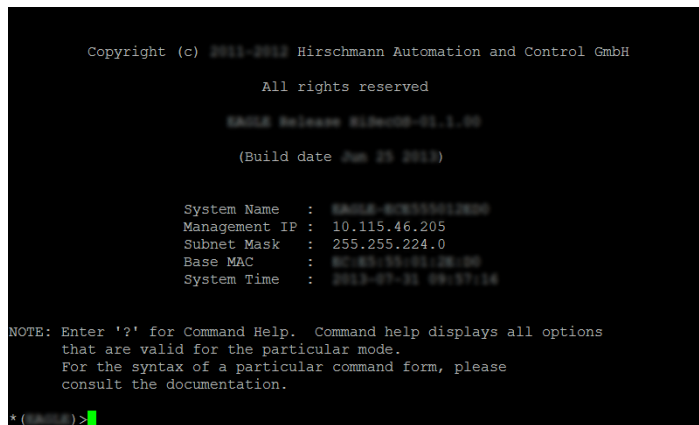
Figure 4: Start screen

1.2.3 CLI access using SSH (Secure Shell)

☐ Start the *PuTTY* program on your computer.
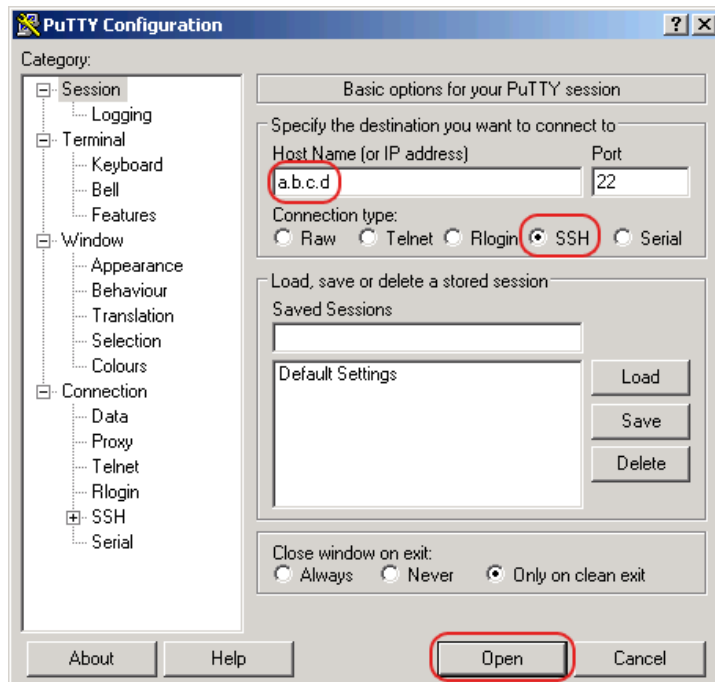
Figure 5: PuTTY input screen

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

☐ To specify the connection type, select the *SSH* radio button in the *Connection type* range.

☐ After selecting and setting the required parameters, the device enables you to set up the data connection using SSH.
Click the *Open* button to set up the data connection to your device. Depending on the device and the time at which SSH was configured, setting up the connection takes up to a minute.

When you first login to your device, towards the end of the connection setup, the *PuTTY* program displays a security alert message and gives you the option of checking the fingerprint of the key.

Figure 6: Security alert prompt for the fingerprint

☐ Check the fingerprint. This helps protect yourself from unwelcome guests.

☐ If the fingerprint matches that of the device key, click the *Yes* button.

The device allows you to display the finger prints of the device keys with the command `show ssh` or in the *Device Security > Management Access > Server* dialog, *SSH* tab.

Note: For experienced network administrators, another way of accessing your device through an SSH is by using the OpenSSH Suite. To set up the data connection, enter the following command:

`ssh admin@10.149.112.53`

`admin` is the user name.
`10.149.112.53` is the IP address of your device.

The Command Line Interface appears on the screen with a window for entering the user name. The device enables up to 2 users to have access to the Command Line Interface at the same time.

`login as: adminadmin@a.b.c.d's password:`

`a.b.c.d` is the IP address of your device.

☐ Enter the user name. The default user name is `admin`. Press the <Enter> key.

☐ Enter the password. The default password is `private`. Press the <Enter> key. The device offers the possibility to change the user name and the password later in the Command Line Interface. These entries are case-sensitive.

The device displays the start screen.

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

Figure 7: Start screen

1.2.4 CLI using the V.24 port

The V.24 interface is a serial interface for the local connection of an external network management station (VT100 terminal or PC with terminal emulation). The interface allows you to set up a data connection to the Command Line Interface (CLI) and to the system monitor.

VT 100 terminal settings	
Speed	9600 bit/s
Data	8 bit
Stopbit	1 bit
Handshake	off
Parity	none

☐ Connect the device to a terminal using V.24. Alternatively connect the device to a COM port of your PC using terminal emulation based on VT100 and press any key.

☐ Alternatively you set up the serial data connection to the device using V.24 with the *PuTTY* program. Press the <Enter> key.
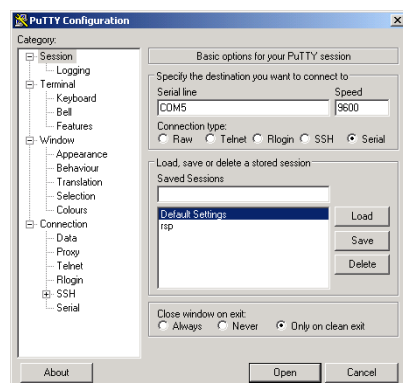
Figure 8: Serial data connection using V.24 with the PuTTY program

After the data connection has been set up successfully, the device displays a window for entering the user name.

Note: You can configure the V.24 interface as a terminal/CLI interface.
Press any key on your terminal keyboard a number of times until the login screen indicates the CLI mode.

☐ Enter the user name. The default user name is `admin`. Press the <Enter> key.
☐ Enter the password. The default password is `private`. Press the <Enter> key. The device offers the possibility to change the user name and the password later in the Command Line Interface. These entries are case-sensitive.

Figure 9: Logging in to the Command Line Interface program

Figure 10: CLI screen after login

1.2.5 User rights

The device functions available to you as a user depend on your access role. The functions of a specific access role are available to you when you are logged on to the user interface with this access role.

The commands available to you as a user, also depend on the Command Line Interface mode in which you are currently working.

■ Access roles

The user interface offers the following access roles:
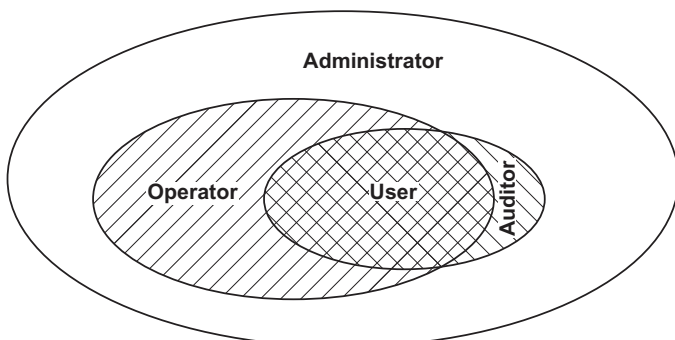
Access role	User authorizations
User	Users logged on with the access role User are authorized to monitor the device.
Auditor	Users logged on with the access role Auditor are authorized to monitor the device and to save the log file in the *Diagnostics > Report > Audit Trail* dialog.
Operator	Users logged on with the access role Operator are authorized to monitor the device and to change the settings – with the exception of security settings for device access.
Administrator	Users logged on with the access role Administrator are authorized to monitor the device and to change the settings.
Unauthorized	Unauthorized users are blocked, and the device rejects the user login. Assign this value to temporarily lock the user account. If a detected error occurs when another access role is being assigned, the device assigns this access role to the user account.

Table 2: Access roles and scope of user authorizations

1.2.6 Mode-based command hierarchy

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

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

The User Exec mode commands are an exception. The Command Line Interface enables you to execute these commands in the Privileged Exec mode, too.

The following figure displays the modes of the Command Line Interface.
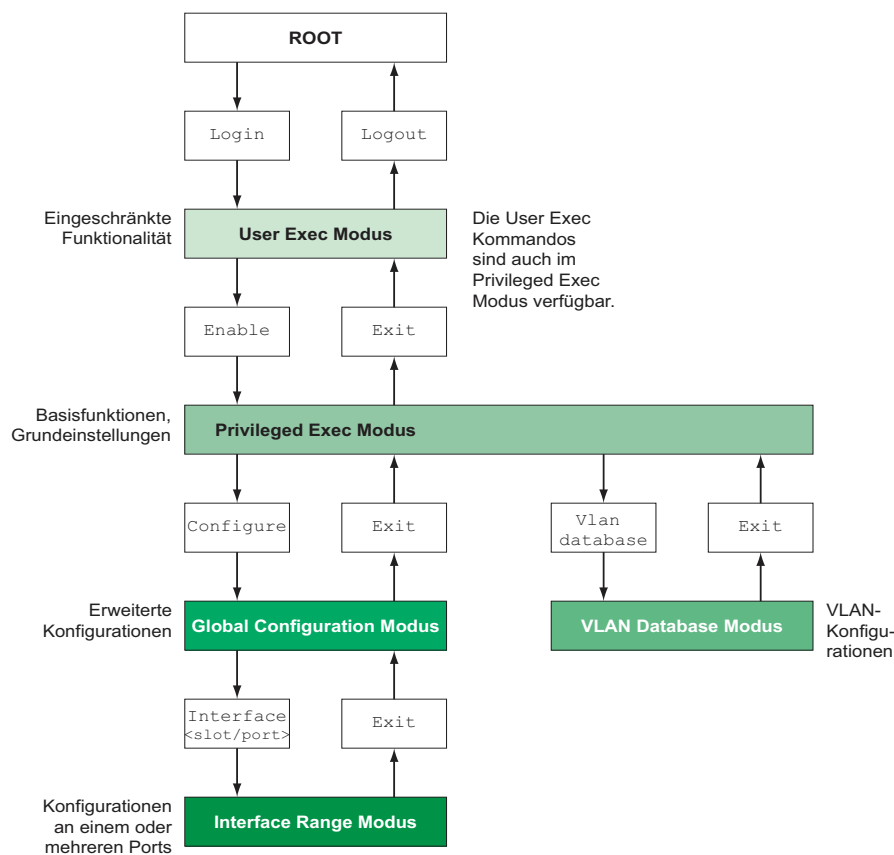
Figure 11: Structure of the Command Line Interface

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

▶ User Exec mode
When you login to the Command Line Interface, you enter the User Exec mode. The User Exec mode contains a limited range of commands.
Command prompt: `(EESX) >`

▶ Privileged Exec mode
To access the entire range of commands, you enter the Privileged Exec mode. If you are authenticated as a privileged user by the login, you are able to enter the Privileged Exec mode. In the Privileged Exec mode, you are able to execute the User Exec mode commands, too.
Command prompt: `(EESX) #`

▶ VLAN mode
The VLAN mode contains VLAN-related commands.
Command prompt: `(EESX) (VLAN)#`

▶ Global Config mode
The Global Config mode allows you to perform modifications to the current configuration. This mode groups general setup commands.
Command prompt: `(EESX) (config)#`

▶ Interface Range mode
The commands in the Interface Range mode affect a specific port, a selected group of multiple ports or all port of the device. The commands modify a value or switch a function on/off on one or more specific ports.

– All physical ports on the device
Command prompt: `(EESX) ((interface) all)#`
Example: When you switch from the Global Config mode to the Interface Range mode, the command prompt changes as follows:
```
(EESX) (config)#interface all
(EESX) ((Interface)all)#
```

– A single port on one interface
Command prompt: `(EESX) (interface <slot/port>)#`
Example: When you switch from the Global Config mode to the Interface Range mode, the command prompt changes as follows:
```
(EESX) (config)#interface 2/1
(EESX) (interface 2/1)#
```

– A range of ports on one interface
Command prompt: `(EESX) (interface <interface range> )#`
Example: When you switch from the Global Config mode to the Interface Range mode, the command prompt changes as follows:
```
(EESX) (config)#interface 1/2-1/4
(EESX) ((Interface)1/2-1/4)#
```

– A list of single ports
Command prompt: `(EESX) (interface <interface list>)#`
Example: When you switch from the Global Config mode to the Interface Range mode, the command prompt changes as follows:
```
(EESX) (config)#interface 1/2,1/4,1/5
(EESX) ((Interface)1/2,1/4,1/5)#
```

– A list of port ranges and single ports
Command prompt: `(EESX) (interface <complex range>)#`
Example: When you switch from the Global Config mode to the Interface Range mode, the command prompt changes as follows:
```
(EESX) (config)#interface 1/2-1/4,1/6-1/9
(EESX) ((Interface)1/2-1/4,1/6-1/9)
```

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

Command mode	Access method	Quit or start next mode

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

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

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

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

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

Table 3:   Command modes

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

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

(EESX)>
```

Figure 12: Commands in the User Exec mode

1.2.7   Executing the commands

■ Syntax analysis

After you login to the Command Line Interface session, you enter the User Exec mode. The Command Line Interface displays the prompt `(EESX)>` on the screen.

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

If the command is outside the Command Line Interface command range, a message informs you of the detected error.

Example:
The user wants to execute the `show system info` command, but enters `info` without `f` and presses the <Enter> key.
The Command Line Interface then displays a message:

```
(EESX)>show system ino
Error: Invalid command 'ino'
```

■ Command tree

The commands in the Command Line Interface are organized in a tree structure. The commands, and, if applicable, the related parameters branch down until the command is completely defined and therefore executable. The Command Line Interface checks the input. If you entered the command and the parameters correctly and completely, you execute the command with the <Enter> key.

After you entered the command and the required parameters, the other parameters entered are treated as optional parameters. If one of the parameters is unknown, the Command Line Interface displays a syntax message.

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

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

1.2.8 Structure of a command

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

■ Format of commands

Most of the commands include parameters.

If the command parameter is missing, the Command Line Interface informs you about the detection of an incorrect command syntax.

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

■ Parameters

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

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

`<command>`	Commands in pointed brackets (`<>`) are obligatory.
`[command]`	Commands in square brackets (`[]`) are optional.
`<parameter>`	Parameters in pointed brackets (`<>`) are obligatory.
`[parameter]`	Parameters in square brackets (`[]`) are optional.
`...`	An ellipsis (3 points in sequence without spaces) after an element indicates that you can repeat the element.
`[Choice1 | Choice2]`	A vertical line enclosed in brackets indicates a selection option. Select one value. Elements separated by a vertical line and enclosed in square brackets indicate an optional selection (Option1 or Option2 or no selection).
`{list}`	Curved brackets (`{}`) indicate that a parameter is to be selected from a list of options.
`{Choice1 | Choice2}`	Elements separated by a vertical line and enclosed in curved brackets (`{}`) indicate an obligatory selection option (option1 or option2).
`[param1 {Choice1 | Choice2}]`	Displays an optional parameter that contains an obligatory selection.
`<a.b.c.d>`	Small letters are wild cards. You enter parameters with the notation a.b.c.d with decimal points (for example IP addresses)
`<cr>`	You press the <Enter> key to create a line break (carriage return).

Table 4:   Parameter and command syntax

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

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

Table 5:   Parameter values in the Command Line Interface

■ Network addresses

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

The IP address is an address allocated by the network administrator. Do not use duplicate addresses in one network area.

The MAC addresses are assigned by the hardware manufacturer. MAC addresses are unique worldwide.

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

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

Table 6:   Format and range of network addresses

■ Strings

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

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

*(EESX)#cli prompt 'Device name'

*(Device name)#
```

1.2.9   Examples of commands

■ Example 1: clear arp-table-switch

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

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

■ Example 2: radius server timeout

Command to configure the RADIUS server timeout value.
```
(EESX) (config)#radius server timeout
 <1..30>              Timeout in seconds (default: 5).
```

`radius server timeout` is the command name.
The parameter is required. The value range is `1..30`.

■ Example 3: radius server auth modify <1..8>

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

`radius server auth modify` is the command name.
The parameter `<1..8>` (RADIUS server index) is required. The value range is `1..8` (integer).
The parameters `[name]`, `[port]`, `[msgauth]`, `[primary]`, `[status]`, `[secret]` and `[encrypted]` are optional.

1.2.10 Input prompt

■ Command mode

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

▶ `(EESX) >`
   User Exec mode

▶ `(EESX) #`
   Privileged Exec mode

▶ `(EESX) (config)#`
   Global Config mode

▶ `(EESX) (Vlan)#`
   VLAN Database mode

▶ `(EESX) ((Interface)all)#`
   Interface Range mode / All ports of the device

▶ `(EESX) ((Interface)2/1)#`
Interface Range mode / A single port on one interface

▶ `(EESX) ((Interface)1/2-1/4)#`
Interface Range mode / A range of ports on one interface

▶ `(EESX) ((Interface)1/2,1/4,1/5)#`
Interface Range mode / A list of single ports

▶ `(EESX) ((Interface)1/1-1/2,1/4-1/6)#`
Interface Range mode / A list of port ranges and single ports

■ Asterisk, pound sign and exclamation point

▶ Asterisk `*`
An asterisk `*` in the first or second position of the input prompt displays you that the settings in the volatile memory and the settings in the non-volatile memory are different. In your configuration, the device has detected modifications which have not been saved.
`*(EESX)>`

▶ Pound sign `#`
A pound sign `#` at the beginning of the input prompt displays you that the boot parameters and the parameters during the boot phase are different.
`*#(EESX)>`

▶ Exclamation point `!`
An exclamation point `!` at the beginning of the input prompt displays: the password for the `user` or `admin` user account corresponds with the default setting.
`!(EESX)>`

■ Wildcards

The device offers you the possibility to change the input prompt.

The Command Line Interface supports the following wildcards:

Wildcard	Description
`%d`	System date
`%t`	System time
`%i`	IP address of the device
`%m`	MAC address of the device
`%p`	Product name of the device

Table 7:   Using wildcards within the Command Line Interface input prompt

```
!(EESX)>enable

!(EESX)#cli prompt %i

!10.100.10.100#cli prompt (EESX)%d

!*(EESX)2014-01-27#cli prompt (EESX)%d%t

!*(EESX)2014-01-2715:45:41#cli prompt %m

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

1.2.11 Key combinations

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

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

Table 8:   Key combinations in the Command Line Interface

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

```
(EESX) #help

HELP:
Special keys:

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

(EESX) #
```

Figure 13: Listing the key combinations with the Help command

1.2.12 Data entry elements

■ **Command completion**

To facilitate making entries, the Command Line Interface gives you the option of command completion (Tab Completion). Thus you are able to abbreviate key words.

▶ Type in the beginning of a keyword. If the characters entered identify a keyword, the Command Line Interface will complete the keyword when you press the tab key or the space key. If there is more than one option for completion, enter the letter or the letters being necessary for uniquely identifying the keyword. Press the tab key or the space key again. After that, the system completes the command or parameter.

▶ If you make a non-unique entry and press <Tab> or <Space> twice, the Command Line Interface provides you with a list of options.

▶ On a non-unique entry and pressing <Tab> or <Space>, the Command Line Interface completes the command up to the end of the uniqueness. If several commands exist: When you press <Tab> or <Space> again, the Command Line Interface provides you with a list of options.

Example:
```
(EESX) (Config)#lo
(EESX) (Config)#log
logging  logout
```

If you enter `lo` and <Tab> or <Space>, the Command Line Interface completes the command up to the end of the uniqueness to `log`.
When you press <Tab> or <Space> again, the Command Line Interface provides you with a list of options (`logging logout`).

■ **Possible commands/parameters**

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

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

When you enter the command without space character in front of the question mark, the device displays the help text for the command itself:
```
!*#(EESX)(Config)#show?
   show          Display device options and settings.
```

1.2.13 Use cases

■ **Saving the Configuration**

To help ensure that your password settings and your other configuration changes are kept after the device is reset or after an interruption of the voltage supply, you save the configuration. To save your current configuration, you proceed as follows:

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

☐ Enter the following command:
```
save [profile]
```

☐ Execute the command by pressing the <Enter> key.

■ Syntax of the „radius server auth add" command

Use this command to add a RADIUS authentication server.
▶ Mode: `Global Config` mode
▶ Privilege Level: Administrator
▶ Format: `radius server auth add <1..8> ip <a.b.c.d>`

  `[name <string>] [port <1..65535>]`
  – `[name]`: RADIUS authentication server name.
  – `[port]`: RADIUS authentication server port (default: 1813).

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

Mode and Privilege Level:
▶ You need to be in Global Config mode to be able to execute the command.
  See "Mode-based command hierarchy" on page 25.
▶ You need to have Administrator Privilege Level to be able to execute the command.

Syntax of commands and parameters:
See "Structure of a command" on page 28.

Examples for executable commands:
▶ `radius server auth add 1 ip 10.115.30.40`
▶ `radius server auth add 2 ip 10.115.40.50 name radiusserver2`
▶ `radius server auth add 3 ip 10.115.50.60 port 1813`
▶ `radius server auth add 4 ip 10.115.60.70 name radiusserver4 port 1814`

1.3 System monitor

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

1.3.1 Functional scope

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

1.3.2 Starting the System Monitor

Prerequisite:
► Terminal cable for connecting the device to your PC (available as an optional accessory).
► PC with VT100 terminal emulation (such as the `PuTTY` program) or serial terminal

Perform the following steps:

☐ Use the terminal cable to connect the V.24 interface of the device with the COM port of the PC.

☐ Start the VT100 terminal emulation on the PC.

☐ Specify the following transmission parameters:

VT 100 terminal settings	
Speed	9600 bit/s
Data	8 bit
Stopbit	1 bit
Handshake	off
Parity	none

☐ Set up a connection to the device.

☐ Switch on the device. If the device is already on, reboot it.
    The screen displays the following message after rebooting:
    `Press <1> to enter System Monitor 1.`

☐ Press the <1> key within 3 seconds.
    The device starts the System Monitor. The screen displays the following view:

```
System Monitor 1
(Selected OS: ...-7.1 (2018-09-20 19:17))

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




sysMon1>
```

Figure 14: System Monitor 1 screen display

☐ Select a menu item by entering the number.

☐ To leave a submenu and return to the main menu of System Monitor 1, press the <ESC> key.

2 Specifying the IP parameters

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

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

▶ Entry using the Command Line Interface.
You choose this "Out-of-Band" method if you preconfigure your device outside its operating environment, or if you restore the network access ("In-Band") to the device.

▶ Entry using the HiDiscovery protocol.
You choose this "In-Band" method on a previously installed network device or if you have another Ethernet connection between your PC and the device

▶ Configuration using the external memory.
You choose this method if you are replacing a device with a device of the same type and have already saved the configuration in the external memory.

▶ Using BOOTP.
You choose this "In-Band" method to configure the installed device using BOOTP. You need a BOOTP server for this method. The BOOTP server assigns the configuration data to the device using its MAC address. The DHCP mode is the default mode for the configuration data reference.

▶ Configuration using DHCP.
You choose this "In-Band" method to configure the installed device using DHCP. You need a DHCP server for this method. The DHCP server assigns the configuration data to the device using its MAC address or its system name.

▶ Configuration using the graphical user interface.
If the device already has an IP address and is reachable using the network, then the graphical user interface provides you with another option for configuring the IP parameters.

2.1 IP parameter basics

2.1.1 IP address (version 4)

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

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

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

Table 9: IP address classes

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

▶ APNIC (Asia Pacific Network Information Center)
Asia/Pacific Region

▶ ARIN (American Registry for Internet Numbers)
Americas and Sub-Sahara Africa

▶ LACNIC (Regional Latin-American and Caribbean IP Address Registry)
Latin America and some Caribbean Islands

▶ RIPE NCC (Réseaux IP Européens)
Europe and Surrounding Regions
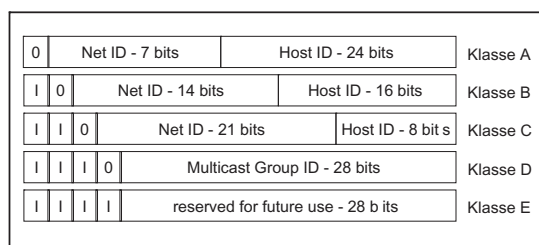
Figure 15: Bit representation of the IP address

The IP addresses belong to class A when their first bit is a zero, for example, the first octet is less than 128.

The IP address belongs to class B if the first bit is a one and the second bit is a zero, for example, the first octet is between 128 and 191.

The IP address belongs to class C when the first 2 bits are a one, for example, the first octet is higher than 191.

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

2.1.2 Netmask

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

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

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

Example of a subnet mask:

Dezimale Darstellung
255.255.192.0

Binäre Darstellung
11111111.11111111.11000000.00000000
                            Subnetzmaskenbits
                            Klasse B

Example of IP addresses with subnetwork assignment when applying the subnet mask:

Dezimale Darstellung
129.218.65.17
                128 < 129 191 › Klasse B
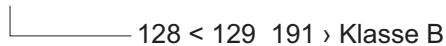
Binäre Darstellung
10000001.11011010.01000001.00010001
                            Subnetz 1
                            Netzadresse

Dezimale Darstellung
129.218.129.17
                128 < 129 191 › Klasse B

Binäre Darstellung
10000001.11011010.10000001.00010001
                            Subnetz 2

■ 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?
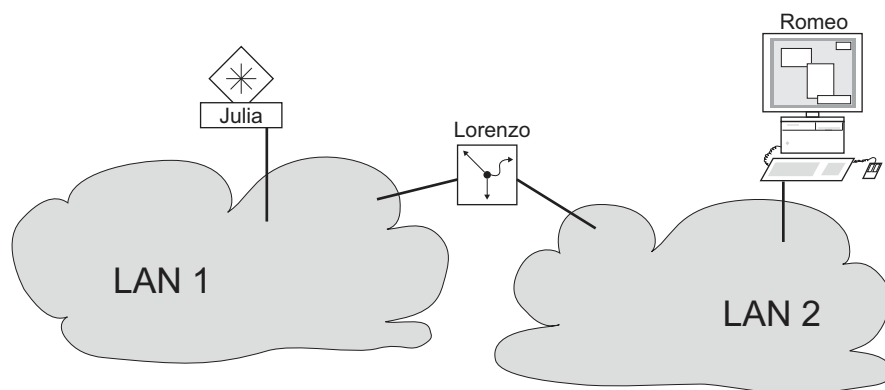
Figure 16: The management agent is separated from its network management station by a router

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

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

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

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

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

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

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

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

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

2.1.3 Classless Inter-Domain Routing

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

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

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

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

Example:

IP-Adresse dezimal	Netzmaske dezimal	IP-Adresse binär
149.218.112.1	255.255.255.128	10010101 11011010 01110000 00000001
149.218.112.127		10010101 11011010 01110000 01111111

├─────── 25 Maskenbits ───────┤

CIDR-Schreibweise: 149.218.112.0/25

└──── Maskenbits

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

2.2 Specifying the IP parameters using the CLI

There are several methods you enter the system configuration, either using BOOTP/DHCP, the HiDiscovery protocol, the external memory. You have the option of performing the configuration using the V.24 interface using the CLI.

The device allows you to specify the IP parameters using the HiDiscovery protocol or using the CLI over the V.24 interface.
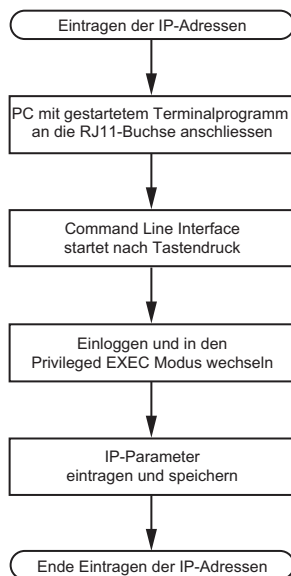
Figure 17: Flow chart for entering IP addresses

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

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

☐ Deactivate DHCP.

☐ Enter the IP parameters.

▶ Local IP address
In the default setting, the local IP address is `0.0.0.0`.

▶ Netmask
If you divided your network into subnetworks, and if these are identified with a netmask, then enter the netmask here. In the default setting, the local netmask is `0.0.0.0`.

▶ IP address of the Gateway.
This entry is only required if the device and the network management station or TFTP server are located in different subnetworks .
Specify the IP address of the Gateway between the subnetwork with the device and the path to the network management station.
In the default setting, the IP address is `0.0.0.0`.

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

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

After entering the IP parameters, you easily configure the device using the graphical user interface.
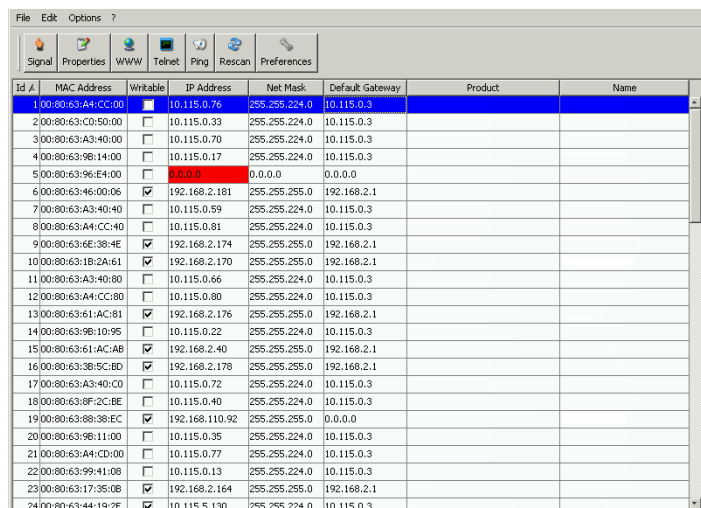
2.3 Specifying the IP parameters using HiDiscovery

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

You easily configure other parameters using the graphical user interface.

Install the HiDiscovery software on your PC. The software is on the product DVD supplied with the device.

☐ To install it, you start the installation program on the DVD.

☐ Start the HiDiscovery program.

Figure 18: HiDiscovery

When HiDiscovery is started, HiDiscovery automatically searches the network for those devices which support the HiDiscovery protocol.

HiDiscovery uses the first network interface found for the PC. If your computer has several network cards, you can select the one you desire in the HiDiscovery toolbar.

HiDiscovery displays a line for every device that responds to a HiDiscovery protocol inquiry.

HiDiscovery enables you to identify the devices displayed.

☐ Select a device line.

☐ To set the LEDs to flashing for the selected device, click the `Signal` button on the tool bar. To stop the flashing, click the `Signal` button again.

☐ By double-clicking a line, you open a window in which you specify the device name and the IP parameter.
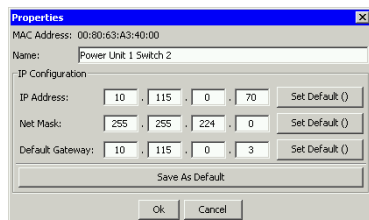
Figure 19: HiDiscovery – assigning IP parameters

Note: For security reasons, disable the HiDiscovery function for the device in the graphical user interface, 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

Perform the following steps:

☐ Open the *Basic Settings > Network* dialog.

In this dialog you first specify the source from which the device gets its IP parameters after starting. You also define the VLAN in which the device management can be accessed, configure the HiDiscovery access and allocate manual IP parameters.

☐ In the *Management interface* frame you first specify where the device gets its IP parameters from:

▶ In the `BOOTP` mode, the configuration is using a BOOTP or DHCP server on the basis of the MAC address of the device.

▶ In the *DHCP* mode, the configuration is using a DHCP server on the basis of the MAC address or the name of the device.

▶ In the `Local` mode, the device uses the network parameters from the internal device memory.

Note: When you change the allocation mode of the IP address, the device activates the new mode immediately after you

click the ✅ button.

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

☐ Note here that you can only access the device management using ports that are members of the relevant VLAN.

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

☐ In the *HiDiscovery protocol v1/v2* frame you specify the settings for accessing the device using the HiDiscovery software.

☐ The HiDiscovery protocol allows you to allocate an IP address to the device on the basis of its MAC address . Activate the HiDiscovery protocol if you want to allocate an IP address to the device from your PC with the HiDiscovery software.

☐ If required, you enter the IP address, the netmask and the Gateway in the *IP parameter* frame.

☐ To save the changes temporarily, click the ✅ button.

2.5   Specifying the IP parameters using BOOTP

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

2.6   Specifying the IP parameters using DHCP

The DHCP (Dynamic Host Configuration Protocol) is a further development of BOOTP, which it has replaced. The DHCP additionally allows the configuration of a DHCP client using a name instead of using the MAC address. For the DHCP, this name is known as the "Client Identifier" in accordance with RFC 2131.

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

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

In addition to the IP address, the DHCP server sends

▶ the netmask

▶ the default Gateway (if available)

▶ the TFTP URL of the configuration file (if available).

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

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

Table 10: DHCP options which the device requests

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

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

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

Note: When using Industrial HiVision network management, verify that DHCP allocates the original IP address to every device.

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

Example of a DHCP-configuration file:
```
# /etc/dhcpd.conf for DHCP Daemon
#
subnet 10.1.112.0 netmask 255.255.240.0 {
option subnet-mask 255.255.240.0;
option routers 10.1.112.96;
}
#
# Host berta requests IP configuration
# with her MAC address
#
host berta {
```

```
hardware ethernet 00:80:63:08:65:42;
fixed-address 10.1.112.82;
}
#
# Host hugo requests IP configuration
# with his client identifier.
#
host hugo {
#
option dhcp-client-identifier "hugo";
option dhcp-client-identifier 00:68:75:67:6f;
fixed-address 10.1.112.83;
server-name "10.1.112.11";
filename "/agent/config.dat";
}
```

Lines beginning with the # character, contain comments.

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

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

For further information, please refer to the DHCP server manual.

2.7 Management address conflict detection

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

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

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

2.7.1 Active and passive detection

Actively checking the network helps prevent the device from connecting to the network with a duplicate IP address. After connecting the device to a network or after configuring the IP address, the device immediately checks whether its IP address exists within the network. To check the network for address conflicts, the device sends 4 ARP probes with the detection delay of 200 ms into the network. If the IP address exists, the device returns to the previous configuration, if possible, and makes another check after the configured release delay time.

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

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

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

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

3 Access to the device

3.1 First login (Password change)

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

Perform the following steps:

☐ Open the Graphical User Interface, the Command Line Interface, or HiView the first time you log on to the device.

☐ Log on to the device with the default password.
The device prompts you to type in a new password.

☐ Type in your new password.
To help increase security, choose a password that contains at least 8 characters which includes upper-case characters, lower-case characters, numerical digits, and special characters.

☐ When you log on to the device with the Command Line Interface, then the device prompts you to confirm your new password.

☐ Log on to the device again with your new password.

If you lost your password, then use the System Monitor to reset the password.

For further information see: hirschmann-support.belden.com.

3.2 Authentication lists

An authentication list contains the policies that the device applies for authentication when a user accesses the device using a specific connection.

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

3.2.1 Applications

The device provides an application for each type of connection through which someone accesses the device:
▶ Access using CLI via a serial connection: `Console(V.24)`
▶ Access using CLI via SSH: `SSH`
▶ Access using CLI via Telnet: `Telnet`
▶ Access using the graphical user interface: `WebInterface`

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

3.2.2 Policies

The device allows users to access its management exclusively when they log in with valid login data. The device authenticates the users using the following policies:
▶ User management of the device
▶ RADIUS

With the port-based access control according to IEEE 802.1X, the device allows connected end devices to access the network if they log in with valid login data. The device authenticates the end devices using the following policies:
▶ RADIUS
▶ IAS (Integrated Authentication Server)

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

3.2.3 Managing authentication lists

You manage the authentication lists in the graphical user interface or in the Command Line Interface.

Perform the following steps:

☐ Open the *Device Security > Authentication List* dialog.
The dialog displays the authentication lists that are set up.

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

☐ Deactivate the authentication list for those applications by means of which no access to the device is performed, for example `8021x`.

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

☐ To save the changes temporarily, click the ✔ button.

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

3.2.4   Adjust the settings

Example:
Set up a separate authentication list for the application `WebInterface` which is by default included in the authentication list `defaultLoginAuthList`. The device forwards authentication requests to a RADIUS server in the network. As a fall-back solution, the device authenticates users using the local user management.

Perform the following steps:

☐ Create an authentication list `loginGUI`.

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

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

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

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

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

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

    ☐ In the *Policy 1* column, select the value `radius`.
    ☐ In the *Policy 2* column, select the value `local`.
    ☐ In the *Policy 3* to *Policy 5* columns, select the value `reject` to help prevent further fall-back.
    ☐ In the *Active* column, mark the checkbox.

    ☐ To save the changes temporarily, click the ✓ button.

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

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

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

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

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

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

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

    ☐ To save the changes temporarily, click the ✓ button.

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

3.3 User management

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

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

3.3.1 Access roles

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

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

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

Role	Description	Authorized for the following activities
Administrator	The user is authorized to monitor and administer the device.	All activities with read/write access, including the following activities reserved for an administrator: ▶ Add, modify or delete user accounts ▶ Activate, deactivate or unlock user accounts ▶ Change every password ▶ Configure password management ▶ Set or change system time ▶ Load files to the device, for example device configurations, certificates or software images ▶ Reset settings and security-related settings to the state on delivery ▶ Configure RADIUS server and authentication lists ▶ Apply CLI scripts ▶ Enable/disable CLI logging and SNMP logging ▶ External memory activation and deactivation ▶ System monitor activation and deactivation ▶ Enable/disable the services for the management access (for example SNMP). ▶ Configure access restrictions to the user interfaces or the CLI based on the IP addresses
Operator	The user is authorized to monitor and configure the device - with the exception of security-related settings.	All activities with read/write access, with the exception of the above-named activities, which are reserved for an administrator:
Auditor	The user is authorized to monitor the device and to save the log file in the *Diagnostics > Report > Audit Trail* dialog.	Monitoring activities with read access.
Guest	The user is authorized to monitor the device - with the exception of security-related settings.	Monitoring activities with read access.
Unauthorized	No access to the device possible. ▶ As an administrator you assign this access role to temporarily lock a user account. ▶ The device assigns this access role to a user account if an error occurs when assigning a different access role.	No activities allowed.

Table 11: Access roles for user accounts

3.3.2 Managing user accounts

You manage the user accounts in the graphical user interface (GUI) or in the CLI.

Perform the following steps:

□ Open the *Device Security > User Management* dialog.
The dialog displays the user accounts that are set up.

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

3.3.3 Default setting

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

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

Table 12: Default settings for the factory setting user accounts

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

3.3.4 Changing default passwords

To help prevent undesired access, change the password of the default user accounts.

Perform the following steps:

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

□ Open the *Device Security > User Management* dialog.
The dialog displays the user accounts that are set up.
□ To obtain a higher level of complexity for the password, mark the checkbox in the *Policy check* column.
Before saving it, the device checks the password according to the policy specified in the *Password policy* frame.

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

□ Click the row of the relevant user account in the *Password* field. Enter a password of at least 6 characters.
Up to 64 alphanumeric characters are allowed.
▶ The device differentiates between upper and lower case.
▶ The minimum length of the password is specified in the *Configuration* frame. The device constantly checks the minimum length of the password.

□ To save the changes temporarily, click the ✓ button.

`enable`	Change to the Privileged EXEC mode.
`configure`	Change to the Configuration mode.
`users password-policy-check <user>` `enable`	Activates the checking of the password for the `<user>` user account based on the specified policy. In this way, you obtain a higher level of complexity for the password.

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

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

3.3.5 Setting up a new user account

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

In the following example, we will set up the user account for a USER user with the role operator. Users with the operator role are authorized to monitor and configure the device - with the exception of security-related settings.

Perform the following steps:

☐ Create a new user account.

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

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

☐ Enter the name in the *User name* field.
In this example, we give the user account the name USER.

☐ Click the *Ok* button.

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

☐ In the *Password* field, enter a password of at least 6 characters.
Up to 64 alphanumeric characters are allowed.
▶ The device differentiates between upper and lower case.
▶ The minimum length of the password is specified in the *Configuration* frame. The device constantly checks the minimum length of the password.

☐ In the *Role* column, select the user role.
In this example, we select the value operator.

☐ To activate the user account, mark the checkbox in the *Active* column.

☐ To save the changes temporarily, click the ✓ button.
The dialog displays the user accounts that are set up.

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

Note: Remember to allocate the password when you are setting up a new user account in the CLI.

3.3.6 Deactivating the user account

After a user account is deactivated, the device denies the related user access to the management functions. In contrast to completely deleting it, deactivating a user account allows you to keep the settings and reuse them in the future.

Perform the following steps:

☐ To keep the user account settings and reuse them in the future, you temporarily deactivate the user account.

☐ Open the *Device Security > User Management* dialog.
The dialog displays the user accounts that are set up.

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

☐ To save the changes temporarily, click the ✓ button.

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

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

☐ Highlight the row for the relevant user account.

☐ Click the 🔲 button.

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

3.3.7   Adjusting policies for passwords

The device allows you to check whether the passwords for the user accounts adhere to the specified policy. You obtain a higher level of complexity for the passwords when they adhere to the policy.

The user management of the device allows you to activate or deactivate the check separately in each user account. When the check is activated, the device accepts a changed password only if it fulfills the requirements of the policy.

In the default settings, practical values for the policy are set up on the device. You have the option of adjusting the policy to meet your requirements.

Perform the following steps:

☐ Adjust the policy for passwords to meet your requirements.

   ☐ Open the *Device Security > User Management* dialog.
   In the *Configuration* frame you specify the number user login attempts before the device locks out the user. You also specify the minimum number of characters that defines a password.
   ☐ Specify the values to meet your requirements.
      ▶ You specify the number of times that a user attempts to log on to the device in the *Login attempts* field. The field allows you to define this value in the range `0..5`.
        In the above example, the value `0` deactivates the function.
      ▶ The *Min. password length* field allows values in the range `1..64`.
   The dialog displays the policy set up in the *Password policy* frame.
   ☐ Adjust the values to meet your requirements.
      ▶ Values in the range `1` through `16` are allowed.
        The value `0` deactivates the relevant policy.
   To apply the entries specified in the *Configuration* and *Password policy* frames, mark the checkbox in the *Policy check* column for a particular user.

   ☐ To save the changes temporarily, click the ✅ button.

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

`show passwords`	Displays the policies that are set up.
`save`	Save the settings in the non-volatile memory (`nvm`) in the "selected" configuration profile.

3.4 SNMP access

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

3.4.1 SNMPv1/v2 access

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

The community names `public` for read accesses and `private` for write accesses are preset in the device. If SNMPv1/v2 is enabled, the device allows anyone who knows the community name to access the device.

Make the following basic provisions to make undesired access to the device more difficult:

☐ Change the default community names in the device.
  Treat the community names with discretion.
  Anyone who knows the community name for write access, has the ability to change the settings of the device.
☐ Specify a different community name for read/write access than for read access.

☐ Use SNMPv1 or SNMPv2 only in environments protected from eavesdropping. The protocols do not use encryption.

☐ We recommend using SNMPv3 and disabling the access using SNMPv1 and SNMPv2 in the device.

3.4.2 SNMPv3 access

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

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

When you set up a new user account on the device, the parameters are preset so that the network management system Industrial HiVision reaches the device immediately.

The user accounts set up in the device use the same passwords in the graphical user interface, in the command line interface (CLI), and for SNMPv3.

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

☐ Open the *Device Security > User Management* dialog.
  The dialog displays the user accounts that are set up.
☐ Click the row of the relevant user account in the *SNMP auth type* field. Select the desired setting.
☐ Click the row of the relevant user account in the *SNMP encryption type* field. Select the desired setting.

☐ To save the changes temporarily, click the ✓ button.

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

3.5 Service Shell

When you need assistance with your device, then the service personnel use the Service Shell to monitor internal conditions, for example switch or CPU registers.

The Service Shell is for service purposes exclusively. This function allows the access on internal functions of the device. In no case, execute internal functions without service technician instructions. Executing internal functions such as deleting the content of the NVM (non-volatile memory) possibly leads to inoperability of your device.

■ Start the Service Shell

Perform the following steps:

☐ To switch from the User Exec mode to the Privileged Exec mode, enter `enable`, or enter `en` and a `Space` character, and press the <Enter> key.

☐ To get a list of the commands available in this mode, press the <?> key.

```
!EESX >enable

!EESX #?
  clear              Clear several items.
  configure          Enter into global config mode.
  copy               Copy different kinds of items.
  debug              Service functions to find configuration errors.
  exit               Exit from current mode.
  help               Display help for various special keys.
  history            Show a list of previously run commands.
  login              Set login parameters.
  logout             Exit this session.
  network            Modify network parameters.
  ping               Send ICMP echo packets to a specified
                     IP address.
  profile            Activate or delete configuration profiles.
  reboot             Reset the device (cold start).
  save               Save configuration.
  serviceshell       Enter system mode.
  set                Set device parameters.
  show               Display device options and settings.
  traceroute         Trace route to a specified host.

!EESX #serviceshell

-> exit
Au revoir!

!*EESX #
```

☐ To start the Service Shell, enter `serviceshell` in the privileged exec mode, or enter `ser` and a `Space` character, and press the <Enter> key.

> To help prevent configuration inconsistencies, log out from the Service Shell before any other user starts uploading a new configuration to the device.

☐ To end the Service Shell, enter `exit` and then press the <Enter> key.

Note: When the Service Shell is active, the timeout of the Command Line Interface is inactive.

■ Deactivate the Service Shell permanently

If you do not need the Service Shell, the device allows you to disable the function. In this case you still have the option to configure the device. Though, the service technician has no possibilities to access internal functions of your device to call up additional required information.

Note: When you deactivate the Service Shell, then you are still able to configure the device, but you limit the service personnel to system diagnostics. The deactivation is irreversible, the Service Shell remains permanently deactivated. **In order to reactivate the Service Shell, the device requires disassembly by the manufacturer.**

Perform the following steps:

☐ To display the Service Shell, enter `serviceshell`, or enter `ser` and a `Space` character, and press the <Enter> key.

☐ This process is irreversible!
To permanently deactivate the Service Shell, enter `deactivate`, or enter `d` and a `Space` character, and press the <Enter> key.

```
!EESX >enable

!EESX #serviceshell?
 [deactivate]           Disable the service shell access permanently
                        (Cannot be undone).
  <cr>                  Press Enter to execute the command.

!EESX #serviceshell deactivate
```

4 Managing configuration profiles

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

In order to keep the changes after a reboot, the device offers the possibility of saving additional settings in a configuration profile in the non-volatile memory (`NVM`). In order to make it possible to quickly switch to other settings, the non-volatile memory offers storage space for multiple configuration profiles.

If an external memory is connected, the device generates a copy of the configuration profile on the external memory automatically. This function can be deactivated.

4.1   Detecting changed settings

Changes made to settings during operation are stored by the device in its memory (RAM). The configuration profile in non-volatile memory (NVM) remains unchanged until you explicitly save it. Until then, the configuration profiles in memory and non-volatile memory differ.

This device helps you recognize changed settings. If the configuration profile in the memory (RAM) differs from the "selected" configuration profile in the non-volatile memory (NVM), you can recognize the difference based on the following criteria:

The status bar at the top of the menu displays the icon . If the configuration profiles match, the icon is hidden.

Tn the *Basic Settings > Load/Save* dialog, the checkbox in the *Information* frame is unmarked. If the configuration profiles match, the checkbox is marked.

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

If the copy in the external memory differs from the configuration profile in the non-volatile memory, you see the difference based on the following criteria:

Tn the *Basic Settings > Load/Save* dialog, the checkbox in the *Information* frame is unmarked. If the configuration profiles match, the checkbox is marked.

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

4.2 Saving the settings

4.2.1 Saving the configuration profile in the device

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

■ Saving a configuration profile

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

Perform the following steps:

- ☐ Open the *Basic Settings > Load/Save* dialog.
- ☐ Verify that the desired configuration profile is "Selected".
  You can recognize the "selected" configuration profile by the fact that the checkbox in the *Selected* column is marked.
- ☐ Click the ✔ button.

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

■ Copying settings to a configuration profile

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

Perform the following steps:

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

The new configuration profile is designated as "Selected".

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

■ Selecting a configuration profile

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

Perform the following steps:

□ Open the *Basic Settings > Load/Save* dialog.
The table displays the configuration profiles present in the device. You can recognize the "selected" configuration profile by the fact that the checkbox in the *Selected* column is marked.
□ In the table, select the entry of the desired configuration profile stored in non-volatile memory (NVM).

□ Click the ☰ button and then the *Select* item.

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

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

4.2.2 Backup the configuration profile on a remote server

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

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

Perform the following steps:

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

□ To save the changes temporarily, click the ✓ button.

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

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

4.2.3 Saving the configuration profile in external memory

When you save a configuration profile, the device automatically creates a copy in external memory when the external memory is connected. In the default setting, the function is enabled. You have the following option of enabling or disabling this function.

Perform the following steps:

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

☐ In order to cause the device to automatically generate a copy in external memory during the saving process, select the checkbox in the *Backup config when saving* column.

☐ To disable the function, remove the checkmark from the checkbox in the *Backup config when saving* column.

☐ To save the changes temporarily, click the ✅ button.

`enable`	Change to the Privileged EXEC mode.
`configure`	Change to the Configuration mode.
`config envm config-save sd`	Enable the function. When you save a configuration profile, the device creates a copy in the external memory. `sd` = External SD memory
`no config envm config-save sd`	Disable the function. The device does not create a copy in the external memory. `sd` = External SD memory
`save`	Save the settings in the non-volatile memory (`nvm`) in the "selected" configuration profile.

4.2.4 Exporting a configuration profile

The device offers you the option of saving a configuration profile to a server as an XML file. If you use the graphical user interface, you have the option to save the XML file directly to your PC.

Prerequisite:
▶ To save the file on a server, you need a configured server on the network.
▶ To save the file to an SCP or SFTP server, you also need the username and password for accessing this server.

Perform the following steps:

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

To export the configuration profile to your PC, perform the following steps:

☐ Click the link in the *Profile name* column.
☐ Select the storage location and specify the file name.
☐ Click the *Ok* button.
The configuration profile is now saved as an XML file in the specified location.

To export the configuration profile to a remote server, perform the following steps:

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

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

`copy config nvm remote sftp://`
`<user_name>:<password>@<IP_address>/`
`<path>/<file_name>`
	Saves the selected configuration profile in the non-volatile memory (`nvm`) on a SFTP server.

`copy config nvm profile config3`
`remote tftp://<IP_address>/ <path>/`
`<file_name>`
	Save the configuration profile `config3` in the non-volatile memory (`nvm`) on a TFTP server.

`copy config nvm profile config3`
`remote ftp://<IP_address>:<port>/<path>/`
`<file_name>`
	Save the configuration profile `config3` in the non-volatile memory (`nvm`) on an FTP server.

4.3 Loading settings

Through loading of settings, the device allows you to quickly switch to other settings if required.

4.3.1 Activating a configuration profile

The non-volatile memory of the device can accommodate several configuration profiles. If you activate a configuration profile stored there, you change the settings on the device on the fly without rebooting.

Perform the following steps:

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

☐ Click the ▤ button and then the *Activate* item.

The device copies the settings to memory (`RAM`) and disconnects from the graphical user interface. The device immediately uses the settings of the configuration profile on the fly.
☐ Reload the graphical user interface.
☐ Log in again.

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

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

4.3.2 Loading the configuration profile from the external memory

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

If the external memory contains the configuration profile of an identical device, this allows you to transfer the settings from one device to another.

Perform the following steps:

☐ Verify that the device loads a configuration profile from the external memory upon restart.

In the default setting, the function is enabled. If the function is disabled, enable it again as follows:

☐ Open the *Basic Settings > External Memory* dialog.
☐ In the *Config priority* column, select the value `first`.

☐ To save the changes temporarily, click the ✓ button.

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

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

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

The device allows you via CLI to copy the settings from the external memory directly into non-volatile memory.

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

4.3.3 Importing a configuration profile

The device allows you to import from a server a configuration profile saved as an XML file. If you use the graphical user interface, you have the option to import the XML file directly from your PC.

Prerequisite:
▶ To save the file on a server, you need a configured server on the network.
▶ To save the file to an SCP or SFTP server, you also need the username and password for accessing this server.

Perform the following steps:

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

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

To import the configuration profile from the local PC or from a remote server, perform the following steps:

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

To import the configuration profile from the external memory, perform the following steps:

☐ In the *Import profile from external memory* frame, *Profile name* drop-down list, select the name of the configuration profile to be imported.
The prerequisite is that the external memory contains an exported configuration profile.
☐ In the *Destination* frame, specify where the device saves the imported configuration profile:
  ☐ In the *Profile name* field, specify the name under which the device saves the configuration profile.
☐ Click the *Ok* button.
The device copies the configuration profile into the non-volatile memory (`NVM`) of the device.
If you specified the value `ram` in the *Destination* frame, the device disconnects the graphical user interface and uses the settings immediately on the fly.

`enable`	Change to the Privileged EXEC mode.
`copy config remote ftp://` `<IP_address>:<port>/<path>/<file_name>` `running-config`	Import and activate the settings of a configuration profile saved on an FTP server. The device copies the settings into the volatile memory and disconnects the CLI connection. The device immediately uses the settings of the imported configuration profile on the fly.

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

4.4 Reset the device to the factory defaults

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

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

The device then reboots and loads the factory settings.

4.4.1 Using the graphical user interface or CLI

Perform the following steps:

☐ Open the *Basic Settings > Load/Save* dialog.
☐ Click the ▾ button, then *Back to factory...*.
   The dialog displays a warning message.
☐ Click the *Ok* button.
The device deletes the configuration profiles in the memory (RAM) and in the non-volatile memory (NVM).
If an external memory is connected, the device also deletes the configuration profiles saved on the external memory.
After a brief period, the device restarts and loads the delivery settings.

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

4.4.2 Using the System Monitor

Prerequisite:
Your PC is connected with the V.24 connection of the device using a terminal cable.

Perform the following steps:

☐ Restart the device.

☐ To switch to the System Monitor, press the <1> key within 3 seconds when prompted during reboot.
   The device loads the System Monitor.

☐ To switch from the main menu to the `Manage configurations` menu, press the <4> key.

☐ To execute the `Clear configs and boot params` command, press the <1> key.

☐ To load the factory settings, press the <Enter> key.
   The device deletes the configuration profiles in the memory (RAM) and in the non-volatile memory (NVM).

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

☐ To switch to the main menu, press the <q> key.

☐ To reboot the device with factory settings, press the <q> key.

5 Loading software updates

Hirschmann is continually working on improving and developing their software. Check regularly whether 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 gives you the following options for updating the device software:
- ▶ Software update from the PC
- ▶ Software update from a server
- ▶ Software update from the external memory
- ▶ Loading an older software

Note: The device settings are kept after updating the device software.
You see the version of the installed device software on the Login page of the graphical user interface. If you are already logged in, perform the following steps to display the version of the installed software.

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

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

5.1   Software update from the PC

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

Perform the following steps:

☐ Navigate to the folder where the image file of the device software is saved.

☐ Open the *Basic Settings > Software* dialog.

☐ Drag and drop the image file in the ⬆ area. Alternatively click in the area to select the file.

☐ To start the update procedure, click the *Start* button.
As soon as the update procedure is completed successfully, the device displays an information that the software is successfully updated.
Upon restart, the device loads the installed device software.

5.2 Software update from a server

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

Perform the following steps:

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

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

5.3 Software update from the external memory

5.3.1 Manually—initiated by the administrator

The device allows you to update the device software with just a few mouse clicks. The prerequisite is that the image file of the device software is located in the external memory.

Perform the following steps:

☐ Open the *Basic Settings > Software* dialog.
☐ In the table, mark the row which displays the name of the desired image file on the external memory.
☐ Right-click to display the context menu.
☐ To start the update procedure, click in the context menu the *Update* item.

   The device copies the currently running device software into the backup memory.
   As soon as the update procedure is completed successfully, the device displays an information that the software is successfully updated.
   Upon restart, the device loads the installed device software.

5.3.2 Automatically—initiated by the device

During a restart the device updates the device software automatically when the following files are located in the external memory:
▶ the image file of the device software
▶ a text file `startup.txt` with the content `autoUpdate=<Image_file_name>.bin`

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

Perform the following steps:

☐ Copy the image file of the new device software into the main directory of the external memory. Use an image file suitable for the device exclusively.
☐ Create a text file `startup.txt` in the main directory of the external memory.
☐ Open the `startup.txt` file in the text editor and add the following line: `autoUpdate=<Image_file_name>.bin`
☐ Install the external memory on the device.
☐ Restart the device.
   During the booting process, the device checks automatically the following criteria:
   – Is an external memory connected?
   – Is a `startup.txt` file in the main directory of the external memory?
   – Does the image file exist which is specified in the `startup.txt` file?
   – Is the software version of the image file more recent than the software currently running on the device?
   If the criteria are fulfilled, the device starts the update procedure.
   The device copies the currently running device software into the backup memory.
   As soon as the update procedure is completed successfully, the device reboots automatically and loads the new software version.

Check the result of the update procedure. The log file in the *Diagnostics > Report > System Log* dialog contains one of the following messages:
▶ `S_watson_AUTOMATIC_SWUPDATE_SUCCESS`
   Software update completed successfully
▶ `S_watson_AUTOMATIC_SWUPDATE_ABORTED`
   Software update aborted
▶ `S_watson_AUTOMATIC_SWUPDATE_ABORTED_WRONG_FILE`
   Software update aborted due to wrong image file
▶ `S_watson_AUTOMATIC_SWUPDATE_ABORTED_SAVING_FILE`
   Software update aborted due to failed saving of the image file to the device

5.4 Loading an older software

The device allows you to replace the device software with an older version. The basic settings on the device are kept after replacing the device software.

Note: The settings for functions which are available in the newer device software version exclusively are lost.

6   Configuring the ports

The following port configuration functions are available.

▶ Enabling/disabling the port
▶ Selecting the operating mode

6.1 Enabling/disabling the port

In the default setting, every port is enabled. For a higher level of access security, disable unconnected ports.

Perform the following steps:

- □ Open the *Basic Settings > Port* dialog, *Configuration* tab.
- □ To enable a port, mark the checkbox in the *Port on* column.
- □ To disable a port, unmark the checkbox in the *Port on* column.

- □ To save the changes temporarily, click the ✓ button.

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

6.2 Selecting the operating mode

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

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

Perform the following steps:

☐ Open the *Basic Settings > Port* dialog, *Configuration* tab.
☐ If the device connected to this port requires a fixed setting:
  ☐ Deactivate the function. Unmark the checkbox in the *Automatic configuration* column.
  ☐ In the *Manual configuration* column, enter the desired operating mode (transmission rate, duplex mode).

☐ To save the changes temporarily, click the ✅ button.

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

7 Assistance in the protection from unauthorized access

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

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

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

7.1 Changing the SNMPv1/v2 community

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

The community names `public` for read accesses and `private` for write accesses are preset. If you are using SNMPv1 or SNMPv2, you change the default community name. Treat the community names with discretion.

Perform the following steps:

☐ Open the *Device Security > Management Access > SNMPv1/v2 Community* dialog.
The dialog displays the communities that are set up.
☐ For the `Write` community, specify in the *Name* column the community name.
  ▶ Up to 32 alphanumeric characters are allowed.
  ▶ The device differentiates between upper and lower case.
  ▶ Specify a different community name than for read access.

☐ To save the changes temporarily, click the ✅ button.

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

7.2 Disabling SNMPv1/v2

If you need SNMPv1 or SNMPv2, use these protocols solely in environments protected from eavesdropping. SNMPv1 and SNMPv2 do not use encryption. The SNMP packets contain the community in clear text. We recommend using SNMPv3 in the device and disabling the access using SNMPv1 and SNMPv2.

Perform the following steps:

☐ Open the *Device Security > Management Access > Server* dialog, *SNMP* tab.
The dialog displays the settings of the SNMP server.
☐ To deactivate the SNMPv1 protocol, you unmark the *SNMPv1* checkbox.
☐ To deactivate the SNMPv2 protocol, you unmark the *SNMPv2* checkbox.

☐ To save the changes temporarily, click the ✓ button.

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

7.3 Disabling HTTP

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

The HTTP protocol is enabled by default. If you disable HTTP, no unencrypted access to the graphical user interface is possible.

Perform the following steps:

□ Open the *Device Security > Management Access > Server* dialog, *HTTP* tab.

□ To disable the HTTP protocol, select the `Off` radio button in the *Operation* frame.

□ To save the changes temporarily, click the ✓ button.

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

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

When the HTTPS protocol is disabled and you also disable HTTP, then the graphical user interface is unaccessible. To work with the graphical user interface, enable the HTTPS server using the command line interface.

Perform the following steps:

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

7.4 Disabling Telnet

The device allows you to remotely access the management functions of the device using Telnet or SSH. Telnet connections are unencrypted, while SSH connections are encrypted.

The Telnet server is enabled on the device by default. If you disable Telnet, unencrypted remote access to the command line interface is no longer possible.

Perform the following steps:

☐ Open the *Device Security > Management Access > Server* dialog, *Telnet* tab.
☐ To disable the Telnet server, select the `Off` radio button in the *Operation* frame.

☐ To save the changes temporarily, click the ✔ button.

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

If the SSH server is disabled and you also disable Telnet, the access to the Command Line Interface is only possible through the V.24 interface of the device. To work remotely with the command line interface, enable SSH.

Perform the following steps:

☐ Open the *Device Security > Management Access > Server* dialog, *SSH* tab.
☐ To enable the *SSH* server, select the `On` radio button in the *Operation* frame.

☐ To save the changes temporarily, click the ✔ button.

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

7.5 Disabling the HiDiscovery access

HiDiscovery allows you to assign IP parameters to the device over the network during commissioning. HiDiscovery communicates in the management VLAN without encryption and authentication.

After the device is commissioned, we recommend to setHiDiscoveryto read-only or to disable HiDiscovery access completely.

Perform the following steps:

□ Open the *Basic Settings > Network* dialog, *Global* tab.
□ To take away write permission from the HiDiscovery software, in the *HiDiscovery protocol v1/v2* frame, specify the value readOnly in the *Access* field.
□ To disable HiDiscovery access completely, select the Off radio button in the *HiDiscovery protocol v1/v2* frame.

□ To save the changes temporarily, click the ✓ button.

```
enable                              Change to the Privileged EXEC mode.
network hidiscovery mode read-only  Disable write permission of the HiDiscovery software.
no network hidiscovery operation    Disable HiDiscovery access.
```

7.6 Activating the IP access restriction

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

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

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

Parameter	Company network	Mobile phone network
Network address	192.168.1.0	109.237.176.0
Netmask	24	24
Desired protocols	https, snmp	ssh

Table 13: Parameters for the IP access restriction

Perform the following steps:

☐ Open the *Device Security > Management Access > IP Access Restriction* dialog.
☐ Unmark the checkbox in the *Active* column for the entry.
  This entry allows access to the device from any IP address and the supported protocols.
Address range of the company network:

☐ To add a table entry, click the [icon] button.

☐ Specify the address range of the company network in the *IP address range* column: `192.168.1.0/24`
☐ For the address range of the corporate network, deactivate the undesired protocols. The *HTTPS*, *SNMP*, and *Active* checkboxes remain marked.
Address range of the mobile phone network:

☐ To add a table entry, click the [icon] button.

☐ Specify the address range of the mobile network in the *IP address range* column: `109.237.176.0/24`
☐ For the address range of the mobile network, deactivate the undesired protocols. The *SSH* and *Active* checkboxes remain marked.
Before you enable the function, verify that at least one active entry in the table allows you access. Otherwise, the connection to the device terminates when you change the settings. To access the management functions is possible solely using the CLI through the V.24 interface of the device.
☐ To enable IP access restriction, select the `On` radio button in the *Operation* frame.

☐ To save the changes temporarily, click the ✓ button.

```
enable                                    Change to the Privileged EXEC mode.
show network management access global     Displays whether IP access restriction is enabled or disabled.
show network management access rules      Display the entries that have been configured.

no network management access operation    Disable the IP access restriction.

network management access add 2           Create the entry for the address range of the company network.
                                          Number of the next available index in this example: 2.
network management access modify 2 ip     Specify the IP address of the company network.
192.168.1.0
network management access modify 2 mask   Specify the netmask of the company network.
24
network management access modify 2 ssh    Deactivate SSH for the address range of the company network.
disable                                   Repeat the operation for every unwanted protocol.
```

`network management access add 3`	Create an entry for the address range of the mobile phone network. Number of the next available index in this example: 3.
`network management access modify 3 ip 109.237.176.0`	Specify the IP address of the mobile phone network.
`network management access modify 3 mask 24`	Specify the netmask of the mobile phone network.
`network management access modify 3 snmp disable`	Deactivate SNMP for the address range of the mobile phone network. Repeat the operation for every unwanted protocol.
`no network management access status 1`	Deactivate the default entry. This entry allows access to the device from any IP address and the supported protocols.
`network management access status 2`	Activate an entry for the address range of the company network.
`network management access status 3`	Activate an entry for the address range of the mobile phone network.
`show network management access rules`	Display the entries that have been configured.
`network management access operation`	Enable the IP access restriction.

7.7 Adjusting the session timeouts

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

You can specify a session timeout for the following applications:
▶ CLI sessions using an SSH connection
▶ CLI sessions using a Telnet connection
▶ CLI sessions using a V.24 connection
▶ Graphical user interface

■ **Session timeout for CLI sessions using a SSH connection**

Perform the following steps:

☐ Open the *Device Security > Management Access > Server* dialog, *SSH* tab.
☐ Specify the timeout period in minutes in the *Configuration* frame, *Session timeout [min]* field.

☐ To save the changes temporarily, click the ✓ button.

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

■ **Timeout for CLI sessions using a Telnet connection**

Perform the following steps:

☐ Open the *Device Security > Management Access > Server* dialog, *Telnet* tab.
☐ Specify the timeout period in minutes in the *Configuration* frame, *Session timeout [min]* field.

☐ To save the changes temporarily, click the ✓ button.

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

■ **Session timeout for CLI sessions using a V.24 connection**

Perform the following steps:

☐ Open the *Device Security > Management Access > CLI* dialog, *Global* tab.
☐ Specify the timeout period in minutes in the *Configuration* frame, *V.24 timeout [min]* field.

☐ To save the changes temporarily, click the ✓ button.

`enable`	Change to the Privileged EXEC mode.
`cli serial-timeout <0..160>`	Specify the timeout period in minutes for CLI sessions using a V.24 connection.

■ **Session timeout for the graphical user interface**

Perform the following steps:

☐ Open the *Device Security > Management Access > Web* dialog.
☐ Specify the timeout period in minutes in the *Configuration* frame, *Web interface session timeout [min]* field.

☐ To save the changes temporarily, click the ✓ button.

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

8 Controlling the data traffic

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

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

The device provides the following functions for controlling the data stream:
- ▶ Service request control (Denial of Service, DoS)
- ▶ Denying access to devices based on their IP or MAC address (Access Control List)

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

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

8.1 Helping protect against unauthorized access

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

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

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

Filter	Action
Activate Null Scan Filter	The device detects and discards TCP packets for which no TCP flags are set.
Activate Xmas Filter	The device detects and discards TCP packets for which the TCP flags FIN, URG and PUSH are simultaneously set.
Activate SYN/FIN Filter	The device detects and discards TCP packets for which the TCP flags SYN and FIN are simultaneously set.
Activate Minimal Header Filter	The device detects and discards TCP packets for which the TCP header is too short.

Table 14: DoS filters for TCP packets

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

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

8.2 ACL

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

The device uses ACLs to filter data packets received on VLANs or on individual or multiple ports. In a ACL, you specify rules that the device uses to filter data packets. When such a rule applies to a packet, the device applies the actions specified in the rule to the packet. The available actions are as follows:

▶ allow (`permit`)
▶ discard (`deny`)
▶ redirect to a certain port (see *Redirection port* field)
▶ mirror (see *Mirror port* field)

The list below contains criteria that you can apply to filter the data packets:

▶ Source or destination address of a packet (MAC)
▶ Source or destination address of a data packet (IPv4)
▶ Source or destination port of a data packet (IPv4)

You can specify the following ACL types:

▶ IP ACLs for VLANs
▶ IP ACLs for ports
▶ MAC ACLs for VLANs
▶ MAC ACLs for ports

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

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

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

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

Note: The number of available ACLs depends on the device. You find more information about the ACL values in the chapter "Technical Data" on page 237.

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

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

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

8.2.1 Creating and editing IPv4 rules

When filtering IPv4 data packets, the device allows you to:
▶ create new groups and rules
▶ add new rules to existing groups

▶ edit an existing rule
▶ activate and deactivate groups and rules
▶ delete existing groups and rules
▶ change the order of existing rules

Perform the following steps:

☐ Open the *Network Security > ACL > IPv4 Rule* dialog.

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

☐ To create a group, specify a meaningful name in the *Group name* field. You can combine several rules in one group.

☐ To add a rule to an existing group, select the name of the group in the *Group name* field.

☐ In the *Index* field you specify the number for the rule within the ACL.
   This number defines the priority of the rule.

☐ Click the *Ok* button.
   The device adds the rule to the table.
   Group and role are active immediately.
   To deactivate group or rules, unmark the checkbox in the *Active* column.

   To remove a rule, highlight the affected table entry and click the 🔳 button.

☐ Edit the rule parameters in the table.
   To change a value, double-click the relevant field.

☐ To save the changes temporarily, click the ✅ button.

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

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

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

8.2.2   Creating and configuring an IP ACL using the CLI

In the following example, you configure ACLs to block communications from computers B and C, to computer A via IP (TCP, UDP, etc.).
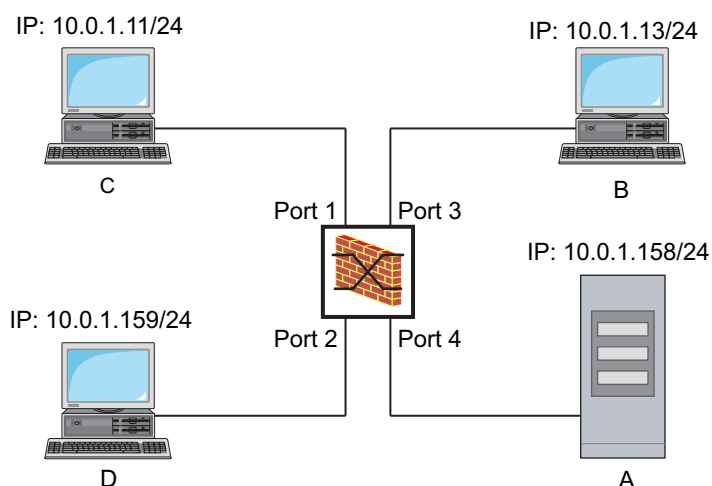
Figure 20: Example of an IP ACL

Perform the following steps:

```
enable                              Change to the Privileged EXEC mode.
configure                           Change to the Configuration mode.
ip acl add 1 filter                 Adds an IP ACL with the ID 1 and the name filter.
```

`ip acl rule add 1 1 deny src 10.0.1.11 0.0.0.0 dst 10.0.1.158 0.0.0.0`	Adds a rule to position `1` of the IP ACL with the ID `1` denying IP data packets from `10.0.1.11` to `10.0.1.158`.
`ip acl rule add 1 2 permit src any any dst any any`	Adds a rule to position `2` of the IP ACL with the ID `1` admitting IP data packets.
`show acl ip rules 1`	Displays the rules of the IP ACL with the ID `1`.
`ip acl add 2 filter2`	Adds an IP ACL with the ID `2` and the name `filter2`.
`ip acl rule add 2 1 deny src 10.0.1.13 0.0.0.0 dst 10.0.1.158 0.0.0.0`	Adds a rule to position `1` of the IP ACL with the ID `2` denying IP data packets from `10.0.1.13` to `10.0.1.158`.
`ip acl rule add 2 2 permit src any any dst any any`	Adds a rule to position `2` of the IP ACL with the ID `2` admitting IP data packets.
`show acl ip rules 2`	Displays the rules of the IP ACL with the ID `2`.
`interface 1/1`	Change to the interface configuration mode of interface `1/1`.
`acl ip assign 1 in 1`	Assigns the IP ACL with the ID `1` to incoming data packets (`in`) on interface `1/1`, with a priority of `1` (highest priority).
`exit`	Leaves the interface mode.
`interface 1/3`	Change to the interface configuration mode of interface `1/3`.
`acl ip assign 2 in 1`	Assigns the IP ACL with the ID `2` to incoming data packets (`in`) on interface `1/3`, with a priority of `1` (highest priority).
`exit`	Leaves the interface mode.
`show acl ip assignment 1`	Displays the assignment of the IP ACL with ID `1`.
`show acl ip assignment 2`	Displays the assignment of the IP ACL with ID `2`.

8.2.3 Creating and editing MAC rules

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

Perform the following steps:

☐ Open the *Network Security > ACL > MAC Rule* dialog.

☐ Click the [⊞] button.
  The dialog displays the *Create* window.

☐ To create a group, specify a meaningful name in the *Group name* field. You can combine several rules in one group.

☐ To add a rule to an existing group, select the name of the group in the *Group name* field.

☐ In the *Index* field you specify the number for the rule within the ACL.
  This number defines the priority of the rule.

☐ Click the *Ok* button.
  The device adds the rule to the table.
  Group and role are active immediately.
  To deactivate group or rules, unmark the checkbox in the *Active* column.

  To remove a rule, highlight the affected table entry and click the [⊞] button.

☐ Edit the rule parameters in the table.
  To change a value, double-click the relevant field.

☐ To save the changes temporarily, click the [✓] button.

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

8.2.4 Creating and configuring a MAC ACL using the CLI

In the following example, AppleTalk and IPX are to be filtered out from the entire network.

Perform the following steps:

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

`mac acl add 1 macfilter`	Adds an MAC ACL with the ID `1` and the name `macfilter`.
`mac acl rule add 1 1 deny src any any dst any any etype appletalk`	Adds a rule to position `1` of the MAC ACL with the ID `1` rejecting packets with EtherType `0x809B (AppleTalk)`.
`mac acl rule add 1 2 deny src any any dst any any etype ipx-old`	Adds a rule to position `2` of the MAC ACL with the ID `1` rejecting packets with EtherType `0x8137 (IPX alt)`.
`mac acl rule add 1 3 deny src any any dst any any etype ipx-new`	Adds a rule to position `3` of the MAC ACL with the ID `1` rejecting packets with EtherType `0x8138 (IPX)`.
`mac acl rule add 1 4 permit src any any dst any any`	Adds a rule to position `4` of the MAC ACL with the ID `1` forwarding packets.
`show acl mac rules 1`	Displays the rules of the MAC ACL with the ID `1`.
`interface 1/1,1/2,1/3,1/4,1/5,1/6`	Change to the interface configuration mode of the interfaces `1/1` to `1/6`.
`acl mac assign 1 in 1`	Assigns the MAC ACL with the ID `1` to incoming data packets (`1/1`) on interfaces `1/6` to `in`.
`exit`	Leaves the interface mode.
`show acl mac assignment 1`	Displays the assignment of the MAC ACL with the ID `1` to interfaces or VLANs.

8.2.5 Assigning ACLs to a port or VLAN

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

Perform the following steps:

☐ Open the *Network Security > ACL > Assignment* dialog.

☐ Click the 🔳 button.
 The dialog displays the *Create* window.
  ☐ In the *Port/VLAN* field, specify the desired port or the desired VLAN.
  ☐ In the *Priority* field, specify the priority.
  ☐ In the *Direction* field, specify the data packets to which the device applies the rule.
  ☐ In the *Group name* field, specify the rule the device assigns to the port or the VLAN.
☐ Click the *Ok* button.

☐ To save the changes temporarily, click the ✅ button.

9 Synchronizing the system time in the network

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

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

The device offers the following options for synchronizing the time on the network:

► The Simple Network Time Protocol (SNTP) is a simple solution for low accuracy requirements. Under ideal conditions, SNTP achieves an accuracy in the millisecond range. The accuracy depends on the signal delay.

9.1 Basic settings

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

9.1.1 Setting the time

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

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

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

Perform the following steps:

- ☐ Open the *Time > Basic Settings* dialog.
- ▶ The *System time (UTC)* field displays the current UTC (Universal Time Coordinated) of the device. UTC is the time relating to the coordinated world time measurement. UTC is the same worldwide and does not take local time shifts into account.
- ▶ The time in the *System time* field comes from the *System time (UTC)* plus the *Local offset [min]* value and a possible shift due to daylight saving time.

- ☐ In order to cause the device to apply the time of your PC to the *System time* field, click the *Set time from PC* button. Based on the value in the *Local offset [min]* field, the device calculates the time in the *System time (UTC)* field: The *System time (UTC)* comes from the *System time* minus the *Local offset [min]* value and a possible shift due to daylight saving time.
- ▶ The *Time source* field displays the origin of the time data. The device automatically selects the source with the greatest accuracy.
  The source is initially `local`.
  If SNTP is active and if the device receives a valid SNTP packet, the device sets its time source to `sntp`.
- ▶ The *Local offset [min]* value specifies the time difference between the local time and the *System time (UTC)*.
- ☐ In order to cause the device to determine the time zone on your PC, click the *Set time from PC* button. The device calculates the local time difference from UTC and enters the difference into the *Local offset [min]* field.

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

- ☐ To save the changes temporarily, click the ✔ button.

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

9.1.2 Automatic daylight saving time changeover

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

When daylight saving time is enabled, the device sets the local system time forward by 1 hour at the beginning of daylight saving time. At the end of daylight saving time, the device sets the local system time back again by 1 hour.

Perform the following steps:

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

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

☐ To save the changes temporarily, click the ✓ button.

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

9.2 SNTP

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

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

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

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

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

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

IP destination address	Send SNTP packets to
0.0.0.0	Nobody
224.0.1.1	Multicast address for SNTP messages
255.255.255.255	Broadcast address

Table 15: Target address classes for Broadcast operation mode

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

9.2.1 Preparation

Perform the following steps:

☐ To get an overview of how the time is passed on, draw a network plan with the devices participating in SNTP.

When planning, bear in mind that the accuracy of the time depends on the delays of the SNTP messages. To minimize delays and their variance, place an SNTP server in each network segment. Each of these SNTP servers synchronizes its own system time as an SNTP client with its parent SNTP server (SNTP cascade). The highest SNTP server in the SNTP cascade has the most direct access to a reference time source.
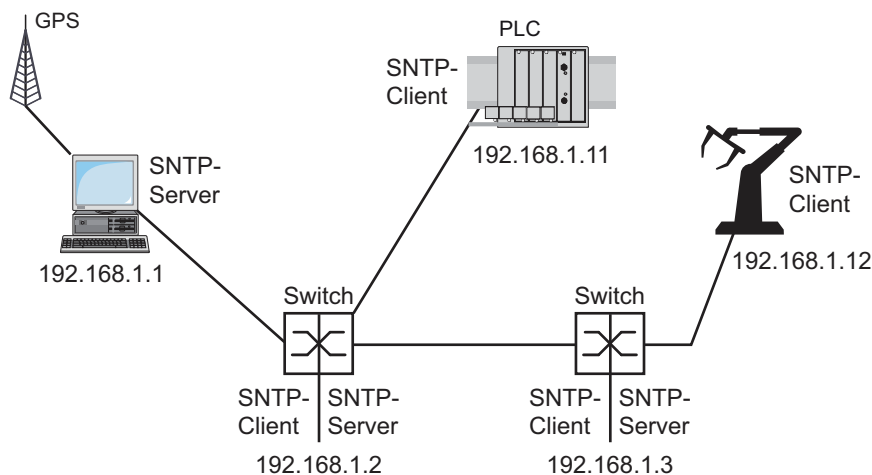
Figure 21: Example of SNTP cascade

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

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

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

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

9.2.2 Defining settings of the SNTP client

As an SNTP client, the device obtains the time information from SNTP or NTP servers and synchronizes its system clock accordingly.

Perform the following steps:

☐ Open the *Time > SNTP > Client* dialog.
☐ Set the SNTP operation mode.
   In the *Configuration* frame, select one of the following values in the *Mode* field:
   ▶ unicast
     The device sends requests to an SNTP server and expects a response from this server.
   ▶ broadcast
     The device waits for Broadcast messages from SNTP servers on the network.
☐ To synchronize the time only once, mark the *Disable client after successful sync* checkbox.
   After synchronization, the device disables the *SNTP Client* function.
▶ The table displays the SNTP server to which the SNTP client sends a request in Unicast operation mode. The table contains up to four SNTP server definitions.

☐ To add a table entry, click the 🖩 button.
☐ Specify the connection data of the SNTP server.
☐ To enable the function, select the On radio button in the *Operation* frame.

☐ To save the changes temporarily, click the ✓ button.

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

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

Table 16: SNTP client settings for the example

9.2.3 Specifying SNTP server settings

When the device operates as an SNTP server, it provides its system time in coordinated world time (UTC) in the network.

Perform the following steps:

☐ Open the *Time > SNTP > Server* dialog.
☐ To enable the function, select the On radio button in the *Operation* frame.

☐ To enable the Broadcast operation mode, select the *Broadcast admin mode* radio button in the *Configuration* frame.
In Broadcast operation mode, the SNTP server sends SNTP messages to the network in specified intervals. The SNTP server also responds to the requests from SNTP clients in Unicast operation mode.

    ☐ In the *Broadcast destination address* field, you set the IP address to which the SNTP server sends the SNTP packets. Set a Broadcast address or a Multicast address.

    ☐ In the *Broadcast UDP port* field, you specify the number of the UDP port to which the SNTP server sends the SNTP packets in Broadcast operation mode.

    ☐ In the *Broadcast VLAN ID* field, you specify the ID of the VLAN to which the SNTP server sends the SNTP packets in Broadcast operation mode.

    ☐ In the *Broadcast send interval [s]* field, you enter the time interval at which the SNTP server of the device sends SNTP Broadcast packets.

☐ To save the changes temporarily, click the ✅ button.

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

Device	192.168.1.1	192.168.1.2	192.168.1.3	192.168.1.11	192.168.1.12
SNTP Server function	On	On	On	Off	Off
UDP port	123	123	123	123	123
Broadcast admin mode	unmarked	unmarked	unmarked	unmarked	unmarked
Broadcast destination address	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0
Broadcast UDP port	123	123	123	123	123
Broadcast VLAN ID	1	1	1	1	1
Broadcast send interval [s]	128	128	128	128	128
Disable server at local time source	unmarked	unmarked	unmarked	unmarked	unmarked

Table 17: Settings for the example

10 Network load control

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

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

10.1 Direct packet distribution

The device reduces the network load with direct packet distribution.

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

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

10.1.1 Learning MAC addresses

If the device receives a data packet, it checks whether the MAC address of the sender is already stored in the MAC address table (FDB). If the MAC address of the sender is unknown, the device generates a new entry. The device then compares the destination MAC address of the data packet with the entries stored in the MAC address table (FDB):
- ▶ The device sends packets with a known destination MAC address directly to ports that have already received data packets from this MAC address.
- ▶ The device floods data packets with unknown destination addresses, that is, the device forwards these data packets to every port.

10.1.2 Aging of learned MAC addresses

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

10.1.3 Static address entries

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

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

You manage the static address entries in the graphical user interface (GUI) or in the CLI.

Perform the following steps:

□ Create a static address entry.

 □ Open the *Switching > Filter for MAC Addresses* dialog.
 □ Add a user-configurable MAC address:

  ▶ Click the ⊞ button.
  The dialog displays the *Create* window.
  ▶ In the *Address* field, specify the destination MAC address.
  ▶ In the *VLAN ID* field, specify the ID of the VLAN.
  ▶ In the *Port* list, select the ports to which the device sends data packets with the specified destination MAC address in the specified VLAN.
  Select exactly one port if you have defined a Unicast MAC address in the *Address* field.
  Select one or more ports if you have defined a Multicast MAC address in the *Address* field.
  Do not select any port if you want the device to discard data packets with the destination MAC address.
  ▶ Click the *Ok* button.

 □ To save the changes temporarily, click the ✓ button.

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

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

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

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

☐ To save the changes temporarily, click the ✓ button.

☐ Disable a static address entry.

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

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

☐ To save the changes temporarily, click the ✓ button.

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

☐ Delete learned MAC addresses.

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

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

10.2 Multicasts

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

The use of IGMP snooping can reduce the network load caused by Multicast data traffic. IGMP snooping allows the device to send Multicast data packets only on those ports to which devices "interested" in Multicast are connected.

10.2.1 Example of a Multicast application

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

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

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

10.2.2 IGMP snooping

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

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

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

Receivers log out with a "Leave" message when leaving a Multicast group (IGMP version 2 and higher) and do not send any more Report messages. The Multicast router removes the routing table entry of a receiver if it does not receive any more Report messages from this receiver within a certain time (aging time).

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

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

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

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

■ **Setting IGMP snooping**

Perform the following steps:

☐ Open the *Switching > IGMP Snooping > Global* dialog.

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

When the *IGMP Snooping* function is disabled, the device behaves as follows:

▶ The device ignores the received query and report messages.

▶ The device sends (floods) received data packets with a Multicast address as the destination address on every port.

☐ To save the changes temporarily, click the ✓ button.

☐ Specifying the settings for a port:

☐ Open the *Switching > IGMP Snooping > Configuration* dialog, *Port* tab.

☐ To activate the *IGMP Snooping* function on a port, mark the checkbox in the *Active* column for the relevant port.

☐ To save the changes temporarily, click the ✓ button.

☐ Specifying the settings for a VLAN:

☐ Open the *Switching > IGMP Snooping > Configuration* dialog, *VLAN ID* tab.

☐ To activate the *IGMP Snooping* function for a specific VLAN, mark the checkbox in the *Active* column for the relevant VLAN.

☐ To save the changes temporarily, click the ✓ button.

■ **Setting the IGMP querier function**

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

Prerequisite:
The *IGMP Snooping* function is enabled globally.

Perform the following steps:

☐ Open the *Switching > IGMP Snooping > Querier* dialog.

☐ In the *Operation* frame, enable/disable the *IGMP Snooping Querier* function of the device globally.

☐ To activate the *IGMP Snooping Querier* function for a specific VLAN, mark the checkbox in the *Active* column for the relevant VLAN.

▶ The device carries out a simple selection process: If the IP source address of the other Multicast querier is lower than its own, the device switches to the passive state, in which it does not send out any more query requests.

▶ In the *Address* column, you specify the IP Multicast address that the device inserts as the sender address in generated query requests. You use the address of the Multicast router.

☐ To save the changes temporarily, click the ✓ button.

■ IGMP snooping enhancements (table)

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

The following settings are possible:

▶ `Static`
Use this setting to set the port as a static query port. The device sends every IGMP message on a static query port, even if it has previously received no IGMP query messages on this port. If the static option is disabled, the device sends IGMP messages on this port only if it has previously received IGMP query messages. If that is the case, the entry displays `L` ("learned").

▶ `Learn by LLDP`
A port with this setting automatically discovers other Hirschmann devices using LLDP (Link Layer Discovery Protocol). The device then learns the IGMP query status of this port from these Hirschmann devices and configures the *IGMP Snooping Querier* function accordingly. The `ALA` entry indicates that the `Learn by LLDP` function is activated. If the device has found another Hirschmann device on this port in this VLAN, the entry also displays an `A` ("automatic").

▶ `Forward All`
With this setting, the device sends the data packets addressed to a Multicast address on this port. The setting is suitable in the following situations, for example:
– For diagnostic purposes.
– For devices in an MRP ring: After the ring is switched, the `Forward All` function allows rapid reconfiguration of the network for data packets with registered Multicast destination addresses. Activate the `Forward All` function on every ring port.

Prerequisite:
The *IGMP Snooping* function is enabled globally.

Perform the following steps:

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

☐ To save the changes temporarily, click the ✓ button.

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

■ Configure Multicasts

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

The settings for unknown Multicast addresses are global for the entire device. The following options can be selected:

▶ The device discards unknown Multicasts.

▶ The device sends unknown Multicasts on every port.

▶ The device sends unknown Multicasts exclusively on ports that have previously received query messages (query ports).

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

For each VLAN, you specify the sending of Multicast packets to known Multicast addresses individually. The following options can be selected:

▶ The device sends known Multicasts on the ports that have previously received query messages (query ports) and to the registered ports. Registered ports are ports with Multicast receivers registered with the corresponding Multicast group. This option helps ensure that the transfer works with basic applications without further configuration.

▶ The device sends out known Multicasts only on the registered ports. The advantage of this setting is that it uses the available bandwidth optimally through direct distribution.

Prerequisite:
The *IGMP Snooping* function is enabled globally.

Perform the following steps:
☐ Open the *Switching > IGMP Snooping > Multicasts* dialog.
☐ In the *Configuration* frame, you specify how the device sends data packets to unknown Multicast addresses.
 ▶ *send to registered ports*
  The device sends packets with unknown Multicast address to every query port.
 ▶ *send to query and registered ports*
  The device sends packets with unknown Multicast address to every port.
☐ In the *Known multicasts* column, you specify how the device sends data packets to known Multicast addresses in the corresponding VLAN. Click the relevant field and select the desired value.

☐ To save the changes temporarily, click the ✓ button.

10.3 Rate limiter

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

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

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

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

Perform the following steps:

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

  To activate the rate limiter on a port, mark the checkbox for at least one category. In the *Threshold unit* column, you specify whether the device interprets the threshold values as percent of the port bandwidth or as packets per second. The threshold value 0 deactivates the rate limiter.

☐ To save the changes temporarily, click the ✓ button.

10.4 QoS/Priority

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

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

10.4.1 Description of prioritization

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

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

■ Assigning traffic classes to the data

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

Both classification criteria are configurable.

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

■ Prioritizing traffic classes

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

► `Strict`
  When transmission of data of a higher traffic class is no longer taking place or the relevant data is still in the queue, the device sends data of the corresponding traffic class. If every traffic class is prioritized according to the `Strict` method, under high network load the device may permanently block the data of lower traffic classes.

► `Weighted Fair Queuing`
  The traffic class is assigned a guaranteed bandwidth. This helps ensure that the device sends the data traffic of this traffic class even if there is a great deal of data traffic in higher traffic classes.

10.4.2 Handling of received priority information

Applications label data packets with the following prioritization information:
▶ VLAN priority based on IEEE 802.1Q/ 802.1D (Layer 2)
▶ Type-of-Service (ToS) or DiffServ (DSCP) for VLAN Management IP packets (Layer 3)

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

10.4.3 VLAN tagging

For the VLAN and prioritizing functions, the IEEE 802.1Q standard provides for integrating a MAC frame in the VLAN tag. The VLAN tag consists of 4 bytes and is between the source address field ("Source Address Field") and type field ("Length / Type Field").
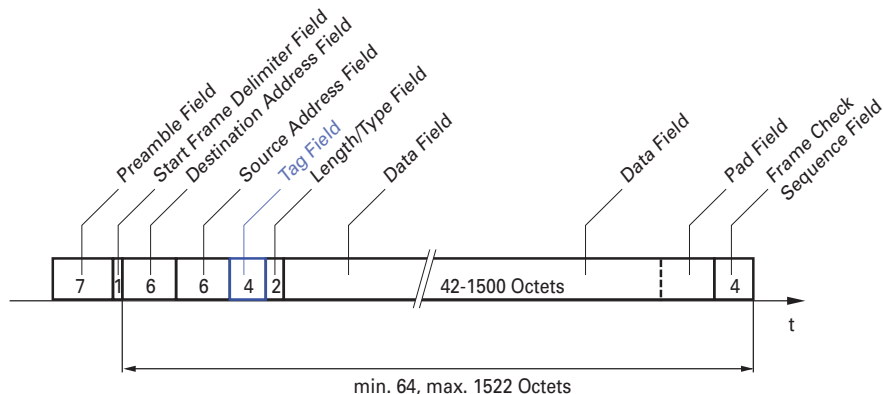
Figure 22: Ethernet data packet with tag

For data packets with VLAN tags, the device evaluates the following information:
▶ Priority information
▶ VLAN tagging, if VLANs are configured
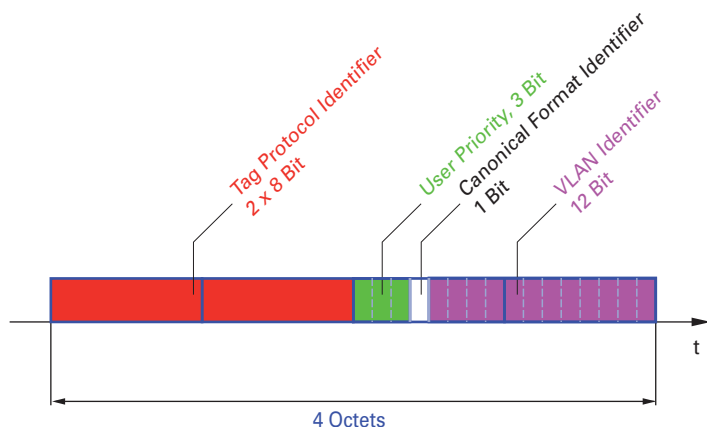
Figure 23: Structure of the VLAN tagging

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

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

When using VLAN prioritizing, consider the following special features:

▶ End-to-end prioritizing requires the VLAN tags to be transmitted to the entire network. The prerequisite is that every network component is VLAN-capable.

▶ Routers are not able to send and receive packets with VLAN tags through port-based router interfaces.

10.4.4 IP ToS (Type of Service)

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

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

Bits	0	1	2	3	4	5	6	7
	Precedence			Type of Service				MBZ

Bits (0-2): IP Precedence Defined	Bits (3-6): Type of Service Defined	Bit (7)
111 - Network Control	0000 - [all normal]	0 - Must be zero
110 - Internetwork Control	1000 - [minimize delay]	
101 - CRITIC / ECP	0100 - [maximize throughput	
100 - Flash Override	0010 - [maximize reliability]	
011 - Flash	0001 - [minimize monetary cost]	
010 - Immediate		
001 - Priority		
000 - Routine		

Table 18: ToS field in the IP header

10.4.5 Handling of traffic classes

The device provides the following options for handling traffic classes:

▶ Strict Priority
▶ Weighted Fair Queuing
▶ Strict Priority combined with Weighted Fair Queuing
▶ Queue management

■ Strict Priority description

With the Strict Priority setting, the device first transmits data packets that have a higher traffic class (higher priority) before transmitting a data packet with the next highest traffic class. The device transmits a data packet with the lowest traffic class (lowest priority) when there are no other data packets remaining in the queue. In unfortunate cases, the device does not send packets with a low priority if there is a high volume of high-priority traffic waiting to be sent on this port.
In delay-sensitive applications, such as VoIP or video, Strict Priority allows data to be sent immediately.

■ Weighted Fair Queuing description

With Weighted Fair Queuing, also called Weighted Round Robin (WRR), the user assigns a minimum or reserved bandwidth to each traffic class. This helps ensure that data packets with a lower priority are also sent when 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 may add up to 100%.

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

■ Combining Strict Priority and Weighted Fair Queuing

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

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

10.4.6 Queue management

■ Defining settings for queue management

Perform the following steps:

☐ Open the *Switching > QoS/Priority > Queue Management* dialog.
The total assigned bandwidth in the *Min. bandwidth [%]* column is 100%.
☐ To activate Weighted Fair Queuing for *Traffic class* = 0, proceed as follows:
  ▶ Unmark the checkbox in the *Strict priority* column.
  ▶ In the *Min. bandwidth [%]* column, specify the value 5.
☐ To activate Weighted Fair Queuing for *Traffic class* = 1, proceed as follows:
  ▶ Unmark the checkbox in the *Strict priority* column.
  ▶ In the *Min. bandwidth [%]* column, specify the value 20.
☐ To activate Weighted Fair Queuing for *Traffic class* = 2, proceed as follows:
  ▶ Unmark the checkbox in the *Strict priority* column.
  ▶ In the *Min. bandwidth [%]* column, specify the value 30.
☐ To activate Strict Priority for *Traffic class* = 3, proceed as follows:
  ▶ Mark the checkbox in the *Strict priority* column.
☐ To activate Weighted Fair Queuing for *Traffic class* = 4, proceed as follows:
  ▶ Unmark the checkbox in the *Strict priority* column.
  ▶ In the *Min. bandwidth [%]* column, specify the value 10.

☐ To save the changes temporarily, click the ✓ button.

`enable`	Change to the Privileged EXEC mode.
`configure`	Change to the Configuration mode.
`cos-queue weighted 0`	Enabling Weighted Fair Queuing for traffic class 0.
`cos-queue min-bandwidth: 0 5`	Assigning a weight of 5 % to traffic class 0.
`cos-queue weighted 1`	Enabling Weighted Fair Queuing for traffic class 1.
`cos-queue min-bandwidth: 1 20`	Assigning a weight of 20 % to traffic class 1.
`cos-queue weighted 2`	Enabling Weighted Fair Queuing for traffic class 2.

```
cos-queue min-bandwidth: 2 30          Assigning a weight of 30 % to traffic class 2.
show cos-queue
Queue Id  Min. bandwidth   Scheduler type
--------  --------------   --------------
0         5                weighted
1         20               weighted
2         30               weighted
3         0                strict
4         0                strict
5         0                strict
6         0                strict
7         0                strict
```

10.4.7 Management prioritization

In order for you to have full access to the management of the device, even when there is a high network load, the device allows you to prioritize management packets.

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

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

▶ On Layer 3, the device modifies the IP-DSCP value.

10.4.8 Setting prioritization

■ Assigning the port priority

Perform the following steps:

☐ Open the *Switching > QoS/Priority > QoS/Priority Port Configuration* dialog.

☐ In the *Port priority* column, you specify the priority with which the device sends the data packets received on this port without a VLAN tag.

☐ In the *Trust mode* column, you specify the criteria the device uses to assign a traffic class to data packets received.

☐ To save the changes temporarily, click the ✓ button.

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

■ Assigning VLAN priority to a traffic class

Perform the following steps:

☐ Open the *Switching > QoS/Priority > 802.1D/p Mapping* dialog.

☐ To assign a traffic class to a VLAN priority, insert the associated value in the *Traffic class* column.

☐ To save the changes temporarily, click the ✓ button.

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

■ Assign port priority to received data packets

Perform the following steps:

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

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

■ Assigning DSCP to a traffic class

Perform the following steps:

□ Open the *Switching > QoS/Priority > IP DSCP Mapping* dialog.
□ Specify the desired value in the *Traffic class* column.

□ To save the changes temporarily, click the ✅ button.

```
enable                                  Change to the Privileged EXEC mode.
configure                               Change to the Configuration mode.
classofservice  ip-dscp-mapping cs1 1   Assigning the DSCP value CS1 to traffic class 1.
show classofservice  ip-dscp-mapping    Displaying the IP DSCP assignments
```

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

■ Assign the DSCP priority to received IP data packets

Perform the following steps:

```
enable                         Change to the Privileged EXEC mode.
configure                      Change to the Configuration mode.
interface 1/1                  Change to the interface configuration mode of interface 1/1.
classofservice trust ip-dscp   Assigning the trust ip-dscp mode globally.
exit                           Change to the Configuration mode.
show classofservice trust      Displaying the Trust mode of the ports/interfaces.
```

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

■ Configuring Layer 2 management priority

Perform the following steps:

☐ Open the *Switching > QoS/Priority > QoS/Priority Global* dialog.

☐ In the *VLAN priority for management packets* field, specify the VLAN priority with which the device sends management data packets.

☐ To save the changes temporarily, click the ✓ button.

`enable`	Change to the Privileged EXEC mode.
`network management priority dot1p 7`	Assigning the VLAN priority of 7 to management packets. The device sends management packets with the highest priority.
`show network parms`	Displaying the priority of the VLAN in which the device management is located.

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

■ Configuring Layer 3 management priority

Perform the following steps:

☐ Open the *Switching > QoS/Priority > QoS/Priority Global* dialog.

☐ In the *IP DSCP value for management packets* field, specify the DSCP value with which the device sends management data packets.

☐ To save the changes temporarily, click the ✓ button.

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

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

10.5 Flow control

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

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

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

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

If the flow control function on ports 1, 2 and 3 of the device is enabled, the device reacts before the funnel overflows. The funnel on the right illustrates ports 1, 2 and 3 sending a message to the transmitting devices to control the transmition speed. This results in the receiving port no longer being overwhelmed and is able to process the incoming traffic.
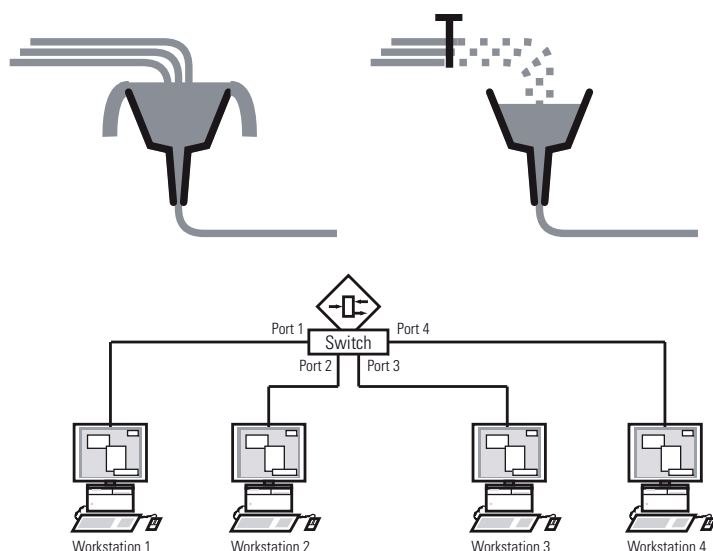
Figure 24: Example of flow control

10.5.1 Halfduplex or fullduplex link

■ Flow Control with a half duplex link

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

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

■ Flow Control with a full duplex link

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

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

10.5.2 Setting up the Flow Control

Perform the following steps:

- ☐ Open the *Switching > Global* dialog.
- ☐ Mark the *Flow control* checkbox.
  With this setting you enable flow control in the device.
- ☐ Open the *Basic Settings > Port* dialog, *Configuration* tab.
- ☐ To enable the Flow Control on a port, mark the checkbox in the *Flow control* column.

- ☐ To save the changes temporarily, click the ✓ button.

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

11 VLANs

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

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

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

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

▶ Network load limiting
VLANs reduce the network load considerably as the devices transmit Broadcast, Multicast, and Unicast packets with unknown (unlearned) destination addresses exclusively inside the virtual LAN. The rest of the data network forwards traffic as normal.

▶ Flexibility
You have the option of forming user groups based on the function of the participants apart from their physical location or medium.

▶ Clarity
VLANs give networks a clear structure and make maintenance easier.

11.1 Examples of VLANs

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

Note: When configuring VLANs you use an interface for management that will remain unchanged. For this example, you use either interface 1/6 or the V.24 serial connection to configure the VLANs.

11.1.1 Example 1

The example displays a minimal VLAN configuration (port-based VLAN). An administrator has connected multiple end devices to a transmission device and assigned them to 2 VLANs. This effectively prohibits any data transmission between the VLANs, whose members communicate only within their own VLANs.
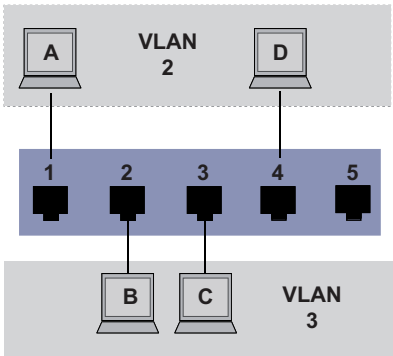
Figure 25: Example of a simple port-based VLAN

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

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

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

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

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

Table 19: Ingress table

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

Table 20: Egress table

Perform the following steps:

☐ Setting up the VLAN

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

- ☐ Click the ▦ button.

  The dialog displays the ***Create*** window.
- ☐ In the ***VLAN ID*** field, specify the value 2.
- ☐ Click the ***Ok*** button.
- ☐ For the VLAN, specify the name VLAN2:

  Double-click in the ***Name*** column and specify the name.

  For VLAN 1, in the ***Name*** column, change the value Default to VLAN1.
- ☐ Repeat the previous steps to create a VLAN 3 with the name VLAN3.

```
enable                              Change to the Privileged EXEC mode.
vlan database                       Change to the VLAN configuration mode.
vlan add 2                          Creates a new VLAN with the VLAN ID 2.
name 2 VLAN2                        Assign the name 2 to the VLAN VLAN2.
vlan add 3                          Creates a new VLAN with the VLAN ID 3.
name 3 VLAN3                        Assign the name 3 to the VLAN VLAN3.
name 1 VLAN1                        Assign the name 1 to the VLAN VLAN1.
exit                                Change to the Privileged EXEC mode.
show vlan brief                     Display the current VLAN configuration.
Max. VLAN ID.................................. 4042
Max. supported VLANs.......................... 128
Number of currently configured VLANs.......... 3
vlan unaware mode............................. disabled
VLAN ID VLAN Name                   VLAN Type VLAN Creation Time
---- -------------------------------- --------- ------------------
1       VLAN1                        default   0 days, 00:00:05
2       VLAN2                        static    0 days, 02:44:29
3       VLAN3                        static    0 days, 02:52:26
```

- ☐ Setting up the ports

  - ☐ Open the ***Switching > VLAN > Port*** dialog.
  - ☐ To assign the port to a VLAN, specify the desired value in the corresponding column.

    Possible values:
    - ▶ T = The port is a member of the VLAN. The port transmits tagged data packets.
    - ▶ U = The port is a member of the VLAN. The port transmits untagged data packets.
    - ▶ F = The port is not a member of the VLAN.
    - ▶ – = The port is not a member of this VLAN.

    Because end devices usually interpret untagged data packets, you specify the value U.

  - ☐ To save the changes temporarily, click the ✓ button.

  - ☐ Open the ***Switching > VLAN > Port*** dialog.
  - ☐ In the ***Port-VLAN ID*** column, specify the VLAN ID of the related VLAN:

    2 or 3
  - ☐ Because end devices usually interpret untagged data packets, in the ***Acceptable packet types*** column, you specify the value admitAll for end device ports.

  - ☐ To save the changes temporarily, click the ✓ button.

  The value in the ***Ingress filtering*** column has no affect on how this example functions.

```
enable                              Change to the Privileged EXEC mode.
configure                           Change to the Configuration mode.
interface 1/1                       Change to the interface configuration mode of interface 1/1.
vlan participation include 2        The port 1/1 becomes a member of the VLAN 2 and transmits the
                                    data packets without a VLAN tag.
vlan pvid 2                         Assign the port VLAN ID 1/1 to port 2.
exit                                Change to the Configuration mode.
interface 1/2                       Change to the interface configuration mode of interface 1/2.
vlan participation include 3        The port 1/2 becomes a member of the VLAN 3 and transmits the
                                    data packets without a VLAN tag.
vlan pvid 3                         Assign the port VLAN ID 1/2 to port 3.
exit                                Change to the Configuration mode.
```

```
interface 1/3                              Change to the interface configuration mode of interface 1/3.
vlan participation include 3               The port 1/3 becomes a member of the VLAN 3 and transmits the
                                           data packets without a VLAN tag.
vlan pvid 3                                Assign the port VLAN ID 1/3 to port 3.
exit                                       Change to the Configuration mode.
interface 1/4                              Change to the interface configuration mode of interface 1/4.
vlan participation include 2               The port 1/4 becomes a member of the VLAN 2 and transmits the
                                           data packets without a VLAN tag.
vlan pvid 2                                Assign the port VLAN ID 1/4 to port 2.
exit                                       Change to the Configuration mode.
exit                                       Change to the Privileged EXEC mode.
show vlan id 3                             Displays details for VLAN 3.
VLAN ID            : 3
VLAN Name          : VLAN3
VLAN Type          : Static
Interface   Current    Configured   Tagging
----------  --------   -----------  --------
1/1         -          Autodetect   Tagged
1/2         Include    Include      Untagged
1/3         Include    Include      Untagged
1/4         -          Autodetect   Tagged
1/5         -          Autodetect   Tagged
```

11.1.2 Example 2

The second example displays a more complex configuration with 3 VLANs (1 to 3). Along with the Switch from example 1, you use a 2nd Switch (on the right in the example).
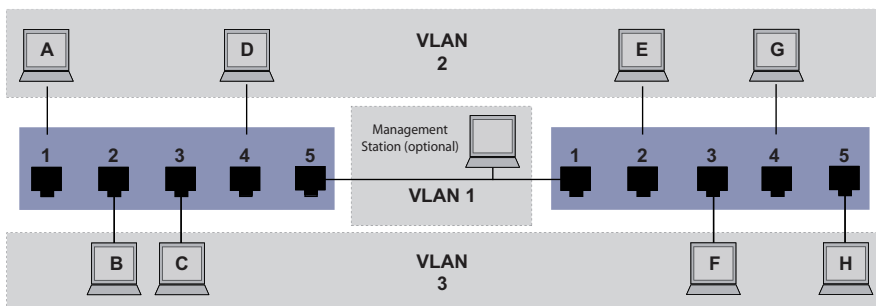

Figure 26: Example of a more complex VLAN configuration

The terminal devices of the individual VLANs (A to H) are spread over 2 transmission devices (Switches). Such VLANs are therefore known as distributed VLANs. An optional network management station is also shown, which enables access to every network component if the VLAN is configured correctly.

Note: In this case, VLAN 1 has no significance for the end device communication, but it is required for the administration of the transmission devices via what is known as the Management VLAN.

As in the previous example, uniquely assign the ports with their connected terminal devices to a VLAN. With the direct connection between the 2 transmission devices (uplink), the ports transport packets for both VLANs. To differentiate these uplinks you use "VLAN tagging", which handles the data packets accordingly. Thus, you maintain the assignment to the respective VLANs.

Perform the following steps:

☐ Add Uplink Port 5 to the ingress and egress tables from example 1.

☐ Create new ingress and egress tables for the right switch, as described in the first example.

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

In this example, tagged packets are used in the communication between the transmission devices (Uplink), as packets for different VLANs are differentiated at these ports.

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

Table 21: Ingress table for device on left

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

Table 22: Ingress table for device on right

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

Table 23: Egress table for device on left

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

Table 24: Egress table for device on right

The communication relationships here are as follows: end devices on ports 1 and 4 of the left device and end devices on ports 2 and 4 of the right device are members of VLAN 2 and can thus communicate with each other. The behavior is the same for the end devices on ports 2 and 3 of the left device and the end devices on ports 3 and 5 of the right device. These belong to VLAN 3.

The end devices "see" their respective part of the network. Participants outside this VLAN cannot be reached. The device also sends Broadcast, Multicast, and Unicast packets with unknown (unlearned) destination addresses exclusively inside a VLAN.

Here, the devices use VLAN tagging (IEEE 802.1Q) within the VLAN with the ID 1 (Uplink). The letter T in the egress table of the ports indicates VLAN tagging.

The configuration of the example is the same for the device on the right. Proceed in the same way, using the ingress and egress tables created above to adapt the previously configured left device to the new environment.

Perform the following steps:

☐ Setting up the VLAN

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

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

☐ In the *VLAN ID* field, specify the VLAN ID, for example 2.

☐ Click the *Ok* button.

☐ For the VLAN, specify the name VLAN2:
Double-click in the *Name* column and specify the name.
For VLAN 1, in the *Name* column, change the value Default to VLAN1.

☐ Repeat the previous steps to create a VLAN 3 with the name VLAN3.

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

```
Max. VLAN ID.................................. 4042
Max. supported VLANs......................... 128
Number of currently configured VLANs........... 3
vlan unaware mode............................. disabled
VLAN ID VLAN Name                   VLAN Type VLAN Creation Time
---- -------------------------------- --------- ------------------
1       VLAN1                        default   0 days, 00:00:05
2       VLAN2                        static    0 days, 02:44:29
3       VLAN3                        static    0 days, 02:52:26
```

☐ Setting up the ports

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

  Because end devicees usually interpret untagged data packets, you specify the value `U`.
  You specify the `T` setting on the uplink port on which the VLANs communicate with each other.

- ☐ To save the changes temporarily, click the ✓ button.
- ☐ Open the *Switching > VLAN > Port* dialog.
- ☐ In the *Port-VLAN ID* column, specify the VLAN ID of the related VLAN:
  `1`, `2` or `3`
- ☐ Because end devices usually interpret untagged data packets, in the *Acceptable packet types* column, you specify the value `admitAll` for end device ports.
- ☐ For the uplink port, in the *Acceptable packet types* column, specify the value `admitOnlyVlanTagged`.
- ☐ Mark the checkbox in the *Ingress filtering* column for the uplink ports to evaluate VLAN tags on this port.

- ☐ To save the changes temporarily, click the ✓ button.

`enable`	Change to the Privileged EXEC mode.
`configure`	Change to the Configuration mode.
`interface 1/1`	Change to the interface configuration mode of interface `1/1`.
`vlan participation include 1`	The port `1/1` becomes a member of the VLAN `1` and transmits the data packets without a VLAN tag.
`vlan participation include 2`	The port `1/1` becomes a member of the VLAN `2` and transmits the data packets without a VLAN tag.
`vlan tagging 2 enable`	The port `1/1` becomes a member of the VLAN `2` and transmits the data packets with a VLAN tag.
`vlan participation include 3`	The port `1/1` becomes a member of the VLAN `3` and transmits the data packets without a VLAN tag.
`vlan tagging 3 enable`	The port `1/1` becomes a member of the VLAN `3` and transmits the data packets with a VLAN tag.
`vlan pvid 1`	Assigning the Port VLAN ID `1` to port `1/1`.
`vlan ingressfilter`	Activate ingress filtering on port `1/1`.
`vlan acceptframe vlanonly`	Port `1/1` only forwards packets with a VLAN tag.
`exit`	Change to the Configuration mode.
`interface 1/2`	Change to the interface configuration mode of interface `1/2`.
`vlan participation include 2`	The port `1/2` becomes a member of the VLAN `2` and transmits the data packets without a VLAN tag.
`vlan pvid 2`	Assigning the Port VLAN ID `2` to port `1/2`.

`exit`	Change to the Configuration mode.
`interface 1/3`	Change to the interface configuration mode of interface `1/3`.
`vlan participation include 3`	The port `1/3` becomes a member of the VLAN `3` and transmits the data packets without a VLAN tag.
`vlan pvid 3`	Assigning the Port VLAN ID `3` to port `1/3`.
`exit`	Change to the Configuration mode.
`interface 1/4`	Change to the interface configuration mode of interface `1/4`.
`vlan participation include 2`	The port `1/4` becomes a member of the VLAN `2` and transmits the data packets without a VLAN tag.
`vlan pvid 2`	Assigning the Port VLAN ID `2` to port `1/4`.
`exit`	Change to the Configuration mode.
`interface 1/5`	Change to the interface configuration mode of interface `1/5`.
`vlan participation include 3`	The port `1/5` becomes a member of the VLAN `3` and transmits the data packets without a VLAN tag.
`vlan pvid 3`	Assigning the Port VLAN ID `3` to port `1/5`.
`exit`	Change to the Configuration mode.
`exit`	Change to the Privileged EXEC mode.
`show vlan id 3`	Displays details for VLAN `3`.

```
VLAN ID.......................3
VLAN Name....................VLAN3
VLAN Type....................Static
VLAN Creation Time...........0 days, 00:07:47 (System Uptime)
VLAN Routing.................disabled

Interface   Current    Configured    Tagging
----------  --------   -----------   --------
1/1         Include    Include       Tagged
1/2         -          Autodetect    Untagged
1/3         Include    Include       Untagged
1/4         -          Autodetect    Untagged
1/5         Include    Include       Untagged
```

11.2   Guest / Unauthenticated VLAN

The guest VLAN function allows a device to provide port-based Network Access Control (IEEE 802.1x) to non-802.1x capable supplicants. This feature provides a mechanism to allow guests to access external networks exclusively. When you connect non-802.1x capable supplicants to an active unauthorized 802.1x port, the supplicants send no responds to 802.1x requests. Since the supplicants send no responses, the port remains in the unauthorized state. The supplicants have no access to external networks.

The guest VLAN supplicant function is a per-port basis configuration. When you configure a port as a guest VLAN and connect non-802.1x capable supplicants to this port, the device assigns the supplicants to the guest VLAN. Adding supplicants to a guest VLAN causes the port to change to the authorized state allowing the supplicants to access to external networks.

The Unauthenticated VLAN function allows the device to provide service to 802.1x capable supplicants which authenticate incorrectly. This function allows the unauthorized supplicants to have access to limited services. When you configure an unauthenticated VLAN on a port with 802.1x port authentication and the global operation enabled, the device places the port in an unauthenticated VLAN. When a 802.1x capable supplicant incorrectly authenticates on the port, the device adds the supplicant to the unauthenticated VLAN. If you also configure a guest VLAN on the port, then non-802.1x capable supplicants use the guest VLAN.

The reauthentication timer counts down when the port has an unauthenticated VLAN assigned. The unauthenticated VLAN reauthenticates when the time specified in the *Reauthentication period [s]* column expires and supplicants are present on the port. If no supplicants are present, the device places the port in the configured guest VLAN.

The following example explains how to create a Guest VLAN. Create an Unauthorized VLAN in the same manner.

Perform the following steps:

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

☐ Click the 🔲 button.

The dialog displays the *Create* window.

☐ In the *VLAN ID* field, specify the value `10`.

☐ Click the *Ok* button.

☐ For the VLAN, specify the name `Guest`:
Double-click in the *Name* column and specify the name.

☐ Click the 🔲 button.

The dialog displays the *Create* window.

☐ In the *VLAN ID* field, specify the value `20`.

☐ Click the *Ok* button.

☐ For the VLAN, specify the name `Not authorized`:
Double-click in the *Name* column and specify the name.

☐ Open the *Network Security > 802.1X Port Authentication > Global* dialog.

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

☐ To save the changes temporarily, click the ✅ button.

☐ Open the *Network Security > 802.1X Port Authentication > Port Configuration* dialog.

☐ Specify the following settings for port `1/4`:
  – The value `auto` in the *Port control* column
  – The value `10` in the *Guest VLAN ID* column
  – The value `20` in the *Unauthenticated VLAN ID* column

☐ To save the changes temporarily, click the ✅ button.

```
enable                          Change to the Privileged EXEC mode.
vlan database                   Change to the VLAN configuration mode.
vlan add 10                     Creates VLAN 10.
vlan add 20                     Creates VLAN 20.
name 10 Guest                   Renames VLAN 10 to Guest.
```

`name 20 Unauth`	Renames VLAN 20 to Unauth.
`exit`	Change to the Privileged EXEC mode.
`configure`	Change to the Configuration mode.
`dot1x system-auth-control enable`	Enable the 802.1X function globally.
`dot1x port-control auto`	Enables port control on port 1/4.
`interface 1/4`	Change to the interface configuration mode of interface 1/4.
`dot1x guest-vlan 10`	Assign the guest vlan to port 1/4.
`dot1x unauthenticated-vlan 20`	Assign the unauthorized vlan to port 1/4.
`exit`	Change to the Configuration mode.

11.3   RADIUS VLAN assignment

The RADIUS VLAN assignment feature allows for a RADIUS VLAN ID attribute to be associated with an authenticated client. When a client authenticates successfully, and the RADIUS server sends a VLAN attribute, the device associates the client with the RADIUS assigned VLAN. As a result, the device adds the physical port as an untagged member to the appropriate VLAN and sets the port VLAN ID (PVID) with the given value.

11.4 VLAN unaware mode

The VLAN-unaware function defines the operation of the device in a LAN segmented by VLANs. The device accepts packets and processes them according to its inbound rules. Based on the IEEE 802.1Q specifications, the function governs how the device processes VLAN tagged packets.

Use the VLAN aware mode to apply the user-defined VLAN topology configured by the network administrator. The device uses VLAN tagging in combination with the IP or Ethernet address when forwarding packets. The device processes inbound and outbound packets according to the defined rules. VLAN configuration is a manual process.

Use the VLAN unaware mode to forward traffic as received, without any modification. The device transmits tagged packets when received as tagged. The device transmits also transmits untagged packets when received as untagged. Regardless of VLAN assignment mechanisms, the device assigns packets to VLAN ID 1 and to a Multicast group, indicating that the packet flood domain is according to the VLAN.

12 Redundancy

12.1 Network Topology vs. Redundancy Protocols

When using Ethernet, an important prerequisite is that data packets follow a single (unique) path from the sender to the receiver. The following network topologies support this prerequisite:
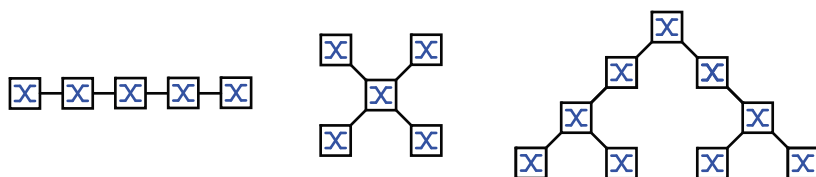
▶ Line topology

▶ Star topology

▶ Tree topology

Figure 27: Network with line, star and tree topologies

To maintain communication when a connection fails, install additional physical connections between the network nodes. Redundancy protocols help ensure that the additional connections remain switched off while the original connection is still working. If the connection fails, the redundancy protocol generates a new path from the sender to the receiver via the alternative connection.

To introduce redundancy onto Layer 2 of a network, you first define which network topology you require. Depending on the network topology selected, you then choose from the redundancy protocols that can be used with this network topology.

12.1.1 Network topologies

■ Meshed topology

For networks with star or tree topologies, redundancy procedures are only possible in connection with physical loop creation. The result is a meshed topology.
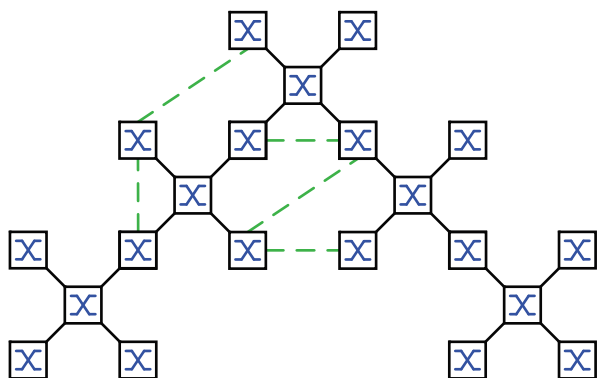

Figure 28: Meshed topology: Tree topology with physical loops

For operating in this network topology, the device provides you with the following redundancy protocols:
▶ Rapid Spanning Tree (RSTP)

■ Ring topology

In networks with a line topology, you can use redundancy procedures by connecting the ends of the line. This creates a ring topology.
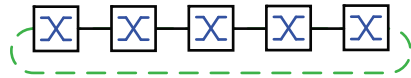

Figure 29: Ring topology: Line topology with connected ends

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

12.1.2 Redundancy Protocols

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

Redundancy protocol	Network topology	Comments
MRP	Ring	The switching time can be selected and is practically independent of the number of devices. An MRP-Ring consits of up to 50 devices that support the MRP protocol according to IEC 62439. If you only use Hirschmann devices, up to 100 devices are possible in the MRP-Ring.
RSTP	Random structure	The switching time depends on the network topology and the number of devices. ▶ typ. < 1 s with RSTP ▶ typ. < 30 s with STP
Link Aggregation	Random structure	A Link Aggregation Group is the combining of 2 or more, full-duplex point-to-point links operating at the same rate, on a single switch to increase bandwidth.
Link Backup	Random structure	When the device detects an error on the primary link, then the device transfers traffic to the backup link. You typically use Link Backup in service-provider or enterprise networks.

Table 25: Overview of redundancy protocols

Note: When you are using a redundancy function, you deactivate the flow control on the participating device ports. If the flow control and the redundancy function are active at the same time, there is a risk that the redundancy function will not operate as intended.

12.1.3 Combinations of Redundancies

	MRP	RSTP/MSTP	Link Aggreg.	Link Backup	Subring	HIPER Ring	Fast MRP	DLR	HSR	PRP
MRP	✓									
RSTP/MSTP [3]	✓ [1]	✓								
Link Aggreg.	✓ [4]	✓ [4]	✓							
Link Backup	✓	✓	✓	✓						

Table 26: Overview of redundancy protocols

Symbol	Meaning
✓	Combination applicable
[1]	Redundant coupling between these network topologies will possibly lead to data loops.
[3]	In combination with MSTP, the failover times of other redundancy protocols may slightly increase.
[4]	Combination applicable on the same port

12.2 Media Redundancy Protocol (MRP)

Since May 2008, the Media Redundancy Protocol (MRP) has been a standardized solution for ring redundancy in the industrial environment.

MRP is compatible with redundant ring coupling, supports VLANs, and is distinguished by very short reconfiguration times.

An MRP-Ring consists of up to 50 devices that support the MRP protocol according to IEC 62439. If you only use Hirschmann devices, up to 100 devices are possible in the MRP-Ring.

You use the fixed MRP redundant port (Fixed Backup) if the primary ring link fails, the Ring Manager sends data traffic to the secondary ring link. When the primary link is restored, the secondary link continues to be in use.

12.2.1 Network Structure

The concept of ring redundancy allows the construction of high-availability, ring-shaped network structures. With the help of the RM (**R**ing **M**anager) function, the two ends of a backbone in a line structure can be closed to a redundant ring. The Ring Manager keeps the redundant line open as long as the line structure is intact. If a segment becomes inoperable, the Ring Manager immediately closes the redundant line, and line structure is intact again.
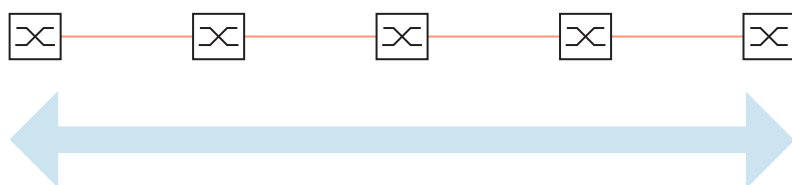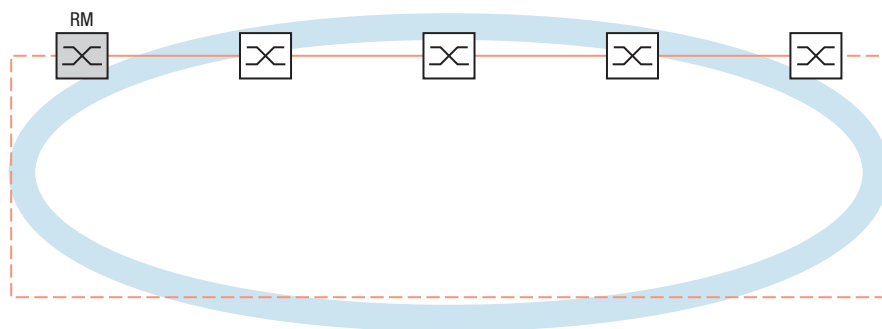

Figure 30: Line structure

Figure 31: Redundant ring structure
RM = Ring Manager
—— main line
- - - redundant line

12.2.2 Reconfiguration time

If a line section fails, the Ring Manager changes the MRP-Ring back into a line structure. You define the maximum time for the reconfiguration of the line in the Ring Manager.

Possible values for the maximum delay time:
- 500 ms
- 200 ms

Note: You only configure the reconfiguration time with a value less than 500 ms if every device in the ring support the shorter delay time.
Otherwise the devices that only support longer delay times might not be reachable due to overloading. Loops can occur as a result.

12.2.3 Advanced mode

For times even shorter than the guaranteed reconfiguration times, the device provides the advanced mode. The advanced mode speeds up the link failure recognition when the ring participants inform the Ring Manager of interruptions in the ring via link-down notifications.

Hirschmann devices support link-down notifications. Therefore, you generally activate the advanced mode in the Ring Manager.

If you are using devices that do not support link-down notifications, the Ring Manager reconfigures the line in the selected maximum reconfiguration time.

12.2.4 Prerequisites for MRP

Before setting up an MRP-Ring, verify that the following conditions are fulfilled:
▶ All ring participants support MRP.
▶ The ring participants are connected to each other via the ring ports. Apart from the device's neighbors, no other ring participants are connected to the respective device.
▶ All ring participants support the configuration time specified in the Ring Manager.
▶ There is exactly 1 Ring Manager in the ring.

If you are using VLANs, configure every ring port with the following settings:

☐ Deactivate ingress filtering - see the Switching:VLAN:Port *Switching > VLAN > Port* dialog.

☐ Define the port VLAN ID (PVID) - see the *Switching > VLAN > Port* dialog.
– PVID = 1 if the device transmits the MRP data packets untagged (VLAN ID = 0 in *Switching > L2–Redundancy > MRP* dialog)
By setting the PVID = 1, the device automatically assigns the received untagged packets to VLAN 1.
– PVID = any if the device transmits the MRP data packets in a VLAN (VLAN ID ≥ 1 in the *Switching > L2–Redundancy > MRP* dialog)

☐ Define egress rules - see *Switching > VLAN > Configuration* dialog.
– U (untagged) for the ring ports of VLAN 1 if the device transmits the MRP data packets untagged (VLAN ID = 0 in the *Switching > L2–Redundancy > MRP* dialog, the MRP ring is not assigned to a VLAN).
– T (tagged) for the ring ports of the VLAN which you assign to the MRP ring. Select T, if the device transmits the MRP data packets in a VLAN (VLAN ID ≥ 1 in the *Switching > L2–Redundancy > MRP* dialog).

12.2.5 Example Configuration

A backbone network contains 3 devices in a line structure. To increase the availability of the network, you convert the line structure to a redundant ring structure. Devices from different manufacturers are used.All devices support MRP. On every device you define ports 1.1 and 1.2 as ring ports.

If the primary ring link fails, the Ring Manager sends data on the secondary ring link. When the primary link is restored, the secondary link reverts back to the backup mode.
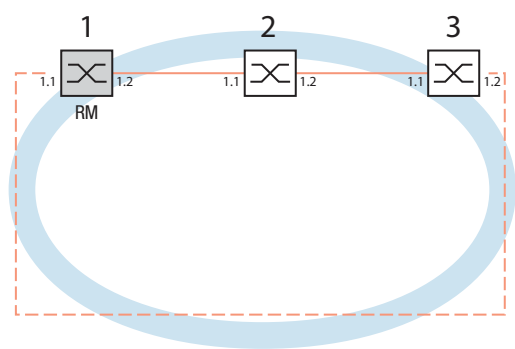
Figure 32: Example of MRP-Ring
RM = Ring Manager
—— main line
- - - redundant line

The following example configuration describes the configuration of the Ring Manager device (1). You configure the 2 other devices (2 to 3) in the same way, but without activating the Ring Manager function. This example does not use a VLAN. You specify 200 ms as the ring recovery time. Every device supports the advanced mode of the Ring Manager.

☐ Set up the network to meet your demands.
☐ Configure every port so that the transmission speed and the duplex settings of the lines correspond to the following table:

Port type	Bit rate	Autonegotiation (automatic configuration)	Port setting	Duplex
TX	100 Mbit/s	off	on	100 Mbit/s full duplex (FDX)
TX	1 Gbit/s	on	on	-
Optical	100 Mbit/s	off	on	100 Mbit/s full duplex (FDX)
Optical	1 Gbit/s	on	on	-
Optical	10 Gbit/s	-	on	10 Gbit/s full duplex (FDX)

Table 27: Port settings for ring ports

Note: You configure optical ports without support for autonegotiation (automatic configuration) with 100 Mbit/s full duplex (FDX) or 1000 Mbit/s full duplex (FDX).

Note: You configure optical ports without support for autonegotiation (automatic configuration) with 100 Mbit/s full duplex (FDX).

Note: Configure every device of the MRP-Ring individually. Before you connect the redundant line, verify that you have completed the configuration of every device of the MRP-Ring. You thus avoid loops during the configuration phase.

☐ You deactivate the flow control on the participating ports.
 If the flow control and the redundancy function are active at the same time, there is a risk that the redundancy function will not operate as intended. (Default setting: flow control deactivated globally and activated on every port.)

☐ Disable Spanning Tree on every device in the network:

 ☐ Open the `Switching > L2-Redundancy > Spanning Tree > Global` dialog.
 ☐ Disable the function.
  In the state on delivery, Spanning Tree is enabled on the device.

```
enable                          Change to the Privileged EXEC mode.
configure                       Change to the Configuration mode.
no spanning-tree operation      Switches Spanning Tree off.
show spanning-tree global       Displays the parameters for checking.
```

☐ Enable MRP on every device in the network:

 ☐ Open the `Switching > L2-Redundancy > MRP` dialog.
 ☐ Specify the desired ring ports.

In the Command Line Interface you first define an additional parameter, the MRP domain ID. Configure every ring participant with the same MRP domain ID. The MRP domain ID is a sequence of 16 number blocks (8-bit values).

When configuring with the graphical user interface, the device uses the default value `255 255 255 255 255 255 255 255 255 255 255 255 255 255 255 255`.

`mrp domain add default-domain`	Creates a new MRP domain with the default domain ID.
`mrp domain modify port   primary 1/1`	Specifies port `1/1` as ring port `1`.
`mrp domain modify port   secondary 1/2`	Specifies port `1/2` as ring port `2`.

☐ Enable the *Fixed backup* port.

> ☐ Enable the Ring Manager.
> For the other devices in the ring, leave the setting as *Off*.
> ☐ To allow the device to continue sending data on the secondary port after the ring is restored, mark the *Fixed backup* checkbox.
>
> **Note:** When the device reverts back to the primary port, the maximum ring recovery time may be exceeded.
>
> If you unmark the *Fixed backup* checkbox, and the ring is restored, then the Ring Manager blocks the secondary port and unblocks the primary port.

`mrp domain modify port secondary 1/2` `fixed-backup enable`	Activates the *Fixed backup* function on the secondary port. The secondary port continues forwarding data after the ring is restored.

> ☐ Enable the Ring Manager.
> For the other devices in the ring, leave the setting as *Off*.

`mrp domain modify mode   manager`	Specifies that the device operates as the *Ring manager*. Do not activate the *Ring manager* function on any other device.

> ☐ Select the checkbox in the *Advanced mode* field.

`mrp domain modify   advanced-mode enabled`	Activates the advanced mode.

> ☐ In the *Ring recovery* field, select the value `200ms`.

`mrp domain modify   recovery-delay 200ms`	Specifies the value `200ms` as the max. delay time for the reconfiguration of the ring.

Note: If selecting 200 ms for the ring recovery does not provide the ring stability necessary to meet the requirements of your network, you select 500 ms.

> ☐ Switch the operation of the MRP-Ring on.
> ☐ To save the changes temporarily, click the ✓ button.

`mrp domain modify operation   enable`	Activates the MRP-Ring.

☐ When every ring participant is configured, close the line to the ring. To do this, you connect the devices at the ends of the line via their ring ports.

☐ Check the messages from the device:

`show mrp`	Displays the parameters for checking.

The *Operation* field displays the operating state of the ring port.

Possible values:
- ▶ `forwarding`
  The port is enabled, connection exists.
- ▶ `blocked`
  The port is blocked, connection exists.
- ▶ `disabled`
  The port is disabled.
- ▶ `not-connected`
  No connection exists.

The *Information* field displays messages for the redundancy configuration and the possible causes of errors.

The following messages are possible if the device is operating as a ring client or a Ring Manager:
- ▶ *Redundancy available*
  The redundancy is set up. When a component of the ring is down, the redundant line takes over its function.
- ▶ *Configuration error: Error on ringport link.*
  Error in the cabling of the ring ports.

The following messages are possible if the device is operating as a Ring Manager:
- ▶ *Configuration error: Packets from another ring manager received.*
  Another device exists in the ring that is operating as the Ring Manager.
  Activate the *Ring manager* function on exactly one device in the ring.
- ▶ *Configuration error: Ring link is connected to wrong port.*
  A line in the ring is connected with a different port instead of with a ring port. The device only receives test data packets on 1 ring port.

☐ If applicable, integrate the MRP ring into a VLAN:

☐ In the *VLAN ID* field, define the MRP VLAN ID. The MRP VLAN ID determines in which of the configured VLANs the device transmits the MRP packets. To set the MRP VLAN ID, first configure the VLANs and the corresponding egress rules in the *Switching > VLAN > Configuration* dialog.

- ▶ If the MRP-Ring is not assigned to a VLAN (like in this example), leave the VLAN ID as `0`.
  In the *Switching > VLAN > Configuration* dialog, specify the VLAN membership as `U` (untagged) for the ring ports in VLAN `1`.
- ▶ If the MRP-Ring is assigned to a VLAN, enter a VLAN ID >`0`.
  In the *Switching > VLAN > Configuration* dialog, specify the VLAN membership as `T` (tagged) for the ring ports in the selected VLAN.

`mrp domain modify vlan  <0..4042>`   Assigns the VLAN ID.

12.3 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 loss of communication across of the network. In order to help avoid this, you can use Spanning Tree. Spanning Tree enables loop-free switching through the systematic deactivation of redundant connections. Redundancy enables the systematic reactivation of individual connections as needed.

RSTP is a further development of the Spanning Tree Protocol (STP) and is compatible with it. If a connection or a bridge becomes inoperable, the STP required 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, the `Max Age` setting of the new root bridge determines the maximum number of devices allowed in a branch.

Note: The RSTP standard dictates that every device within a network work with the (Rapid) Spanning Tree Algorithm. If STP and RSTP are used at the same time, the advantages of faster reconfiguration with RSTP are lost in the network segments that are operated in combination.
A device that only supports RSTP works together with MSTP devices by not assigning an MST region to itself, but rather the CST (Common Spanning Tree).

12.3.1 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. If a path is interrupted because a network component becomes inoperable, STP reactivates the previously deactivated path again. This allows redundant links to increase the availabiliy of communication.
STP determines a bridge that represents the STP tree structure's base. This bridge is called root bridge.

Features of the STP algorithm:

▶ automatic reconfiguration of the tree structure in the case of a bridge becoming inoperable or the interruption of a data path
▶ the tree structure is stabilized up to the maximum network size,
▶ stabilization of the topology within a short time period
▶ topology can be specified and reproduced by the administrator
▶ transparency for the end devices
▶ low network load relative to the available transmission capacity due to the tree structure created

■ **Bridge parameters**

In the context of Spanning Tree, each bridge and its connections are uniquely described by the following parameters:

▶ Bridge Identifier
▶ Root Path Cost for the bridge ports,
▶ Port Identifier

■ **Bridge Identifier**

The Bridge Identifier consists of 8 bytes. The 2 highest-value bytes are the priority. The default setting for the priority number is 32,768, but the Management Administrator can change this when configuring the network. The 6 lowest-value bytes of the bridge identifier are the bridge's MAC address. The MAC address allows each bridge to have unique bridge identifiers.
The bridge with the smallest number for the bridge identifier has the highest priority.
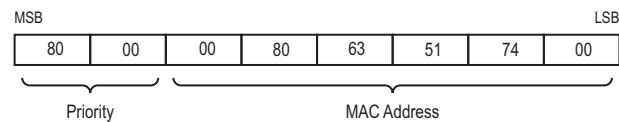
Figure 33: Bridge Identifier, Example (values in hexadecimal notation)

■ **Root Path Cost**

Each path that connects 2 bridges is assigned a cost for the transmission (path cost). The device determines this value based on the transmission speed (see table 28). It 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.
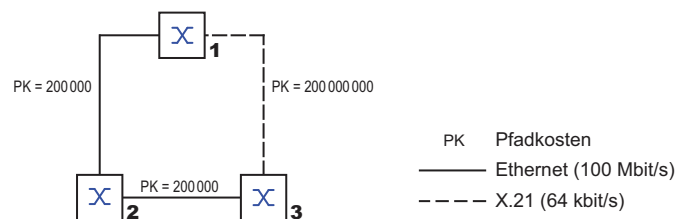

Figure 34: Path costs

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

Table 28: Recommended path costs for RSTP based on the data rate.

a. Bridges that conform with IEEE 802.1D 1998 and only support 16-bit values for the path costs should use the value 65,535 (FFFFH) for path costs when they are used in conjunction with bridges that support 32-bit values for the path costs.

■ Port Identifier

The port identifier consists of 2 bytes. One part, the lower-value byte, contains the physical port number. This provides a unique identifier for the port of this bridge. The second, higher-value part is the port priority, which is specified by the Administrator (default value: 128). It also applies here that the port with the smallest number for the port identifier has the highest priority.
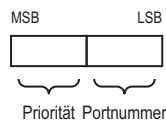
Figure 35: Port Identifier

■ Max Age and Diameter

The "Max Age" and "Diameter" values largely determine the maximum expansion of a Spanning Tree network.

■ Diameter

The number of connections between the devices in the network that are furthest removed from each other is known as the network diameter.
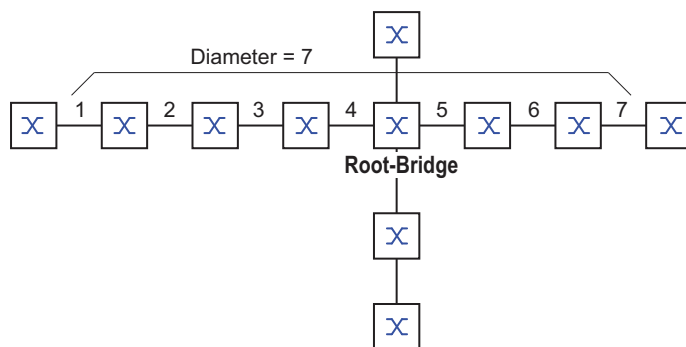

Figure 36: Definition of diameter

The network diameter that can be achieved in the network is MaxAge-1.
In the state on delivery, MaxAge = 20 and the maximum diameter that can be achieved = 19. If you set the maximum value of 40 for MaxAge, the maximum diameter that can be achieved = 39.

■ MaxAge

Every STP-BPDU contains a "MessageAge" counter. When a bridge is passed through, the counter increases by 1.
Before forwarding a STP-BPDU, the bridge compares the "MessageAge" counter with the "MaxAge" value specified in the device:
☐ If MessageAge < MaxAge, the bridge forwards the STP-BPDU to the next bridge.
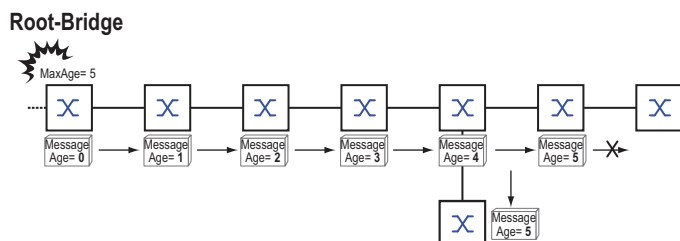☐ If MessageAge = MaxAge, the bridge discards the STP-BPDU.

Figure 37: Transmission of an STP-BPDU depending on MaxAge

12.3.2 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.
▶ If 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). If 2 bridges have the same priority, the bridge with the numerically larger MAC address has the numerically higher ID, which is logically the worse one.
▶ If 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 35). 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). If 2 ports have the same priority, the port with the higher port number has the numerically higher ID, which is logically the worse one.
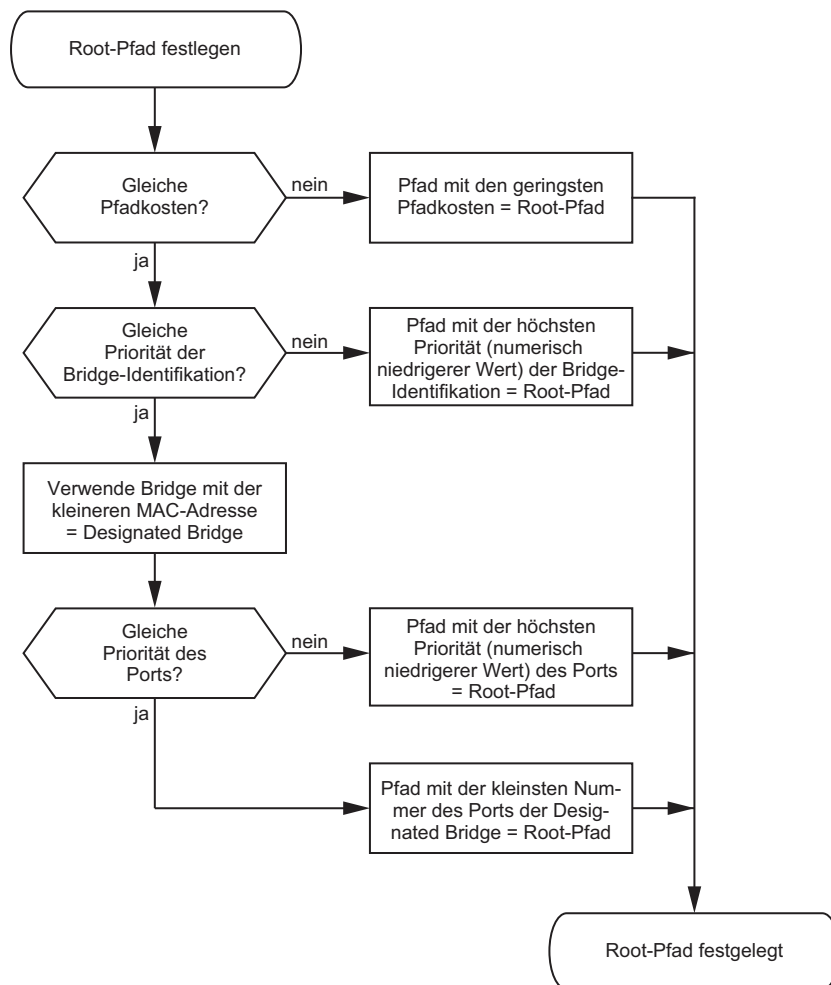
Figure 38: Flow diagram for specifying the root path

12.3.3 Examples

■ Example of determining the root path

You can use the network plan (see figure 39) to follow the flow chart (see figure 38) for determining the root path. The administrator has specified a priority in the bridge identification for each bridge. The bridge with the smallest numerical value for the bridge identification takes on the role of the root bridge, in this case, bridge 1. In the example every sub-path has the same path costs. The protocol blocks the path between bridge 2 and bridge 3 as a connection from bridge 3 via bridge 2 to the root bridge would result in higher path costs.

The path from bridge 6 to the root bridge is interesting:

▶ The path via bridge 5 and bridge 3 creates the same root path costs as the path via bridge 4 and bridge 2.
▶ STP selects the path using the bridge that has the lowest MAC address in the bridge identification (bridge 4 in the illustration).
▶ There are also 2 paths between bridge 6 and bridge 4.
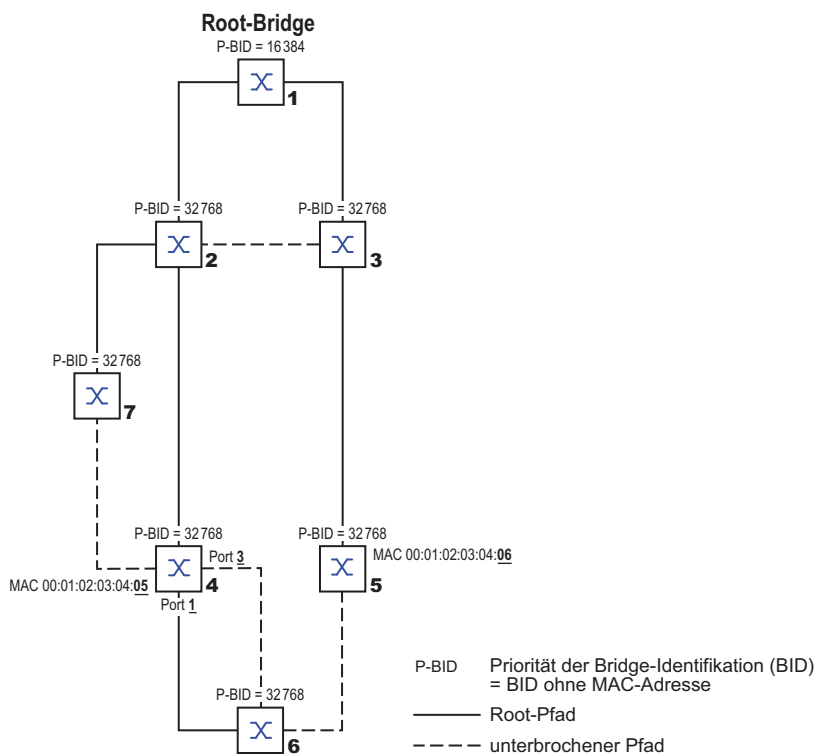The port identifier is decisive here (Port 1 < Port 3).

Figure 39: Example of determining the root path

Note: 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, the MAC address in the bridge identifier alone determines which bridge becomes the new root bridge if the current root bridge goes down.

■ **Example of manipulating the root path**

You can use the network plan (see figure 40) to follow the flow chart (see figure 38) for determining the root path. The Administrator has performed the following:
– Left the default value of 32768 (8000H) for every bridge apart from bridge 1 and bridge 5, and
– assigned to bridge 1 the value 16384 (4000H), thus making it the root bridge.
– To bridge 5 he assigned the value 28672 (7000H).
The protocol blocks the path between bridge 2 and bridge 3 as a connection from bridge 3 via bridge 2 to the root bridge would mean higher path costs.

The path from bridge 6 to the root bridge is interesting:
▶ The bridges select the path via bridge 5 because the value 28672 for the priority in the bridge identifier is smaller than value 32768.
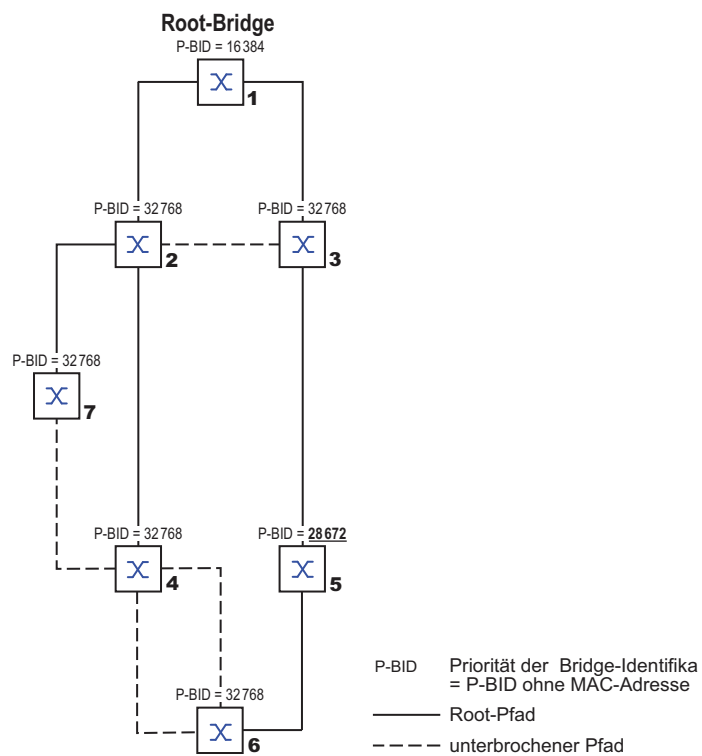
Figure 40: Example of manipulating the root path

■ **Example of manipulating the tree structure**

The Management Administrator soon discovers that this configuration with bridge 1 as the root bridge is invalid. On the paths from bridge 1 to bridge 2 and bridge 1 to bridge 3, the control packets which the root bridge sends to every other bridge add up.
If the Management Administrator configures bridge 2 as the root bridge, the burden of the control packets on the subnetworks is distributed much more evenly. The result is the configuration shown here (see figure 41). The path costs for most of the bridges to the root bridge have decreased.
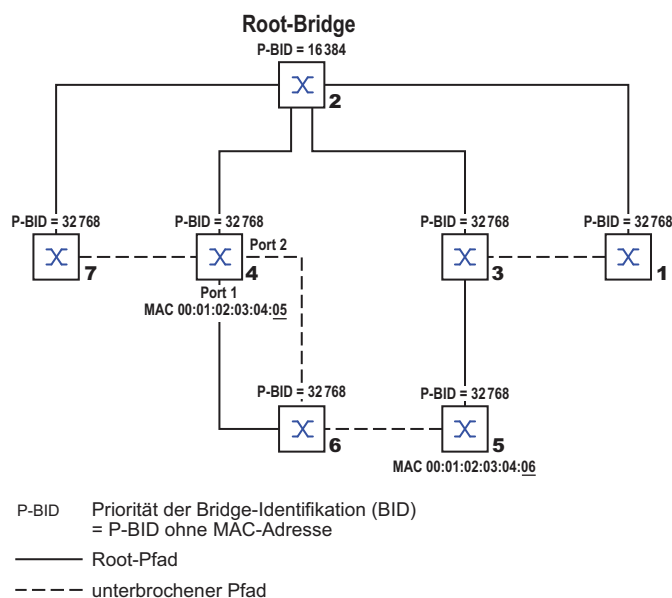

Figure 41: Example of manipulating the tree structure

12.3.4 The Rapid Spanning Tree Protocol

The RSTP uses the same algorithm for determining the tree structure as STP. RSTP merely changes parameters, and adds new parameters and mechanisms that speed up the reconfiguration if a link or bridge becomes inoperable.

The ports play a significant role in this context.

■ **Port roles**

RSTP assigns each bridge port one of the following roles (see figure 42):

▶ Root Port:
This is the port at which a bridge receives data packets with the lowest path costs from the root bridge.
If 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.
If 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 38).
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.
If more than 1 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. If a bridge is connected to a network segment with more than one port (via a hub, for example), the bridge gives the role of the designated port to the port with the better port ID.

▶ Edge port
Every network segment with no additional RSTP bridges is connected with exactly one designated port. In this case, this designated port is also an edge port. The distinction of an edge port is the fact that it does not receive any RST BPDUs (Rapid Spanning Tree Bridge Protocol Data Units).

▶ Alternate port
This is a blocked port that takes over the task of the root port if the connection to the root bridge is lost. The alternate port provides a backup 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.
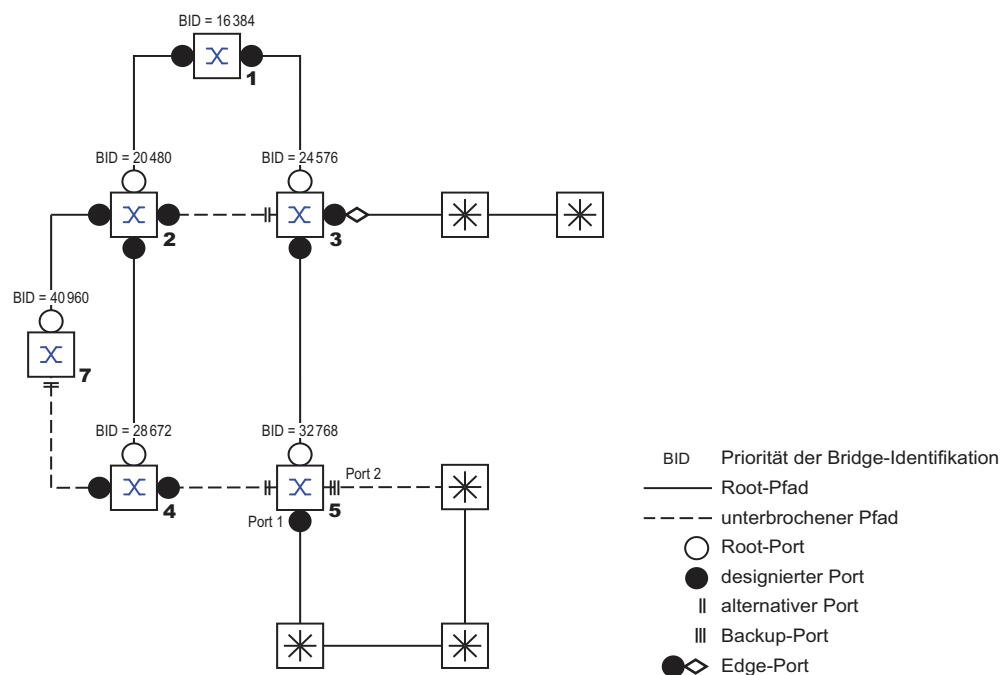

Figure 42: Port role assignment

■ Port states

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

STP port state	Administrative bridge port state	MAC Operational	RSTP Port state	Active topology (port role)
DISABLED	Disabled	FALSE	Discarding[a]	Excluded (disabled)
DISABLED	Enabled	FALSE	Discarding[a]	Excluded (disabled)
BLOCKING	Enabled	TRUE	Discarding[b]	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)

Table 29: Relationship between port state values for STP and RSTP

a. The dot1d-MIB displays "Disabled"
b. The dot1d-MIB displays "Blocked"

Meaning of the RSTP port states:

▶ Disabled: Port does not belong to the active topology
▶ Discarding: No address learning in FDB, no data traffic except for STP-BPDUs

▶ Learning: Address learning active (FDB), no data traffic apart from STP-BPDUs
▶ Forwarding: Address learning active (FDB), sending and receiving of every packet type (not only STP-BPDUs)

■ Spanning Tree Priority Vector

To assign roles to the ports, the RSTP bridges exchange configuration information with each other. This information is known as the Spanning Tree Priority Vector. It is part of the RSTP BPDUs and contains the following information:

▶ Bridge identification of the root bridge
▶ Root path costs of the sending bridge
▶ Bridge identification of the sending bridge
▶ Port identifiers of the ports through which the message was sent
▶ Port identifiers of the ports through which the message was received

Based on this information, the bridges participating in RSTP are able to determine port roles themselves and define the port states of their own ports.

■ Fast reconfiguration

Why can RSTP react faster than STP to an interruption of the root path?

▶ Introduction of edge-ports:
During a reconfiguration, RSTP switches an edge port into the transmission mode after three seconds (default setting) and then waits for the "Hello Time" to elapse, to be sure that no bridge sending BPDUs is connected. When the user verifies that a end device is and remains connected to this port, there are no waiting times at this port in the case of a reconfiguration.
▶ Introduction of alternate ports:
As the port roles are already distributed in normal operation, a bridge can immediately switch from the root port to the alternate port after the connection to the root bridge is lost.
▶ Communication with neighboring bridges (point-to-point connections):
Decentralized, direct communication between neighboring bridges enables reaction without wait periods to status changes in the spanning tree topology.
▶ Address table:
With STP, the age of the entries in the FDB determines the updating of communication. RSTP immediately deletes the entries in those ports affected by a reconfiguration.
▶ Reaction to events:
Without having to adhere to any time specifications, RSTP immediately reacts to events such as connection interruptions, connection reinstatements, etc.

Note: The downside of this fast reconfiguration is the possibility that data packages could be duplicated and/or arrive at the recipient in the wrong order during the reconfiguration phase of the RSTP topology. If this is unacceptable for your application, use the slower Spanning Tree Protocol or select one of the other, faster redundancy procedures described in this manual.

■ **STP compatibility mode**

The STP compatibility mode allows you to operate RSTP devices in networks with old installations. If an RSTP device detects an older STP device, it switches on the STP compatibility mode at the relevant port.

12.3.5 Configuring the device

RSTP configures the network topology completely independently. 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.

☐ 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, there is a risk that the redundancy function will not operate as 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 on the device.

  ☐ Open the *Switching > L2-Redundancy > Spanning Tree > Global* dialog.

  ☐ Enable the function.

  ☐ To save the changes temporarily, click the ✓ button.

`enable`	Change to the Privileged EXEC mode.
`configure`	Change to the Configuration mode.
`spanning-tree operation`	Enables Spanning Tree.
`show spanning-tree global`	Displays the parameters for checking.

☐ Now connect the redundant lines.

☐ Define the settings for the device that takes over the role of the root bridge.

  ☐ In the *Priority* field you enter a numerically lower value.
     The bridge with the numerically lowest bridge ID has the highest priority and becomes the root bridge of the network.

  ☐ To save the changes temporarily, click the ✓ button.

`spanning-tree mst priority 0 <0..61440 in 4096er-Schritten>`	Specifies the bridge priority of the device.

  After saving, the dialog shows the following information:
  – The *Bridge is root* checkbox is marked.
  – The *Root port* field shows the value `0.0`.
  – The *Root path cost* field shows the value `0`.

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

  ☐ If applicable, change the values in the *Forward delay [s]* and *Max age* fields.
     – The root bridge transmits the changed values to the other devices.

  ☐ To save the changes temporarily, click the ✓ button.

`spanning-tree forward-time <4..30>`	Specifies the delay time for the status change in seconds.
`spanning-tree max-age <6..40>`	Specifies the maximum permissible branch length, for example the number of devices to the root bridge.
`show spanning-tree global`	Displays the parameters for checking.

Note: The parameters *Forward delay [s]* and *Max age* have the following relationship:
Forward delay [s] ≥ (*Max age*/2) + 1
If you enter values in the fields that contradict this relationship, the device replaces these values with the last valid values or with the default value.

Note: If 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.

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

12.3.6 Guards

The device allows you to activate various protection functions (guards) on the device ports.
The following protection functions help protect your network from incorrect configurations, loops and attacks with STP-BPDUs:

▶ BPDU Guard – for manually specified edge ports (end device ports)
You activate this protection function globally in the device.
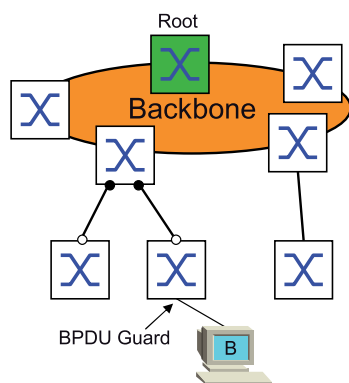
Terminal device ports do not normally receive any STP-BPDUs. If an attacker still attempts to feed in STP-BPDUs at this port, the device deactivates the device port.

▶ Root Guard – for designated ports
You activate this protection function separately for every device port.
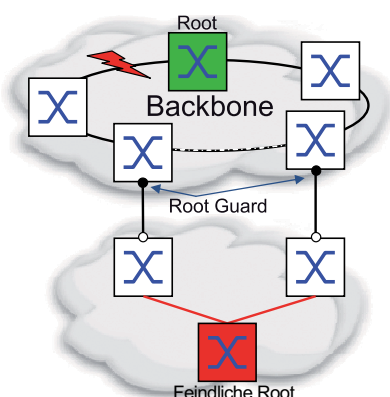
If a designated port receives an STP-BPDU with better path information to the root bridge, the device discards the STP-BPDU and sets the transmission state of the port to `discarding` instead of `root`.
If there are no STP-BPDUs with better path information to the root bridge, after 2 x *Hello time [s]* the device resets the state of the port to a value according to the port role.

▶ TCN Guard – for ports that receive STP-BPDUs with a Topology Change flag
You activate this protection function separately for every device port.
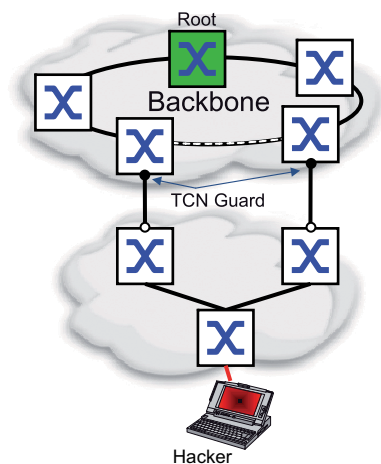
If the protection function is activated, the device ignores Topology Change flags in received STP-BPDUs. This does not change the content of the address table (FDB) of the device port. However, additional information in the BPDU that changes the topology is processed by the device.

▶ Loop Guard – for root, alternate and backup ports
You activate this protection function separately for every device port.
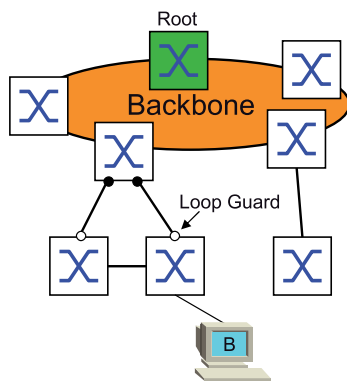
This protection function helps prevent the transmission status of a port from unintentionally being changed to `forwarding` if the port does not receive any more STP-BPDUs. If this situation occurs, the device designates the loop status of the port as inconsistent, but does not forward any data packets.

■ **Activating the BPDU Guard**

☐ Open the *Switching > L2-Redundancy > Spanning Tree > Global* dialog.

☐ Mark the *BPDU guard* checkbox.

☐ To save the changes temporarily, click the ✓ button.

`enable`	Change to the Privileged EXEC mode.
`configure`	Change to the Configuration mode.
`spanning-tree bpdu-guard`	Activates the BPDU Guard.
`show spanning-tree global`	Displays the parameters for checking.

☐ Open the *Switching > L2-Redundancy > Spanning Tree > Port* dialog.

☐ Switch to the *CIST* tab.

☐ For end device ports, mark the checkbox in the *Admin edge port* column.

☐ To save the changes temporarily, click the ✓ button.

`interface <x/y>`	Change to the interface configuration mode of interface `<x/y>`.
`spanning-tree edge-port`	Designates the port as a terminal device port (edge port).
`show spanning-tree port x/y`	Displays the parameters for checking.
`exit`	Leaves the interface mode.

If an edge port receives an STP-BPDU, the device behaves as follows:
▶ The device deactivates this port.
  In the *Basic Settings > Port* dialog, *Configuration* tab, the checkbox for this port in the *Port on* column is `unmarked`.
▶ The device designates the port.

In the *Switching > L2-Redundancy > Spanning Tree > Port* dialog, *Guards* tab, the checkbox in the *BPDU guard effect* column is `marked`.

`show spanning-tree port x/y`	Displays the parameters of the port for checking. The value of the *BPDU guard effect* parameter is `enabled`.

To reset the status of the device port to the value `forwarding`, you proceed as follows:
☐ If the port is still receiving BPDUs:
  – Remove the manual definition as an edge port (end device port).
    or
  – Deactivate the BPDU Guard.
☐ Activate the device port again.

■ Activating Root Guard / TCN Guard / Loop Guard

☐ Open the *Switching > L2-Redundancy > Spanning Tree > Port* dialog.
☐ Switch to the *Guards* tab.
☐ For designated ports, select the checkbox in the *Root guard* column.
☐ For ports that receive STP-BPDUs with a Topology Change flag, select the checkbox in the *TCN guard* column.
☐ For root, alternate or backup ports, mark the checkbox in the *Loop guard* column.

Note: The *Root guard* and *Loop guard* functions are mutually exclusive. If you try to activate the *Root guard* function while the *Loop guard* function is activated, the device deactivates the *Loop guard* function.

☐ To save the changes temporarily, click the ✓ button.

`enable`	Change to the Privileged EXEC mode.
`configure`	Change to the Configuration mode.
`interface <x/y>`	Change to the interface configuration mode of interface `<x/y>`.
`spanning-tree guard-root`	Switches the Root Guard on at the designated port.
`spanning-tree guard-tcn`	Switches the TCN Guard on at the port that receives STP-BPDUs with a Topology Change flag.
`spanning-tree guard-loop`	Switches the Loop Guard on at a root, alternate or backup port.
`exit`	Leaves the interface mode.
`show spanning-tree port x/y`	Displays the parameters of the port for checking.

12.3.7 Ring only mode

You use the *Ring only mode* function to recognize full-duplex connectivity and to configure the ports that are connected to the end stations. The *Ring only mode* function allows the device to transition to the 'forwarding' state, and suppress the Topology Change Notification PDUs.

■ Configuring the Ring only mode

When you activate the *Ring only mode* function on the ports, and the device ignores the message age of normal BDPUs, the device sends Topology Change messages with the message age of 1.

■ Example

The given example describes the configuration of the *Ring only mode* function.

- ☐ Open the *Switching > L2−Redundancy > Spanning Tree > Spanning Tree Global* dialog.
- ☐ In the *Ring only mode* frame, select the port 1/1 in the *First port* field.
- ☐ In the *Ring only mode* frame, select the port 1/2 in the *Second port* field.
- ☐ To activate the function, in the *Ring only mode* frame, mark the *Active* checkbox.

- ☐ To save the changes temporarily, click the ✅ button.

`enable`	Change to the Privileged EXEC mode.
`configure`	Change to the Configuration mode.
`spanning-tree ring-only-mode operation`	Enable the *Ring only mode* function.
`spanning-tree ring-only-mode first-port 1/1`	Specify port 1/1 as the first interface.
`spanning-tree ring-only-mode second-port 1/2`	Specify port 1/2 as the second interface.

12.4 Link Aggregation

Link Aggregation using the single switch method helps you overcome 2 limitations with ethernet links, namely bandwidth, and redundancy.

The first problem that the Link Aggregation Group (LAG) function helps you with is bandwidth limitations of individual ports. LAG allows you to combine 2 or more links in parallel, creating 1 logical link between 2 devices. The parallel links increase the bandwidth for traffic between the 2 devices.

You typically use Link Aggregation on the network backbone. The function provides you an inexpensive way to incrementally increase bandwidth.

Furthermore, Link Aggregation provides for redundancy with a seemless failover. With 2 or more links configured in parallel, when a link goes down, the other links in the group continue to forward traffic.

The default settings for a new Link Aggregation instance are as follows:
▶ In the *Active* column, the checkbox is marked.
▶ In the *Send trap (Link up/down)* column, the checkbox is marked.
▶ In the *Static link aggregation* column, the checkbox is unmarked.
▶ In the *Active ports (min.)* column, the value is 1.

12.4.1 Methods of Operation

The device operates on the Single Switch method. The Single Switch method provides you an inexpensive way to grow your network. The single switch method states that you need 1 device on each side of a link to provide the physical ports. The device balances the traffic load across the group member ports.

The device also uses the Same Link Speed method in which the group member ports are full-duplex, point-to-point links having the same transmission rate. The first port the user adds to the group is the master port and determines the bandwidth for the other member ports of the Link Aggregation Group.

The device allows you to set up up to 2 Link Aggregation groups. The number of useable ports per Link Aggregation group depends on the device.

12.4.2 Link Aggregation Example

Connect multiple workstations using one aggregated link group between switch 1 and 2. By aggregating multiple links, higher speeds are achievable without a hardware upgrade.
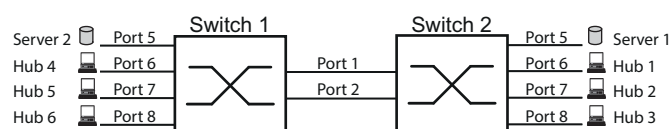

Figure 43: Link Aggregation Switch to Switch Network

Use the following steps to setup switch 1 and 2 in the graphical user interface.

☐ Open the *Switching > L2-Redundancy > Link Aggregation* dialog.

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

☐ In the *Trunk port* drop-down list, select the instance number of the link aggregation group.

☐ In the *Port* drop-down list, select the port 1/1.

☐ Click the *Ok* button.

☐ Repeat the preceding steps and select the port 1/2.

☐ Click the *Ok* button.

☐ To save the changes temporarily, click the ✅ button.

```
enable                        Change to the Privileged EXEC mode.
configure                     Change to the Configuration mode.
link-aggregation add lag/1    Creates a Link Aggregation Group lag/1.
```

```
link-aggregation modify lag/1 addport 1/1   Adds port 1/1 to the Link Aggregation Group.
link-aggregation modify lag/1 addport 1/2   Adds port 1/2 to the Link Aggregation Group.
```

12.5 Link Backup

Link Backup provides a redundant link for traffic on Layer 2 devices. When the device detects an error on the primary link, then the device transfers traffic to the backup link. You typically use Link Backup in service-provider or enterprise networks.

You set up the backup links in pairs, one as a primary and one as a backup. When providing redundancy for enterprise networks for example, the device allows you to set up more than 1 pair. The maximum number of link backup pairs is: total number of physical ports / 2. Furthermore, the device sends an SNMP trap when the state of a port participating in a link backup pair changes.

When configuring link backup pairs remember the following rules:
▶ A link pair consists of any combination of physical ports. For example, when 1 port is a 100 Mbit port and the other is a 1000 Mbit SFP port.
▶ A specific port is a member of 1 link backup pair at any given time.
▶ Verify that the ports of a link backup pair are members of the same VLAN with the same VLAN ID. When the primary port or backup port is a member of a VLAN then, assign the second port of the pair to the same VLAN.

The default setting for this function is inactive without any link backup pairs.

Note: Verify that the Spanning Tree Protocol is disabled on the Link Backup ports.

12.5.1 Fail Back Description

Link Backup also allows you to set up a Fail Back option. When you activate the fail back function and the primary link returns to normal operation, the device first blocks traffic on the backup port and then forwards traffic on the primary port. This process helps protect the device from causing loops in the network.

When the primary port returns to the link up and active state, the device supports 2 modes of operation:
▶ When you inactivate *Fail back*, the primary port remains in the blocking state until the backup link fails.
▶ When you activate *Fail back*, and after the *Fail back delay [s]* timer expires, the primary port returns to the forwarding state and the backup port changes to down.

In the cases listed above, the port forcing its link to forward traffic, first sends a "flush FDB" packet to the remote device. The flush packet helps the remote device quickly relearn the MAC addresses.

12.5.2 Example Configuration

In the example network below, you connect ports `2/3` and `2/4` on switch A to the uplink switches B and C. When you set up the ports as a Link Backup pair, 1 of the ports forwards traffic and the other port is in the blocking mode.

The primary, port `2/3` on switch A, is the active port and is forwarding traffic to port 1 on switch B. Port `2/4` on switch A is the backup port and is blocking traffic.

When switch A disables port `2/3` because of a detected error, then port `2/4` on switch A starts forwarding traffic to port 2 on switch C.

When port `2/3` returns to the active state, "no shutdown", with *Fail back* activated, and *Fail back delay [s]* set to 30 seconds. After the timer expires, port `2/4` first blocks the traffic and then port `2/3` starts forwarding the traffic.
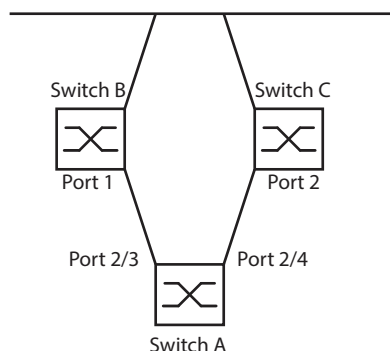
Figure 44: `Link Backup` example network

The following tables contain examples of parameters for Switch A set up.

☐ Open the *Switching > L2-Redundancy > Link Backup* dialog.

☐ Enter a new Link Backup pair in the table:

  ☐ Click the [icon] button.
    The dialog displays the *Create* window.
  ☐ In the *Primary port* drop-down list, select port 2/3.
    In the *Backup port* drop-down list, select port 2/4.
  ☐ Click the *Ok* button.

☐ In the *Description* textbox, enter Link_Backup_1 as the name for the backup pair.

☐ To activate the Fail Back function for the link backup pair, mark the *Fail back* checkbox.

☐ Set the fail back timer for the link backup pair, enter 30 s in *Fail back delay [s]*.

☐ To activate the link backup pair, mark the *Active* checkbox.

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

enable	Change to the Privileged EXEC mode.
configure	Change to the Configuration mode.
interface 2/3	Change to the interface configuration mode of interface 2/3.
link-backup add 2/4	Creates a Link Backup instance where port 2/3 is the primary port and port 2/4 is the backup port.
link-backup modify 2/4 description Link_Backup_1	Specifies the string Link_Backup_1 as the name of the backup pair.
link-backup modify 2/4 failback-status enable	Enables the fail back timer.
link-backup modify 2/4 failback-time 30	Specifies the fail back delay time as 30 s.
link-backup modify 2/4 status enable	Enables the Link Backup instance.
exit	Change to the Configuration mode.
link-backup operation	Enables the *Link Backup* function globally on the device.

13 Operation diagnosis

The device provides you with the following diagnostic tools:
▶ Sending SNMP traps
▶ Monitoring the Device Status
▶ Out-of-Band signaling using the signal contact
▶ Port status indication
▶ Event counter at port level
▶ Detecting non-matching duplex modes
▶ Auto-Disable
▶ Displaying the SFP status
▶ Topology discovery
▶ Detecting IP address conflicts
▶ Detecting loops
▶ Reports
▶ Monitoring data traffic on a port (port mirroring)
▶ Syslog
▶ Event log
▶ Cause and action management during selftest

13.1 Sending SNMP traps

The device immediately reports unusual events which occur during normal operation to the network management station. This is done by messages called SNMP traps that bypass the polling procedure ("polling" means querying the data stations at regular intervals). SNMP traps allow you to react quickly to unusual events.

Examples of such events are:

▶ Hardware reset
▶ Changes to the configuration
▶ Segmentation of a port

The device sends SNMP traps to various hosts to increase the transmission reliability for the messages. The unacknowledged SNMP trap message consists of a packet containing information about an unusual event.

The device sends SNMP traps to those hosts entered in the trap destination table. The device allows you to configure the trap destination table with the network management station using SNMP.

13.1.1 List of SNMP traps

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

Name of the SNMP trap	Meaning
authenticationFailure	This is sent if a station attempts to access an agent without authorisation.
coldStart	Sent after a restart.
hm2DevMonSenseExtNvmRemoval	This is sent when the external memory has been removed.
linkDown	This is sent if the connection to a port is interrupted.
linkUp	This is sent when connection is established to a port.
hm2SigConStateChange	This is sent if the status of the signal contact changes in the operation monitoring.
newRoot	This is sent if the sending agent becomes the new root of the spanning tree.
topologyChange	This is sent when the port changes from blocking to forwarding or from forwarding to blocking.
alarmRisingThreshold	This is sent if the RMON input exceeds its upper threshold.
alarmFallingThreshold	This is sent if the RMON input goes below its lower threshold.
hm2AgentPortSecurityViolation	This is sent if a MAC address detected on this port does not match the current settings of the parameter hm2AgentPortSecurityEntry.
hm2DiagSelftestActionTrap	Sent if a self test for the four categories "task", "resource", "software", and "hardware" is performed according to the configured settings.
hm2MrpReconfig	This is sent if the configuration of the MRP ring changes.
hm2DiagIfaceUtilizationTrap	This is sent if the threshold of the interface exceeds or undercuts the upper or lower threshold specified.
hm2LogAuditStartNextSector	This trap is sent if the audit trail after completing one sector starts a new one.
hm2ConfigurationSavedTrap	This is sent after the device has successfully saved its configuration locally.
hm2ConfigurationChangedTrap	This is sent when you change the configuration of the device for the first time after it has been saved locally.
hm2PlatformStpInstanceLoopInconsistentStartTrap	This is sent if the port in this STP instance changes to the "loop inconsistent" status.
hm2PlatformStpInstanceLoopInconsistentEndTrap	This is sent if the port in this STP instance leaves the "loop inconsistent" status when receiving a BPDU packet.

Table 30: Possible SNMP traps

13.1.2 SNMP traps for configuration activity

After you save a configuration in the memory, the device sends a hm2ConfigurationSavedTrap. This SNMP trap contains both the Non-Volatile Memory (NVM) and External Non-Volatile Memory (ENVM) state variables indicating whether the running configuration is in sync with the NVM, and with the ENVM. You can also trigger this SNMP trap by copying a configuration file to the device, replacing the active saved configuration.

Furthermore, the device sends a hm2ConfigurationChangedTrap, whenever you change the local configuration, indicating a mismatch between the running and saved configuration.

13.1.3 SNMP trap setting

The device offers you the option of sending an SNMP trap as a reaction to specific events. Create at least 1 trap destination that receives SNMP traps.

Perform the following steps:

☐ Open the *Diagnostics > Status Configuration > Alarms (Traps)* dialog.

☐ Click the [⊞] button.
   The dialog displays the *Create* window.

☐ In the *Name* frame, specify the name that the device uses to identify itself as the source of the SNMP trap.

☐ In the *Address* frame, specify the IP address of the trap destination to which the device sends the SNMP traps.

☐ In the *Active* column you select the entries that the device should take into account when it sends SNMP traps.

☐ To save the changes temporarily, click the [✓] button.

For example, in the following dialogs you specify when the device triggers an SNMP trap:

▶ *Basic Settings > Port* dialog
▶ *Network Security > Port Security* dialog
▶ *Switching > L2-Redundancy > Link Aggregation* dialog
▶ *Diagnostics > Status Configuration > Device Status* dialog
▶ *Diagnostics > Status Configuration > Security Status* dialog
▶ *Diagnostics > Status Configuration > Signal Contact* dialog
▶ *Diagnostics > System > IP Address Conflict Detection* dialog
▶ *Diagnostics > System > Selftest* dialog
▶ *Diagnostics > Ports > Port Monitor* dialog

13.1.4 ICMP messaging

The device allows you to use the Internet Control Message Protocol (ICMP) for diagnostic applications, for example ping and trace route. The device also uses ICMP for time-to-live and discarding messages in which the device forwards an ICMP message back to the packet source device.

Use the ping network tool to test the path to a particular host across an IP network. The traceroute diagnostic tool displays paths and transit delays of packets across a network.

13.2 Monitoring the Device Status

The device status provides an overview of the overall condition of the device. Many process visualization systems record the device status for a device in order to present its condition in graphic form.

The device displays its current status as `error` or `ok` in the *Device status* frame. The device determines this status from the individual monitoring results.

The device enables you to:

▶ Out-of-Band signalling using a signal contact

▶ signal the changed device status by sending an SNMP trap

▶ detect the device status in the *Basic Settings > System* dialog of the graphical user interface

▶ query the device status in the Command Line Interface

The *Global* tab of the *Diagnostics > Status Configuration > Device Status* dialog allows you to configure the device to send a trap to the management station for the following events:
▶ When the device is operating outside of the user-defined temperature threshold
▶ Loss of the redundancy (in ring manager mode)
▶ The interruption of link connection(s)
  Configure at least one port for this feature. In the *Port* tab of the *Diagnostics > Status Configuration > Device Status* dialog in the *Propagate connection error* row, you specify which ports the device signals if the link is down.
▶ The removal of the external memory.
▶ The configuration in the external memory is out-of-sync with the configuration in the device.

Select the corresponding entries to decide which events the device status includes.

13.2.1 Events which can be monitored

Name	Meaning
Temperature	If the temperature exceeds or falls below the value specified.
Ring redundancy	Enable this function to monitor if ring redundancy is present.
Connection errors	Enable this function to monitor every port link event in which the *Propagate connection error* checkbox is active.
External memory removal	Enable this function to monitor the presence of an external storage device.
External memory not in sync	The device monitors synchronization between the device configuration and the configuration stored on the ENVM.

Table 31: Device Status events

13.2.2 Configuring the Device Status

Perform the following steps:

☐ Open the *Diagnostics > Status Configuration > Device Status* dialog, *Global* tab.
☐ For the parameters to be monitored, mark the checkbox in the *Monitor* column.
☐ To send an SNMP trap to the management station, activate the *Send trap* function in the *Traps* frame.
☐ In the *Diagnostics > Status Configuration > Alarms (Traps)* dialog, create at least 1 trap destination that receives SNMP traps.

☐ To save the changes temporarily, click the ✓ button.

☐ Open the *Basic Settings > System* dialog.
☐ To monitor the temperature, at the bottom of the *System data* frame, you specify the temperature thresholds.

☐ To save the changes temporarily, click the ✓ button.

```
enable                    Change to the Privileged EXEC mode.
configure                 Change to the Configuration mode.
device-status trap        Sending an SNMP trap if the device status changes.
```

`device-status monitor envm-not-in-sync`	Monitors the configuration profiles in the device and in the external memory. The *Device status* changes to `error` in the following situations: – The configuration profile solely exists in the device. – The configuration profile in the device differs from the configuration profile in the external memory.
`device-status monitor envm-removal`	Monitors the active external memory. The value in the *Device status* frame changes to `error` if you remove the active external memory from the device.
`device-status monitor ring-redundancy`	Monitors the ring redundancy. The *Device status* changes to `error` in the following situations: – The redundancy function becomes active (loss of redundancy reserve). – The device is a normal ring participant and detects an error in its settings.
`device-status monitor temperature`	Monitors the temperature in the device. The value in the *Device status* frame changes to `error` if the temperature exceeds or falls below the specified limit.

In order to enable the device to monitor an active link without a connection, first enable the global function, then enable the individual ports.

Perform the following steps:

☐ Open the *Diagnostics > Status Configuration > Device Status* dialog, *Global* tab.

☐ For the *Connection errors* parameter, mark the checkbox in the *Monitor* column.

☐ Open the *Diagnostics > Status Configuration > Device Status* dialog, *Port* tab.

☐ For the *Propagate connection error* parameter, mark the checkbox in the column of the ports to be monitored.

☐ To save the changes temporarily, click the ✅ button.

`enable`	Change to the Privileged EXEC mode.
`configure`	Change to the Configuration mode.
`device-status monitor link-failure`	Monitors the ports/interfaces link. The value in the *Device status* frame changes to `error` if the link interrupts on a monitored port/interface.
`interface 1/1`	Change to the interface configuration mode of interface `1/1`.
`device-status link-alarm`	Monitors the port/interface link. The value in the *Device status* frame changes to `error` if the link interrupts on the port/interface.

Note: The above CLI commands activate monitoring and trapping for the supported components. If you want to activate or deactivate monitoring for individual components, you will find the corresponding syntax in the "Command Line Interface" reference manual or in the help of the CLI console. (Enter a question mark `?` for the CLI prompt.)

13.2.3 Displaying the Device Status

Perform the following steps:

☐ Open the *Basic Settings > System* dialog.

`show device-status all`	In the EXEC Privilege mode: Displays the device status and the setting for the device status determination.

13.3 Security Status

The Security Status provides an overview of the overall security of the device. Many processes aid in system visualization by recording the security status of the device and then presenting its condition in graphic form. The device displays the overall security status in the *Basic Settings > System* dialog, *Security status* frame.

In the *Global* tab of the *Diagnostics > Status Configuration > Security Status* dialog the device displays its current status as `error` or `ok` in the *Security status* frame. The device determines this status from the individual monitoring results.

The device enables you to:

▶ Out-of-Band signalling using a signal contact

▶ signal the changed security status by sending an SNMP trap

▶ detect the security status in the *Basic Settings > System* dialog of the graphical user interface

▶ query the security status in the Command Line Interface

13.3.1 Events which can be monitored

☐ Specify the events that the device monitors.
   For the corresponding parameter, mark the checkbox in the *Monitor* column.

Name	Meaning
Password default settings unchanged	After installation change the passwords to increase security. The device monitors if the default passwords remain unchanged.
Min. password length < 8	Create passwords more than 8 characters long to maintain a high security posture. When active the device monitors the *Min. password length* setting.
Password policy settings deactivated	The device monitors the settings located in the *Device Security > User Management* dialog for password policy requirements.
User account password policy check deactivated	The device monitors the settings of the *Policy check* checkbox. When *Policy check* is inactive, the device sends an SNMP trap.
Telnet server active	The device monitors when you enable the Telnet function.
HTTP server active	The device monitors when you enable the HTTP connection function.
SNMP unencrypted	The device monitors when you enable the SNMPv1 or v2 connection function.
Access to system monitor with V.24 possible	The device monitors the System Monitor status.
Saving the configuration profile on the external memory possible	The device monitors the possibility to save configurations to the external non-volatile memory.
Link interrupted on enabled device ports	The device monitors the link status of active ports.
Access with HiDiscovery possible	The device monitors when you enable the HiDiscovery read/write access function.
Load unencrypted config from external memory	The device monitors the security settings for loading the configuration from the external NVM.
IEC61850-MMS active	The device monitors the IEC 61850-MMS protocol activation setting.
Modbus TCP active	The device monitors the Modbus TCP/IP protocol activation setting.
Self-signed HTTPS certificate present	The device monitors the HTTPS server for self-created digital certificates.

Table 32: Security Status events

13.3.2 Configuring the Security Status

Perform the following steps:

☐ Open the *Diagnostics > Status Configuration > Security Status* dialog, *Global* tab.

☐ For the parameters to be monitored, mark the checkbox in the *Monitor* column.

☐ To send an SNMP trap to the management station, activate the *Send trap* function in the *Traps* frame.

☐ To save the changes temporarily, click the ✓ button.

☐ In the *Diagnostics > Status Configuration > Alarms (Traps)* dialog, create at least 1 trap destination that receives SNMP traps.

`enable`	Change to the Privileged EXEC mode.
`configure`	Change to the Configuration mode.
`security-status monitor pwd-change`	Monitors the password for the locally set up user accounts `user` and `admin`. The value in the **Security status** frame changes to `error` if the password for the `user` or `admin` user accounts is the default setting.
`security-status monitor pwd-min-length`	Monitors the value specified in the **Min. password length** policy. The value in the **Security status** frame changes to `error` if the value for the **Min. password length** policy is less than `8`.
`security-status monitor pwd-policy-config`	Monitors the password policy settings. The value in the **Security status** frame changes to `error` if the value for at least one of the following policies is specified as `0`. – **Upper-case characters (min.)** – **Lower-case characters (min.)** – **Digits (min.)** – **Special characters (min.)**
`security-status monitor pwd-policy-inactive`	Monitors the password policy settings. The value in the **Security status** frame changes to `error` if the value for at least one of the following policies is specified as `0`.
`security-status monitor telnet-enabled`	Monitors the Telnet server. The value in the **Security status** frame changes to `error` if you enable the Telnet server.
`security-status monitor http-enabled`	Monitors the HTTP server. The value in the **Security status** frame changes to `error` if you enable the HTTP server.
`security-status monitor snmp-unsecure`	Monitors the SNMP server. The value in the **Security status** frame changes to `error` if at least one of the following conditions applies: – The **SNMPv1** function is enabled. – The **SNMPv2** function is enabled. – The encryption for SNMPv3 is disabled. You enable the encryption in the **Device Security > User Management** dialog, in the **SNMP encryption type** field.
`security-status monitor sysmon-enabled`	To monitor the activation of System Monitor 1 on the device.
`security-status monitor extnvm-upd-enabled`	To monitor the activation of the external non volatile memory update.
`security-status monitor iec61850-mms-enabled`	Monitors the **IEC61850-MMS** function. The value in the **Security status** frame changes to `error` if you enable the **IEC61850-MMS** function.
`security-status trap`	Sending an SNMP trap if the device status changes.

In order to enable the device to monitor an active link without a connection, first enable the global function, then enable the individual ports.

Perform the following steps:

☐ Open the **Diagnostics > Status Configuration > Security Status** dialog, **Global** tab.
☐ For the **Link interrupted on enabled device ports** parameter, mark the checkbox in the **Monitor** column.

☐ To save the changes temporarily, click the ✓ button.

☐ Open the **Diagnostics > Status Configuration > Device Status** dialog, **Port** tab.
☐ For the **Link interrupted on enabled device ports** parameter, mark the checkbox in the column of the ports to be monitored.

☐ To save the changes temporarily, click the ✓ button.

`enable`	Change to the Privileged EXEC mode.
`configure`	Change to the Configuration mode.
`security-status monitor no-link-enabled`	Monitors the link on active ports. The value in the **Security status** frame changes to `error` if the link interrupts on an active port.
`interface 1/1`	Change to the interface configuration mode of interface `1/1`.
`security-status monitor no-link`	Monitors the link on interface/port `1`.

13.3.3 Displaying the Security Status

Perform the following steps:

☐ Open the *Basic Settings > System* dialog.

`show security-status all`	In the EXEC Privilege mode, display the security status and the setting for the security status determination.

13.4   Out-of-Band signaling

The device uses the signal contact to control external devices and monitor device functions. Function monitoring enables you to perform remote diagnostics.
The device reports the operating status using a break in the potential-free signal contact (relay contact, closed circuit) for the selected mode. The device monitors the following functions:

▶ Incorrect supply voltage
  – at least one of the 2 supply voltages is not operating
  – the internal supply voltage is not operating
▶ When the device is operating outside of the user-defined temperature threshold
▶ Events for ring redundancy
  Loss of the redundancy (in ring manager mode)
  In the default setting, ring redundancy monitoring is inactive. The device is a normal ring participant and detects an error in the local configuration.
▶ The interruption of link connection(s)
  Configure at least one port for this feature. In the *Propagate connection error* frame, you specify which ports the device signals if the link is down. In the default setting, link monitoring is inactive.
▶ The removal of the external memory.
▶ The configuration on the external memory does not match that in the device.

Select the corresponding entries to decide which events the device status includes.

Note: With a non-redundant voltage supply, the device reports the absence of a supply voltage. To disable this message, feed the supply voltage over both inputs or ignore the monitoring.

13.4.1   Controlling the Signal contact

With the `Manual setting` mode you control this signal contact remotely.

Application options:
▶ Simulation of an error detected during SPS error monitoring
▶ Remote control of a device using SNMP, such as switching on a camera

Perform the following steps:
☐ Open the *Diagnostics > Status Configuration > Signal Contact* dialog, *Global* tab.
☐ To control the signal contact manually, in the *Configuration* frame, *Mode* drop-down list, select the value `Manual setting`.
☐ To open the signal contact, you select the `open` radio button in the *Configuration* frame.
☐ To close the signal contact, you select the `close` radio button in the *Configuration* frame.

☐ To save the changes temporarily, click the ✓ button.

```
enable                          Change to the Privileged EXEC mode.
configure                       Change to the Configuration mode.
signal-contact 1 mode manual    Select the manual setting mode for signal contact 1.
signal-contact 1 state open     Open signal contact 1.
signal-contact 1 state closed   Close signal contact 1.
```

13.4.2 Monitoring the Device and Security Statuses

In the *Configuration* field, you specify which events the signal contact indicates.

▶ `Device status`
Using this setting the signal contact indicates the status of the parameters monitored in the *Diagnostics > Status Configuration > Device Status* dialog.

▶ `Security status`
Using this setting the signal contact indicates the status of the parameters monitored in the *Diagnostics > Status Configuration > Security Status* dialog.

▶ `Device/Security status`
Using this setting the signal contact indicates the status of the parameters monitored in the *Diagnostics > Status Configuration > Device Status* and the *Diagnostics > Status Configuration > Security Status* dialog.

■ **Configuring the operation monitoring**

Perform the following steps:

☐ Open the *Diagnostics > Status Configuration > Signal Contact* dialog, *Global* tab.

☐ To monitor the device functions using the signal contact, in the *Configuration* frame, specify the value `Monitoring correct operation` in the *Mode* field.

☐ For the parameters to be monitored, mark the checkbox in the *Monitor* column.

☐ To send an SNMP trap to the management station, activate the *Send trap* function in the *Traps* frame.

☐ To save the changes temporarily, click the ✓ button.

☐ In the *Diagnostics > Status Configuration > Alarms (Traps)* dialog, create at least 1 trap destination that receives SNMP traps.

☐ To save the changes temporarily, click the ✓ button.

☐ You specify the temperature thresholds for the temperature monitoring in the *Basic Settings > System* dialog.

`enable`	Change to the Privileged EXEC mode.
`configure`	Change to the Configuration mode.
`signal-contact 1 monitor temperature`	Monitors the temperature in the device. The signal contact opens if the temperature exceeds / falls below the threshold values.
`signal-contact 1 monitor ring-redundancy`	Monitors the ring redundancy. The signal contact opens in the following situations: – The redundancy function becomes active (loss of redundancy reserve). – The device is a normal ring participant and detects an error in its settings.
`signal-contact 1 monitor link-failure`	Monitors the ports/interfaces link. The signal contact opens if the link interrupts on a monitored port/interface.
`signal-contact 1 monitor envm-removal`	Monitors the active external memory. The signal contact opens if you remove the active external memory from the device.
`signal-contact 1 monitor envm-not-in-sync`	Monitors the configuration profiles in the device and in the external memory. The signal contact opens in the following situations: – The configuration profile solely exists in the device. – The configuration profile in the device differs from the configuration profile in the external memory.
`signal-contact 1 monitor power-supply 1`	Monitors the power supply unit 1. The signal contact opens if the device has a detected power supply fault.
`signal-contact 1 monitor module-removal 1`	Monitors module 1. The signal contact opens if you remove module 1 from the device.
`signal-contact 1 trap`	Enables the device to send an SNMP trap when the status of the operation monitoring changes.
`no signal-contact 1 trap`	Disabling the SNMP trap

In order to enable the device to monitor an active link without a connection, first enable the global function, then enable the individual ports.

Perform the following steps:

- ☐ In the *Monitor* column, activate the *Link interrupted on enabled device ports* function.
- ☐ Open the *Diagnostics > Status Configuration > Device Status* dialog, *Port* tab.

`enable`	Change to the Privileged EXEC mode.
`configure`	Change to the Configuration mode.
`signal-contact 1 monitor link-failure`	Monitors the ports/interfaces link. The signal contact opens if the link interrupts on a monitored port/interface.
`interface 1/1`	Change to the interface configuration mode of interface `1/1`.
`signal-contact 1 link-alarm`	Monitors the port/interface link. The signal contact opens if the link interrupts on the port/interface.

■ Events which can be monitored

Name	Meaning
Temperature	If the temperature exceeds or falls below the value specified.
Ring redundancy	Enable this function to monitor if ring redundancy is present.
Connection errors	Enable this function to monitor every port link event in which the *Propagate connection error* checkbox is active.
External memory not in sync with NVM	The device monitors synchronization between the device configuration and the configuration stored on the ENVM.
External memory removed	Enable this function to monitor the presence of an external storage device.

Table 33: Device Status events

■ Displaying the signal contact's status

The device gives you additional options for displaying the status of the signal contact:
▶ Display in the graphical user interface
▶ Query in the Command Line Interface

- ☐ Open the *Basic Settings > System* dialog.
  The *Signal contact status* frame displays the signal contact status and informs you about alarms that have occurred. When an alarm currently exists, the frame is highlighted.

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

13.5 Port event counter

The port statistics table enables experienced network administrators to identify possible detected problems in the network.

This table displays the contents of various event counters. The packet counters add up the events sent and the events received. In the *Basic Settings > Restart* dialog, you can reset the event counters.

Counter	Indication of known possible weakness
Received fragments	– Non-functioning controller of the connected device
	– Electromagnetic interference in the transmission medium
CRC Error	– Non-functioning controller of the connected device
	– Electromagnetic interference in the transmission medium
	– Inoperable component in the network
Collisions	– Non-functioning controller of the connected device
	– Network over extended/lines too long
	– Collision or a detected fault with a data packet

Table 34: Examples indicating known weaknesses

Perform the following steps:

- ☐ To display the event counter, open the *Basic Settings > Port* dialog, *Statistics* tab.
- ☐ To reset the counters, in the *Basic Settings > Restart* dialog, click the *Clear port statistics* button.

13.5.1 Detecting non-matching duplex modes

Problems occur when 2 ports directly connected to each other have mismatching duplex modes. These problems are difficult to track down. The automatic detection and reporting of this situation has the benefit of recognizing mismatching duplex modes before problems occur.

This situation arises from an incorrect configuration, for example, if you deactivate the automatic configuration on the remote port.

A typical effect of this non-matching is that at a low data rate, the connection seems to be functioning, but at a higher bi-directional traffic level the local device records a lot of CRC errors, and the connection falls significantly below its nominal capacity.

The device allows you to detect this situation and report it to the network management station. In the process, the device evaluates the error counters of the port in the context of the port settings.

■ Possible causes of port error events

The following table lists the duplex operating modes for TX ports, with the possible fault events. The meanings of terms used in the table are as follows:
▶ Collisions
  In half-duplex mode, collisions mean normal operation.
▶ Duplex problem
  Mismatching duplex modes.
▶ EMI
  Electromagnetic interference.
▶ Network extension
  The network extension is too great, or too many cascading hubs.
▶ Collisions, Late Collisions
  In full-duplex mode, no incrementation of the port counters for collisions or Late Collisions.
▶ CRC Error
  The device evaluates these errors as non-matching duplex modes in the manual full duplex mode.

No.	Automatic configuration	Current duplex mode	Detected error events (≥ 10 after link up)	Duplex modes	Possible causes
1	`marked`	Half duplex	None	OK	
2	`marked`	Half duplex	Collisions	OK	

Table 35: Evaluation of non-matching of the duplex mode

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

Table 35: Evaluation of non-matching of the duplex mode (cont.)

13.6 Auto-Disable

The device can disable a port due to several configurable reasons. Each reason causes the port to "shut down". In order to recover the port from the shut down state, you can manually clear the condition which caused the port to shut down or specify a timer to automatically re-enable the port.

If the configuration displays a port as enabled, but the device detects an error or change in the condition, the software shuts down that port. In other words, the device software disables the port because of a detected error or change in the condition.

When a port is auto-disabled, the device effectively shuts down the port and the port blocks traffic. The port LED blinks green 3 times per period and identifies the reason for the shutdown. In addition, the device creates a log file entry which lists the causes of the deactivation. When you re-enable the port after a timeout using the *Auto-Disable* function, the device generates a log entry.

The *Auto-Disable* function provides a recovery function which automatically enables an auto-disabled port after a user-defined time. When this function enables a port, the device sends an SNMP trap with the port number, but without a value for the *Reason* parameter.

The *Auto-Disable* function serves the following purposes:
▶ It assists the network administrator in port analysis.
▶ It reduces the possibility that this port causes the network to be instable.

The *Auto-Disable* function is available for the following functions:
▶ *Link flap* (*Port Monitor* function)
▶ *CRC/Fragments* (*Port Monitor* function)
▶ Duplex Mismatch detection (*Port Monitor* function)
▶ *Spanning Tree*
▶ *Port Security*
▶ *Overload detection* (*Port Monitor* function)
▶ *Link speed/Duplex mode detection* (*Port Monitor* function)

In the following example, you configure the device to disable a port due to detected violations to the thresholds specified the *Diagnostics > Ports > Port Monitor > CRC/Fragments* tab and then automatically re-enable the disabled port.

Perform the following steps:
☐ Open the *Diagnostics > Ports > Port Monitor* dialog, *CRC/Fragments* tab.
☐ Verify that the thresholds specified in the table concur to your preferences for port `1/1`.
☐ Open the *Diagnostics > Ports > Port Monitor* dialog, *Global* tab.
☐ To enable the function, select the `On` radio button in the *Operation* frame.
☐ To allow the device to disable the port due to detected errors, mark the checkbox in the *CRC/Fragments on* column for port `1/1`.
☐ In the *Action* column you can choose how the device reacts to detected errors. In this example, the device disables port `1/1` for threshold violations and then automatically re-enables the port.
  ▶ To allow the device to disable and automatically re-enable the port, select the value `auto-disable` and configure the *Auto-Disable* function. The value `auto-disable` only works in conjunction with the *Diagnostics > Ports > Auto-Disable* function.

  The device can also disable a port without auto re-enabling.
  ▶ To allow the device to disable the port only, select the value `disable port`.
    To manually re-enable a disabled port, highlight the port.

    Click the ☰ button and then the *Reset* item.
  ▶ When you configure the *Auto-Disable* function, the value `disable port` also automatically re-enables the port.
☐ Open the *Diagnostics > Ports > Port Monitor* dialog, *Auto-disable* tab.
☐ To allow the device to auto re-enable the port after it was disabled due to detected threshold violations, mark the checkbox in the *CRC error* column.
☐ Open the *Diagnostics > Ports > Port Monitor* dialog, *Port* tab.
☐ Specify the delay time as 120 s in the *Reset timer [s]* column for the ports you want to enable.

Note: The *Reset* item allows you to enable the port before the time specified in the *Reset timer [s]* column counts down.

`enable`	Change to the Privileged EXEC mode.
`configure`	Change to the Configuration mode.
`interface 1/1`	Change to the interface configuration mode of interface `1/1`.
`port-monitor condition crc-fragments count 2000`	Specifying the CRC-Fragment counter to 2000 parts per million.
`port-monitor condition crc-fragments interval 15`	Sets the measure interval to 15 seconds for CRC-Fragment detection.
`auto-disable timer 120`	Specifies the waiting period of `120` seconds, after which the ***Auto-disable*** function re-enables the port.
`exit`	Change to the Configuration mode.
`auto-disable reason crc-error`	Activate the auto-disable CRC function.
`port-monitor condition crc-fragments mode`	Activate the CRC-Fragments condition to trigger an action.
`port-monitor operation`	Activate the ***Port Monitor*** function.

When the device disables a port due to threshold violations the device allows you to use the following CLI commands to manually reset the disabled port.

Perform the following steps:

`enable`	Change to the Privileged EXEC mode.
`configure`	Change to the Configuration mode.
`interface 1/1`	Change to the interface configuration mode of interface `1/1`.
`auto-disable reset`	Allows you to enable the port before the Timer counts down.

13.7 Displaying the SFP status

The SFP status display allows you to look at the current SFP module connections and their properties. The properties include:
- ▶ module type
- ▶ serial number of media module
- ▶ temperature in ° C
- ▶ transmission power in mW
- ▶ receive power in mW

Perform the following steps:

☐ Open the *Diagnostics > Ports > SFP* dialog.

13.8 Topology discovery

IEEE 802.1AB defines the Link Layer Discovery Protocol (LLDP). LLDP allows the user to automatically detect the LAN network topology.

Devices with LLDP active:

▶ broadcast their connection and management information to neighboring devices on the shared LAN.
   Evaluation of the devices occur when the receiving device has its LLDP function active.
▶ receive connection and management information from neighbor devices on the shared LAN, provided these adjacent devices also have LLDP active.
▶ build a management information database and object definitions for storing information about adjacent devices with LLDP active.

As the main element, the connection information contains an exact, unique identifier for the connection end point: MAC (Service Access Point). This is made up of a device identifier which is unique on the entire network and a unique port identifier for this device.

▶ Chassis identifier (its MAC address)
▶ Port identifier (its port-MAC address)
▶ Description of port
▶ System name
▶ System description
▶ Supported system capabilities
▶ System capabilities currently active
▶ Interface ID of the management address
▶ VLAN-ID of the port
▶ Auto-negotiation status on the port
▶ Medium, half/full duplex setting and port speed setting
▶ Information about the VLANs installed in the device (VLAN-ID and VLAN name, irrespective of whether the port is a VLAN participant).

A network management station can call up this information from devices with activated LLDP. This information enables the network management station to map the topology of the network.

Non-LLDP devices normally block the special Multicast LLDP IEEE MAC address used for information exchange. Non-LLDP devices therefore discard LLDP packets. When positioning a non-LLDP capable device between 2 LLDP capable devices, the non-LLDP capable device prohibits information exchanges between the 2 LLDP capable devices.

The Management Information Base (MIB) for a device with LLDP capability holds the LLDP information in the lldp MIB and in the private HM2-LLDP-EXT-HM-MIB and HM2-LLDP-MIB.

13.8.1 Displaying the Topology discovery results

To show the topology of the network:

☐ Open the *Diagnostics > LLDP > LLDP Topology Discovery* dialog, *LLDP* tab.

If you use a port to connect several devices, for example via a hub, the table contains a line for each connected device.

Activating Display FDB Entries at the bottom of the table allows you to display devices without active LLDP support in the table. In this case, the device also includes information from its FDB (forwarding database).

If you connect the port to devices with the topology discovery function active, then the devices exchange LLDP Data Units (LLDPDU) and the topology table displays these neighboring devices.

When a port connects devices without an active topology discovery exclusively, the table contains a line for this port to represent the connected devices. This line contains the number of connected devices.

The FDB address table contains MAC addresses of devices that the topology table hides for the sake of clarity.

13.9 Detecting loops

Loops in the network cause connection interruptions or data losses. This also applies to temporary loops. The automatic detection and reporting of this situation allows you to detect it faster and diagnose it more easily.

An incorrect configuration causes loops, for example, if you deactivate Spanning Tree.

The device allows you to detect the effects typically caused by loops and report this situation automatically to the network management station. You have the option here to specify the magnitude of the loop effects that trigger the device to send a report.

BPDU frames sent from the designated port and received on either a different port of the same device or the same port within a short time, is a typical effect of a loop.

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

13.10 Reports

The following lists reports and buttons available for diagnostics:

► System Log file
The log file is an HTML file in which the device writes important device-internal events.

► Audit Trail
Logs successful CLI commands and user comments. The file also includes SNMP logging.

► Persistent Logging
The device saves log entries in a file in the external memory, when present. These files are available after power down. The maximum size, maximum number of retainable files and the severity of logged events are configurable. After obtaining the user-defined maximum size or maximum number of retainable files, the device archives the entries and starts a new file. The device deletes the oldest file and renames the other files to maintain the configured number of files. To review these files use the CLI or copy them to an external server for future reference.

► Download Support Information
This button allows you to download system information as files in a ZIP archive.

In service situations, these reports provide the technician with the necessary information.

13.10.1 Global settings

Using this dialog you enable or disable where the device sends reports, for example, to a Console, a Syslog Server, or a CLI connection. You also set at which severity level the device writes events into the reports.

Perform the following steps:

☐ Open the *Diagnostics > Report > Report Global* dialog.
☐ To send a report to the console, specify the desired level in the *Console logging* frame, *Severity* field.
☐ To enable the function, select the `On` radio button in the *Console logging* frame.

☐ To save the changes temporarily, click the ✔️ button.

The device buffers logged events in 2 separate storage areas so that the device keeps log entries for urgent events. Specify the minimum severity for events that the device logs to the buffered storage area with a higher priority.

Perform the following steps:

☐ To send events to the buffer, specify the desired level in the *Buffered logging* frame, *Severity* field.

☐ To save the changes temporarily, click the ✔️ button.

When you activate the logging of SNMP requests, the device logs the requests as events in the Syslog. The *Log SNMP get request* function logs user requests for device configuration information. The *Log SNMP set request* function logs device configuration events. Specify the minimum level for events that the device logs in the Syslog.

Perform the following steps:

☐ Enable the *Log SNMP get request* function for the device in order to send SNMP Read requests as events to the Syslog server.
To enable the function, select the `On` radio button in the *SNMP logging* frame.
☐ Enable the *Log SNMP set request* function for the device in order to send SNMP Write requests as events to the Syslog server.
To enable the function, select the `On` radio button in the *SNMP logging* frame.
☐ Choose the desired severity level for the get and set requests.

☐ To save the changes temporarily, click the ✔️ button.

When active, the device logs configuration changes made using the CLI commands, to the audit trail. This feature is based on the IEEE 1686 standard for Substation Intelligent Electronic Devices.

Perform the following steps:

☐ Open the *Diagnostics > Report > Report Global* dialog.

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

☐ To save the changes temporarily, click the ✓ button.

The device allows you to save the following system information data in one ZIP file on your PC:

▶ `audittrail.html`
▶ `CLICommands.txt`
▶ `defaultconfig.xml`
▶ `script`
▶ `runningconfig.xml`
▶ `supportinfo.html`
▶ `systeminfo.html`
▶ `systemlog.html`

The device creates the file name of the ZIP archive automatically in the format `<IP_address>_<system_name>.zip`.

Perform the following steps:

☐ Click the ☰ button and then the *Download support information* item.

☐ Select the directory in which you want to save the support information.

☐ To save the changes temporarily, click the ✓ button.

13.10.2 Syslog

The device enables you to send messages about important device internal events to one or more Syslog servers (up to 8). Additionally, you also include SNMP requests to the device as events in the Syslog.

Note: To display the logged events, open the *Diagnostics > Report > Audit Trail* dialog or the *Diagnostics > Report > System Log* dialog.

Perform the following steps:

☐ Open the *Diagnostics > Syslog* dialog.

☐ To add a table entry, click the ⊞ button.

☐ In the *IP address* column, enter the IP address of the Syslog server.

☐ In the *Destination UDP port* column, specify the UDP port on which the Syslog server expects the log entries.

☐ In the *Min. severity* column, specify the minimum severity level that an event requires for the device to send a log entry to this Syslog server.

☐ Mark the checkbox in the *Active* column.

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

☐ To save the changes temporarily, click the ✓ button.

In the *SNMP logging* frame, configure the following settings for read and write SNMP requests:

Perform the following steps:

☐ Open the *Diagnostics > Report > Report Global* dialog.

☐ Enable the *Log SNMP get request* function for the device in order to send SNMP Read requests as events to the Syslog server.
To enable the function, select the `On` radio button in the *SNMP logging* frame.

☐ Enable the *Log SNMP set request* function for the device in order to send SNMP Write requests as events to the Syslog server.
To enable the function, select the `On` radio button in the *SNMP logging* frame.

□ Choose the desired severity level for the get and set requests.

□ To save the changes temporarily, click the ✅ button.

```
enable                              Change to the Privileged EXEC mode.
configure                           Change to the Configuration mode.
logging host add 1 addr  10.0.1.159  Adds a new recipient in the Syslog servers list. The value 3
severity 3                          specifies the severity level of the event that the device logs. The
                                    value 3 means Error.
logging syslog operation            Enable the Syslog function.
exit                                Change to the Privileged EXEC mode.
show logging host                   Display the Syslog host settings.

No.    Server IP      Port   Max. Severity   Type        Status
-----  -------------- -----  --------------  ----------  -------
1      10.0.1.159     514    error           systemlog   active

configure                           Change to the Configuration mode.
logging snmp-requests get   operation    Logs SNMP GET requests.
logging snmp-requests get   severity 5   The value 5 specifies the severity level of the event that the device
                                         logs in case of SNMP GET requests. The value 5 means Notice.
logging snmp-requests set   operation    Logs SNMP SET requests.
logging snmp-requests set   severity 5   The value 5 specifies the severity level of the event that the device
                                         logs in case of SNMP SET requests. The value 5 means Notice.
exit                                Change to the Privileged EXEC mode.
show logging snmp                   Display the SNMP logging settings.

Log SNMP GET requests              : enabled
Log SNMP GET severity              : notice
Log SNMP SET requests              : enabled
Log SNMP SET severity              : notice
```

13.10.3 System Log

The device allows you to call up a log file of the system events. The table in the `Diagnostics > Report > System Log` dialog lists the logged events.

Perform the following steps:

□ To update the content of the log, click "Reload".
□ To search the content of the log for a key word, click "Search".
□ To archive the content of the log as an html file, click "Save".

Note: You have the option to also send the logged events to one or more Syslog servers.

13.10.4 Audit Trail

The `Diagnostics > Report > Audit Trail` dialog contains system information and changes to the device configuration performed through CLI and SNMP. In the case of device configuration changes, the dialog displays Who changed What and When. To log changes to the device configuration, use in the `Diagnostics > Report > Audit Trail` dialog the functions `Log SNMP get request` and `Log SNMP set request`.

The `Diagnostics > Syslog` dialog allows you to configure up to 8 Syslog servers to which the device sends Audit Trails.

The following list contains log events:
▶ changes to configuration parameters
▶ CLI commands (except `show` commands)
▶ CLI command `logging audit-trail <string>` which logs the comment
▶ Automatic changes to the System Time
▶ watchdog events
▶ locking a user after several unsuccessful login attempts
▶ User login, either locally or remote, using CLI
▶ Manual, user-initiated, logout
▶ Timed logout after a user-defined period of CLI inactivity

▶ file transfer operation including a Firmware Update
▶ Configuration changes using HiDiscovery
▶ Automatic configuration or firmware updates using the external memory
▶ Blocked management access due to invalid login
▶ rebooting
▶ opening and closing SNMP over HTTPS tunnels
▶ Detected power failures

▶ file transfer operation including a Firmware Update

13.11 Network analysis with TCPdump

Tcpdump is a packet-sniffing UNIX utility used by network administrators to sniff and analyze traffic on a network. A couple of reasons for sniffing traffic on a network is to verify connectivity between hosts, or to analyze the traffic traversing the network.

TCPDump on the device provides the possibility to decode or capture packets received and transmitted by the Management CPU. This function is available using the `debug` CLI command. Refer to the "Command Line Interface" reference manual for further information about the TCPDump function.

13.12 Monitoring the data traffic

The device allows you to forward data packets that pass through the device to a destination port. There you can monitor and evaluate the data packets.

The device provides you with the following options:
▶ Port Mirroring

13.12.1 Port Mirroring

The *Port Mirroring* function allows you to copy data packets from physical source ports to a physical destination port.

You monitor the data traffic on the source ports in the sending and receiving directions with a management tool connected on the destination port, for example an RMON probe. The function has no affect on the data traffic running on the source ports.
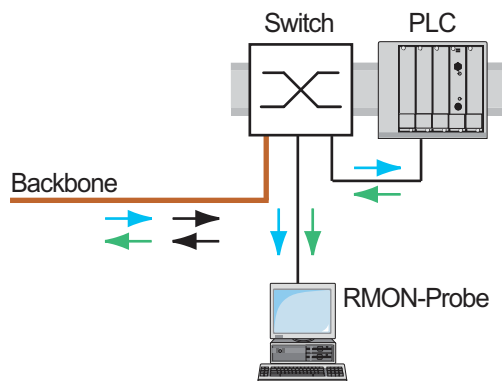
Figure 45: Example

On the destination port, the device exclusively sends the data packets copied from the source ports.

Before you switch on the *Port Mirroring* function, mark the checkbox *Allow management* to access the management functions via the destination port. The device allows access to the management functions via the destination port without interrupting the active *Port Mirroring* session.

Note: The device duplicates multicasts, broadcasts and unknown unicasts on the destination port.
The VLAN settings on the destination port remain unchanged. Prerequisite for management access at the destination port is that the destination port is a member of the management VLAN.

■ Enabling the Port Mirroring function

Perform the following steps:

☐ Open the *Diagnostics > Ports > Port Mirroring* dialog.
☐ Specify the source ports.
  Mark the checkbox in the *Enabled* column for the relevant ports.
☐ Specify the destination port.
  In the *Destination port* frame, select the desired port in the *Primary port* drop-down list.
  The drop-down list only displays available ports. Ports that are already specified as source ports are unavailable.
☐ If needed, specify a second destination port.
  In the *Destination port* frame, select the desired port in the *Secondary port* drop-down list.
  The prerequisite is that you have already specified the primary destination port.
☐ In order to access the management functions of the device via the destination port:
  In the *Destination port* frame, mark the *Allow management* checkbox.

☐ To save the changes temporarily, click the ✓ button.

To deactivate the *Port Mirroring* function and restore the default settings, click the ☰ button and then the *Reset config* item.

13.13 Self-test

The device checks its assets during the boot process and occasionally thereafter. The device checks system task availability or termination and the available amount of memory. Furthermore, the device checks for application functionality and if there is any hardware degradation in the chip set.

When the device detects a loss in integrity, the device responds to the degradation with a user-defined action. The following categories are available for configuration.
▶ `task`
  Action to be taken when a task is unsuccessful.
▶ `resource`
  Action to be taken due to the lack of resources.
▶ `software`
  Action taken for loss of software integrity; for example, code segment checksum or access violations.
▶ `hardware`
  Action taken due to hardware degradation

Configure each category to produce an action when the device detects a loss in integrity. The following actions are available for configuration.
▶ `log only`
  This action writes a message to the logging file.
▶ `send trap`
  Sends an SNMP trap to the trap destination.
▶ `reboot`
  An error in the category, when activated, will cause the device to reboot

Perform the following steps:

☐ Open the *Diagnostics > System > Selftest* dialog.
☐ In the *Action* column, specify the action to perform for a cause.

☐ To save the changes temporarily, click the ✓ button.

`enable`	Change to the Privileged EXEC mode.
`configure`	Change to the Configuration mode.
`selftest action task log-only`	To send a message to the event log when a task is unsuccessful.
`selftest action resource send-trap`	Sending an SNMP trap if there are insufficient resources.
`selftest action software send-trap`	Sending an SNMP trap if the software integrity has been lost.
`selftest action hardware reboot`	To reboot the device when hardware degradation occurs.

Disabling these functions lets you decrease the time required to restart the device after a cold start. You find these options in the *Diagnostics > System > Selftest* dialog, *Configuration* frame.
▶ *RAM test*
  Activates/deactivates the RAM test function during a cold start.
▶ *SysMon1 is available*
  Activates/deactivates the System Monitor function during a cold start.
▶ *Load default config on error*
  Activates/deactivates the loading of the default device configuration if no readable configuration is available during a restart.

Note: The following settings block your access to the device permanently if the device does not detect any readable configuration profile when it is restarting. This is the case, for example, if the password of the configuration profile that you are loading differs from the password set in the device.
▶ The *SysMon1 is available* checkbox is unmarked.
▶ The *Load default config on error* checkbox is unmarked.
To have the device unlocked again, contact your sales partner.

`selftest ramtest`	Enable RAM selftest on cold start.
`no selftest ramtest`	Disable the "ramtest" function.
`selftest system-monitor`	Enable the "SysMon1" function.
`no selftest system-monitor`	Disable the "SysMon1" function.

| `show selftest action` | Show status of the actions to be taken in the event of device degradation. |
| `show selftest settings` | Display the settings for "ramtest" and "SysMon" settings in event of a cold start. |

13.14 Copper cable test

Use this feature to test copper cables attached to an interface for a short or open circuit. The test interrupts traffic flow, when in progress, on this port.

The table displays the state and lengths of each individual pair. The device returns a result with the following meaning:

▶ normal - indicates that the cable is operating properly
▶ open - indicates an interruption in the cable
▶ short circuit - indicates a short circuit in the cable
▶ untested - indicates an untested cable
▶ Unknown - cable unplugged

14 Advanced functions of the device

14.1 DHCP L2 Relay

A network administrator uses the DHCP Layer 2 Relay agent to add DHCP client information. This information is required by Layer 3 Relay agents and DHCP servers to assign an address and configuration to a client.

When a DHCP client and server are in the same IP subnet, they exchange IP address requests and replies directly. However, having a DHCP server on each subnet is expensive and often impractical. An alternative to having a DHCP server in every subnet is to use the network devices to relay packets between a DHCP client and a DHCP server located in a different subnet.

A Layer 3 Relay agent is generally a router that has IP interfaces in both the client and server subnets and routes traffic between them. However, in Layer 2 switched networks, there are one or more network devices, switches for example, between the client and the Layer 3 Relay agent or DHCP server. In this case, this device provides a Layer 2 Relay agent to add the information that the Layer 3 Relay agent and DHCP server require to perform their roles in address and configuration assignment.

The following list contains the default settings for this function:
- ▶ Global setting:
  - Active setting: disable
- ▶ Interface settings:
  - Active setting: disable
  - Trusted Port: disable
- ▶ VLAN settings:
  - Active setting: disable
  - Circuit ID: enable
  - Remote ID Type: mac
  - Remote ID: blank

14.1.1 Circuit and Remote IDs

Before forwarding the request of a client to the DHCP server, the device adds the Circuit ID and the Remote ID to the Option 82 field of the DHCP request packet.

- ▶ The Circuit ID stores on which port the device received the request of the client.

- ▶ The remote ID contains the MAC address, the IP address, the system name, or a user-defined character string. Using it, the participating devices identify the relay agent that received the request of the client.

The device and other relay agents use this information to re-direct the answer from the DHCP relay agent to the original client. The DHCP server is able to analyze this data for example to assign the client an IP address from a specific address pool.

Also, the replay packet of the DHCP server contains the Circuit-ID and the Remote ID. Before forwarding the answer to the client, the device removes the information from the Option 82 field.

14.1.2 DHCP L2 Relay configuration

The *Advanced > DHCP L2 Relay > Configuration* dialog allows you to activate the function on the active ports and on the VLANs.

The device forwards DHCP packets with Option 82 information on those ports for which the checkbox in the *DHCP L2 Relay* column and in the *Trusted port* column is marked. Typically, these are ports in the network of the DHCP server.

The ports to which the DHCP clients are connected, you activate the *DHCP L2 Relay* function, but leave the *Trusted port* checkbox unmarked. On these ports, the device discards DHCP packets with Option 82 information.
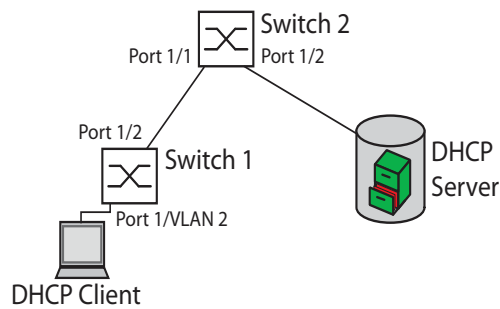
Figure 46: DHCP Layer 2 Example Network

Perform the following steps on Switch 1:

☐ Open the ***Advanced > DHCP L2 Relay > Configuration*** dialog, ***Interface*** tab.
☐ For port `1/1`, specify the settings as follows:
– Mark the checkbox in the ***Active*** column.
☐ For port `1/2`, specify the settings as follows:
– Mark the checkbox in the ***Active*** column.
– Mark the checkbox in the ***Trusted port*** column.
☐ Open the ***Advanced > DHCP L2 Relay > Configuration*** dialog, ***VLAN*** tab.
☐ Specify the settings for VLAN 2 as follows:
– Mark the checkbox in the ***Active*** column.
– Mark the checkbox in the ***Circuit ID*** column.
– To use the IP address of the device as the Remote ID, in the ***Remote ID type*** column, specify the value `ip`.
☐ To enable the function, select the `On` radio button in the ***Operation*** frame.

☐ To save the changes temporarily, click the ✓ button.

Perform the following steps on Switch 2:

☐ Open the ***Advanced > DHCP L2 Relay > Configuration*** dialog, ***Interface*** tab.
☐ For port `1/1` and `1/2`, specify the settings as follows:
– Mark the checkbox in the ***Active*** column.
– Mark the checkbox in the ***Trusted port*** column.
☐ To enable the function, select the `On` radio button in the ***Operation*** frame.

☐ To save the changes temporarily, click the ✓ button.

Verify that VLAN 2 is present then perform the following steps on Switch 1:

☐ Configure VLAN 2, and specify port `1/1` as a member of VLAN 2.

`enable`	Change to the Privileged EXEC mode.
`vlan database`	Change to the VLAN configuration mode.
`dhcp-l2relay circuit-id 2`	Activate the Circuit ID and the DHCP Option 82 on VLAN `2`.
`dhcp-l2relay remote-id ip 2`	Specify the IP address of the device as the Remote ID on VLAN `2`.
`dhcp-l2relay mode 2`	Activate the ***DHCP L2 Relay*** function on VLAN `2`.
`exit`	Change to the Privileged EXEC mode.
`configure`	Change to the Configuration mode.
`interface 1/1`	Change to the interface configuration mode of interface `1/1`.
`dhcp-l2relay mode`	Activate the ***DHCP L2 Relay*** function on the port.
`exit`	Change to the Configuration mode.
`interface 1/2`	Change to the interface configuration mode of interface `1/2`.
`dhcp-l2relay trust`	Specify the port as ***Trusted port***.
`dhcp-l2relay mode`	Activate the ***DHCP L2 Relay*** function on the port.

`exit`	Change to the Configuration mode.
`dhcp-l2relay mode`	Enable the *DHCP L2 Relay* function on the device.

Perform the following steps on Switch 2:

`enable`	Change to the Privileged EXEC mode.
`configure`	Change to the Configuration mode.
`interface 1/1`	Change to the interface configuration mode of interface `1/1`.
`dhcp-l2relay trust`	Specify the port as *Trusted port*.
`dhcp-l2relay mode`	Activate the *DHCP L2 Relay* function on the port.
`exit`	Change to the Configuration mode.
`interface 1/2`	Change to the interface configuration mode of interface `1/2`.
`dhcp-l2relay trust`	Specify the port as *Trusted port*.
`dhcp-l2relay mode`	Activate the *DHCP L2 Relay* function on the port.
`exit`	Change to the Configuration mode.
`dhcp-l2relay mode`	Enable the *DHCP L2 Relay* function on the device.

14.2   MRP-IEEE

The IEEE 802.1ak amendment to the IEEE 802.1Q standard introduced the Multiple Registration Protocol (MRP) to replace the Generic Attribute Registration Protocol (*GARP*). The IEEE also modified and replaced the *GARP* applications, *GARP* Multicast Registration Protocol (*GMRP*) and *GARP* VLAN Registration Protocol (*GVRP*), with the Multiple MAC Registration Protocol (*MMRP*) and the Multiple VLAN Registration Protocol (*MVRP*).

To confine traffic to the required areas of a network, the MRP applications distribute attribute values to MRP enabled devices across a LAN. The MRP applications register and de-register Multicast group memberships and VLAN identifiers.

Note: The Multiple Registration Protocol (MRP) requires a loop free network. To help prevent loops in your network, use a network protocol such as the Media Redundancy Protocol, Spanning Tree Protocol, or Rapid Spanning Tree Protocol with MRP.

14.2.1   MRP operation

Each participant contains an applicant component and an MRP Attribute Declaration (MAD) component. The applicant component is responsible for forming the attribute values and their registration and de-registration. The MAD component generates MRP messages for transmission and processes messages received from other participants. The MAD component encodes and transmits the attributes to other participants in MRP Data Units (MRPDU). In the switch, an MRP Attribute Propagation (MAP) component distributes the attributes to participating ports.

A participant exists for each MRP application and each LAN port. For example, a participant application exists on an end device and another application exists on a switch port. The Applicant state machine records the attribute and port for each MRP participant declaration on an end device or switch. Applicant state machine variable changes trigger the transmission of MRPDUs to communicate the declaration or withdrawal.

To establish an *MMRP* instance, an end device first sends a Join empty (JoinMt) message with the appropriate attributes. The switch then floods the JoinMt to the participating ports and to the neighboring switches. The neighboring switches flood the message to their participating port, and so on, establishing a path for the group traffic.

14.2.2   MRP timers

The default timer settings help prevent unnecessary attribute declarations and withdraws. The timer settings allow the participants to receive and process MRP messages before the Leave or LeaveAll timers expire.

Maintain the following relationships when you reconfigure the timers:
▶ To allow for re-registration after a Leave or LeaveAll event, even if there is a lost message, set the value of the LeaveTime as follows: ≥ (2x JoinTime) + 60 in 1/100 s
▶ To minimize the volume of rejoining traffic generated following a LeaveAll, specify the value for the LeaveAll timer larger than the LeaveTime.

The following list contains various MRP events that the device transmits:
▶ Join - Controls the interval for the next Join message transmission
▶ Leave - Controls the length of time that a switch waits in the Leave state before changing to the withdraw state
▶ LeaveAll - Controls the frequency with which the switch generates LeaveAll messages

The Periodic timer, when expired, initiates a Join request MRP message that the switch sends to participants on the LAN. The switches use this message to help prevent unnecessary withdraws.

14.2.3 MMRP

When a device receives Broadcast, Multicast or unknown traffic on a port, the device floods the traffic to the other ports. This process causes unnecessary use of bandwidth on the LAN.

The Multiple MAC Registration Protocol (*MMRP*) allows you to control the traffic flooding by distributing an attribute declaration to participants on a LAN. The attribute values that the MAD component encodes and transmits on the LAN in MRP messages are Group service requirement information and 48-bit MAC addresses.

The switch stores the attributes in a filtering database as MAC address registration entries. The forwarding process uses the filtering database entries solely to transmit dat through those ports necessary to reach Group member LANs.

Switches facilitate the group distribution mechanisms based on the Open Host Group concept, receiving packets on the active ports and forward exclusively on ports with group members. This way, any *MMRP* participants requiring packets transmitted to a particular group or groups, requests membership in the group. MAC service users send packets to a particular group from anywhere on the LAN. A group receives these packets on the LANs attached to registered *MMRP* participants. *MMRP* and the MAC Address Registration Entries thus restrict the packets to required segments of a loop-free LAN.

In order to maintain the registration and deregistration state and to receive traffic, a port declares interest periodically. Every device on a LAN with the *MMRP* function enabled maintains a filtering database and forwards traffic having the group MAC addresses to listed participants.

■ MMRP example

In this example, Host A intends to listen to traffic destined to group G1. Switch A processes the *MMRP* Join request received from host A and sends the request to both of the neighboring switches. The devices on the LAN now recognize that there is a host interested in receiving traffic destined for group G1. When Host B starts transmitting data destined for group G1, the data flows on the path of registrations and Host A receives it.
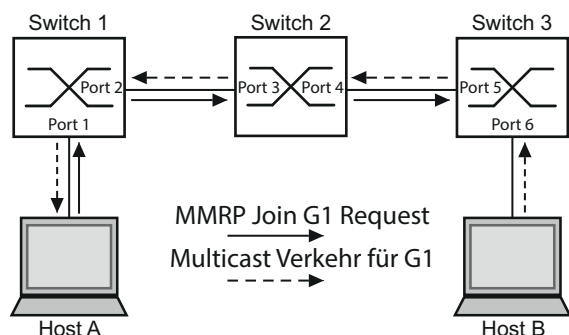
Figure 47: MMRP Network for MAC address Registration

To enable the *MMRP* function on the switches, proceed as follows.

Perform the following steps:

- ☐ Open the *Switching > MRP-IEEE > MMRP* dialog, *Configuration* tab.
- ☐ To activate port 1 and port 2 as *MMRP* participants, mark the checkbox in the *MMRP* column for port 1 and port 2 on switch 1.
- ☐ To activate port 3 and port 4 as *MMRP* participants, mark the checkbox in the *MMRP* column for port 3 and port 4 on switch 2.
- ☐ To activate port 5 and port 6 as *MMRP* participants, mark the checkbox in the *MMRP* column for port 5 and port 6 on switch 3.
- ☐ To send periodic events allowing the device to maintain the registration of the MAC address group, enable the *Periodic state machine*. Select the On radio button in the *Configuration* frame.

- ☐ To save the changes temporarily, click the ✓ button.

To enable the *MMRP* ports on switch 1, use the following CLI commands. Substituting the appropriate interfaces in the CLI commands, enable the *MMRP* functions and ports on switches 2 and 3.

```
enable                                Change to the Privileged EXEC mode.
configure                             Change to the Configuration mode.
interface 1/1                         Change to the interface configuration mode of interface 1/1.
mrp-ieee mmrp operation               Enabling the MMRP function on the port.
interface 1/2                         Change to the interface configuration mode of interface 1/2.
mrp-ieee mmrp operation               Enabling the MMRP function on the port.
exit                                  Change to the Configuration mode.
mrp-ieee mrp periodic-state-machine   Enabling the Periodic state machine function globally.
mrp-ieee mmrp operation               Enabling the MMRP function globally.
```

14.2.4 MVRP

The Multiple VLAN Registration Protocol (*MVRP*) is an MRP application that provides dynamic VLAN registration and withdraw services on a LAN.

The *MVRP* function provides a maintenance mechanism for the Dynamic VLAN Registration Entries, and for transmitting the information to other devices. This information allows *MVRP*-aware devices to establish and update their VLAN membership information. When members are present on a VLAN, the information indicates through which ports the switch forwards traffic to reach those members.

The main purpose of the *MVRP* function is to allow switches to discover some of the VLAN information that you otherwise manually set up. Discovering this information allows switches to overcome the limitations of bandwidth consumption and convergence time in large VLAN networks.

■ MVRP example

Set up a network comprised of MVRP aware switches (1 - 4) connected in a ring topology with end device groups, A1, A2, B1, and B2 in 2 different VLANs, A and B. With STP enabled on the switches, the ports connecting switch 1 to switch 4 are in the discarding state, helping prevent a loop condition.
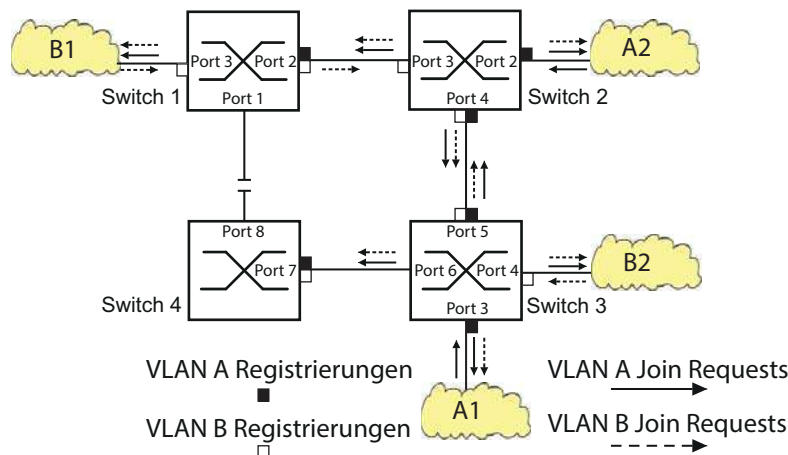
Figure 48: MVRP Example Network for VLAN Registration

In the MVRP example network, the LANs first send a Join request to the switches. The switch enters the VLAN registration in the forwarding database for the port receiving the frames.

The switch then propagates the request to the other ports, and sends the request to the neighboring LANs and switches. This process continues until the switches have registered the VLANs in the forwarding database of the receive port.

To enable MVRP on the switches, use the following steps.

- ☐ Open the *Switching > MRP-IEEE > MVRP* dialog, *Configuration* tab.
- ☐ To activate the ports 1 through 3 as *MVRP* participants, mark the checkbox in the *MVRP* column for the ports 1 through 3 on switch 1.

□ To activate the ports 2 through 4 as *MVRP* participants, mark the checkbox in the *MVRP* column for the ports 2 through 4 on switch 2.

□ To activate the ports 3 through 6 as *MVRP* participants, mark the checkbox in the *MVRP* column for the ports 3 through 6 on switch 3.

□ To activate port 7 and port 8 as *MVRP* participants, mark the checkbox in the *MVRP* column for port 7 and port 8 on switch 4.

□ To maintain the registration of the VLANs, enable the *Periodic state machine*.
Select the On radio button in the *Configuration* frame.

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

□ To save the changes temporarily, click the ✅ button.

To enable the *MVRP* ports on switch 1, use the following CLI commands. Substituting the appropriate interfaces in the CLI commands, enable the *MVRP* functions and ports on switches 2, 3 and 4.

`enable`	Change to the Privileged EXEC mode.
`configure`	Change to the Configuration mode.
`interface 1/1`	Change to the interface configuration mode of interface 1/1.
`mrp-ieee mvrp operation`	Enabling the *MVRP* function on the port.
`interface 1/2`	Change to the interface configuration mode of interface 1/2.
`mrp-ieee mvrp operation`	Enabling the *MVRP* function on the port.
`exit`	Change to the Configuration mode.
`mrp-ieee mvrp periodic-state-machine`	Enabling the *Periodic state machine* function globally.
`mrp-ieee mvrp operation`	Enabling the *MVRP* function globally.

14.3 CLI client

The device supports an CLI client that directly opens a connection to the SSH server using the TCP Port specified in the *Device Security > Management Access > Server* dialog, *SSH* tab. The CLI client allows you to configure the device using CLI commands.

The prerequisite to using the CLI client is that you enable the function in the *Device Security > Management Access > Server* dialog, *SSH* tab.

For detailed information on CLI commands, review the "Command Line Interface" reference manual.

15 Industry Protocols

For a long time, automation communication and office communication were on different paths. The requirements and the communication properties were too different.

Office communication moves large quantities of data with low demands with respect to the transfer time. Automation communication moves small quantities of data with high demands with respect to the transfer time and availability.

While the transmission devices in the office are usually kept in temperature-controlled, relatively clean rooms, the transmission devices used in automation are exposed to wider temperature ranges. Dirty, dusty and damp ambient conditions make additional demands on the quality of the transmission devices.

With the continued development of communication technology, the demands and the communication properties have moved closer together. The high bandwidths now available in Ethernet technology and the protocols they support enable large quantities to be transferred and exact transfer times to be specified.

With the creation of the first optical LAN to be active worldwide, at the University of Stuttgart in 1984, Hirschmann laid the foundation for industry-compatible office communication devices. Thanks to Hirschmann's initiative with the world's first rail hub in the 1990s, Ethernet transmission devices such as switches, routers and firewalls are now available for the toughest automation conditions.

The desire for uniform, continuous communication structures encouraged many manufacturers of automation devices to come together and use standards to aid the progress of communication technology in the automation sector. This is why we now have protocols that enable us to communicate via Ethernet from the office right down to the field level.
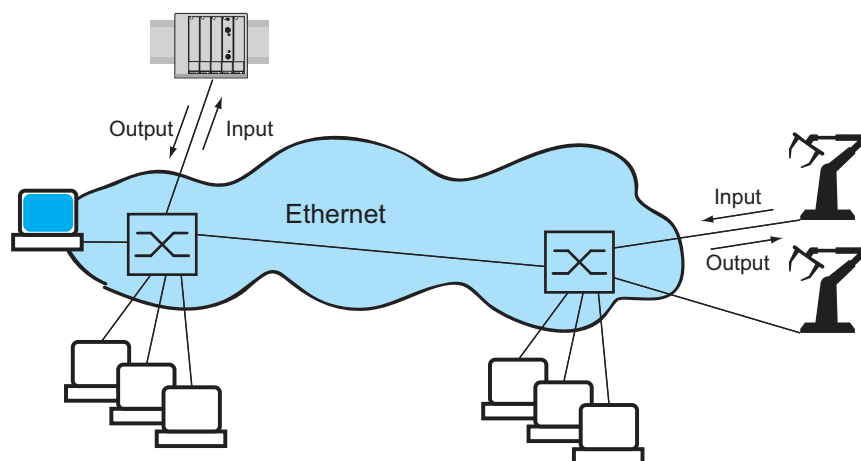
Figure 49: Example of communication.

15.1 IEC 61850/MMS

IEC 61850/MMS is an industrial communication protocol standardized by the International Electrotechnical Commission (IEC). The protocol is to be found in substation automation, for example in the control technology of energy suppliers.

This protocol, which works in a packet-oriented way, is based on the TCP/IP transport protocol and uses the Manufacturing Messaging Specification (MMS) for the client-server communication. The protocol is object-oriented and defines a standardized configuration language that comprises, among other things, functions for SCADA, Intelligent Electronic Devices (IED) and for the network control technology.

Part 6 of the IEC 61850 standard defines the configuration language SCL (Substation Configuration Language). SCL describes the properties of the device and the system structure in an automatically processable form. The properties of the device described with SCL are stored in the ICD file on the device.

15.1.1 Switch model for IEC 61850

The Technical Report, IEC 61850 90-4, specifies a bridge model. The bridge model represents the functions of a switch as objects of an Intelligent Electronic Device (IED). An MMS client (for example the control room software) uses these objects to monitor and configure the device.
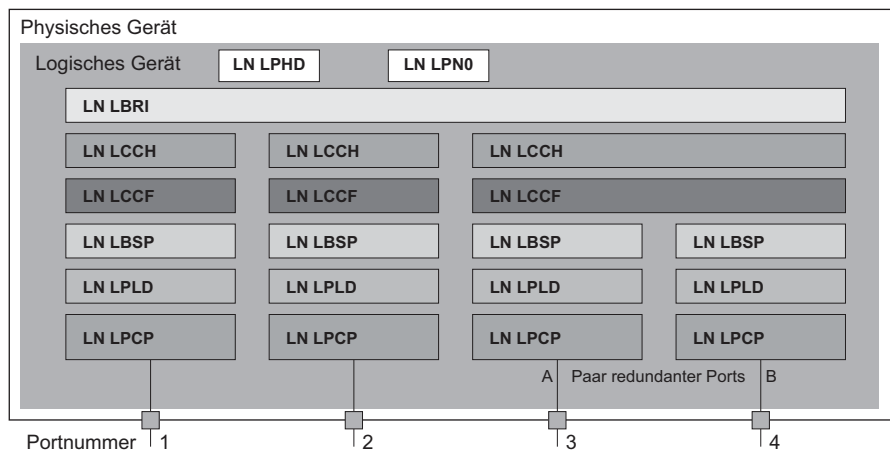
Figure 50: Bridge model based on Technical Report IEC 61850 90-4

Class	Description
LN LLN0	`Zero` logical node of the `Bridge` IED: Defines the logical properties of the device.
LN LPHD	`Physical Device` logical node of the `Bridge` IED: Defines the physical properties of the device.
LN LBRI	`Bridge` logical node: Represents general settings of the bridge functions of the device.
LN LCCH	`Communication Channel` logical node: Defines the logical `Communication Channel` that consists of one or more physical device ports.
LN LCCF	`Channel Communication Filtering` logical node: Defines the VLAN and Multicast settings for the higher-level `Communication Channel`.
LN LBSP	`Port Spanning Tree Protocol` logical node: Defines the Spanning Tree statuses and settings for the respective physical device port.
LN LPLD	`Port Layer Discovery` logical node: Defines the LLDP statuses and settings for the respective physical device port.
LN LPCP	`Physical Communication Port` logical node: Represents the respective physical device port.

Table 36: Classes of the bridge model based on TR IEC61850 90-4

15.1.2 Integration into a Control System

■ **Preparation of the device**

☐ Check that the device has an IP address assigned.

☐ Open the *Advanced > Industrial Protocols > IEC61850-MMS* dialog.

☐ To start the MMS server, select in the *Operation* frame the `On` radio button, and click ✅ button.

Afterwards, an MMS client is able to connect to the device and to read and monitor the objects defined in the bridge model.

NOTICE
RISK OF UNAUTHORIZED ACCESS TO THE DEVICE
IEC61850/MMS does not provide any authentication mechanisms. If the write access for IEC61850/MMS is activated, every client that can access the device using TCP/IP is capable of changing the settings of the device. This in turn can result in an incorrect configuration of the device and to failures in the network.   Only activate the write access if you have taken additional measures (for example Firewall, VPN, etc.) to eliminate the risk of unauthorized access.
Failure to follow these instructions can result in equipment damage.

☐ To allow the MMS client to change the settings, mark the *Write access* checkbox, and click the ✅ button.

■ **Offline configuration**

The device allows you to download the ICD file using the graphical user interface. This file contains the properties of the device described with SCL and enables you to configure the substation without directly connecting to the device.

☐ Open the *Advanced > Industrial Protocols > IEC61850-MMS* dialog.

☐ To load the ICD file to your PC, click the ▤ button and then the *Download* item.

■ **Monitoring the device**

The IEC 61850/MMS server integrated into the device allows you to monitor multiple statuses of the device by means of the Report Control Block (RCB). Up to 5 MMS clients can register for a Report Control Block at the same time.

The device allows the following statuses to be monitored:

Class	RCB object	Description
LN LPHD	TmpAlm	Changes when the temperature measured in the device exceeds or falls below the set temperature thresholds.
	PhyHealth	Changes when the status of the LPHD.TmpAlm RCB object changes.
LN LPHD	TmpAlm	Changes when the temperature measured in the device exceeds or falls below the set temperature thresholds.
	PhyHealth	Changes when the status of the LPHD.PwrSupAlm or LPHD.TmpAlm RCB object changes.
LN LBRI	RstpRoot	Changes when the device takes over or relinquishes the role of the root bridge.
	RstpTopoCnt	Changes when the topology changes due to a change of the root bridge.
LN LCCH	ChLiv	Changes when the link status of the physical port changes.
LN LPCP	PhyHealth	Changes when the link status of the physical port changes.

Table 37: Statuses of the device that can be monitored with IEC 61850/MMS

15.2 Modbus TCP

Modbus TCP is an application layer messaging protocol providing client/server communication between the client and devices connected in Ethernet TCP/IP networks.

The *Modbus TCP* function allows you to install the device in networks already using *Modbus TCP* and retrieve information saved in the registers in the device.

15.2.1 Client/Server Modbus TCP/IP Mode

The device supports the client/server model of Modbus TCP/IP. This device operates as a server in this constellation and responds to requests from a client for information saved in the registers. The client / server model uses four types of messages to exchange data between the client and server:
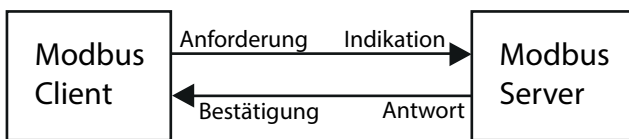
Figure 51: Client/Server Modbus TCP/IP Mode

▶ Modbus TCP/IP Request, the client creates a request for information and sends it to the server.
▶ Modbus TCP/IP Indication, the server receives a request as an indication that a client requires information.
▶ Modbus TCP/IP Response, when the required information is available, the server sends a reply containing the requested information. When the requested information is unavailable, the server sends an Exception Response to notify the client of the error detected during the processing. The Exception Response contains an exception code indicating the reason for the detected error.
▶ Modbus TCP/IP Confirmation, the client receives a response from the server, containing the requested information.

15.2.2 Supported Functions and Memory Mapping

The device supports functions with the public codes `0x03Read Holding Registers` and `0x05Write Single Coil`. The codes allow the user to read information saved in the registers such as the system information, including the system name, system location, software version, IP address, MAC address. The codes also allow the user to read the port information and port statistics. The `0x05` code allows the user to reset the port counters individually or globally.

The following list contains definitions for the values entered in the `Format` column:

▶ Bitmap: a group of 32-bits, encoded into the Big-endian byte order and saved in 2 registers. Big-endian systems save the most significant byte of a word in the smallest address and save the least significant byte in the largest address.

▶ F1: 16-bit unsigned integer

▶ F2: Enumeration - power supply alarm
  – 0 = power supply good
  – 1 = power supply failure detected

▶ F3: Enumeration - OFF/ON
  – 0 = Off
  – 1 = On

▶ F4: Enumeration - port type
  – 0 = Giga - Gigabit Interface Converter (GBIC)
  – 1 = Copper - Twisted Pair (TP)
  – 2 = Fiber - 10 Mb/s
  – 3 = Fiber - 100 Mb/s
  – 4 = Giga - 10/100/1000 Mb/s (triple speed)
  – 5 = Giga - Copper 1000 Mb/s TP
  – 6 = Giga - Small Form-factor Pluggable (SFP)

▶ F9: 32-bit unsigned long

▶ String: octets, saved in sequence, 2 octets per register.

■ Modbus TCP/IP Codes

The table below lists addresses that allow the client to reset port counters and retrieve specific information from the device registers.

■ Port Information

Address	Qty	Description	Min	Max	Step	Unit	Format
0400	1	Port 1 Type	0	6	1	–	F4
0401	1	Port 2 Type	0	6	1	–	F4
		...					
043F	1	Port 64 Type	0	6	1	–	F4
0440	1	Port 1 Link Status	0	1	1	–	F1
0441	1	Port 2 Link Status	0	1	1	–	F1
		...					
047F	1	Port 64 Link Status	0	1	1	–	F1
0480	1	Port 1 STP State	0	1	1	–	F1
0481	1	Port 2 STP State	0	1	1	–	F1
		...					
04BF	1	Port 64 STP State	0	1	1	–	F1
04C0	1	Port 1 Activity	0	1	1	–	F1
04C1	1	Port 2 Activity	0	1	1	–	F1
		...					
04FF	1	Port 64 Activity	0	1	1	–	F1
0500	1	Port 1 Counter Reset	0	1	1	–	F1
0501	1	Port 2 Counter Reset	0	1	1	–	F1
		...					
053F	1	Port 64 Counter Reset	0	1	1	–	F1

Table 38: Port Information

■ Port Statistics

Address	Qty	Description	Min	Max	Step	Unit	Format
0800	1	Port1 – Number of bytes received	0	4294967295	1	–	F9
0802	1	Port1 – Number of bytes sent	0	4294967295	1	–	F9
0804	1	Port1 – Number of frames received	0	4294967295	1	–	F9
0806	1	Port1 – Number of frames sent	0	4294967295	1	–	F9
0808	1	Port1 – Total bytes received	0	4294967295	1	–	F9
080A	1	Port1 – Total frames received	0	4294967295	1	–	F9
080C	1	Port1 – Number of broadcast frames received	0	4294967295	1	–	F9
080E	1	Port1 – Number of multicast frames received	0	4294967295	1	–	F9
0810	1	Port1 – Number of frames with CRC error	0	4294967295	1	–	F9
0812	1	Port1 – Number of oversized frames received	0	4294967295	1	–	F9
0814	1	Port1 – Number of bad fragments rcvd(<64 bytes)	0	4294967295	1	–	F9
0816	1	Port1 – Number of jabber frames received	0	4294967295	1	–	F9

Table 39: Port Statistics

Address	Qty	Description	Min	Max	Step	Unit	Format
0818	1	Port1 – Number of collisions occurred	0	4294967295	1	–	F9
081A	1	Port1 – Number of late collisions occurred	0	4294967295	1	–	F9
081C	1	Port1 – Number of 64-byte frames rcvd/sent	0	4294967295	1	–	F9
081E	1	Port1 – Number of 65-127 byte frames rcvd/sent	0	4294967295	1	–	F9
0820	1	Port1 – Number of 128-255 byte frames rcvd/sent	0	4294967295	1	–	F9
0822	1	Port1 – Number of 256-511 byte frames rcvd/sent	0	4294967295	1	–	F9
0824	1	Port1 – Number of 512-1023 byte frames rcvd/sent	0	4294967295	1	–	F9
0826	1	Port1 – Number of 1023-MAX byte frames rcvd/sent	0	4294967295	1	–	F9
0828	1	Port1 – Number of Mac Error Packets	0	4294967295	1	–	F9
082A	1	Port1 – Number of dropped received packets	0	4294967295	1	–	F9
082C	1	Port1 – Number of multicast frames sent	0	4294967295	1	–	F9
082E	1	Port1 – Number of broadcast frames sent	0	4294967295	1	–	F9
0830	1	Port1 – Number of <64 byte fragments w/ good CRC	0	4294967295	1	–	F9
		...					
147E	1	Port64 – Number of <64 byte fragments w/ good CRC	0	4294967295	1	–	F9

Table 39: Port Statistics

15.2.3 Example Configuration

In this example, you configure the device to respond to client requests. The prerequisite for this configuration is that the client device is configured with an IP address within the given range. The *Write access* function remains inactive for this example. When you activate the *Write access* function, the device allows you to reset the port counters only. In the default configuration the *Modbus TCP* and *Write access* functions are inactive.

NOTICE

RISK OF UNAUTHORIZED ACCESS TO THE DEVICE

The *Modbus TCP* protocol does not provide any authentication mechanisms. If the write access for *Modbus TCP* is activated, every client that can access the device using TCP/IP is capable of changing the settings of the device. This in turn can result in an incorrect configuration of the device and to failures in the network.
Only activate the write access if you have taken additional measures (for example Firewall, VPN, etc.) to eliminate the risk of unauthorized access.

Failure to follow these instructions can result in equipment damage.

☐ Open the *Device Security > Management Access > IP Access Restriction* dialog.

☐ To add a table entry, click the ⊞ button.

☐ Specify the IP address range, in *Index* row 2, enter 10.17.1.0/29 in the *IP address range* column.

☐ Verify that the *Modbus TCP* function is activated.

☐ To activate the range, mark the *Active* checkbox.

☐ Open the *Diagnostics > Status Configuration > Security Status > Global* dialog.

☐ Verify that the *Modbus TCP active* checkbox contains a mark.

☐ Open the *Advanced > Industrial Protocols > Modbus TCP* dialog.

☐ The standard *Modbus TCP* listening port, port 502, is the default value. However, if you wish to listen on another TCP port, enter the value for the listening port in the *TCP port* field.

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

When you enable the *Modbus TCP* function, the *Security Status* function detects the activation and displays an alarm in the *Basic Settings > System* dialog, *Security status* frame.

`enable`	Change to the Privileged EXEC mode.
`network management access add 2`	Creates the entry for the address range in the network. Number of the next available index in this example: 2.
`network management access modify 2 ip 10.17.1.0`	Specifies the IP address.
`network management access modify 2 mask 29`	Specifies the netmask.
`network management access modify 2 modbus-tcp enable`	Specifies that *Modbus TCP* is allowed to have management access.
`network management access operation`	Enables the IP access restriction.
`configure`	Change to the Configuration mode.
`security-status monitor modbus-tcp-enabled`	Specifies that the device monitors the activation of the *Modbus TCP* server.
`modbus-tcp operation`	Activates the *Modbus TCP* server.
`modbus-tcp port <1..65535>`	Specify the TCP port for *Modbus TCP* communication (optionally). The default value is port 502.
`show modbus-tcp`	Display the *Modbus TCP* Server settings.

```
Modbus TCP/IP server settings
-------------------------
Modbus TCP/IP server operation................enabled
Write-access..................................disabled
Listening port................................502
Max number of sessions........................5
Active sessions...............................0
```

`show security-status monitor`	Display the security-status settings.

```
Device Security Settings
Monitor
---------------------------------
Password default settings unchanged...........monitored
...
Write access using HiDiscovery is possible....monitored
Loading unencrypted configuration from ENVM...monitored
IEC 61850 MMS is enabled......................monitored
Modbus TCP/IP server active...................monitored
```

`show security-status event`	Display occurred security status events.

```
Time stamp           Event                    Info
-------------------  ----------------------   ------
2014-01-01 01:00:39  password-change(10)        -
......................................................
2014-01-01 01:00:39  ext-nvm-load-unsecure(21)  -
2014-01-01 23:47:40  modbus-tcp-enabled(23)     -
```

```
show network management access rules 1
Restricted management access settings
-----------------------------------
Index.......................................1
IP Address.................................10.17.1.0
Prefix Length..............................29
HTTP.......................................yes
SNMP.......................................yes
Telnet.....................................yes
SSH........................................yes
HTTPS......................................yes
IEC61850-MMS...............................yes
Modbus TCP/IP..............................yes
Active.....................................[x]
```

Display the restricted management access rules for index 1.

A Setting up the configuration environment

A.1 Setting up a DHCP/BOOTP server

The following example describes the configuration of a DHCP server using the haneWIN DHCP Server software. This shareware software is a product of IT-Consulting Dr. Herbert Hanewinkel. You can download the software from https://www.hanewin.net. You can test the software for 30 calendar days from the date of the first installation, and then decide whether you want to purchase a license.

☐ To install the DHCP servers on your PC put the product CD in the CD drive of your PC and under Additional Software select *haneWIN DHCP-Server*. To carry out the installation, follow the installation assistant.

☐ Start the *haneWIN DHCP-Server* program.

Figure 52: Start window of the haneWIN DHCP-Server *program*

Note: The installation procedure includes a service that is automatically started in the basic configuration when Windows is activated. This service is also active if the program itself has not been started. When started, the service responds to DHCP queries.

☐ Open the window for the program settings in the menu `Options > Preferences` and select the `DHCP` tab.

☐ Specify the settings displayed in the figure.

☐ Click the `OK` button.
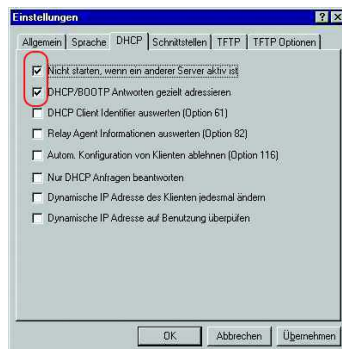
Figure 53: DHCP setting

☐ To enter the configuration profiles, select `Options > Configuration Profiles` in the menu bar.

☐ Specify the name for the new configuration profile.

☐ Click the `Add` button.
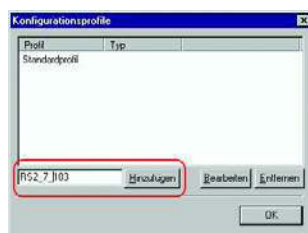
Figure 54: Adding configuration profiles

☐ Specify the netmask.

☐ Click the `Apply` button.
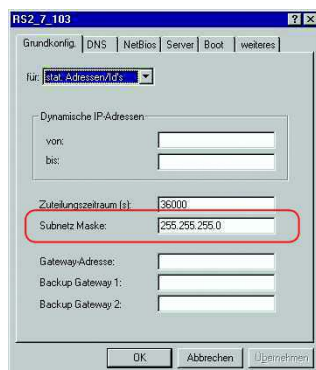
Figure 55: Netmask in the configuration profile

☐ Select the `Boot` tab.

☐ Enter the IP address of your tftp server.

☐ Enter the path and the file name for the configuration file.

☐ Click the **Apply** button and then the **OK** button.
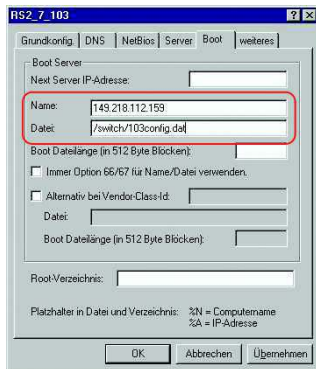
Figure 56: Configuration file on the tftp server

☐ Add a profile for each device type.
If devices of the same type have different configurations, then you add a profile for each configuration.

☐ To complete the addition of the configuration profiles, click the **OK** button.
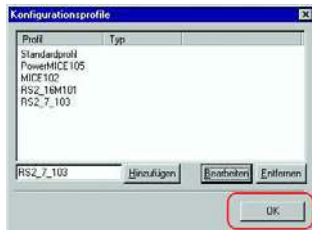
Figure 57: Managing configuration profiles

☐ To enter the static addresses, in the main window, click the **Static** button.

Figure 58: Static address input

☐ Click the **Add** button.

Figure 59: Adding static addresses

☐ Enter the MAC address of the device.

☐ Enter the IP address of the device.

☐ Select the configuration profile of the device.

☐ Click the `Apply` button and then the `OK` button.

Figure 60: Entries for static addresses

☐ Add an entry for each device that will get its parameters from the DHCP server.

Figure 61: DHCP server with entries

A.2 Setting up a DHCP server with Option 82

The following example describes the configuration of a DHCP server using the haneWIN DHCP Server software. This shareware software is a product of IT-Consulting Dr. Herbert Hanewinkel. You can download the software from https://www.hanewin.net. You can test the software for 30 calendar days from the date of the first installation, and then decide whether you want to purchase a license.

☐ To install the DHCP servers on your PC put the product CD in the CD drive of your PC and under Additional Software select *haneWIN DHCP-Server*. To carry out the installation, follow the installation assistant.

☐ Start the *haneWIN DHCP-Server* program.

Figure 62: Start window of the haneWIN DHCP-Server *program*

Note: The installation procedure includes a service that is automatically started in the basic configuration when Windows is activated. This service is also active if the program itself has not been started. When started, the service responds to DHCP queries.
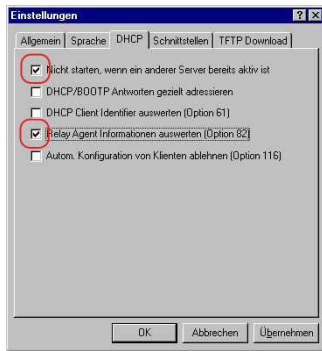
Figure 63: DHCP setting

□ To enter the static addresses, click the `Add` button.

Figure 64: Adding static addresses

□ Mark the `Circuit Identifier` checkbox.

□ Mark the `Remote Identifier` checkbox.
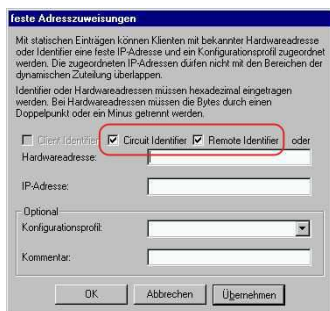
Figure 65: Default setting for the fixed address assignment

□ In the `Hardware address` field, specify the value `Circuit Identifier` and the value `Remote Identifier` for the switch and port.
The DHCP server assigns the IP address specified in the `IP address` field to the device that you connect to the port specified in the `Hardware address` field.

The hardware address is in the following form:
`ciclhhvvvvssmmpprirlxxxxxxxxxxxx`
▶ `ci`
Sub-identifier for the type of the Circuit ID
▶ `cl`
Length of the Circuit ID.
▶ `hh`
Hirschmann identifier:
`01` if a Hirschmann device is connected to the port, otherwise `00`.
▶ `vvvv`
VLAN ID of the DHCP request.
Default setting: `0001` = VLAN 1
▶ `ss`
Socket of device at which the module with that port is located to which the device is connected. Specify the value `00`.

▶ `mm`
Module with the port to which the device is connected.

▶ `pp`
Port to which the device is connected.

▶ `ri`
Sub-identifier for the type of the Remote ID

▶ `rl`
Length of the Remote ID.

▶ `xxxxxxxxxxxx`
Remote ID of the device (for example MAC address) to which a device is connected.

Figure 66: Specifying the addresses
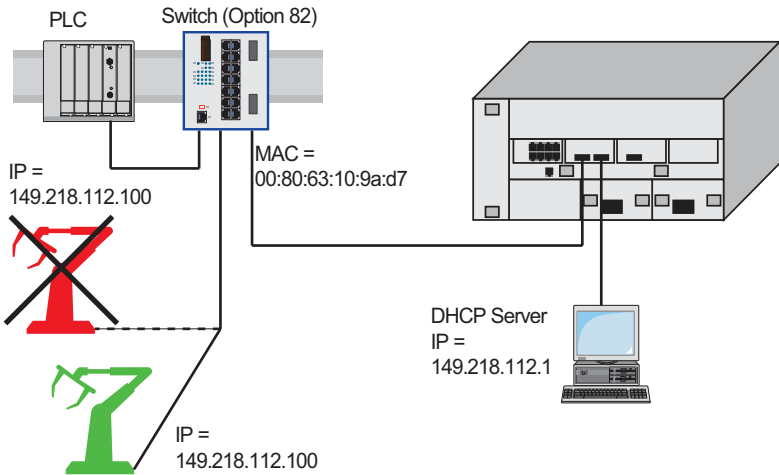
Figure 67: Application example of using Option 82

A.3 Changing the MAC address

The device allows you to change the burned in MAC Address to a user-defined MAC Address. The user-defined MAC address is:
▶ Configurable by CLI and GUI.
▶ Stored in the internal boot parameter block.
▶ Retrieved during the boot phase.

The user-defined MAC Address is configured using either the Web Interface or the CLI.

Perform the following steps:

☐ Open the *Basic Settings > Network* dialog, *MAC configuration* tab.

☐ In the *Configuration* frame, specify the user-defined MAC address in the *Local admin MAC address* field.

☐ To save the changes temporarily, click the ✓ button.

The device applies the change upon restart.

`enable`	Change to the Privileged EXEC mode.
`configure`	Change to the Configuration mode.
`network management mac <local-addr>`	Configure the loacally administered MAC address.
`show network management mac`	Display the MAC address settings of the device.

Note: Changes to the MAC address require you to reboot the device before the new address is assigned.

A.4 Specify the Management port

You can configure the device to restrict management access to one port or allow management access on every port.

Perform the following steps:

☐ Open the *Basic Settings > Network* dialog, *MAC configuration* tab.

☐ To allow accessing the management of the device through exactly one port, in the *Configuration* frame, specify the port to be used in the *Management port* field.

☐ To save the changes temporarily, click the ✓ button.

`network management port <port>`	Specifies the ports for the management access. The value `all` allows the access from any port.
`show network management port`	Displays the ports that allow management access to the device.

A.5 Preparing access via SSH

To access the device using SSH, perform the following steps:

▶ Generate a key on the device.
   or
▶ Upload your own key on the device.
▶ Prepare access to the device in the SSH client program.

Note: In the default setting, the key is already existing and access using SSH is enabled.

A.5.1 Generating a key on the device

The device allows you to generate the key directly on the device.

Perform the following steps:

☐ Open the *Device Security > Management Access > Server* dialog, *SSH* tab.
☐ Disable the SSH server.
   To disable the function, select the `Off` radio button in the *Operation* frame.

☐ To save the changes temporarily, click the ✓ button.

☐ To create a RSA key, in the *Signature* frame, click the *Create* button.
☐ Enable the SSH server.
   To enable the function, select the `On` radio button in the *Operation* frame.

☐ To save the changes temporarily, click the ✓ button.

```
enable                    Change to the Privileged EXEC mode.
configure                 Change to the Configuration mode.
ssh key rsa generate      Generate a new RSA key.
```

A.5.2 Loading your own key onto the device

OpenSSH gives experienced network administrators the option of generating an own key. To generate the key, enter the following commands on your PC:
```
ssh-keygen(.exe) –q –t rsa –f rsa.key –C '' –N ''
rsaparam –out rsaparam.pem 2048
```

The device allows yout to upload the own SSH key to the device.

Perform the following steps:

- ☐ Open the *Device Security > Management Access > Server* dialog, *SSH* tab.
- ☐ Disable the SSH server.
  To disable the function, select the `Off` radio button in the *Operation* frame.

- ☐ To save the changes temporarily, click the ✅ button.

- ☐ If the host key is located on your PC or on a network drive, drag and drop the file that contains the key in the ⬆ area. Alternatively click in the area to select the file.
- ☐ Click the *Start* button in the *Key import* frame to load the key onto the device.
- ☐ Enable the SSH server.
  To enable the function, select the `On` radio button in the *Operation* frame.

- ☐ To save the changes temporarily, click the ✅ button.

☐ Copy the self-generated key from your PC to the external memory.

☐ Copy the key from the external memory into the device.

```
enable                          Change to the Privileged EXEC mode.
copy sshkey envm <file name>    Load your own key onto the device from the external memory.
```

A.5.3 Preparing the SSH client program

The *PuTTY* program allows you to access the device using SSH. This program is provided on the product CD.

Perform the following steps:

☐ Start the program by double-clicking on it.
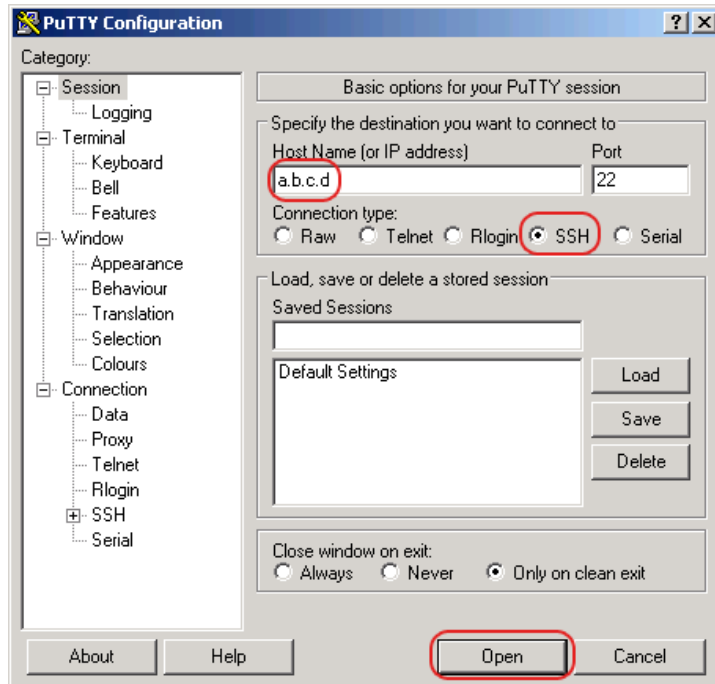
Figure 68: PuTTY input screen

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

☐ To select the connection type, select the *SSH* radio button in the *Connection type* range.

☐ Click the *Open* button to set up the data connection to your device.

Just before the connection is established, the *PuTTY* program displays a security alarm message and gives you the option of checking the key fingerprint.

Figure 69: Security alert prompt for the fingerprint

☐ Check the fingerprint of the key to help ensure that you have actually connected to the desired device.

☐ If the fingerprint matches your key, click the *Yes* button.

The *PuTTY* program also displays another security alarm message at the specified warning threshold.

For experienced network administrators, another way of accessing your device through an SSH is by using the OpenSSH Suite. To set up the data connection, enter the following command:

```
ssh admin@10.0.112.53
```

`admin` is the user name.
`10.0.112.53` is the IP address of your device.

A.6 HTTPS certificate

Your web browser establishes the connection to the device using the HTTPS protocol. The prerequisite is that you enable the *HTTPS server* function in the *Device Security > Management Access > Server* dialog, *HTTPS* tab.

Note: Third-party software such as web browsers validate certificates based on criteria such as their expiration date and current cryptographic parameter recommendations. Old certificates can cause errors, for example, when they expire or cryptographic recommendations change. Upload your own, up-to-date certificate or regenerate the certificate with the latest firmware to solve validation conflicts with third-party software.

A.6.1 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 on the device.

☐ Open the *Device Security > Management Access > Server* dialog, *HTTPS* tab.
☐ To create a X509/PEM certificate, in the *Certificate* frame, click the *Create* button.

☐ To save the changes temporarily, click the ✅ button.
☐ Restart the HTTPS server to activate the key. Restart the server using the Command Line Interface (CLI).

`enable`	Change to the Privileged EXEC mode.
`configure`	Change to the Configuration mode.
`https certificate generate`	Generate a https X.509/PEM Certificate.
`no https server`	Disable the *HTTPS* function.
`https server`	Enable the *HTTPS* function.

☐ The device enables you also to upload an externally generated X.509/PEM Standard certificate to the device:

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

☐ If the certificate is located on your PC or on a network drive, drag and drop the certificate in the ⬆ area. Alternatively click in the area to select the certificate.
☐ Click on the *Start* button to copy the certificate to the device.

☐ To save the changes temporarily, click the ✅ button.

`enable`	Change to the Privileged EXEC mode.
`copy httpscert envm <file name>`	Copy HTTPS certificate from external non-volatile memory device.
`configure`	Change to the Configuration mode.
`no https server`	Disable the *HTTPS* function.
`https server`	Enable the *HTTPS* function.

Note: If you upload or create a certificate, be sure to reboot the device or the HTTPS server in order to activate the certificate. Restart the server using the Command Line Interface (CLI).

A.6.2 Access through HTTPS

The default setting for HTTPS data connection is TCP port `443`. If you change the number of the HTTPS port, reboot the device or the HTTPS server. Thus the change becomes effective.

Perform the following steps:

- ☐ Open the *Device Security > Management Access > Server* dialog, *HTTPS* tab.
- ☐ To enable the function, select the `On` radio button in the *Operation* frame.
- ☐ To access the device by HTTPS, enter HTTPS instead of HTTP in your browser, followed by the IP address of the device.

`enable`	Change to the Privileged EXEC mode.
`configure`	Change to the Configuration mode.
`https port 443`	Specifies the number of the TCP port on which the web server receives HTTPS requests from clients.
`https server`	Enable the *HTTPS* function.
`show https`	Displays the status of the *HTTPS* server and the port number.

If you make changes to the HTTPS port number, disable the HTTPS server and then enable it again in order to make the changes effective.
The device uses HTTPS protocol and establishes a new data connection. At the end of the session, when the user logs out, the device terminates the data connection.

B Appendix

B.1 Literature references

▶ "Optische Übertragungstechnik in industrieller Praxis"
Christoph Wrobel (ed.)
Hüthig Buch Verlag Heidelberg
ISBN 3-7785-2262-0

▶ Hirschmann Manual
"Basics of Industrial ETHERNET and TCP/IP"
280 710-834

▶ "TCP/IP Illustrated", Vol. 1
W.R. Stevens
Addison Wesley 1994
ISBN 0-201-63346-9

B.2 Maintenance

Hirschmann is continually working on improving and developing their software. Check regularly whether 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 (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.

If 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 `1`, which means that the power supply is ready for operation.

Definition of the syntax terms used:	
Integer	An integer in the range -2^{31} - 2^{31}-1
IP address	xxx.xxx.xxx.xxx (xxx = integer in the range 0..255)
MAC address	12-digit hexadecimal number in accordance with ISO/IEC 8802-3
Object Identifier	x.x.x.x… (for example 1.3.6.1.1.4.1.248...)
Octet String	ASCII character string
PSID	Power supply identifier (number of the power supply unit)
TimeTicks	Stopwatch, Elapsed time = numerical value / 100 (in seconds) numerical value = integer in the range $0-2^{32}$-1
Timeout	Time value in hundredths of a second time value = integer in the range $0-2^{32}$-1
Type field	4-digit hexadecimal number in accordance with ISO/IEC 8802-3
Counter	Integer ($0-2^{32-1}$), whose value is increased by 1 when certain events occur.
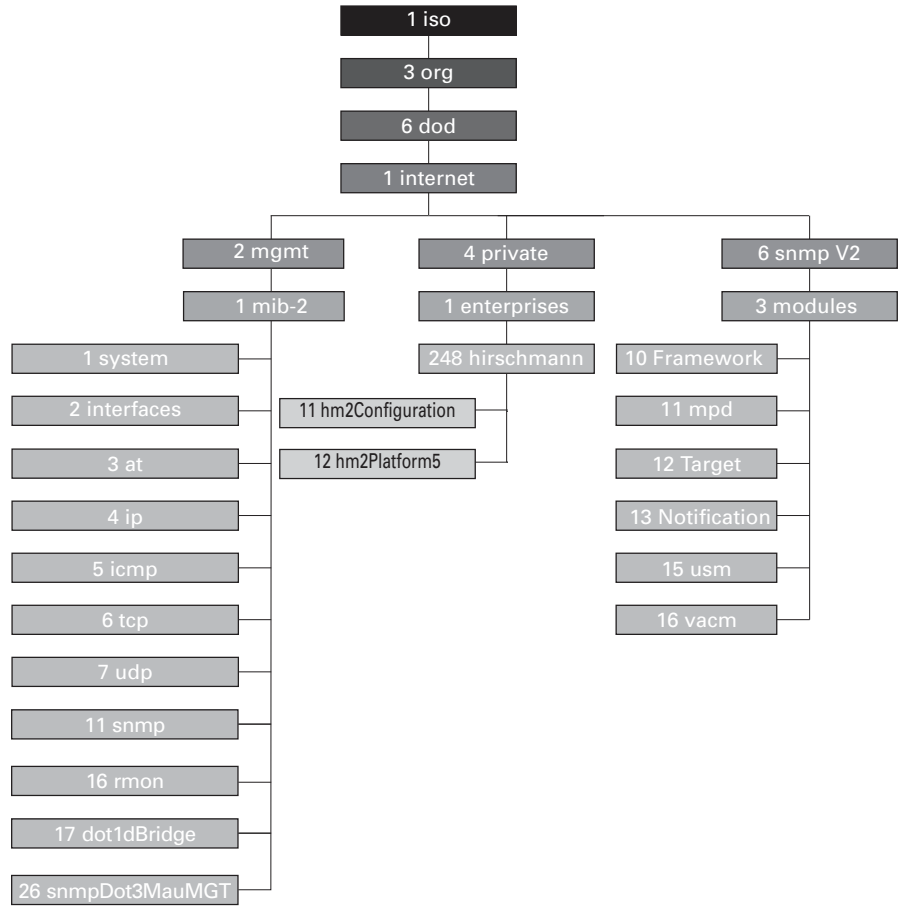
Figure 70: Tree structure of the Hirschmann MIB

A description of the MIB can be found on the product CD provided with the device.

B.4 List of RFCs

RFC 768	UDP
RFC 783	TFTP
RFC 791	IP
RFC 792	ICMP
RFC 793	TCP
RFC 826	ARP
RFC 854	Telnet
RFC 855	Telnet Option
RFC 951	BOOTP
RFC 1112	IGMPv1
RFC 1157	SNMPv1
RFC 1155	SMIv1
RFC 1212	Concise MIB Definitions
RFC 1213	MIB2
RFC 1493	Dot1d
RFC 1542	BOOTP-Extensions
RFC 1643	Ethernet-like -MIB
RFC 1757	RMON
RFC 1867	Form-Based File Upload in HTML
RFC 1901	Community based SNMP v2
RFC 1905	Protocol Operations for SNMP v2
RFC 1906	Transport Mappings for SNMP v2
RFC 1945	HTTP/1.0
RFC 2068	HTTP/1.1 protocol as updated by draft-ietf-http-v11-spec-rev-03
RFC 2131	DHCP
RFC 2132	DHCP-Options
RFC 2233	The Interfaces Group MIB using SMI v2
RFC 2236	IGMPv2
RFC 2246	The TLS Protocol, Version 1.0
RFC 2346	AES Ciphersuites for Transport Layer Security
RFC 2365	Administratively Scoped IP Multicast
RFC 2578	SMIv2
RFC 2579	Textual Conventions for SMI v2
RFC 2580	Conformance statements for SMI v2
RFC 2613	SMON
RFC 2618	RADIUS Authentication Client MIB
RFC 2620	RADIUS Accounting MIB
RFC 2674	Dot1p/Q
RFC 2818	HTTP over TLS
RFC 2851	Internet Addresses MIB
RFC 2863	The Interfaces Group MIB
RFC 2865	RADIUS Client
RFC 2866	RADIUS Accounting

RFC 2868	RADIUS Attributes for Tunnel Protocol Support
RFC 2869	RADIUS Extensions
RFC 2869bis	RADIUS support for EAP
RFC 2933	IGMP MIB
RFC 3164	The BSD Syslog Protocol
RFC 3376	IGMPv3
RFC 3410	Introduction and Applicability Statements for Internet Standard Management Framework
RFC 3411	An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks
RFC 3412	Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)
RFC 3413	Simple Network Management Protocol (SNMP) Applications
RFC 3414	User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)
RFC 3415	View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP)
RFC 3418	Management Information Base (MIB) for the Simple Network Management Protocol (SNMP)
RFC 3580	802.1X RADIUS Usage Guidelines
RFC 3584	Coexistence between Version 1, Version 2, and Version 3 of the Internet-standard Network Management Framework
RFC 4022	Management Information Base for the Transmission Control Protocol (TCP)
RFC 4113	Management Information Base for the User Datagram Protocol (UDP)
RFC 4188	Definitions of Managed Objects for Bridges
RFC 4251	SSH protocol architecture
RFC 4252	SSH authentication protocol
RFC 4253	SSH transport layer protocol
RFC 4254	SSH connection protocol
RFC 4293	Management Information Base for the Internet Protocol (IP)
RFC 4318	Definitions of Managed Objects for Bridges with Rapid Spanning Tree Protocol
RFC 4330	Simple Network Time Protocol (SNTP) Version 4 for IPv4, IPv6 and OSI
RFC 4363	Definitions of Managed Objects for Bridges with Traffic Classes, Multicast Filtering, and Virtual LAN Extensions
RFC 4541	Considerations for Internet Group Management Protocol (IGMP) and Multicast Listener Discovery (MLD) Snooping Switches
RFC 4836	Definitions of Managed Objects for IEEE 802.3 Medium Attachment Units (MAUs)

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 802.1X	Port Authentication
IEEE 802.3	Ethernet
IEEE 802.3ac	VLAN Tagging
IEEE 802.3x	Flow Control
IEEE 802.3af	Power over Ethernet

B.6 Underlying IEC Norms

IEC 62439	High availability automation networks MRP – Media Redundancy Protocol based on a ring topology

B.7 Underlying ANSI Norms

ANSI/TIA-1057	Link Layer Discovery Protocol for Media Endpoint Devices, April 2006

B.8 Technical Data

Switching	
Size of the MAC address table (incl. static filters)	16384
Max. number of statically configured MAC address filters	100
Max. number of MAC address filters learnable through IGMP Snooping	512
Max. number of MAC address entries (MMRP)	64
Number of priority queues	8 Queues
Port priorities that can be set	0..7
MTU (max. length of packets)	1518 Bytes

VLAN	
VLAN ID range	1..4042
Number of VLANs	max. 128 simultaneously per device max. 128 simultaneously per port

Access Control Lists (ACL)	
Max. number of ACLs	
Max. number of rules per port	
Max. number of rules per ACL	
Number of total configurable rules	
Max. number of VLAN assignments (in)	12
Max. number of rules which log an event	
Max. number of Ingress rules	

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 *Help > Licenses* dialog.

B.10 Abbreviations used

ACA	AutoConfiguration Adapter
ACL	Access Control List
BOOTP	Bootstrap Protocol
CLI	Command Line Interface
DHCP	Dynamic Host Configuration Protocol
FDB	Forwarding Database
GUI	Graphical User Interface
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
ICMP	Internet Control Message Protocol
IEEE	Institute of Electrical and Electronics Engineers
IGMP	Internet Group Management Protocol
IP	Internet Protocol
LED	Light Emitting Diode
LLDP	Link Layer Discovery Protocol
MAC	Media Access Control
MIB	Management Information Base
MRP	Media Redundancy Protocol
NMS	Network Management System
PC	Personal Computer
QoS	Quality of Service
RFC	Request For Comment
RM	Redundancy Manager
RSTP	Rapid Spanning Tree Protocol
SCP	Secure Copy
SFP	Small Form-factor Pluggable
SFTP	SSH File Transfer Protocol
SNMP	Simple Network Management Protocol
SNTP	Simple Network Time Protocol
TCP	Transmission Control Protocol
TFTP	Trivial File Transfer Protocol
TP	Twisted Pair
UDP	User Datagram Protocol
URL	Uniform Resource Locator
UTC	Coordinated Universal Time
VLAN	Virtual Local Area Network

C Index

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 http://www.hirschmann.com.

A list of local telephone numbers and email addresses for technical support directly from Hirschmann is available at https://hirschmann-support.belden.com.

This site also includes a free of charge knowledge base and a software download section.

Hirschmann Competence Center

The Hirschmann Competence 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 http://www.hicomcenter.com.
▶ Support ranges from the first installation through the standby service to maintenance concepts.

With the Hirschmann Competence Center, you decided against making any compromises. Our client-customized package leaves you free to choose the service components you want to use.

Internet:
http://www.hicomcenter.com

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 01RD-NT
Stuttgarter Str. 45-51
72654 Neckartenzlingen