HIRSCHMANN

A BELDEN BRAND

Reference Manual

GUI Graphical User Interface
Embedded Ethernet Switch (HiOS-2E EES)

RM GUI HiOS-2E EES
Release 4.0 07/2014

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

The naming of copyrighted trademarks in this manual, even when not specially indicated, should not be taken to mean that these names may be considered as free in the sense of the trademark and tradename protection law and hence that they may be freely used by anyone.

The performance features described here are binding only if they have been expressly agreed when the contract was made. This document was produced by Hirschmann Automation and Control GmbH according to the best of the company's knowledge. Hirschmann reserves the right to change the contents of this document without prior notice. Hirschmann can give no guarantee in respect of the correctness or accuracy of the information in this document.

Hirschmann can accept no responsibility for damages, resulting from the use of the network components or the associated operating software. In addition, we refer to the conditions of use specified in the license contract.

You can get the latest version of this manual on the Internet at the Hirschmann product site (http://www.hirschmann.com).

Printed in Germany
Hirschmann Automation and Control GmbH
Stuttgarter Str. 45-51
72654 Neckartenzlingen
Germany
Tel.: +49 1805 141538

Rel. 4.0 - 07/2014 – 23.07.2014

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 “GUI” reference manual contains detailed information on using the graphical 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 “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

Key

The designations used in this manual have the following meanings:

▶	List
□	Work step
■	Subheading
Link	Cross-reference with link
Note:	A note emphasizes an important fact or draws your attention to a dependency.
`Courier`	ASCII representation in the graphical user interface

Graphical User Interface

■ System requirements

Use HiView to open the graphical user interface. 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).

Alternatively you have the option to open the graphical user interface in a Web browser, e.g. in Mozilla Firefox version 3.5 or higher or Microsoft Internet Explorer version 6 or higher. You need to install the Java Runtime Environment (JRE) in the most recently released version. You can find installation packages for your operating system at http://java.com.

■ Starting the graphical user interface

The prerequisite for starting the graphical user interface, first configure the IP parameters of the device correctly. The “Basic Configuration” user manual contains detailed information that you need to specify the IP parameters.

Start the graphical user interface in HiView:

□ Start HiView.

□ In the URL field of the start window, enter the IP address of your device.

□ Click "Open".

HiView sets up the connection to the device and displays the login window.

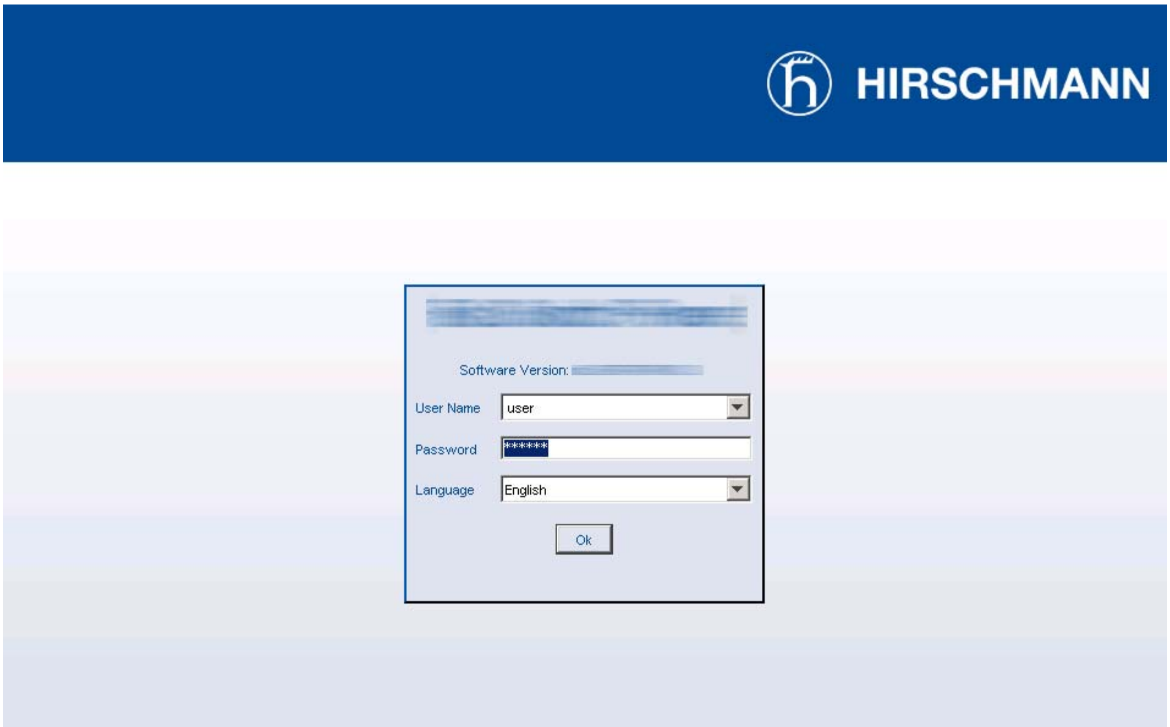
Start the graphical user interface in the Web browser:

– This requires that Java is enabled in the security settings of your Web browser.

□ 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 window.



Software Version:

User Name: user

Password: ******

Language: English

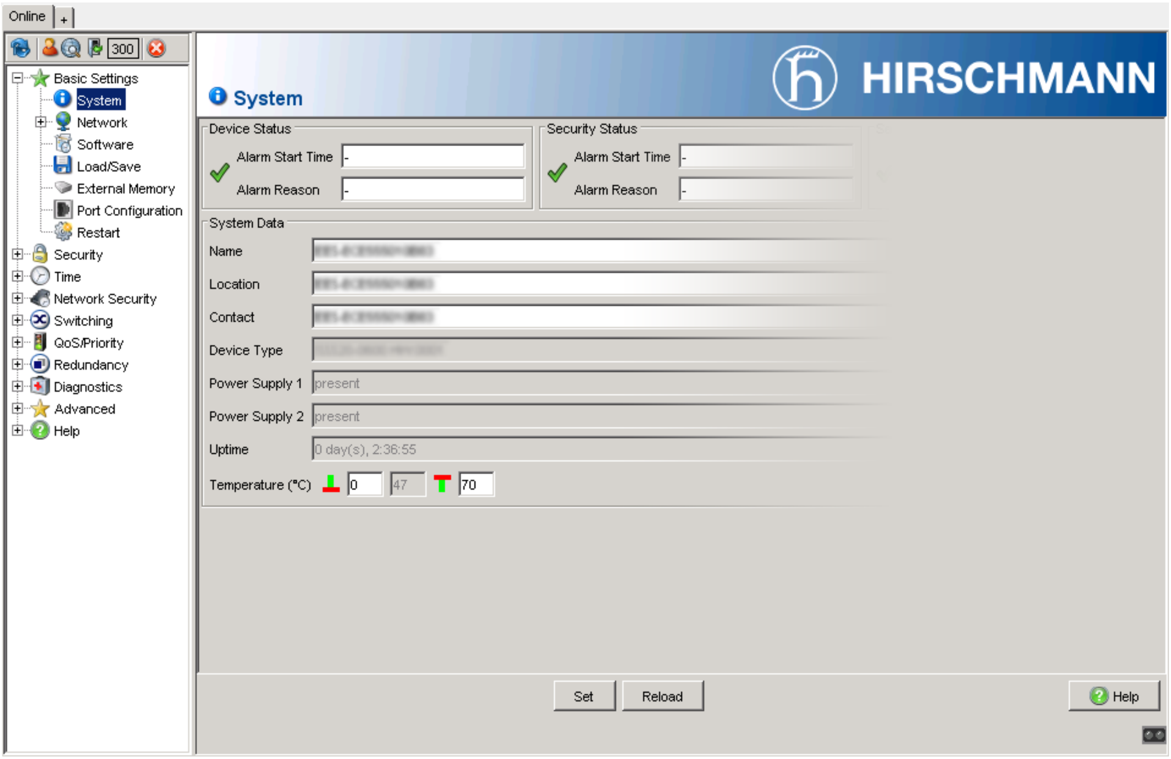
Figure 1: Login window

□ Select the user name and enter the password.

□ Select the language in which you want to use the graphical user interface.

□ Click "Ok".

The Web browser displays the graphical user interface.



Device Status

Alarm Start Time	-
Alarm Reason	-

Security Status

Alarm Start Time	-
Alarm Reason	-

System Data

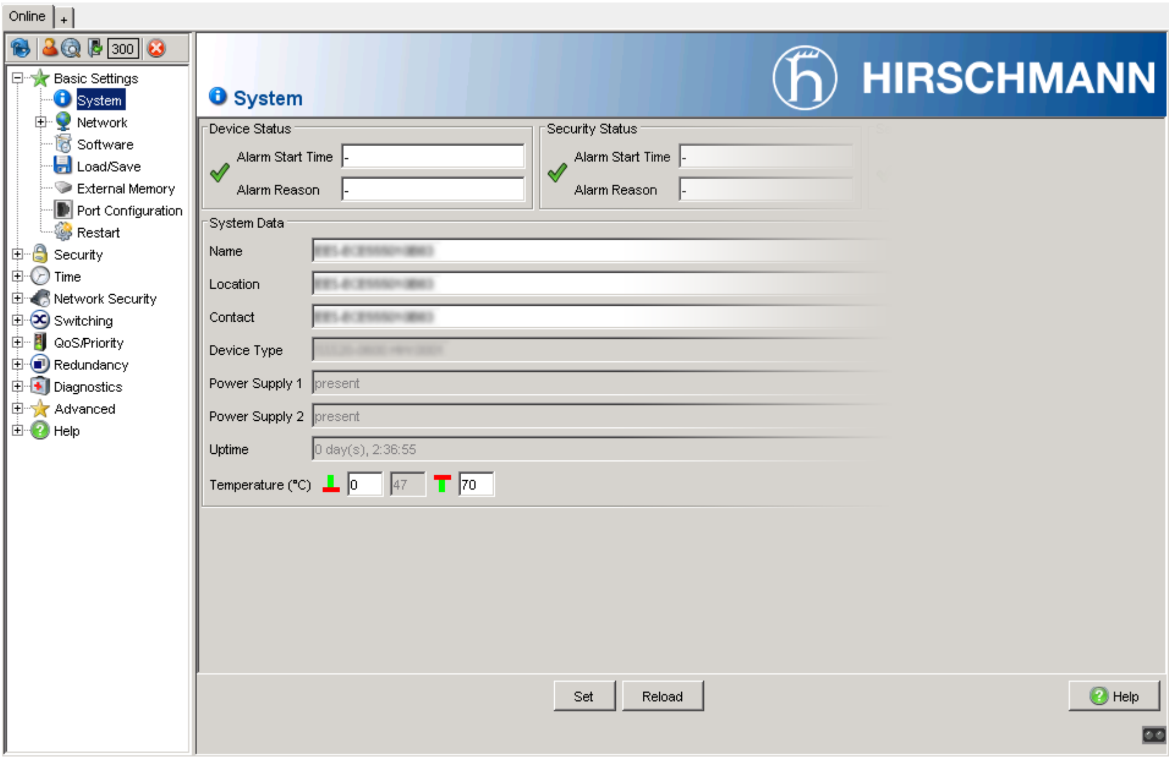
Name	[redacted]
Location	[redacted]
Contact	[redacted]
Device Type	[redacted]
Power Supply 1	present
Power Supply 2	present
Uptime	0 day(s), 2:36:55
Temperature (°C)	0 47 70

Figure 2: Graphical user interface of the device

Operating Instructions

The graphical user interface of the device is divided as follows:

- Tab area (at the upper edge)
- menu section (left)
- dialog section (right).



System

Device Status

Alarm Start Time	-
Alarm Reason	-

Security Status

Alarm Start Time	-
Alarm Reason	-

System Data

Name	[redacted]
Location	[redacted]
Contact	[redacted]
Device Type	[redacted]
Power Supply 1	present
Power Supply 2	present
Uptime	0 day(s), 2:36:55
Temperature (°C)	0 47 70

Figure 3: Graphical user interface of the device

In the default setting, the tab area displays the following tabs at the upper edge.

- "Online" tab
  This tab contains the menus and dialogs with the current settings of the device. You right-click the tab to open the context menu.
- "+" tab
  This tab allows you to create a snapshot or to display a previously created snapshot.
  A snapshot contains the settings and operating parameters the device had at a given time in the past. The device allows you to compare the current operating status with the operating status the device had at a given time in the past.

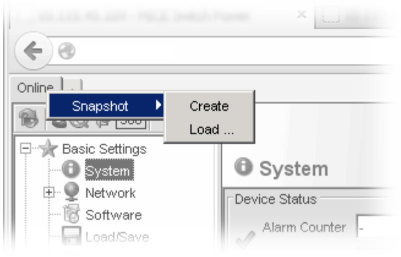


Figure 4: “Online” tab with context menu

Designation		Meaning
Snapshot		
	Create	The device generates a snapshot of the current settings. This will take 20 s or longer, depending on the device settings. In the tab area at the upper edge, the device adds the "Snapshot …" tab. ▶ While the device is generating the snapshot, the tab displays the symbol ⊗. The menu section and the dialog section are concealed meanwhile. To continue to work, change back to the "Online" tab. ▶ If the snapshot is entirely generated, the symbol on the tab disappears. The menu section and the dialog section are visible.
	Load …	The device loads a previously generated snapshot from a file. This will take 10 s or longer, depending on the device settings. In the tab area at the upper edge, the device adds the "Snapshot …" tab. ▶ While the device is loading the snapshot, the tab displays the symbol ⊗. The menu section and the dialog section are concealed meanwhile. To continue to work, change back to the "Online" tab. ▶ If the snapshot is entirely generated, the symbol on the tab disappears. The menu section and the dialog section are visible.

Table 1: “Online” tab: functions in the context menu

The "Snapshot …" tab displays the values in the usual way in the dialog fields. The fields are write-protected, thus modifying the values is impossible. You right-click the tab to open the context menu.

Designation	Meaning
Save As...	Exports the snapshot and saves the settings and operating parameters as a file on your PC.
Close	Closes the "Snapshot …" tab. Unsaved information are lost.

Table 2: “Snapshot” tab: functions in the context menu

The menu displays the menu items. When you click a menu item, the user interface displays the corresponding dialog in the dialog area.

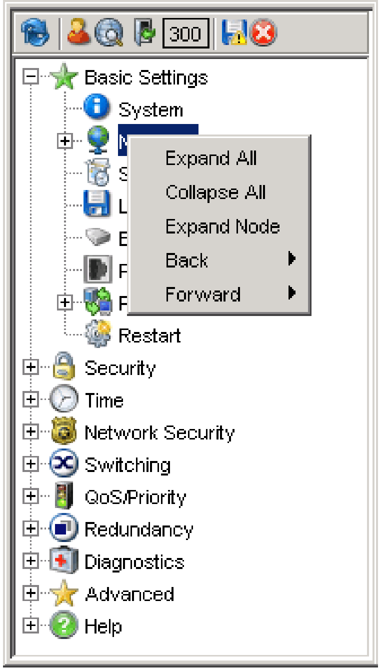


Figure 5: Menu section with context menu

You right-click the menu section to open the context menu.

Designation	Meaning
Expand All	Expands the nodes in the menu tree. The menu section displays the menu items for all levels.
Collapse All	Collapses the nodes in the menu tree. The menu section displays the menu items for the top level.

Table 3: Menu section: Functions in the context menu

Designation	Meaning
Expand Node	Expands the selected node and collapses the other nodes in the menu tree. This function allows you to expand a main node without scrolling and without collapsing other nodes manually.
Back	Allows you to quickly jump back to a previously selected menu item.
Forward	Allows you to quickly jump forward to a previously selected menu item when you have previously used the "Back" function.

Table 3: Menu section: Functions in the context menu (cont.)

The status line is located in the top part of the menu section.

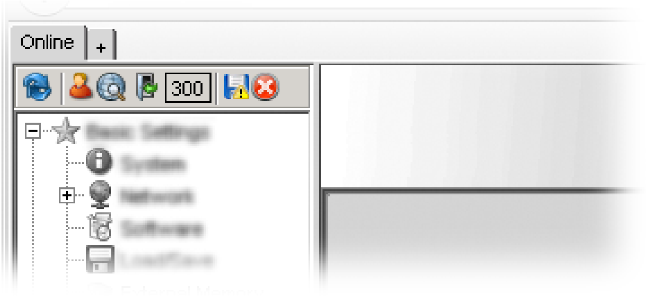


Figure 6: Status line

The status line contains the following buttons:

Button	Function
🔄	Refreshes the status line. The buttons display the values loaded from the volatile memory (`RAM`) of the device.
⊗	Terminates the refreshing of the status line.
👤	When you position the mouse pointer over the button, the user interface opens a bubble help with the following information: ▶ The time at which the device last refreshed the values ▶ Name of the user logged in ▶ Device name ▶ Network protocol by means of which you are logged in to the device. The device automatically refreshes the values once a minute. To refresh the display manually, click the 🔄 button. By right-clicking this symbol you can open the `Basic Settings > System` dialog and the `Basic Settings > Network` dialog directly.

Table 4: Buttons in the status line

Button	Function
🔍	When you position the mouse pointer over the button, the user interface opens a bubble help with the summary of the `Diagnostics > System > Configuration Check` dialog. To refresh the display, click the ⟳ button. By right-clicking this symbol you can open the `Diagnostics > System > Configuration Check` dialog directly.
🚪	Ends the session and terminates the connection to the device.
297	Displays the time in seconds after which the device automatically ends the session when the user is inactive. You specify the timeout period in the `Device Security > Management Access > Web` dialog.

Table 4: Buttons in the status line (cont.)

Button	Function
💾	Displays that the configuration profile in the volatile memory (RAM) differs from the Selected configuration profile in the permanent memory (NVM). Save the current device settings permanently so that they are available to you after a restart. To permanently save the changes, 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 "Select" button. ☐ Click the "Save" button. The device automatically compares the configuration profiles once a minute. To refresh the display manually, click the 🔄 button. If the configuration profiles match, the button is hidden. By right-clicking this symbol you have the option of opening the Basic Settings > Load/Save dialog directly.
⊗	When you position the mouse pointer over the button, the user interface opens a bubble help with the following information: ▶ The "Last Update" section displays the time at which the device last refreshed the values. ▶ The "Device Status" 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. ▶ The "Security Status" 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. ▶ The "Boot Parameter" section displays a note if you permanently save changes to the settings and at least one boot parameter differs from the configuration profile used during the last restart. The following settings cause the boot parameters to change: – Basic Settings > Network dialog, "MAC Configuration" tab, "Local Admin MAC Address" parameter – Device Security > Management Access > Server dialog, "SNMP" tab, "Port Number" parameter – Diagnostics > System > Selftest dialog, "RAM Test" parameter – Diagnostics > System > Selftest dialog, "Activate SysMon1" parameter – Diagnostics > System > Selftest dialog, "Load default config on error" parameter

Table 4: Buttons in the status line (cont.)

■ Notes on Saving the Configuration Profile

- □ To copy changed settings to the volatile memory (`RAM`), click the "Set" button.
- □ To refresh the display in the dialogs, click the "Reload" button.
- □ To keep the changed settings even after restarting the device, click the "Save" button in the `Basic Settings > Load/Save` dialog.

Note: Unintentional changes to the settings may cause the connection between your PC and the device to be terminated. Before you change the settings, enable the "Undo Modifications of Configuration" function in the `Basic Settings > Load/Save` dialog. With this function, the device restores the active configuration profile saved in the non-volatile memory (NVM) if the connection is interrupted after the settings have been changed. The device remains reachable.

1 Basic Settings

With this menu you can configure the basic settings of the device.

The menu contains the following dialogs:

- System
- Network
- Software
- Load/Save
- Port
- Restart

1.1 System

With this dialog you can display device properties and monitor individual operating statuses.

Device Status

The fields in this frame display the device status and inform you about alarms that have occurred. You specify the parameters that the device monitors in the `Diagnostics > Status Configuration > Device Status` dialog.

Parameters	Meaning
Symbol	Displays the device status. Possible values: ✓ The device status is OK. The monitored parameters have the desired status. ⊗ An alarm has occurred. At least one monitored parameter differs from the desired status.
Alarm Counter	Displays the number of current alarms.
Alarm Reason	Displays the cause of the alarm and the time at which the device triggered the alarm. If the "Alarm Counter" displays more than `1` alarm, use the arrow buttons to call up the other alarm states. Possible values: ▶ Cause of the event (Date and time in the format `Month, Day, Year hh:mm:ss AM/PM`). The device triggers an alarm if a monitored parameter differs from the desired status. In the `Diagnostics > Status Configuration > Device Status` dialog the parameters are sorted by priority: High priority at the top, low priority at the bottom.

Security Status

The fields in this frame display the security status and inform you about alarms that have occurred. You specify the parameters that the device monitors in the `Diagnostics > Status Configuration > Security Status` dialog.

Parameters	Meaning
Symbol	Displays the security status. Possible values: ✓ The device status is OK. The monitored parameters have the desired status. ⊗ An alarm has occurred. At least one monitored parameter differs from the desired status.
Alarm Counter	Displays the number of current alarms.
Alarm Reason	Displays the cause of the alarm and the time at which the device triggered the alarm. If the "Alarm Counter" displays more than `1` alarm, use the arrow buttons to call up the other alarm states. Possible values: ▶ Cause of the event (Date and time in the format `Month, Day, Year hh:mm:ss AM/PM`). The device triggers an alarm if a monitored parameter differs from the desired status. In the `Diagnostics > Status Configuration > Security Status` dialog the parameters are sorted by priority: High priority at the top, low priority at the bottom.

System Data

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

Parameters	Meaning
Name	Specifies the device name. Possible values: ▶ Alphanumeric ASCII character string with 0..255 characters
Location	Specifies the location of the device. Possible values: ▶ Alphanumeric ASCII character string with 0..255 characters
Contact	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.

Parameters	Meaning
Power Supply {0}	Displays the status of the power supply unit on the voltage supply connection. Possible values: ▶ present ▶ not present ▶ defective
Uptime	Displays the time that has elapsed since this device was last restarted. Possible values: ▶ Time in the format `day(s), hh:mm:ss`

Reloading

The graphical user interface automatically updates the display of the dialog every 100 seconds. In the process, it updates the fields and symbols with the values that are saved in the volatile memory (`RAM`) of the device. At the bottom left of the dialog, you will find the time of the next update.

Reloading data in 70 s

Figure 7: Time to next Reload

Note: The graphical user interface uses this function to update the display in the `Basic Settings > System` dialog.

Buttons

Button	Meaning
Set	Transfers the changes to the volatile memory (`RAM`) of the device and applies them. 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 "Select" button. □ Click the "Save" button.

Button	Meaning
Reload	Updates the fields with the values that are saved in the volatile memory (`RAM`) of the device.
Help	Opens the online help.

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 menu contains the following dialogs:

- Global
- MAC Configuration

1.2.1 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: ▶ `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. ▶ `Local` (default setting) The device uses the IP parameters from the internal memory. You specify the settings for this in the "IP Parameter" frame. **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 ID of the VLAN in which the device management is accessible through the network. Possible values: ▶ `1..4042` (default setting: `1`) You access the device management through device ports that are members of this VLAN. You specify which VLAN a certain device port is assigned to in the `Switching > VLAN > Configuration` dialog.
MAC Address	Displays the MAC address of the device. The device management can be accessed via the network using the MAC address.

■ HiDiscovery Protocol

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

On a PC the HiDiscovery software displays you the Hirschmann devices in the network that can be accessed on which the HiDiscovery function is switched on. You can access these devices even if they have invalid IP parameters or none at all. The HiDiscovery software allows you to change the IP parameters in the device.

Parameters	Meaning
Operation	Activates/deactivates the HiDiscovery function in the device. Possible values: ▶ `On` (default setting) HiDiscovery is activated. You can use the HiDiscovery software to access the device from your PC. ▶ `Off` HiDiscovery is deactivated.
Access	Activates/deactivates 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: ▶ `unmarked` (default setting) The flashing of the port LEDs is inactive. ▶ `marked` The flashing of the port LEDs is active. The port LEDs flash until you disable the function again.

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

■ 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 "Name" field in the `Basic Settings > System` dialog.

■ IP Parameter

This frame allows you to assign the IP parameters manually. These fields can be edited if you have selected the value `Local` in the "Management Interface" frame, "IP Address Assignment" field.

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 (default setting: —)

Buttons

Button	Meaning
Set	Transfers the changes to the volatile memory (`RAM`) of the device and applies them. 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 "Select" button. ☐ Click the "Save" button.
Reload	Updates the fields with the values that are saved in the volatile memory (`RAM`) of the device.
Help	Opens the online help.

1.2.2 MAC Configuration

With the default values, you access the management functions through every device port. This tab allows you to restrict the access so that the management functions are accessible through one device port exclusively. In addition, you have the option of adding a user-specified MAC address to the management.

■ 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 accessable with the MAC address specified by the manufacturer. ▶ `local` The device management is accessable 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.

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, e.g. `001122334455` – separated by spaces, e.g. `00 11 22 33 44 55` – separated by colons, e.g. `00:11:22:33:44:55` – separated by hyphens, e.g. `00-11-22-33-44-55` – separated by points, e.g. `00.11.22.33.44.55` – separated by points after every 4th character, e.g. `0011.2233.4455` **Note:** Permanently save changes to this field before you restart the device.
Management Port	Specifies the device 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 device port. ▶ `<Port number>` The device management is accessable through the selected device port exclusively.

Buttons

Button	Meaning
Set	Transfers the changes to the volatile memory (`RAM`) of the device and applies them. 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 "Select" button. □ Click the "Save" button.
Reload	Updates the fields with the values that are saved in the volatile memory (`RAM`) of the device.
Help	Opens the online help.

1.3 Software

This dialog allows you to update the device software and display information about the device software.

■ 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.
Export	Exports the "Stored Version" of the device software and saves it as an image file on your PC.
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.
Bootcode	Displays the version number and creation date of the boot code.

Software Update

Parameters	Meaning
File	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, click the " … " button and select the file there. ▶ Software update from a TFTP server If the file is located on a TFTP server, enter 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, enter the URL for the file in one of the following forms: – `scp://` or `sftp://<IP address>/<path>/<file name>` When you click the "Update" button, the device displays the "Authentication" window. There you enter "Username" and "Password", to login to the server. – `scp://` or `sftp://<user>:<password>@<IP address>/<path>/<file name>`
…	Displays the "Open" dialog. If the image file is located on your PC or on a network drive, you select the image file here.
Update	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. 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.

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
Index	Displays the index of the device software.
File name	Displays the device-internal file name of the device software.

Parameters	Meaning
Firmware	Displays the version number and creation date of the device software.
Applet	Displays the version number of the graphical user interface (GUI).
Logic	Displays the version number of the logic module for devices with programmable hardware (FPGA).

■ Buttons

Button	Meaning
Reload	Updates the fields with the values that are saved in the volatile memory (`RAM`) of the device.
Help	Opens the online help.

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. Vice versa you 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 in the frame a password, the device saves the current and the afterwards created configuration profiles encrypted.

Unintentional changes to the settings may cause the connection between your PC and the device to be terminated. To maintain the device accessible, enable the "Undo Modifications of Configuration" function before changing settings. If the connection terminates, the device loads the configuration profile saved in the non-volatile memory (`NVM`).

■ Configuration Encryption

Parameters	Meaning
Active	Displays whether the configuration encryption is switched on in the device. Possible values: ▶ `unmarked` The configuration encryption is switched off. The device loads a configuration profile from the non-volatile memory solely (`NVM`) if it is unencrypted. ▶ `marked` The configuration encryption is switched on. 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. If the "Config Priority" field has the value `first` and the configuration profile is unencrypted, the "Security Status" frame in the `Basic Settings >` System dialog displays an alarm.

Parameters	Meaning
Set Password	Encrypts configuration profiles and uses a password to make unauthorized access more difficult. □ Enter the new password in the "Set Password" dialog. □ When you are changing an existing password, also enter the existing password. □ Mark the "Save Configuration afterwards" checkbox to use encryption also for the Selected configuration profile in the non-volatile memory(`NVM`). **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.
Delete	Cancels the configuration encryption in the device. □ Enter the existing password in the "Delete" dialog. □ Mark the "Save Configuration afterwards" checkbox to remove the encryption also for the Selected configuration profile in the non-volatile memory(`NVM`). **Note:** If you keep additional encrypted configuration profiles in the memory, the device prevents 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. The device saves changes temporarily if, for example, you click on "Set" in a dialog while the device is operating.

■ Undo Modifications of Configuration

Parameters	Meaning
Operation	When a user switches on the function, the device continuously checks whether it can still be reached from the IP address of the user. 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` Function is switched on: – You specify the time period between the loss of the connection and the loading of the configuration profile in the field "Period to undo while Connection is lost [s]". – If the non-volatile memory (`NVM`) contains multiple configuration profiles, the device loads the configuration profile designated as "Selected". ▶ `Off` (default setting) Function is switched off. Switch the function off again before you close the graphical user interface. You thus prevent the device from restoring the configuration profile designated as "Selected". **Note:** Before you switch on the function, save the settings in the configuration profile. Current changes, that are saved temporarily, are therefore maintained in the device.
Period to undo while Connection is lost [s]	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 activated 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 Modifications of Configuration". 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. If you highlight a configuration profile in the table and click "Activate", the device loads this configuration profile into the volatile memory (`RAM`).
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-defined name by highlighting an existing configuration profile in the table and clicking the "Save As..." button.
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 Modifications of Configuration". – When you click "Save", 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 and click "Activate".

Parameters	Meaning
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.
Fingerprint Verified	Displays whether the checksum in the configuration profile is valid. The device calculates the checksum again and compares it with the checksum in the configuration profile. Possible values: ▶ `marked` The saved settings are consistent. The checksums match. ▶ `unmarked` The configuration profile contains modified settings. The checksums are different. Possible causes: – The file is damaged. – A user has exported the configuration profile and changed the XML file outside the device. **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

Button	Meaning
Set	Transfers the changes to the volatile memory (`RAM`) of the device and applies them. 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 "Select" button. □ Click the "Save" button.
Reload	Updates the fields with the values that are saved in the volatile memory (`RAM`) of the device.
Save	Transfers the settings from the volatile memory (`RAM`) into the configuration profile designated as “Selected” in the non-volatile memory (`NVM`). **Note:** If you intend to downgrade to the software version HiOS 2.x.xx, note the the following information: Using an up-to-date software version, the device saves the settings in a compressed configuration profile. When booting with the above mentioned software version, the device is able to read uncompressed configuration profiles exclusively. If upon booting solely a compressed configuration profile is available, the device boots applying the delivery settings. The settings in the compressed configuration profile are then lost. To save the configuration profile which is compatible with the software version mentioned above, you proceed as follows: ▶ Before downgrading □ Click the ▾ and "Export..."buttons to export the configuration profile as an unencrypted XML file. ▶ After downgrading □ Click the ▾ and "Import..."buttons to import the configuration profile.

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. Switch on the function "Undo Modifications of Configuration" 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 settings of new functions to the default value.
Delete	Removes the configuration profile highlighted in the table from the non-volatile memory (`NVM`). If the configuration profile is designated as "Selected", the device prevents you from removing the configuration profile.
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 Modifications of Configuration". ▶ Designate an unencrypted configuration profile solely as "Selected" when the configuration encryption in the device is disabled. ▶ Designate an encrypted configuration profile solely 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 solely mark configuration profiles saved in the non-volatile memory (`NVM`).

Button	Meaning
▼	Opens a menu with the following buttons.
Export...	Exports the configuration profile selected in the table and saves it as an XML file on the PC or on a server. The device gives you the following options for exporting a configuration profile: ▶ Export to the PC To save the file on your PC or on a network drive, click the " ... " button and select the storage location and specify the file name. ▶ Export to a TFTP server To save the file on a TFTP server, enter 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, enter 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 "Authentication" window. There you enter "Username" and "Password", to login to the server. – `scp://` or `sftp://<user>:<password>@<IP address>/<path>/<file name>`

Button	Meaning
Import...	Imports a configuration profile saved in XML format from a PC or from a server in the network. ▶ You specify the storage location for the configuration profile to be imported in the "Storage Type" field. ▶ You specify the name of the configuration profile to be imported in the "Name" field. The device gives you the following options for importing a configuration profile: ▶ Import from the PC If the file is located on your PC or on a network drive, click the " … " button and select the file there. ▶ Import from a TFTP server If the file is located on a TFTP server, enter 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, enter 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 "Authentication" window. There you enter "Username" and "Password", to login to the server. – `scp://` or `sftp://<user>:<password>@<IP address>/<path>/<file name>` If the configuration encryption is inactive, the device imports the configuration profile when it is unencrypted. If the configuration encryption is active, the device imports the configuration profile when it is unencrypted and the password matches the password saved in the device.
View...	Displays the settings of the configuration profile highlighted in the table in clear text as an XML. If the configuration profile is encrypted, enter the password in order to see the settings in clear text.
Save As...	Copies the configuration profile highlighted in the table and saves it with a user-defined 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.
Back to factory defaults...	Resets the settings in the device to the default values. ▶ The device deletes the saved configuration profiles from the volatile memory (`RAM`) and from the non-volatile memory (`NVM`). ▶ After a brief period, the device reboots and loads the default values.
Help	Opens the online help.

1.5 Port

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

The dialog contains the following tabs:
- ▶ Configuration
- ▶ Statistics
- ▶ Utilization

1.5.1 Configuration

■ Table

Parameters	Meaning
Port	Displays the number of the device port to which the table entry relates.
Name	Name of the device port. Enter the name of your choice. Possible values: ▶ Alphanumeric ASCII character string with 0..64 characters
Port on	Activates/deactivates the device port. Possible values: ▶ `marked` (default setting) The device port is activated. ▶ `unmarked` The device port is deactivated. The device port does not send or receive any data.
State	Displays whether the device port is currently physically switched on or off. Possible values: ▶ `marked` The device port is switched on. ▶ `unmarked` The device port is switched off. If the "Port on" function is switched on, the "Auto Disable" function has switched off the device port. You specify the settings of the "Auto Disable" function in the `Diagnostics > Ports > Auto Disable` dialog.
Power State (Port off)	Physically switches off the device port, or leaves it on when you deactivate the "Port on" function. Possible values: ▶ `marked` The device port remains physically switched on. A connected device receives an active link. ▶ `unmarked` (default setting) The device port is physically switched off.
Auto Power Down	Specifies how the device port behaves when no cable is connected. Possible values: ▶ `no-power-save` (default setting) The device port remains activated. ▶ `auto-power-down` The device port switches to the energy-saving mode. ▶ `unsupported` The device port does not support this function and remains activated.

Parameters	Meaning
Automatic Configuration	Enables/disables the automatic selection of the operating mode for the device port. Possible values: ▶ `marked` (default setting) The device 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 device port. Elapse several seconds until the device port has set the operating mode. ▶ `unmarked` The device port operates with the values you specify in the "Manual Configuration" field and in the "Manual Cable Crossing (Auto. Conf. off)" field.
Manual Configuration	Specifies the operating mode of the device ports when the function "Automatic Configuration" is inactive. 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` (default setting) Full duplex connection The operating modes actually available depend on the media module used.
Link/ Current Settings	Displays the operating mode which the device 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

Parameters	Meaning
Manual Cable Crossing (Auto. Conf. off)	Specifies the devices connected to a TP port. The prerequisite is that the function "Automatic Configuration" is disabled. Possible values: ▶ `mdi` The device interchanges the send- and receive-line pairs on the device port. ▶ `mdix` (default setting on TP ports) The device prevents the interchange of the send- and receive-line pairs on the device 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 a 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 device port does not support this function.
Flow Control	Activates/deactivates the flow control on the device port. Possible values: ▶ `unmarked` Flow control on the device port is deactivated. ▶ `marked` (default setting) The sending and evaluating of pause data packets (full-duplex operation) or collisions (half-duplex operation) is activated on the port. □ To switch on the flow control in the device, also switch on the "Activate 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”). 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.
Signal	Activates/deactivates the port LED flashing. This function allows you to identify the port in the field. Possible values: ▶ `unmarked` (default setting) The flashing of the port LEDs is inactive. ▶ `marked` The flashing of the port LEDs is active. The port LEDs flash until you disable the function again.

■ Buttons

Button	Meaning
Set	Transfers the changes to the volatile memory (`RAM`) of the device and applies them. 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 "Select" button. □ Click the "Save" button.
Reload	Updates the fields with the values that are saved in the volatile memory (`RAM`) of the device.
Reset port counters	Resets the counter for the port statistics to `0`.
Help	Opens the online help.

1.5.2 Statistics

This tab displays the following overview per device 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`, click the "Reset port counters" button.

- in the `Basic Settings > Port > Statistics` dialog, or
- in the `Basic Settings > Restart` dialog

Buttons

Button	Meaning
Set	Transfers the changes to the volatile memory (`RAM`) of the device and applies them. 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 "Select" button. □ Click the "Save" button.
Reload	Updates the fields with the values that are saved in the volatile memory (`RAM`) of the device.
Reset port counters	Resets the counter for the port statistics to `0`.
Help	Opens the online help.

1.5.3 Utilization

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

■ Table

Parameters	Meaning
Port	Displays the number of the device port to which the table entry relates.
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 device port falls below this value, the "Alarm" field 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 device port exceeds this value, the "Alarm" field 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 device port is below the value specified in the "Lower Threshold [%]" field or above the value specified in the "Upper Threshold [%]" field. The device sends a SNMP trap. ▶ `unmarked` The utilization of the device port is above the value specified in the "Lower Threshold [%]" field and below the value specified in the "Upper Threshold [%]" field. The prerequisite for sending SNMP traps is that you enable the function in the `Diagnostics > Status Configuration > Alarms (Traps)` dialog and at least 1 SNMP manager is specified.

Buttons

Button	Meaning
Set	Transfers the changes to the volatile memory (`RAM`) of the device and applies them. 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 "Select" button. □ Click the "Save" button.
Reload	Updates the fields with the values that are saved in the volatile memory (`RAM`) of the device.
Reset port counters	Resets the counter for the port statistics to `0`.
Help	Opens the online help.

1.6 Restart

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

■ Restart

Parameters	Meaning
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 "Yes" in the <"Warning" dialog. ☐ To discard the changes, click "No" in the "Warning" dialog. ▶ In the "Delay (hh:mm:ss)" lield 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 switched on 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 `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.
Restart in (hh:mm:ss)	Specifies whether the device monitors module removal. Possible values: ▶ `00:00:00..596:31:23` (Delayed restart activated) ▶ `-` (Delayed restart deactivated) To refresh the display of the remaining time, click "Reload".
Interrupt	Aborts a delayed restart.

Buttons

Button	Meaning
Reset MAC Address Table	Removes the MAC addresses from the forwarding table that have the value `learned` in the "Status" field in the `Switching > Filter for MAC Addresses` dialog.
Reset ARP Table	Removes the dynamically set up addresses from the ARP table - see the `Diagnostics > System > ARP Table` dialog.
Reset port counters	Resets the counter for the port statistics to `0` - see the `Basic Settings >` Port dialog, "Statistics" tab.
Reset IGMP Snooping counters	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.
Reload	Updates the fields with the values that are saved in the volatile memory (`RAM`) of the device.
Help	Opens the online help.

2 Time

The device allows you to synchronize the system time in the device and in the network with SNTP (Simple Network Time Protocol) and PTP (Precision Time Protocol). PTP is significantly more accurate than SNTP. If both protocols are activated in the device, PTP has priority.

After a restart, the device initializes its clock to January 1, 00:00h. Reset the time when you disconnect the device from the power supply or restart it. Alternatively you specify, that the device automatically obtains the current time from an SNTP server or from a PTP clock.

The menu contains the following dialogs:

- Basic Settings
- IRIG-B/PPS
- SNTP
- PTP

2.1 Basic Settings

With this dialog you can specify time-related settings independently of the time synchronization protocol specified.

The dialog contains the following tabs:

- Global
- Daylight Saving Time

2.1.1 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).
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"
Set Time from PC	The device uses the time on the PC as the system 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. ▶ `ptp` PTP is activated and the clock of the device is synchronized with a PTP master clock.
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`)
Set Offset from PC	The device determines the time zone on your PC and uses it to calculate the difference between the local time and "System Time (UTC)".

■ Buttons

Button	Meaning
Set	Transfers the changes to the volatile memory (`RAM`) of the device and applies them. 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 "Select" button. □ Click the "Save" button.
Reload	Updates the fields with the values that are saved in the volatile memory (`RAM`) of the device.
Help	Opens the online help.

2.1.2 Daylight Saving Time

On this tab you activate the automatic daylight saving time function. You specify the beginning and the end of summertime using a predefined 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	When you enable the function, the device automatically changes between summertime and wintertime. Possible values: ▶ `On` ▶ `Off` (default setting) 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 predefined 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 "Systemtime" 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) ▶ `sun` ▶ `mon` ▶ `tue` ▶ `wed` ▶ `thu` ▶ `fri` ▶ `sat`
Month	Specifies the month. Possible values: ▶ `none` (default setting) ▶ `jan` ▶ `feb` ▶ `mar` ▶ `apr` ▶ `may` ▶ `jun` ▶ `jul` ▶ `aug` ▶ `sep` ▶ `oct` ▶ `nov` ▶ `dec`
Systemtime	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 "Systemtime" 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) ▶ `sun` ▶ `mon` ▶ `tue` ▶ `wed` ▶ `thu` ▶ `fri` ▶ `sat`
Month	Specifies the month. Possible values: ▶ `none` (default setting) ▶ `jan` ▶ `feb` ▶ `mar` ▶ `apr` ▶ `may` ▶ `jun` ▶ `jul` ▶ `aug` ▶ `sep` ▶ `oct` ▶ `nov` ▶ `dec`
Systemtime	Specifies the time. Possible values: ▶ `<HH:MM>` (default setting: `00:00`)

■ Buttons

Button	Meaning
Set	Transfers the changes to the volatile memory (`RAM`) of the device and applies them. 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 "Select" button. ☐ Click the "Save" button.
Reload	Updates the fields with the values that are saved in the volatile memory (`RAM`) of the device.
Help	Opens the online help.

2.2 IRIG-B/PPS

The device provides you with the option of outputting binary-coded time signals. The time signals allow other devices to be synchronized.

The dialog contains the following tabs:

- IRIG-B
- PPS

2.2.1 IRIG-B

You configure the IRIG-B output of the device in this tab.

The device provides a pulse width-modulated time signal with 100 pulses per second at the IRIG-B output. Prerequisite for this is that the PTP slave clock of the device has been synchronized.

■ Operation

Parameters	Meaning
Operation	The IRIG-B output of the device is activated when the function is on. Possible values: ▶ `On` The IRIG-B output of the device is activated. The "Configuration" frame displays whether a time signal is present. ▶ `Off` (default setting) The IRIG-B output of the device is deactivated.

■ Configuration

Parameters	Meaning
Output active	Displays whether the time signal is present on the IRIG-B output. Possible values: ▶ `enable` The time signal is present on the IRIG-B output. The PTP slave clock of the device is synchronized with a PTP master clock. ▶ `disable` No time signal is present on the IRIG-B output. The PTP slave clock of the device is not synchronized.

■ Information

Parameters	Meaning
Mode	Specifies the code of the time signal. Every code contains specific time information. Possible values: ▶ `irig-b000` contains BCDtoy, CF, SBS ▶ `irig-b001` contains BCDtoy, CF ▶ `irig-b002` contains BCDtoy ▶ `irig-b003` (default setting) contains BCDtoy, SBS ▶ `irig-b004` contains BCDtoy, BCDyear, CF, SBS. ▶ `irig-b005` contains BCDtoy, BCDyear, CF ▶ `irig-b006` contains BCDtoy, BCDyear ▶ `irig-b007` contains BCDtoy, BCDyear, SBS Explanation: – BCDtoy = binary coded decimal time of year – BCDyear = binary coded decimal year – CF = control functions (according to IEEE 1344) – SBS = straight binary seconds of day
Time Mode	Specifies which time information of the internal clock the device transmits. Possible values: ▶ `local` The device transmits the time information with reference to the local time. ▶ `utc` (default setting) The device transmits the time information with reference to the Universal Time Coordinated (UTC).
Quality	Displays the accuracy of the time signal (“time quality” according to IEEE 1344): ▶ `failure` No time signal available or time source unreliable. ▶ `locked` Time source present.

■ Buttons

Button	Meaning
Set	Transfers the changes to the volatile memory (`RAM`) of the device and applies them. 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 "Select" button. ☐ Click the "Save" button.
Reload	Updates the fields with the values that are saved in the volatile memory (`RAM`) of the device.
Help	Opens the online help.

2.2.2 PPS

You configure the PPS output of the device in this tab.

The device provides the time signal as a PPS signal (1 pulse per second) at the PPS output.

■ Operation

Parameters	Meaning
Operation	The PPS output of the device is activated when the function is on. Possible values: ▶ `On` The PPS output of the device is activated. The time signal is present on the PPS output. The cycle duration of the pulse is 1 second (200 ms high, 800 ms low). ▶ `Off` (default setting) The PPS output of the device is deactivated.

■ Buttons

Button	Meaning
Set	Transfers the changes to the volatile memory (`RAM`) of the device and applies them. 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 "Select" button. □ Click the "Save" button.
Reload	Updates the fields with the values that are saved in the volatile memory (`RAM`) of the device.
Help	Opens the online help.

2.3 SNTP

SNTP (Simple Network Time Protocol) 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

2.4 SNTP Client

With 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	When the function is on, the device operates as an SNTP client. Possible values: ▶ `On` ▶ `Off` (default setting)

■ 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`)

Parameters	Meaning
Broadcast Recv Timeout [s]	Specifies the time in seconds a client in broadcast client mode waits before changing the status from `synchronizedToRemoteServer` to `notSynchronized` when the client receives no broadcast packets. Possible Values: ▶ `128..2048` (default setting: `320`)
Disable Client after successful Synchronization	Specifies whether the device disables the SNTP client when it has successfully synchronized the time. Possible values: ▶ `marked` The device deactivates the SNTP client after successful synchronization. ▶ `unmarked` (default setting) The SNTP client remains activated after successful 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. ▶ `syncToRemoteServer` 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 a sequential number to which the table entry relates. Possible values: ▶ `1..4` The device automatically defines 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.
Description	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`)
Target 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. ▶ `serverUnsynchronized` 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

Button	Meaning
Set	Transfers the changes to the volatile memory (`RAM`) of the device and applies them. 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 "Select" button. □ Click the "Save" button.
Reload	Updates the fields with the values that are saved in the volatile memory (`RAM`) of the device.
Create	Adds a new table entry.
Remove	Removes the highlighted table entry.
Help	Opens the online help.

2.5 SNTP Server

With 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	When the function is on, the device operates as an SNTP server. Possible values: ▶ `On` ▶ `Off` (default setting) 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.

Parameters	Meaning
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 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..4042` (default setting `1`) If you set the value to `0`, the SNTP server of the device sends the SNTP packets in the same VLAN in which the management functions of the device can be accessed. See the `Basic Settings > Network` dialog.
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	Specifies whether the device disables the SNTP Broadcast server when the device is synchronized to the local clock. Possible values: ▶ `marked` The device disables the SNTP Broadcast 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 SNTP Broadcast 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, e.g. PTP. ▶ `syncToRemoteServer` The SNTP server is synchronized with an SNTP server that is higher than the device in a cascade.

Buttons

Button	Meaning
Set	Transfers the changes to the volatile memory (`RAM`) of the device and applies them. 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 "Select" button. □ Click the "Save" button.
Reload	Updates the fields with the values that are saved in the volatile memory (`RAM`) of the device.
Help	Opens the online help.

2.6 PTP

PTP (Precision Time Protocol) is a procedure described in the IEEE 1588-2008 standard that supplies the devices in the network with a precise time. The procedure enables the clocks in the network to be synchronized to a degree of precision of just a few 100 ns. The protocol uses Multicast communication, so the load on the network due to the PTP synchronization messages is negligible.

Using the “Best Master Clock” algorithm, the devices determine the devices in the network with the most accurate time which are to be used as a reference time source (Grandmaster). Subsequently the participating devices synchronize themselves with this reference time source.

If you want to transport PTP time accurately through your network, use devices with PTP hardware support exclusively on the transport paths.

The protocol differentiates between the following clocks:

- Boundary Clock (BC)
  This clock has any number of PTP ports and operates as both PTP master and PTP slave. In its respective network segment, the clock operates as an Ordinary Clock.
  - As PTP slave, the clock synchronizes itself with a PTP master that is higher than the device in the cascade.
  - As PTP master, the clock forwards the time information via the network to PTP slaves that are higher than the device in the cascade.
- Transparent Clock (TC)
  This clock has any number of PTP ports. In contrast to the Boundary Clock, this clock corrects the time information before forwarding it, without synchronizing itself.

The menu contains the following dialogs:

- PTP Global
- Boundary Clock
- Transparent Clock

2.7 PTP Global

With this dialog you can configure basic settings for PTP.

■ Operation IEEE 1588/PTP

Parameters	Meaning
Operation IEEE 1588/PTP	When the function is on, the device synchronizes its clock with PTP. If SNTP is activated in the device at the same time, PTP has priority. When the function is off, the device transmits the PTP synchronization messages without any correction at all device ports. Possible values: ▶ `On` ▶ `Off` (default setting)

■ Configuration IEEE 1588/PTP

Parameters	Meaning
PTP Mode	Specifies the PTP version and mode of the local clock. Possible values: ▶ `v2-transparent-clock` (default setting) ▶ `v2-boundary-clock`
Sync Lower Bound [ns]	Specifies the lower threshold value in nanoseconds for the path difference between the local clock and the reference time source (Grandmaster). If the path difference falls below this value one time, then the local clock is classed as synchronized. Possible values: ▶ `0..999999999` (default setting `30`)

Parameters	Meaning
Sync Upper Bound [ns]	Specifies the upper boundary in nanoseconds for the path difference between the local clock and the reference time source (Grandmaster). If the path difference exceeds this value one time, then the local clock is classed as unsynchronized. Possible values: ▶ `31..1000000000` (default setting `5000`)
Enable PTP Management	Activates/deactivates the PTP management defined in the PTP standard. Possible values: ▶ `marked` PTP management is activated. ▶ `unmarked` (default setting) PTP management is deactivated.

■ Status

Parameters	Meaning
Is Synchronized	Displays whether the local clock is synchronized with the reference clock (Grandmaster). The local clock is synchronized when the path difference between the local clock and the reference clock (Grandmaster) falls below the synchronization lower boundary one time. This status is kept until the path difference exceeds the synchronization upper boundary one time. You specify the synchronization boundaries in the "Configuration IEEE 1588/PTP" frame.
Max Offset Absolute [ns]	Displays the maximum path difference in nanoseconds that has occurred since the local clock was synchronized with the reference clock (Grandmaster).
PTP Time	Displays the date and time for the PTP time scale when the local clock is synchronized with the reference clock (Grandmaster). Format: `Month Day, Year  hh:mm:ss AM/PM`

■ Buttons

Button	Meaning
Set	Transfers the changes to the volatile memory (`RAM`) of the device and applies them. 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 "Select" button. □ Click the "Save" button.
Reload	Updates the fields with the values that are saved in the volatile memory (`RAM`) of the device.
Help	Opens the online help.

2.8 Boundary Clock

With this menu you can configure the Boundary Clock mode for the local clock.

The menu contains the following dialogs:

- Boundary Clock Global
- Boundary Clock Port

2.9 Boundary Clock Global

With this dialog you enter general, cross-port settings for the Boundary Clock mode for the local clock. The Boundary Clock (BC) operates according to PTP version 2 (IEEE 1588-2008).

The settings are effective when the local clock operates as the Boundary Clock (BC). For this, you select in the `Time > PTP > Global` dialog in the "PTP Mode" field the value `v2-boundary-clock`.

■ Operation IEEE 1588/PTPv2 BC

Parameters	Meaning
Priority 1	Specifies priority 1 for the port. Possible values: ▶ `0..255` (default setting `128`) The “Best Master Clock” algorithm first evaluates priority 1 of the participating devices in order to determine the reference time source (Grandmaster). The lower you set this value, the more probable it is that the device becomes the reference time source (Grandmaster). See “Grandmaster” on page 90.
Priority 2	Specifies priority 2 for the port. Possible values: ▶ `0..255` (default setting `128`) The “Best Master Clock” algorithm evaluates priority 2 of the participating devices if the previously evaluated criteria are the same for multiple devices. The lower you set this value, the more probable it is that the device becomes the reference time source (Grandmaster). See “Grandmaster” on page 90.
Domain Number	Assigns the device to a PTP domain. Possible values: ▶ `0..255` (default setting: `0`) The device transmits time information from and to devices in the same domain exclusively.

Status IEEE1588 / PTPv2 BC

Parameters	Meaning
Two Step	Displays that the clock is operating in Two-Step mode.
Steps Removed	Displays the number of communication paths passed through between the local clock of the device and the reference clock (Grandmaster). For a PTP slave, the value `1` means that the clock is connected with the reference time source (Grandmaster) directly via 1 communication path.
Offset to Master [ns]	Displays the measured difference (offset) between the local clock and the reference clock (Grandmaster) in nanoseconds. The PTP slave calculates the difference from the time information received. In Two-Step mode the time information consists of 2 PTP synchronization messages each, which the PTP master sends cyclically: ▶ The first synchronization message (sync message) contains an estimated value for the exact sending time of the message. ▶ The second synchronization message (follow-up message) contains the exact sending time of the first message. The PTP slave uses the two PTP synchronization messages to calculate the difference (offset) from the master and corrects its clock by this difference. Here the PTP slave also considers the "Delay to Master [ns]".
Delay to Master [ns]	Displays the delay when transmitting the PTP synchronization messages from the PTP master to the PTP slave in nanoseconds. The PTP slave sends a “Delay Request” packet to the PTP master and thus determines the exact sending time of the packet. When it receives the packet, the PTP master generates a time stamp and sends this in a “Delay Response” packet back to the PTP slave. The PTP slave uses the two packets to calculate the delay, and considers this starting from the next offset measurement. Prerequisite: The delay mechanism of the slave ports is set to the value `e2e`.

Identities

Parameters	Meaning
Clock Identity	Displays the device’s own identification number (UUID).
Parent Port Identity	Displays the port identification number (UUID) of the directly superior master device.
Grandmaster Identity	Displays the identification number (UUID) of the reference clock device.

The device displays the identities as byte sequences in hexadecimal notation.

The identification numbers (UUID) are made up as follows:

- The device identification number consists of the MAC address of the device, with the values `ff` and `fe` added between byte 3 and byte 4.
- The port UUID consists of the device identification number followed by a 16-bit port ID.

Grandmaster

This frame displays the criteria that the “Best Master Clock” algorithm evaluates when determining the reference clock (Grandmaster).

The algorithm first evaluates priority 1 of the participating devices. The device with the smallest value for priority 1 becomes the reference time source (Grandmaster).If the value is the same for multiple devices, the algorithm takes the next criterion, and if this is also the same, it takes the next criterion after this one. If all the values are the same for multiple devices, the smallest value in the "Clock Identifier" field decides which device becomes the reference time source (Grandmaster).

The device allows you to influence which device in the network becomes the reference clock (Grandmaster). To do this, you go to the "Operation IEEE1588 / PTPv2 BC" frame and modify the value in the "Priority 1" field or the "Priority 2" field.

Parameters	Meaning
Priority 1	Displays priority 1 for the device that is currently the reference time source (Grandmaster).
Clock Class	Class of the reference clock (Grandmaster). Parameter for the Best Master Clock algorithm.
Clock Accuracy	Estimated accuracy of the reference clock (Grandmaster). Parameter for the Best Master Clock algorithm.
Clock Variance	Variance of the reference clock, also known as the “offset scaled log variance”. Parameter for the Best Master Clock algorithm.
Priority 2	Displays priority 2 for the device that is currently the reference time source (Grandmaster).

Local Time Properties

Parameters	Meaning
Time Source	Specifies the time source from which the local clock gets its time information. Possible values: ▶ `atomicClock` ▶ `gps` ▶ `terrestrialRadio` ▶ `ptp` ▶ `ntp` ▶ `handSet` ▶ `other` ▶ `internalOscillator` (default setting)
UTC Offset [s]	Specifies the difference between the PTP time scale and the UTC. See the "PTP Timescale" field. Possible values: ▶ `-32768..32767` (default setting `35`)
UTC Offset Valid	Specifies whether the value entered in the "UTC Offset [s]" field is correct. Possible values: ▶ `marked` ▶ `unmarked` (default setting)
Time Traceable	Displays whether the device gets the time from a primary UTC reference, e.g. from an NTP server. Possible values: ▶ `marked` ▶ `unmarked`
Frequency Traceable	Displays whether the device gets the frequency from a primary UTC reference, e.g. from an NTP server. Possible values: ▶ `marked` ▶ `unmarked`
PTP Timescale	Displays whether the device uses the PTP time scale. Possible values: ▶ `marked` ▶ `unmarked` According to IEEE 1588, the PTP time scale is the TAI atomic time started on 01.01.1970. In contrast to UTC, TAI does not use leap seconds. On 01.01.2011, the difference between TAI and UTC was +34 seconds.

Buttons

Button	Meaning
Set	Transfers the changes to the volatile memory (`RAM`) of the device and applies them. 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 "Select" button. □ Click the "Save" button.
Reload	Updates the fields with the values that are saved in the volatile memory (`RAM`) of the device.
Help	Opens the online help.

2.10 Boundary Clock Port

With this dialog you specify special settings for the Boundary Clock (BC) on every individual device port.

The settings are effective when the local clock operates as the Boundary Clock (BC). For this, you select in the `Time > PTP > Global` dialog in the "PTP Mode" field the value `v2-boundary-clock`.

■ Table

Parameters	Meaning
Port	Displays the number of the device port to which the table entry relates.
PTP Enable	Specifies whether the device port transmits PTP synchronization messages. Possible values: ▶ `marked` (default setting) The device port sends and receives PTP synchronization messages. ▶ `unmarked` The device port blocks PTP synchronization messages.
PTP Status	Displays the current status of the device port. Possible values: ▶ `initializing` Initialization phase ▶ `faulty` Faulty mode: error in the PTP protocol. ▶ `disabled` PTP is disabled on the device port. ▶ `listening` Device port is waiting for PTP synchronization messages. ▶ `pre-master` PTP pre-master mode ▶ `master` PTP master mode ▶ `passive` PTP passive mode ▶ `uncalibrated` PTP uncalibrated mode ▶ `slave` PTP slave mode

Parameters	Meaning
Sync Interval	Specifies the interval in seconds at which the device port transmits PTP synchronization messages. Possible values: ▶ `0.25` ▶ `0.5` ▶ `1` (default setting) ▶ `2`
Delay Mechanism	Specifies the mechanism with which the device measures the delay for transmitting the PTP synchronization messages: Possible values: ▶ `disabled` The measurement of the delay for the PTP synchronization messages for the connected PTP devices is inactive. ▶ `E2E` (default setting) End-to-end: As the PTP slave, the device port measures the delay for the PTP synchronization messages to the PTP master. The device displays the measured value in the `Time > PTP >` Boundary Clock `> Global` dialog. ▶ `P2P` Peer-to-peer: The device measures the delay for the PTP synchronization messages for the connected PTP devices, provided that these devices support P2P. This mechanism saves the device from having to determine the delay again in the case of a reconfiguration. **Note:** If you specify the value `P2P`, in the "Network Protocol" field is the value `IEEE 802.3` available exclusively.
P2P Delay	Displays the measured Peer-to-Peer delay for the PTP synchronization messages. The prerequisite is that you select the value `p2p` in the "Delay Mechanism" field.
P2P Delay Interval	Specifies the interval in seconds at which the device port measures the Peer-to-Peer delay. Prerequisite: You have set the value `p2p` on this device port and on the port of the remote terminal. See the "Delay Mechanism" field in the `Time >` PTP `> Boundary Clock > Global` dialog. Possible values: ▶ `1` (default setting) ▶ `2` ▶ `4` ▶ `8` ▶ `16` ▶ `32`

Parameters	Meaning
Network Protocol	Specifies which protocol the device port uses to transmit the PTP synchronization messages. If you change the value for a port, the device changes after clicking the "Set" button every port to this value. Possible values: ▶ `IEEE 802.3` (default setting) ▶ `UDP/IPv4` This value is available solely if in the "Delay Mechanism" field another value than `P2P` is specified.
Announce Interval [s]	Specifies the interval in seconds at which the device port transmits messages for the PTP topology discovery. Assign the same value to all devices of a PTP domain. Possible values: ▶ `1` ▶ `2` (default setting) ▶ `4` ▶ `8` ▶ `16`
Announce Timeout	Specifies the timeout for the announce interval. Possible values: ▶ `2..10` (default setting `3`) The value represents the number of the announce intervals. Assign the same value to all devices of a PTP domain. Example: For the standard setting (Announce Interval = 2 s and Announce Timeout = 3), the Timeout is 3 x 2 s = 6 s.
E2E Delay Interval [s]	Displays the interval in seconds at which the device port measures the End-to-End delay: ▶ If the device port is operating as the PTP master, the device assigns the port the value `8`. ▶ If the device port is operating as the PTP slave, the value is specified by the PTP master connected to the port.

Parameters	Meaning
V1 Hardware Compatibility	Specifies whether the device port adjusts the length of the PTP synchronization messages when you have set in the "Network Protocol" field the value `UDP/IPv4`. It is possible that other devices in the network expect the PTP synchronization messages to be the same length as PTPv1 messages. Possible values: ▶ `auto` (default setting) The device automatically detects whether other devices in the network expect the PTP synchronization messages to be the same length as PTPv1 messages. If this is the case, the device extends the length of the PTP synchronization messages before transmitting them. ▶ `on` The device extends the length of the PTP synchronization messages before transmitting them. ▶ `off` The device transmits PTP synchronization messages without changing the length.
Asymmetry	Corrects the measured delay value corrupted by asymmetrical transmission paths. Possible values: ▶ `-2000000000..2000000000` (default setting: `0`) The value represents the delay symmetry in nanoseconds. A measured delay value of x ns corresponds to an asymmetry of x·2 ns. The value is positive if the delay from the PTP master to the PTP slave is longer than in the opposite direction.
VLAN	Specifies the VLAN ID with which the device marks the PTP synchronization messages on this port. Possible values: ▶ `none` (default setting) The device transmits PTP synchronization messages without a VLAN tag. ▶ `0..4042` You specify VLANs that you have already set up in the device from the list. Verify that that the device port is a member of the VLAN. See the `Switching > VLAN > Configuration` dialog.
VLAN Priority	Specifies the priority with which the device transmits the PTP synchronization messages marked with a VLAN ID (Layer 2, IEEE 802.1p). Possible values: ▶ `0..7` (default setting `4`) If you have specified in the "VLAN" field the value `none`, the device ignores the VLAN priority.

Buttons

Button	Meaning
Set	Transfers the changes to the volatile memory (RAM) of the device and applies them. 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 "Select" button. ☐ Click the "Save" button.
Reload	Updates the fields with the values that are saved in the volatile memory (RAM) of the device.
Help	Opens the online help.

2.11 Transparent Clock

With this menu you can configure the Transparent Clock mode for the local clock.

The menu contains the following dialogs:

- ▶ Transparent Clock Global
- ▶ Transparent Clock Port

2.12 Transparent Clock Global

With this dialog you can enter general, cross-port settings for the Transparent Clock mode for the local clock. The Transparent Clock (BC) operates according to PTP version 2 (IEEE 1588-2008).

The settings are effective when the local clock operates as the Transparent Clock (TC). For this, you select in the `Time > PTP > Global` dialog in the "PTP Mode" field the value `v2-transparent-clock`.

■ Operation IEEE 1588/PTPv2 TC

Parameters	Meaning
Delay Mechanism	Specifies the mechanism with which the device measures the delay for transmitting the PTP synchronization messages. Possible values: ▶ `E2E` (default setting) As the PTP slave, the device port measures the delay for the PTP synchronization messages to the PTP master. The device displays the measured value in the `Time > PTP > Transparent Clock > Global` dialog. ▶ `P2P` The device measures the delay for the PTP synchronization messages for every connected PTP device, provided that the device supports P2P. This mechanism saves the device from having to determine the delay again in the case of a reconfiguration. If you specify this value, in the "Network Protocol" field is the value `IEEE 802.3` available exclusively. ▶ `E2E-optimized` Like `E2E`, with the following special characteristics: – The device transmits the delay requests of the PTP slaves solely to the PTP master, even though these requests are multicast messages. The device thus spares the other devices from unnecessary multicast requests. – If the master-slave topology changes, the device relearns the device port for the PTP master as soon as it receives a synchronization message from another PTP master. – If the device does not know a PTP master, it transmits delay requests to the device ports. ▶ `disabled` The delay measuring is disabled on the device port. The device discards messages for the delay measuring.
Primary Domain	Assigns the device to a PTP domain. Possible values: ▶ `0..255` (default setting: `0`) The device transmits time information from and to devices in the same domain exclusively.
Network Protocol	Specifies which protocol the device port uses to transmit the PTP synchronization messages. Possible values: ▶ `IEEE 802.3` (default setting) ▶ `UDP/IPv4` This value is available solely if in the "Delay Mechanism" field another value than `P2P` is specified.

Parameters	Meaning
Multi Domain Mode	Specifies the PTP domains in which the device corrects PTP synchronization messages. Possible values: ▶ `marked` The device corrects PTP synchronization messages in every PTP domain. ▶ `unmarked` (default setting) The device corrects PTP synchronization messages in the primary PTP domain exclusively. See the "Primary Domain" field.
VLAN ID	Specifies the VLAN ID with which the device marks the PTP synchronization messages on this port. Possible values: ▶ `none` (default setting) The device transmits PTP synchronization messages without a VLAN tag. ▶ `0..4042` You specify VLANs that you have already set up in the device from the list.
VLAN Priority	Specifies the priority with which the device transmits the PTP synchronization messages marked with a VLAN ID (Layer 2, IEEE 802.1p). Possible values: ▶ `0..7` (default setting `4`) If you have specified the value `none` in the "VLAN ID" field the device ignores the specified value.

■ Local Synchronization

Parameters	Meaning
Syntonize	Specifies whether the device synchronizes the frequency of the Transparent Clock with the PTP master. Possible values: ▶ `marked` (default setting) The device synchronizes the frequency. ▶ `unmarked` The frequency remains constant.
Synchronize local clock	Specifies whether the device synchronizes the local system time. Possible values: ▶ `marked` The device synchronizes the local system time with the time received via PTP. The prerequisite is that the function in the "Syntonize" field is activated. ▶ `unmarked` (default setting) The local system time remains constant.

Parameters	Meaning
Current Master	Displays the port identification number (UUID) of the master device on which the device synchronizes its frequency. If the value contains zeros exclusively, this is because: ▶ The "Syntonize" function is deactivated. or ▶ The device cannot find a PTP master.
Offset to Master [ns]	Displays the measured difference (offset) between the local clock and the PTP master in nanoseconds. The device calculates the difference from the time information received. Prerequisite: The "Synchronize local clock" function is activated.
Delay to Master [ns]	Displays the delay when transmitting the PTP synchronization messages from the PTP master to the PTP slave in nanoseconds. Prerequisite: ▶ The "Synchronize local clock" function is activated. ▶ In the "Delay Mechanism" field, the value `e2e` is selected.

Status IEEE1588 / PTPv2 TC

Parameters	Meaning
Clock Identity	Displays the device’s own identification number (UUID). The device displays the identities as byte sequences in hexadecimal notation. The device identification number consists of the MAC address of the device, with the values `ff` and `fe` added between byte 3 and byte 4.

Buttons

Button	Meaning
Set	Transfers the changes to the volatile memory (`RAM`) of the device and applies them. 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 "Select" button. □ Click the "Save" button.
Reload	Updates the fields with the values that are saved in the volatile memory (`RAM`) of the device.
Help	Opens the online help.

2.13 Transparent Clock Port

With this dialog you specify special settings for the Transparent Clock (TC) on each individual device port.

The settings are effective when the local clock operates as the Transparent Clock (TC). For this, you select in the `Time > PTP > Global` dialog in the "PTP Mode" field the value `v2-transparent-clock`.

■ Table

Parameters	Meaning
Port	Displays the number of the device port to which the table entry relates.
PTP Enable	Specifies whether the device port transmits PTP synchronization messages. Possible values: ▶ `marked` (default setting) The device port sends and receives PTP synchronization messages. ▶ `unmarked` The device port blocks PTP synchronization messages.
P2P Delay Interval [s]	Specifies the interval in seconds at which the device port measures the Peer-to-Peer delay. Prerequisite: You have set the value `p2p` on this device port and on the port of the remote terminal. See the "Delay Mechanism" field in the `Time >` PTP `> Transparent Clock > Global` dialog. Possible values: ▶ `1` (default setting) ▶ `2` ▶ `4` ▶ `8` ▶ `16` ▶ `32`

Parameters	Meaning
P2P Delay	Displays the measured Peer-to-Peer delay for the PTP synchronization messages. The prerequisite is that you select the value `p2p` in the "Delay Mechanism" field.
Asymmetry	Corrects the measured delay value corrupted by asymmetrical transmission paths. Possible values: ▶ `-2000000000.. 2000000000` (default setting: `0`) The value represents the delay symmetry in nanoseconds. A measured delay value of x ns corresponds to an asymmetry of x·2 ns. The value is positive if the delay from the PTP master to the PTP slave is longer than in the opposite direction.

■ Buttons

Button	Meaning
Set	Transfers the changes to the volatile memory (`RAM`) of the device and applies them. 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 "Select" button. ☐ Click the "Save" button.
Reload	Updates the fields with the values that are saved in the volatile memory (`RAM`) of the device.
Help	Opens the online help.

3 Device Security

This menu allows you to specify the settings for the access to the device.

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 functions 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 method 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
Number of 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.
Minimum 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" field. The prerequisite is that you mark the "Policy Check" checkbox.

Parameters	Meaning
Minimum Upper Cases	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.
Minimum Lower Cases	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.
Minimum Numbers	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.
Minimum Special Characters	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 access to the management functions of 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 "Create" 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 always 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 minimum length of the password is specified in the "Configuration" frame. The device differentiates between upper and lower case. If you mark the checkbox in the "Policy Check" field, the device checks the password according to the policy specified in the "Password Policy" frame. The device always checks the minimum length of the password, even if the checkbox in the "Policy Check" field is unmarked.

Parameters	Meaning
Access Role	Specifies the access 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 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. ▶ `guest` (default value) 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.
User locked	Locks/unlocks the user's access to the management functions of the device. Possible values: ▶ `marked` The user's access is locked. The device automatically locks a user if the user makes too many unsuccessful login attempts. ▶ `unmarked` (default value) The user's access is unlocked.
Policy Check	Specifies whether the device checks the password according to the specified policy when it is being set up or changed. Possible values: ▶ `marked` The device checks the password according to the policy specified in the "Password Policy" frame. ▶ `unmarked` (default value) The device accepts the password without checking it.

Parameters	Meaning
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

Button	Meaning
Set	Transfers the changes to the volatile memory (`RAM`) of the device and applies them. 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 "Select" button. □ Click the "Save" button.
Set and back	Transfers the changes to the volatile memory (`RAM`) of the device and goes back to the previous dialog.
Back	Displays the previous dialog again. Changes are lost.
Reload	Updates the fields with the values that are saved in the volatile memory (`RAM`) of the device.
Remove	Removes the highlighted table entry.
Create	Adds a new table entry.
Help	Opens the online help.

3.2 Authentication List

The device allows users to access its management functions when they log in with valid login data exclusively. The device authenticates the users either using the local user management or with a RADIUS server in the network.

With the port-based access control according to IEEE 802.1X, the device allows connected terminal devices to access the network if they log in with valid login data. The device authenticates the terminal devices either with a RADIUS server in the network or with an integrated authentication server implemented in the device.

In this dialog you manage the authentication lists. In a list you specify which method the device uses for the authentication. Here you have the option to differentiate the application with which the device is accessed, e.g. via a console or with the graphical user interface.

Table

Parameters	Meaning
Name	Displays the name of the list. To create a new list, click the "Create" button. Possible values: ▶ Alphanumeric ASCII character string with 1..32 characters
Policy 1 Policy 2 Policy 3 Policy 4 Policy 5	Displays the authentication method that the device uses for access via the application specified in the "Dedicated Applications" field. To change the value, click the relevant field. The device gives you the option of a fall-back solution. For this, you specify one other method in each of the "Policy 2" to "Policy 5" fields. If the authentication with the specified method is unsuccessful, the device uses 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. ▶ `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 rejects the authentication request from the user. ▶ `ias` The device authenticates the terminal devices logging in via 802.1X with the integrated authentication server (IAS) implemented on the device. The integrated authentication server manages the login data in a separate database, see the `Network Security > 802.1X Port Authentication > Integrated Authentication Server` dialog.
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 "Allocate Applications" button. 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 access to the management functions 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

Button	Meaning
Set	Transfers the changes to the volatile memory (`RAM`) of the device and applies them. 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 "Select" button. □ Click the "Save" button.
Set and back	Transfers the changes to the volatile memory (`RAM`) of the device and goes back to the previous dialog.
Back	Displays the previous dialog again. Changes are lost.
Reload	Updates the fields with the values that are saved in the volatile memory (`RAM`) of the device.
Remove	Removes the highlighted table entry.
Create	Adds a new table entry.
Allocate Applications	Opens the "Allocate Applications" window. ▶ The "Possible Applications" field displays the applications that can be allocated to the highlighted list. ▶ The "Dedicated Applications" field displays the applications that are allocated to the highlighted list. ▶ Buttons: – > : Moves the highlighted entries from the "Possible Applications" field to the "Dedicated Applications" field. – >> : Moves all entries to the "Dedicated Applications" field. – < : Moves the highlighted entries from the "Dedicated Applications" field to the "Possible Applications" field. – << : Moves all entries to the "Possible Applications" field.
Help	Opens the online help.

3.3 Management Access

This dialog allows you to set up the server services with which users or applications can access the management functions of the device. You also have the option of restricting the access for IP address ranges and individual management services.

The menu contains the following dialogs:

- Server
- IP Access Restriction
- Web
- Command Line Interface
- SNMPv1/v2 Community

3.4 Server

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

The dialog contains the following tabs:

- Information
- SNMP
- Telnet
- HTTP
- HTTPS
- SSH

3.4.1 Information

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

■ Table

Parameters	Meaning
Function	Displays the name of the server services. Possible values: ▶ SNMPv1 enabled This server service allows access to the device through SNMP version 1, see the "SNMP" tab. ▶ SNMPv2 enabled This server service allows access to the device through SNMP version 2, see the "SNMP" tab. ▶ SNMPv3 enabled This server service allows access to the device through SNMP version 3, see the "SNMP" tab. ▶ Telnet Server This server service allows access to the device through Telnet, see the "Telnet" tab. ▶ HTTP Server This server service allows access to the device through HTTP, see the "HTTP" tab. ▶ HTTPS Server This server service allows access to the device through HTTPS, see the "HTTPS" tab. ▶ SSH This server service allows access to the device through SSH, see the "SSH" tab.
Status	Displays whether the device port is currently physically enabled or disabled. Possible values: ▶ `marked` Server service is enabled. ▶ `unmarked` Server service is disabled.

■ Buttons

Button	Meaning
Set	Transfers the changes to the volatile memory (`RAM`) of the device and applies them. 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 "Select" button. □ Click the "Save" button.
Reload	Updates the fields with the values that are saved in the volatile memory (`RAM`) of the device.
Help	Opens the online help.

3.4.2 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 access to the management functions of the device with SNMP-based applications, for example with the graphical user interface.

■ Configuration

Parameters	Meaning
SNMPv1 enabled	Activates/deactivates the access to the device with SNMP version 1. Possible values: ▶ `marked` (default setting) Access activated. ▶ `unmarked` Access deactivated. You specify the community name in the `Device Security > Management Access > SNMPv1/v2 Community` dialog.
SNMPv2 enabled	Activates/deactivates the access to the device with SNMP version 2. Possible values: ▶ `marked` (default setting) Access activated. ▶ `unmarked` Access deactivated. You specify the community name in the `Device Security > Management Access > SNMPv1/v2 Community` dialog.
SNMPv3 enabled	Activates/deactivates the access to the device with SNMP version 3. Possible values: ▶ `marked` (default setting) Access activated. ▶ `unmarked` Access deactivated. Use this function, for example, for the Industrial HiVision network management software to make changes to the settings.

Parameters	Meaning
Port Number	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 "Set" button. □ Select in the `Basic Settings > Load/Save` dialog the active configuration profile and click the "Save" button. □ Restart the device.
SNMPover802 enabled	Activates/deactivates the access to the device through SNMP over IEEE-802. Possible values: ▶ `unmarked` (default setting) Access inactive. ▶ `marked` Access active. The HiDiscovery software uses SNMP over IEEE-802 to access devices without an IP address.

■ Buttons

Button	Meaning
Set	Transfers the changes to the volatile memory (`RAM`) of the device and applies them. 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 "Select" button. □ Click the "Save" button.
Reload	Updates the fields with the values that are saved in the volatile memory (`RAM`) of the device.
Help	Opens the online help.

3.4.3 Telnet

This tab allows you to specify settings for the Telnet server of the device and to switch the server on/off.

The Telnet server enables access to the management functions of the device with the Command Line Interface via a Telnet connection.

■ Operation

Parameters	Meaning
Operation	If the function is on, the Telnet server is activated. Possible values: ▶ `Off` Server is deactivated. ▶ `On` (default setting) Server is activated. You can access the management functions of the device via Telnet.

■ Configuration

Parameters	Meaning
TCP Port	Specifies the number of the TCP port on which the server receives 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.
Connection Count	Displays how many clients are currently logged on to the server. Possible values: ▶ `0..5` (default setting: `5`)

Parameters	Meaning
Max. Number of Connections	Specifies how many clients can be logged on to the server at the same time. Possible values: ▶ `0..5` (default setting: `5`)
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. The user remains logged on when inactive. A change in the value takes effect the next time a user logs into the device.

Buttons

Button	Meaning
Set	Transfers the changes to the volatile memory (`RAM`) of the device and applies them. 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 "Select" button. □ Click the "Save" button.
Reload	Updates the fields with the values that are saved in the volatile memory (`RAM`) of the device.
Help	Opens the online help.

3.4.4 HTTP

This tab allows you to specify settings for the HTTP server of the device and to switch the server on/off.

The HTTP server provides the graphical user interface (GUI) via an HTTP connection. The graphical user interface communicates with the device based on SNMP and enables access to the management functions.

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

■ Operation

Parameters	Meaning
Operation	Enables/disables the HTTP server. Possible values: ▶ `Off` The server is disabled. ▶ `On` (default setting) The server is enabled. The management functions of the device are accessible through an unencrypted HTTP connection.

Note: When you change the setting and click the "Set" button, the device ends the session and terminates the connection. Then login again.

■ Configuration

Parameters	Meaning
TCP Port	Specifies the number of the TCP port on which the server receives requests from clients. Possible values: ▶ `1..65535` (default setting `80`) Exception: Port `2222` is reserved for internal functions. The server restarts automatically after the port is changed. In the process, the device terminates open connections to the server.

Buttons

Button	Meaning
Set	Transfers the changes to the volatile memory (`RAM`) of the device and applies them. 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 "Select" button. □ Click the "Save" button.
Reload	Updates the fields with the values that are saved in the volatile memory (`RAM`) of the device.
Help	Opens the online help.

3.4.5 HTTPS

This tab allows you to specify settings for the HTTPS server of the device and to switch the server on/off.

The HTTP server provides the graphical user interface (GUI) via an encrypted HTTP connection. The graphical user interface communicates with the device based on SNMP via the encrypted HTTP connection and enables access to the management functions.

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

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.

■ Operation

Parameters	Meaning
Operation	Enables/disables the HTTPS server. Possible values: ▶ `Off` The server is disabled. ▶ `On` (default setting) The server is enabled. The management functions of the device are accessible through an encrypted HTTPS connection. The device can then be started if there is a certificate on the device exclusively.

Note: When you change the setting and click the "Set" button, the device ends the session and terminates the connection. Then login again.

Note: When you switch off the server, the connection between the graphical user interface (GUI) and the device is interrupted. To continue working with the graphical user interface, switch the server on again via the Command Line Interface (CLI).

■ Configuration

Parameters	Meaning
TCP Port	Specifies the number of the TCP port on which the server receives requests from clients. Possible values: ▶ `1..65535` (default setting `443`) Exception: Port `2222` is reserved for internal functions. The server restarts automatically after the port is changed. In the process, the device terminates open connections to the server.

■ 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	Creates a digital certificate on the device. To get the server to use this certificate, click the "Create" button and restart the server. You can restart the server via the Command Line Interface (CLI) exclusively. Alternatively, you have the option to copy your own certificate to the device—see the "Certificate Import" dialog.
Delete	Deletes the digital certificate. To permanently remove the certificate from the device, save the changes. In the process, the device switches off the HTTPS server.
Oper Status	Displays whether the device is generating a digital certificate at the moment. Possible values: ▶ `none` The device does not create a certificate. ▶ `busy` The device does not create a certificate at the moment. It is possible that another user triggered this action.

Note: In the Web browser, a warning appears when you are loading the graphical user interface if you are using a certificate that has not been verified by a certifying organization. To load the graphical user interface, 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. X.509 certificates (PEM) are permitted. The device gives you the following options for copying the certificate to the device: ▶ Import from the PC If the certificate is on your PC or on a network drive, click the " … " button and select the file that contains the certificate. ▶ Import from a TFTP server If the certificate is on a TFTP server, enter 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 enter the URL for the file in the following form: – `scp://` or `sftp://<IP address>/<path>/<file name>` When you click the "Import" button, the device displays the "Authentication" window. There you enter "Username" and "Password", to login to the server. – `scp://` or `sftp://<user>:<password>@<IP address>/<path>/<file name>`
…	Displays the "Open" dialog. Here you select the certificate file to be copied if the file is located on your PC or on a network drive.
Import	Copies the certificate specified in the "URL" field to the device. To get the server to use this certificate, click the "Set" button and restart the server. Restarting the server is possible solely through the Command Line Interface (CLI).

■ Buttons

Button	Meaning
Set	Transfers the changes to the volatile memory (`RAM`) of the device and applies them. 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 "Select" button. ☐ Click the "Save" button.
Reload	Updates the fields with the values that are saved in the volatile memory (`RAM`) of the device.
Help	Opens the online help.

3.4.6 SSH

This tab allows you to switch the SSH server on/off in the device and specify its settings.

The server works with SSH version 2. The SSH server enables access to the management functions of the device with the Command Line Interface via an encrypted connection (secure shell).

The SSH server identifies itself to the clients using its public RSA or DSA key. When first setting up the connection, the client program displays the user the fingerprint of this key. The fingerprint contains a hexadecimal number sequence that is easy to check. When you make this number sequence available to the users via a reliable channel, they have the option to compare both fingerprints. If the number 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 and DSA directly on the device. Otherwise you have the option to copy your own keys to the device in PEM format.

■ Operation

Parameters	Meaning
Operation	If the function is on, encrypted access to the management functions of the device is possible via the Command Line Interface (CLI). Possible values: ▶ `Off` Server is deactivated. ▶ `On` (default setting) Server is activated. You can access the management functions of the device via SSH. The server can solely then be started if there is an RSA or DSA signature on the device. When the function is off, existing connections remain in place. However, the device prevents new connections from being set up.

■ Configuration

Parameters	Meaning
TCP Port	Specifies the number of the TCP port on which the server receives 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.
Session Count	Displays how many connections to the server are currently set up.
Max. Number of Sessions	Specifies the maximum number of connections to the server that can be set up simultaneously. Possible values: ▶ `1..5` (default setting `5`)
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: ▶ `1..160` (default setting: `5`) The value `0` deactivates the function. The user remains logged on when inactive. A change in the value takes effect the next time a user logs into the device.

■ Fingerprint

The fingerprint is an easily verified hexadecimal number sequence that uniquely identifies the RSA or DSA key (host key) of the SSH server.

Parameters	Meaning
DSA	Number sequence of the public DSA key of the server.
RSA	Number sequence of the public RSA key of the server.

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

■ Signature

Parameters	Meaning
DSA Present	Displays whether a DSA key (host key) is present on the device. Possible values: ▶ `marked` A key is present. ▶ `unmarked` No key is present.
RSA Present	Displays whether an RSA key (host key) is present on the device. Possible values: ▶ `marked` A key is present. ▶ `unmarked` No key is present.
Create	Creates a key (host key) on the device. The device creates the key solely when the server is deactivated. Length of the key created: ▶ 2048 bit (RSA) ▶ 1024 bit (DSA) To get the server to use the key created, click the "Set" button. Then you switch the server `on`. Alternatively, you have the option to copy your own key to the device in PEM format—see the "Key Import" frame.
Delete	Removes the key (host key) from the device. To permanently remove the key from the device, click the "Set" button. Until you restart the server, the existing connections remain in place. However, the device prevents new connections from being set up.
Oper Status	Displays whether the device is generating a key (host key) at the moment. Possible values: ▶ `none` The device does not create a key. ▶ `busy` The device does not create a key at the moment. It is possible that another user triggered this action.

Key Import

Parameters	Meaning
URL	Specifies the path and file name of your own DSA/RSA key (host key). The device accepts the DSA/RSA key if it has the following key length: ▶ 2048 bit (RSA) ▶ 1024 bit (DSA) The device gives you the following options for copying the key to the device: ▶ Import from the PC If the key is on your PC or on a network drive, click the " … " button and select the file that contains the key (host key). ▶ Import from a TFTP server If the key is on a TFTP server, enter 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 enter the URL for the file in the following form: – `scp://` or `sftp://<IP address>/<path>/<file name>` When you click the "Import" button, the device displays the "Authentication" window. There you enter "Username" and "Password", to login to the server. – `scp://` or `sftp://<user>:<password>@<IP address>/<path>/<file name>`
…	Displays the "Open" dialog. Here you select the key to be copied if the file is located on your PC or on a network drive.
Import	Copies the key (host key) specified in the "URL" field to the device. To get the server to use this key, click the "Set" button and restart the server.

Buttons

Button	Meaning
Set	Transfers the changes to the volatile memory (`RAM`) of the device and applies them. 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 "Select" button. □ Click the "Save" button.
Reload	Updates the fields with the values that are saved in the volatile memory (`RAM`) of the device.
Help	Opens the online help.

3.5 IP Access Restriction

This dialog enables you to restrict the access to the management functions of the device to specific IP address ranges and selected IP-based applications.

- If the function is switched off, you can access the management functions of the device from any IP address and via all applications.
- If the function is switched on, the access is restricted. You access the management functions under the following conditions:
  - 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	If the function is on, the access to the management functions of the device is restricted. Possible values: ▶ `Off` (default setting) ▶ `On` Access to the management functions of the device is restricted.

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 CLI through the V.24 interface of the device.

■ Table

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

Parameters	Meaning
Index	Displays a sequential number to which the table entry relates. The device automatically defines this number. Possible values: ▶ `1..16` 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.
IP Address Range	Specifies the IP address range for which you specify the access to the management functions with this table entry. Possible values: ▶ Valid IPv4 address and netmask in CIDR notation ▶ `0.0.0.0/0` (default setting for newly created entries)
HTTP	Activates/deactivates the HTTP access. Possible values: ▶ `marked` (default setting) Access is activated for the adjacent IP address range. ▶ `unmarked` Access is deactivated.
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.

Parameters	Meaning
SSH	Activates/deactivates the SSH access. 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 access to its management functions to the adjacent IP address range and the selected IP-based applications. ▶ `unmarked` Table entry is deactivated.

In the default setting, there is an entry in the table for the IP address range `0.0.0.0/0`, in which the access for all applications is activated. This table entry allows you access to the device regardless of your location, e.g. to initially configure the function. You have the option to change or delete this table entry. When you create a new table entry it has the same properties.

Note: To start the graphical user interface in a web browser you require the "HTTP" or "HTTPS" service, see the `Device Security > Management Access > Server` dialog.

■ Buttons

Button	Meaning
Set	Transfers the changes to the volatile memory (`RAM`) of the device and applies them. 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 "Select" button. □ Click the "Save" button.
Reload	Updates the fields with the values that are saved in the volatile memory (`RAM`) of the device.
Create	Adds a new table entry.
Remove	Removes the highlighted table entry.
Help	Opens the online help.

3.6 Web

With this dialog you specify settings for the graphical user interface (Web-based 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

Button	Meaning
Set	Transfers the changes to the volatile memory (`RAM`) of the device and applies them. 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 "Select" button. ☐ Click the "Save" button.
Reload	Updates the fields with the values that are saved in the volatile memory (`RAM`) of the device.
Help	Opens the online help.

3.7 Command Line Interface

With 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

3.7.1 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: `(EES)` Changes to this setting are immediately effective in the active CLI session.
V.24 Timeout [min]	Defines 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 into the device. For Telnet and SSH, you specify the timeout in the `Device Security >` Management Access `> Server` dialog.

■ Buttons

Button	Meaning
Set	Transfers the changes to the volatile memory (`RAM`) of the device and applies them. 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 "Select" button. □ Click the "Save" button.
Reload	Updates the fields with the values that are saved in the volatile memory (`RAM`) of the device.
Help	Opens the online help.

3.7.2 Login Banner

This tab page allows you to 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 on this tab page, 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	When this function is on, the device displays the text information specified in the "Banner Text" field to the users that login to the device via the Command Line Interface (CLI). When the function is off, the CLI start screen displays information about the device. The text information in the "Banner Text" field is kept. Possible values: ▶ `Off` (default setting) ▶ `On`

■ Banner Text

Parameters	Meaning
Banner Text	Defines the character string that the device displays in the Command Line Interface at the start of every command line. Possible values: ▶ Alphanumeric ASCII character string with 0..1024 characters (`0x20..0x7E`) including space character ▶ Tab `\t` ▶ Line break `\n`
Remaining Characters	Displays how many characters are still remaining in the "Banner Text" field for the text information. Possible values: ▶ `1024..0`

Buttons

Button	Meaning
Set	Transfers the changes to the volatile memory (`RAM`) of the device and applies them. 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 "Select" button. □ Click the "Save" button.
Reload	Updates the fields with the values that are saved in the volatile memory (`RAM`) of the device.
Help	Opens the online help.

3.8 SNMPv1/v2 Community

With 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

Button	Meaning
Set	Transfers the changes to the volatile memory (`RAM`) of the device and applies them. 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 "Select" button. □ Click the "Save" button.
Reload	Updates the fields with the values that are saved in the volatile memory (`RAM`) of the device.
Help	Opens the online help.

3.9 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	When this function is on, the device displays a greeting or information text in the login dialog of the graphical user interface (GUI) and of the Command Line Interface (CLI). Possible values: ▶ `Off` (default setting) 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. ▶ `On` The device displays the text specified in the "Banner Text" field in the login dialog.

Banner Text

Parameters	Meaning
Banner Text	Specifies the greeting or 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 character ▶ Tab `\t` ▶ Line break `\n`
Remaining Characters	Displays how many characters are still remaining in the "Banner Text" field. Possible values: ▶ `512..0`

Buttons

Button	Meaning
Set	Transfers the changes to the volatile memory (`RAM`) of the device and applies them. 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 "Select" button. □ Click the "Save" button.
Reload	Updates the fields with the values that are saved in the volatile memory (`RAM`) of the device.
Help	Opens the online help.

4 Network Security

This menu allows you to specify settings which help to protect the network against undesired or dangerous access.

The menu contains the following dialogs:

- Port Security
- 802.1X Port Authentication
- RADIUS
- DoS

4.1 Port Security

The device allows you to transmit data packets from desired sources. 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 sources and registers this event. If the "Auto Disable" function is also enabled, the device disables the port. This restriction makes MAC Spoofing attacks more difficult.

In this dialog a "Wizard" helps you to connect the device ports with one or more desired sources. In the device these addresses are known as "Static Addresses".

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 Addresses". 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 Addresses", the device always 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	When this function is enabled, the device checks the VLAN ID and MAC address of the source before it transmits a data packet. Possible values: ▶ `On` The device transmits solely a received data packet if its source is desired on the relevant device port. Also activate the checking of the source on the relevant device ports. ▶ `Off` (default setting) The device transmits every received data packet without checking the source.

Table

Parameters	Meaning
Port	Displays the number of the device port to which the table entry relates.
Active	Activates/deactivates the checking of the source on the device port. Possible values: ▶ `marked` The device checks every data packet received on the device 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.
Violation Traps	Specifies if the device sends an SNMP trap when it discards data packets from an undesired source on the port. Possible values: ▶ `marked` The device sends an SNMP trap. ▶ `unmarked` (default setting) The device does not send an SNMP trap. The prerequisite for sending SNMP traps is that you enable the function in the `Diagnostics > Status Configuration > Alarms (Traps)` dialog and at least 1 SNMP manager is specified.

Parameters	Meaning
Violation Trap Frequency [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 Addresses"). 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. Prerequisite is that in the `Diagnostics > Ports >` Auto Disable dialog you mark the "Port Security" checkbox in the "Configuration" frame. Possible values: ▶ `0..600` (default setting: `600`) The value `0` deactivates the automatic registering of sources on this port.
Static Limit	Specifies the upper limit for the number of sources connected to the port ("Static Addresses"). The "Wizard" helps you to connect the port with one or more desired sources. Possible values: ▶ `0..64` (default setting: `64`) The value `0` prevents you from connecting a source with the port.
Current Dynamic	Displays the number of senders that the device automatically detected. See the wizard, field "Dynamic Addresses".
Current Static	Displays the number of senders that are linked with the port. See the wizard, field "Static Addresses".
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.
Trapped Violations	Displays the number of discarded data packets on this device port that caused the device to send an SNMP trap.

■ Buttons

Button	Meaning
Set	Transfers the changes to the volatile memory (`RAM`) of the device and applies them. 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 "Select" button. □ Click the "Save" button.
Reload	Updates the fields with the values that are saved in the volatile memory (`RAM`) of the device.
Wizard	Opens the "Port Security" dialog. In the "Port Security" dialog you assign the permitted MAC addresses to a port.
Help	Opens the online help.

4.1.1 Wizard

■ Select Port

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

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

■ Addresses

The Wizard helps you to connect the device ports with one or more desired sources. When you have specified the settings, click the "Finish" button. To save the changes, click in the `Network Security > Port Security` the "Set" button.

Parameters	Meaning
VLAN	Specifies the VLAN ID of the desired source. Possible values: ▶ `1..4042` To transfer the VLAN ID and the MAC address to the "Static Addresses" field, click the "Add" button.
MAC Address	Specifies the MAC address of the desired source. Possible values: ▶ Valid unicast MAC address 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` To transfer the VLAN ID and the MAC address to the "Static Addresses" field, click the "Add" button.
Add	Transfers the values specified in the "VLAN ID" and "MAC Address" fields to the "Static Addresses" field.

Parameters	Meaning
Static Addresses	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.
Remove	Removes the entries highlighted in the "Static Addresses" field.
<	Moves the entries highlighted in the "Dynamic Addresses" field to the "Static Addresses" field.
<<	Moves every entry from the "Dynamic Addresses" field to the "Static Addresses" field. If the "Dynamic Addresses" field contains more entries than are allowed in the "Static Addresses" field, the device moves the foremost entries until the upper limit is reached.
Dynamic Addresses	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 Addresses" field. In this way, you connect relevant sender 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.

■ Buttons

Button	Meaning
Back	Displays the previous page again. Changes are lost.
Next	Saves the changes and opens the next page.
Finish	Saves the changes and closes the wizard.
Cancel	Closes the Wizard. Changes are lost.

After closing the Wizard, click the "Set" button to save your settings.

4.2 802.1X Port Authentication

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

The device supports the following methods to authenticate terminal devices:

- `radius`
  A RADIUS server in the network authenticates the terminal devices.
- `ias`
  The Integrated Authentication Server (IAS) implemented in the device authenticates the terminal 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
- Integrated Authentication Server

4.3 802.1X Global

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

■ Operation

Parameters	Meaning
Operation	When this function is enabled, the device checks the access to the network from connected end devices. Possible values: ▶ `On` The port-based access control is enabled. ▶ `Off` (default setting) The port-based access control is disabled.

Configuration

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

Information

Parameters	Meaning
Monitor Mode Clients	Displays to how many end devices the device gave network access even though they did not login successfully. This requires that you activate the "Activate Monitor Mode " function; see the "Configuration" frame.

Parameters	Meaning
Non Monitor Mode Clients	Displays the number of end devices to which the device gave network access after successful login.
Authentication Method	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

Button	Meaning
Set	Transfers the changes to the volatile memory (`RAM`) of the device and applies them. 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 "Select" button. □ Click the "Save" button.
Reload	Updates the fields with the values that are saved in the volatile memory (`RAM`) of the device.
Help	Opens the online help.

4.4 802.1X Port Configuration

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

■ Table

Parameters	Meaning
Port	Displays the number of the device port.
Port Initialization	Initializes the device port 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: ▶ `unmarked` (default setting) Keeps the current status of the device port. ▶ `marked` Initializes the device port. When initialization is complete, the device changes the value to `unmarked` again.
Port Reauthentication	If this function is enabled, the authenticator requests the end device to login again. Use this function exclusively to ports in which the "Port Control" column contains the value `auto`. Possible values: ▶ `unmarked` (default setting) Keeps the end device logged in. ▶ `marked` Requests the end device to login again. Afterwards, the device changes the value to `unmarked` again. The device also allows you to periodically request the end device to login again, see the "Reauthentication Enabled" column.
Authentication Activity	Displays the current state of the authenticator (authenticator PAE state). Possible values: ▶ `initialize` ▶ `disconnected` ▶ `connecting` ▶ `authenticating` ▶ `authenticated` ▶ `aborting authenticating` ▶ `held` ▶ `force Authorized` ▶ `force Unauthorized`

Parameters	Meaning
Backend Authentication State	Displays the current state of the connection to the authentication server (backend authentication state). Possible values: ▶ `request` ▶ `response` ▶ `success` ▶ `fail` ▶ `timeout` ▶ `idle` ▶ `initialize`
Authentication State	Displays the current state of the authentication on the device port (controlled port status). Possible values: ▶ `authorized` The terminal device is logged in successfully. ▶ `unauthorized` The terminal device is not logged in.
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 a 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 a end device is connected to the port that logs in at the authenticator. If other end devices are connected through the same port, they get access to the network without additional authentication. ▶ `ForceAuthorized` (default setting) The device grants access to the network. You use this setting if a 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 login attempt. 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`)

Parameters	Meaning
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`)
Max Request Constant	Specifies how often the authenticator requests the end device to login until the time specified in the "Supplicant Timeout Period [s]" field 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 device ports in the `Network Security > 802.1X Port Authentication > Port Clients` dialog. To ports in which the "Port Control" column contains the value `macBased`: the device assigns the VLAN tag based on the MAC address of the end device when it receives data packets without a VLAN tag.
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 device ports 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
Reauthentication Enabled	If this function is enabled, the authenticator periodically requests the end device to login again. Possible values: ▶ `marked` Periodically requests the end device to login again. You specify this time period in the "Reauthentication Period [s]" field. This setting becomes ineffective if the authenticator has assigned the end device the ID of a Voice, Unauthenticated or Guest VLAN. ▶ `unmarked` (default setting) 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 login during the time period specified in the "Guest VLAN Period" field. 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 802.1X support, 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 guest VLAN to the port. **Note:** Assign to the port a VLAN set up statically in the device.
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" field. 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

Button	Meaning
Set	Transfers the changes to the volatile memory (`RAM`) of the device and applies them. 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 "Select" button. ☐ Click the "Save" button.
Reload	Updates the fields with the values that are saved in the volatile memory (`RAM`) of the device.
Help	Opens the online help.

4.5 802.1X Port Clients

This dialog displays information on the connected end devices.

Table

Parameters	Meaning
Port	Displays the number of the device port.
User Name	Displays the user name with which the terminal device logged in.
MAC Address	Displays the MAC address of the terminal device.
Assigned VLAN ID	Displays the VLAN ID that the authenticator assigned to the port after the successful authentication of the end device. For ports for which in the `Network Security > 802.1X Port Authentication > Port Configuration` dialog, column "Port Control" the value is `macBased`: the device assigns the VLAN tag based on the MAC address of the end device when it receives data packets without a VLAN tag.
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 login of the end device expires. This value applies solely if for the port in the `Network Security >` 802.1X Port Authentication `> Port Configuration` dialog, column "Port Control" the value is `auto`. 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

Button	Meaning
Reload	Updates the fields with the values that are saved in the volatile memory (`RAM`) of the device.
Help	Opens the online help.

4.6 802.1X 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 number of the device port.
Received Frames	Displays the total number of EAPOL data packets that the device received on the port.
Transmitted Frames	Displays the total number of EAPOL data packets that the device sent on the port.
Start Frames	Displays the number of EAPOL start data packets that the device received on the port.
Logoff Frames	Displays the number of EAPOL logoff data packets that the device received on the port.
Response/ID Frames	Displays the number of EAP response/identity data packets that the device received on the port.
Response Frames	Displays the number of valid EAP response data packets that the device received on the port (without EAP response/identity data packets).
Request/ID Frames	Displays the number of EAP request/identity data packets that the device received on the port.
Request Frames	Displays the number of valid EAP request data packets that the device received on the port (without EAP request/identity data packets).
Invalid Frames	Displays the number of EAPOL data packets with an unknown frame type that the device received on the port.
Error Frames	Displays the number of EAPOL data packets with an invalid packet body length field that the device received on the port.
Frame Version	Displays the protocol version number of the EAPOL data packet that the device last received on the port.
Frame Source	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

Button	Meaning
Reload	Updates the fields with the values that are saved in the volatile memory (`RAM`) of the device.
Reset	Resets the entire table.
Help	Opens the online help.

4.7 802.1X 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 number of the device port.
Authentification Time Stamp	Displays the time at which the authenticator authenticated the terminal device.
Result Age	Displays since when this entry has been entered in the table.
MAC Address	Displays the MAC address of the terminal device.
VLAN ID	Displays the ID of the VLAN that was assigned to the terminal device before the login.
Authentication Status	Displays the status of the authentication on the device port. Possible values: ▶ `success` The authentication was successful. ▶ `failure` The authentication failed.
Access Status	Displays whether the device grants the terminal device access to the network. Possible values: ▶ `granted` The device grants the terminal device access to the network. ▶ `denied` The device denies the terminal device access to the network.
Assigned VLAN ID	Displays the ID of the VLAN that the authenticator assigned to the port.

Parameters	Meaning
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.

■ Port

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 device port. ▶ <Port number> The table displays the entries that apply to the port selected here.

■ Buttons

Button	Meaning
Reload	Updates the fields with the values that are saved in the volatile memory (`RAM`) of the device.
Reset	Resets the entire table.
Help	Opens the online help.

4.8 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 terminal devices. The device allows you to set up up to 100 sets of login data.

To authenticate the end devices through the Integrated Authentication Server you assign 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 "Create" 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. A end device has the option of logging in through 802.1x using this login data. ▶ `unmarked` (default setting) The login data is inactive.

■ Buttons

Button	Meaning
Set	Transfers the changes to the volatile memory (`RAM`) of the device and applies them. 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 "Select" button. ☐ Click the "Save" button.
Reload	Updates the fields with the values that are saved in the volatile memory (`RAM`) of the device.
Create	Opens the "Create" dialog to add a new entry to the table. In the "User Name" field, you specify the user name of the end device.
Remove	Removes the highlighted table entry.
Help	Opens the online help.

4.9 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 manage the users at a central location 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 terminal 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 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

4.10 RADIUS Global

This dialog allows you to specify basic settings for RADIUS.

■ RADIUS Configuration

Parameters	Meaning
Max. Number of Retransmits	Specifies how often 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`)
Enable Accounting Mode	Enables/disables the accounting function: Possible values: ▶ `unmarked` (default setting) The accounting function is inactive. ▶ `marked` The accounting function is active. The active server specified in the `Network Security > RADIUS >` RADIUS Accounting Server dialog registers the traffic data that occurs during the authentication and the authorization.
NAS IP-Address (Attribute 4)	Specifies the IP address that the device transfers to the authentication server as attribute 4. Enter 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

Button	Meaning
Set	Transfers the changes to the volatile memory (RAM) of the device and applies them. 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 "Select" button. □ Click the "Save" button.
Reload	Updates the fields with the values that are saved in the volatile memory (RAM) of the device.
Clear RADIUS Statistics ...	Deletes the statistics in the Network Security > RADIUS > Authentication Statistics dialog and in the Network Security > RADIUS > Accounting Statistics dialog.
Help	Opens the online help.

4.11 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 secondary 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 a sequential number to which the table entry relates. The device automatically defines this number. 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
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.

Parameters	Meaning
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. 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

Button	Meaning
Set	Transfers the changes to the volatile memory (`RAM`) of the device and applies them. 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 "Select" button. ☐ Click the "Save" button.
Reload	Updates the fields with the values that are saved in the volatile memory (`RAM`) of the device.
Create	Opens the "Create" dialog to add a new entry to the table. In the "Address" field, you specify the IP address of the server.
Remove	Removes the highlighted table entry.
Help	Opens the online help.

4.12 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. Prerequisite is that you activate in the `Network Security > RADIUS > Global` menu the "Enable Accounting Mode" 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 a sequential number to which the table entry relates. The device automatically defines this number. 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
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.

Parameters	Meaning
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

Button	Meaning
Set	Transfers the changes to the volatile memory (`RAM`) of the device and applies them. 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 "Select" button. □ Click the "Save" button.
Reload	Updates the fields with the values that are saved in the volatile memory (`RAM`) of the device.
Create	Opens the "Create" dialog to add a new entry to the table. In the "Address" field, you specify the IP address of the server.
Remove	Removes the highlighted table entry.
Help	Opens the online help.

4.13 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 often no response to the server was received before the specified waiting time elapsed.

Parameters	Meaning
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

Button	Meaning
Reload	Updates the fields with the values that are saved in the volatile memory (`RAM`) of the device.
Help	Opens the online help.

4.14 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 often 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

Button	Meaning
Reload	Updates the fields with the values that are saved in the volatile memory (`RAM`) of the device.
Help	Opens the online help.

4.15 DoS

The device supports you in protecting against invalid or fake data traffic that aims to bring down specific services or devices (Denial of Service, DoS). With this menu you can use various filters to restrict the data traffic for Denial of Service attacks.

The menu contains the following dialog:

▶ DoS Global

4.16 DoS Global

With this dialog you can configure the DoS settings for the TCP/UDP, IP and ICMP protocols.

■ TCP/UDP

The attaching stations uses port scans to prepare network attacks. Here the station attempts to use the network to detect the devices present and the services they provide.

This frame allows you to activate or deactivate the detection of port scans.

The device detects the following scan types:
- Null scan
- Xmas scan
- SYN/FIN scan
- TCP offset protection
- TCP SYN protection
- L4 port protection
- Minimal header scan

Parameter	Meaning
Activate Null Scan Filter	Activates/deactivates the null scan. Possible values: ▶ `marked` The device detects incoming data packets with no TCP flags set and the TCP sequence number reset to 0 and discards them. ▶ `unmarked` (default setting) The null scan is inactive.
Activate Xmas Filter	Activates/deactivates the Xmas scan. Possible values: ▶ `marked` The device detects incoming data packets with the TCP flags FIN, URG and PUSH set simultaneously and the TCP sequence number reset to 0 and discards them. ▶ `unmarked` (default setting) The Xmas scan is inactive.

Parameter	Meaning
Activate SYN/FIN Filter	Activates/deactivates the SYN/FIN scan. Possible values: ▶ `marked` The device detects incoming data packets with the TCP flags SYN and FIN set simultaneously and discards these. ▶ `unmarked` (default setting) The SYN/FIN scan is inactive.
Activate TCP Offset Protection	Activates/deactivates the TCP offset scan. Possible values: ▶ `marked` The device detects incoming TCP data packets whose fragment offset field of the IP header is equal to 1 and discards them. The device accepts UDP and ICMP packets whose fragment offset field of the IP header is equal to 1. ▶ `unmarked` (default setting) The TCP offset scan is inactive.
Activate TCP SYN Protection	Activates/deactivates the TCP SYN scan. Possible values: ▶ `marked` The device detects incoming data packets with the TCP flag SYN set and a L4 source port <1024 and discards them. ▶ `unmarked` (default setting) The TCP SYN scan is inactive.
Activate L4 Port Protection	Activates/deactivates the L4 port scan. Possible values: ▶ `marked` The device detects incoming TCP and UDP data packets whose source port number and destination port number are identical and discards them. ▶ `unmarked` (default setting) The L4 port scan is inactive.
Activate Minimal Header Filter	Activates/deactivates the minimal header scan. Possible values: ▶ `marked` The device detects incoming data packets whose data offset value multiplied by 4 is smaller than the minimum TCP header size and discards them. ▶ `unmarked` (default setting) The minimal header scan is inactive.

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.

Parameter	Meaning
Activate Land Attack Filter	Activates/deactivates the land attack scan. Possible values: ▶ `marked` The device detects incoming IP data packets whose source and destination IP address are identical and discards them. ▶ `unmarked` (default setting) The land attack scan 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

Parameter	Meaning
Filter Fragmented Packets	Activates/deactivates the filter for fragmented ICMP packets. Possible values: ▶ `marked` The device detects fragmented ICMP packets and discards these. ▶ `unmarked` (default setting) The filter for fragmented ICMP packets is inactive.

Parameter	Meaning
Allowed Packet Size	Specifies the maximum allowed size of ICMP packets in bytes. Possible values: ▶ 0..1472 (default setting: 512) **Note:** Mark the "Filter by Packetsize" checkbox if you want the device to discard incoming data packets whose size exceeds the maximum allowed size for ICMP packets.
Filter by Packetsize	Activates/deactivates the filter for incoming ICMP data packets whose size exceeds the maximum allowed packet size. Possible values: ▶ marked The device detects ICMP data packets whose size exceeds the packet size specified in the "Allowed Packet Size" field and discards them. ▶ unmarked (default setting) The device forwards ICMP data packets whose size exceeds the allowed packet size.

■ Buttons

Button	Meaning
Set	Transfers the changes to the volatile memory (RAM) of the device and applies them. 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 "Select" button. □ Click the "Save" button.
Reload	Updates the fields with the values that are saved in the volatile memory (RAM) of the device.
Help	Opens the online help.

5 Switching

This menu allows you to specify the switching settings for transmitting data on layer 2 of the ISO/OSI layer model.

The menu contains the following dialogs:

- Switching Global
- Rate Limiter
- Filter for MAC Addresses
- IGMP Snooping
- QoS/Priority
- MRP-IEEE
- VLAN
- L2-Redundancy

5.1 Switching Global

This dialog allows you to specify the following settings:

- Change the aging time of the address table (forwarding database)
- Switch on the flow control in the device
- Switch on the VLAN Unaware Mode

If a large number of data packets are received in the sending 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 ensures 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 terminal 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 switch on the VLAN Unaware Mode, this deactivates the VLAN settings in the device. The device then transparently forwards the data packets on the ports 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 (Forwarding Database). You find the address table in the `Switching > Filter for MAC Addresses` dialog. In connection with the router redundancy, specify a time ≥ 30 s.

Parameters	Meaning
Activate Flow Control	Activates/deactivates the flow control globally in the device. Possible values: ▶ `unmarked` (default setting) The flow control is inactive in the device. ▶ `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. 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.
VLAN Unaware Mode	Specifies the bridging mode of the device. Possible values: ▶ `unmarked` (default setting) 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. ▶ `marked` The device works in the VLAN Unaware bridging mode (802.1D): – 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. The device ports are assigned to VLAN 1. – The device evaluates the priority information contained in the data packet. **Note:** You specify the VLAN ID `1` for the functions on the device that use VLAN settings. Among other things, this applies to static filters, MRP and IGMP Snooping.

■ Buttons

Button	Meaning
Set	Transfers the changes to the volatile memory (`RAM`) of the device and applies them. 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 "Select" button. □ Click the "Save" button.
Reload	Updates the fields with the values that are saved in the volatile memory (`RAM`) of the device.
Help	Opens the online help.

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. With the following measures you reduce the effects on, for example, the TCP traffic:

- Restricting the rate limiter function to specific data packets, e.g. to Broadcasts, Multicasts and Unicasts with an unknown destination address. Excluding Unicasts with a known destination address from this restriction.
- Using the egress limiter function instead of the ingress limiter function. The egress limiter function works somewhat better with the TCP flow control due to the device-internal buffering of the data packets.
- Increasing the aging time for learned Unicast addresses.

On this tab you activate the rate limiter function for received data packets. By entering a threshold value you specify the maximum amount of traffic the port transmits on the ingress side. If the traffic on this port exceeds the threshold value, the device discards the excess traffic on this port.

Parameters	**Meaning**
Port	Displays the number of the device port to which the table entry relates.
Threshold	Specifies the threshold value for broadcast, multicast, and unicast traffic on this port: Possible values: ▶ `0..24414` at 100 MBit/s `0..244140` at1000 MBit/s (default setting: `0`) The value `0` deactivates the rate limiter function on this port. □ Enter a percentage from 0 through 100 if you select in the "Threshold Unit" column the value `percent`. □ Enter an absolute value for the data rate if you select in the "Threshold Unit" column the value `pps`. The rate limiter function calculates the threshold based on 512-byte-sized packets.
Threshold Unit	Specifies the unit for the threshold value: Possible values: ▶ `Percent` (default setting) Enter the threshold value as a percentage of the data rate of the port. ▶ `pps` Enter the threshold value in data packets per second.
Broadcast Mode	Activates/deactivates the rate limiter function for received broadcast data packets. Possible values: ▶ `unmarked` (default setting) ▶ `marked` If the threshold value is exceeded, the device discards the excess broadcast data packets on this port.

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

■ Buttons

Button	Meaning
Set	Transfers the changes to the volatile memory (`RAM`) of the device and applies them. 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 "Select" button. □ Click the "Save" button.
Reload	Updates the fields with the values that are saved in the volatile memory (`RAM`) of the device.
Help	Opens the online help.

5.3 Filter for MAC Addresses

This dialog allows you to display and edit address filters for the address table (forwarding database). 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 all the other ports.

Table

Parameters	Meaning
Address	Displays the destination MAC address to which the table entry applies.
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. ▶ `invalid` Deletes a manually set up address filter. ▶ `MRP-MMRP` Multicast address filter automatically set up by MMRP.

Parameters	Meaning
VLAN ID	Displays the ID of the VLAN to which the table entry applies. Possible values: ▶ `1..4042` The device learns the MAC addresses for every VLAN separately (independent VLAN learning).
<Port number>	Displays how the corresponding device 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 (Forwarding Database), click in the `Basic Settings > Restart` dialog the "Reset MAC Address Table" button.

Edit Entry

To manually adapt the settings for a table entry, click the "Edit Entry" button.

Parameters	Meaning
Possible Ports	This column contains the ports available in the device.
Dedicated Ports	This column contains the device ports that are assigned to the table entry.

■ Buttons

Button	Meaning
Set	Transfers the changes to the volatile memory (`RAM`) of the device and applies them. 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 "Select" button. □ Click the "Save" button.
Reload	Updates the fields with the values that are saved in the volatile memory (`RAM`) of the device.
Create	Opens the "Create" dialog to add a new entry to the table. ▶ In the "VLAN ID" field, you specify the ID of the VLAN. ▶ In the "Address" field, you specify the destination MAC address. ▶ In the "Possible Ports" field, you specify the device 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.
Edit Entry	Opens the "Edit Entry" window. ▶ The "Possible Ports" field displays the available device ports. ▶ The "Dedicated Ports" field displays the device ports that are assigned to the MAC address. ▶ Buttons: – > : Moves the highlighted entries from the "Possible Ports" field to the "Dedicated Ports" field. – >> : Moves every entry to the "Dedicated Ports" field. – < : Moves the highlighted entries from the "Dedicated Ports" field to the "Possible Ports" field. – << : Moves every entry to the "Possible Ports" field.
Reset MAC Address Table	Removes the MAC addresses from the forwarding table that have the value `learned` in the "Status" field.
Help	Opens the online help.

5.4 IGMP Snooping

The IGMP protocol (Internet Group Management protocol) is a protocol for dynamically managing Multicast groups. The protocol describes the distribution of Multicast data packets between routers and terminal 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 all the ports.
- 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(Forwarding Database). 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 Querier
- IGMP-Multicasts

5.5 IGMP Snooping Global

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

Operation

Parameters	Meaning
Operation	When the function is switched on, the IGMP Snooping function according to RFC 4541 (Considerations for Internet Group Management Protocol (IGMP) and Multicast Listener Discovery (MLD) Snooping Switches) is activated in the device. Possible values: ▶ `On` When the function is switched on, the IGMP Snooping protocol is activated globally in the device. ▶ `Off` (default setting) When the function is switched off, the device transmits received query, report and leave data packets without evaluating them. Received data packets with a Multicast destination address are transmitted to all ports by the device.

Information

Parameters	Meaning
Multicast Control Frames 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 counters" 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

Button	Meaning
Set	Transfers the changes to the volatile memory (`RAM`) of the device and applies them. 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 "Select" button. ☐ Click the "Save" button.
Reload	Updates the fields with the values that are saved in the volatile memory (`RAM`) of the device.
Reset IGMP Snooping counters	Removes the IGMP Snooping entries and resets the counter in the "Information" frame to `0`.
Help	Opens the online help.

5.6 IGMP Snooping Configuration

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

The dialog contains the following tabs:

- VLAN
- Port

5.6.1 VLAN

This tab page allows you to configure the IGMP Snooping protocol for every VLAN.

■ Table

Parameters	Meaning
VLAN ID	Displays the ID of the VLAN to which the table entry applies. Possible values: ▶ `1..4042` (VLAN IDs that are set up)
Active	Activates/deactivates the IGMP Snooping protocol for this VLAN. Prerequisite: The IGMP Snooping protocol is activated globally in the device. Possible values: ▶ `Off` (default setting) IGMP Snooping is deactivated for this VLAN. The VLAN has left the Multicast data stream. ▶ `on` IGMP Snooping is activated for this VLAN. The VLAN has joined 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. In the "Group Membership Interval" field, specify a value larger than the value in the "Max Response Time" field. 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. In the "Max Response Time" field, specify a value smaller than the value in the "Group Membership Interval" field. Possible values: ▶ `1..25` (default setting: `10`)

Parameters	Meaning
Fast Leave Admin Mode	Activates/deactivates the Fast Leave function for this VLAN. Possible values: ▶ `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. ▶ `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.
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

Button	Meaning
Set	Transfers the changes to the volatile memory (`RAM`) of the device and applies them. 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 "Select" button. ☐ Click the "Save" button.
Reload	Updates the fields with the values that are saved in the volatile memory (`RAM`) of the device.
Help	Opens the online help.

5.6.2 Port

This tab page allows you to configure the IGMP Snooping protocol for every port.

■ Table

Parameters	Meaning
Port	Displays the number of the device port to which the table entry relates.
Active	Activates/deactivates the IGMP Snooping protocol for this port. Prerequisite: The IGMP Snooping protocol is enabled globally in the device. Possible values: ▶ `unmarked` (default setting) IGMP Snooping is inactive on this port. The port left the multicast data stream. ▶ `marked` IGMP Snooping is active on this port. The device includes the port in 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" field.
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" field.
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`)

Parameters	Meaning
Fast Leave Admin Mode	Activates/deactivates the Fast Leave function for this port. Possible values: ▶ `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. ▶ `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.
Static Query Port	Specifies the port in the configured VLANs as static query port. Possible values: ▶ `unmarked` (default setting) The port is not a static query port. The device transmits IGMP report messages to the port solely if it receives IGMP queries. ▶ `marked` The port is a static query port.
VLAN IDs	Displays the ID of the VLANs to which the table entry applies.

■ Buttons

Button	Meaning
Set	Transfers the changes to the volatile memory (`RAM`) of the device and applies them. 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 "Select" button. □ Click the "Save" button.
Reload	Updates the fields with the values that are saved in the volatile memory (`RAM`) of the device.
Help	Opens the online help.

5.7 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. Possible values: ▶ `1..4042` (VLAN IDs that are set up)
<Port number>	Displays for every VLAN set up in the device whether the relevant device 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. 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. ☐ On the "Configuration" page, mark the "Static" checkbox. ▶ `P` = Learn by LLDP (manual setting) A user specified the port as `Learn by LLDP`. With LLDP (Link Layer Discovery Protocol), 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. ☐ 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. ☐ 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. ▶ `Learn 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

Button	Meaning
Set	Transfers the changes to the volatile memory (`RAM`) of the device and applies them. 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 "Select" button. □ Click the "Save" button.
Reload	Updates the fields with the values that are saved in the volatile memory (`RAM`) of the device.
Wizard	Opens the Wizard that assists you in selecting and configuring the ports.
Help	Opens the online help.

5.7.1 Wizard

■ Select VLAN - Port

On this page you assign a VLAN ID to device port.

Parameters	Meaning
VLAN ID	Select the ID of the VLAN. Possible values: ▶ `1..4042`
Port	Select the device ports. Possible values: ▶ `1/1` ▶ `1/2` etc.

■ Configuration

On this page you specify the settings for the device port.

Parameters	Meaning
VLAN ID	Displays the ID of the VLAN to which the table entry applies.
Port	Displays the number of the device port to which the table entry relates. Possible values: ▶ `1/1` ▶ `1/2` etc.
Static	Specifies the port as a “static query port”. 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 `Learned 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 all data packets with a Multicast address in the destination address field.

■ Buttons

Button	Meaning
Back	Displays the previous page again. Changes are lost.
Next	Saves the changes and opens the next page.
Finish	Saves the changes and closes the wizard.
Cancel	Closes the Wizard. Changes are lost.

After closing the Wizard, click the "Set" button to save your settings.

5.8 IGMP 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	Activates/deactivates 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` (IGMP v2, default setting) ▶ `3` (IGMP v3)

Parameters	Meaning
Query Interval	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: ▶ `unmarked` (default setting) The IGMP Snooping Querier function is inactive for this VLAN. ▶ `marked` The IGMP Snooping Querier function is active for this VLAN.
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 IP multicast 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, default setting) ▶ `3` (IGMP v3)

Parameters	Meaning
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 to prevent all the Multicast group members from responding to the query at the same time. In the "Max Response Time" field, specify a value smaller than the value in the "Group Membership Interval" field. Possible values: ▶ `1..25` (default setting: `10`)
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 protocol version that the Multicast router used when sending out the last IGMP query received in this VLAN.

■ Buttons

Button	Meaning
Set	Transfers the changes to the volatile memory (`RAM`) of the device and applies them. 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 "Select" button. ☐ Click the "Save" button.
Reload	Updates the fields with the values that are saved in the volatile memory (`RAM`) of the device.
Help	Opens the online help.

5.9 IGMP-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 all ports, 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: ▶ `Send to Query Ports` The device sends data packets with an unknown MAC/IP Multicast address to the query ports. ▶ `Send To All Ports` (default setting) The device sends data packets with an unknown MAC/IP Multicast address to the ports. ▶ `Discard` The device discards data packets with an unknown MAC/IP Multicast address.

■ 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 query ports and to registered ports. ▶ `Send To Registered Ports` (default setting) The device sends data packets with an unknown MAC/IP Multicast address to registered ports.

■ Buttons

Button	Meaning
Set	Transfers the changes to the volatile memory (`RAM`) of the device and applies them. 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 "Select" button. □ Click the "Save" button.
Reload	Updates the fields with the values that are saved in the volatile memory (`RAM`) of the device.
Help	Opens the online help.

5.10 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. Prerequisite for this 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 (e.g. 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, frame "Configuration" the "Activate Flow Control" checkbox is unmarked.

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

5.11 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..63` (default setting: `0(be/cs0)`) Some values in the list also have a DSCP keyword, for example `be/cs0`, `af11` or `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.
Number of Queues per Port	Displays the number of priority queues per port. You assign very priority queue to a specific traffic class (traffic class according to IEEE 802.1D). The device has 4 priority queues per port.

Buttons

Button	Meaning
Set	Transfers the changes to the volatile memory (`RAM`) of the device and applies them. 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 "Select" button. □ Click the "Save" button.
Reload	Updates the fields with the values that are saved in the volatile memory (`RAM`) of the device.
Help	Opens the online help.

5.12 Port Configuration

In this dialog, you specify the QoS/priority settings for each device port for received data packets.

■ Table

Parameters	Meaning
Port	Displays the number of the device port.
Port Priority	Specifies the VLAN priority of the data packets that the port receives. The device applies this setting to data packets depending on the value in the "Trust Mode" column: – Trust Mode =`untrusted` The device transmits the data packet with the VLAN priority specified here. – Trust Mode = `trustDot1p` If the data packet does not contain any VLAN or priority tag, the device transmits the data packet with the VLAN priority specified here. – Trust Mode = `trustIpDscp` If the data packet is not an IP packet, the device transmits the data packet with the priority specified here. 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. 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.

Parameters	Meaning
Trust Mode	Specifies how the device handles received data packets that contain a QoS/priority information. Possible values: ▶ `untrusted` The device transmits the data packet with the VLAN priority specified in the "Port Priority" field. The device ignores the QoS/priority information contained in the data packet. ▶ `trustDot1p` (default setting) – If the data packet contains a VLAN tag, the device transmits the data packet based on the contained QoS/priority information. In the `Switching > QoS/Priority > 802.1D/p Mapping` dialog, you assign a traffic class to every VLAN priority. 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. – If the data packet does not contain a VLAN tag, the device transmits the data packet with the VLAN priority specified in the "Port Priority" field. ▶ `trustIpDscp` – If the data packet is an IP data packet, the device transmits the data packet based on the contained IP DSCP value. In the `Switching >` QoS/Priority `> IP DSCP Mapping` dialog you assign a traffic class to every IP DSCP value. 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. – If the data packet is not an IP data packet, the device transmits the data packet with the VLAN priority specified in the "Port Priority" field.
Untrusted Traffic Class	Displays the traffic class. The device assigns data packets to this traffic class if in the "Trust Mode" field the value `untrusted` is specified. Possible values: ▶ `0..3` In the `Switching > QoS/Priority > 802.1D/p Mapping` dialog, you assign a traffic class to every VLAN priority. 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.
Bandwidth [%]	Specifies the egress transmission rate. This value specifies the percentage of overall link speed for the port in 1% increments. Possible values: ▶ `0..100` (default setting: `0`) A value of 0 disables the bandwidth limitation.

■ Buttons

Button	Meaning
Set	Transfers the changes to the volatile memory (`RAM`) of the device and applies them. 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 "Select" button. □ Click the "Save" button.
Reload	Updates the fields with the values that are saved in the volatile memory (`RAM`) of the device.
Help	Opens the online help.

5.13 802.1D/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..3` `0` assigned to the priority queue with the lowest priority. `3` assigned to the priority queue with the highest priority. **Note:** Network management protocols and redundancy mechanisms use the highest traffic class. Therefore, select another traffic class for application data.

■ Buttons

Button	Meaning
Set	Transfers the changes to the volatile memory (`RAM`) of the device and applies them. 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 "Select" button. □ Click the "Save" button.
Reload	Updates the fields with the values that are saved in the volatile memory (`RAM`) of the device.
Help	Opens the online help.

■ Default assignment of the VLAN priority to traffic classes

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

5.14 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..3` `0` assigned to the priority queue with the lowest priority. `3` assigned to the priority queue with the highest priority.

■ Buttons

Button	Meaning
Set	Transfers the changes to the volatile memory (`RAM`) of the device and applies them. 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 "Select" button. ☐ Click the "Save" button.
Reload	Updates the fields with the values that are saved in the volatile memory (`RAM`) of the device.
Help	Opens the online help.

Default assignment of the DSCP values to traffic classes

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

5.15 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".

You also have the option of assigning a minimum bandwidths to every traffic classes which the device uses to process the priority queues with "Weighted Fair Queuing"

■ Table

Parameters	Meaning
Traffic Class	Displays the traffic class.

Parameters	Meaning
Strict Priority	Specifies whether the device processes the priority queues of the ports for this traffic class with "Strict Priority" or with "Weighted Fair Queuing". Possible values: ▶ `marked` = "Strict-Priority" (default setting) – The device 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 never sends 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` = "Weighted Fair Queuing"/"Weighted Round Robin" (WRR) – 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 entered 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

Button	Meaning
Set	Transfers the changes to the volatile memory (`RAM`) of the device and applies them. 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 "Select" button. □ Click the "Save" button.
Reload	Updates the fields with the values that are saved in the volatile memory (`RAM`) of the device.
Help	Opens the online help.

5.16 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
- Multiple MAC Registration Protocol
- Multiple VLAN Registration Protocol

5.17 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 number of the device port.
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

Button	Meaning
Set	Transfers the changes to the volatile memory (`RAM`) of the device and applies them. 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 "Select" button. ☐ Click the "Save" button.
Reload	Updates the fields with the values that are saved in the volatile memory (`RAM`) of the device.
Help	Opens the online help.

5.18 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 frames 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 frames to the 2 end devices.

The dialog contains the following tabs:

- Configuration
- Service Requirement
- Statistics

5.18.1 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 number of the device port.
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) Disables the restriction of dynamic MAC address registration using MMRP on the port.

Buttons

Button	Meaning
Set	Transfers the changes to the volatile memory (`RAM`) of the device and applies them. 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 "Select" button. □ Click the "Save" button.
Reload	Updates the fields with the values that are saved in the volatile memory (`RAM`) of the device.
Help	Opens the online help.

5.18.2 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 `ForwardAll` 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

Button	Meaning
Set	Transfers the changes to the volatile memory (`RAM`) of the device and applies them. 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 "Select" button. □ Click the "Save" button.
Reload	Updates the fields with the values that are saved in the volatile memory (`RAM`) of the device.
Help	Opens the online help.

5.18.3 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 number of the device port.
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

Button	Meaning
Reset	Resets the port statistics counters and the "Last Received MAC Address" field.
Set	Transfers the changes to the volatile memory (`RAM`) of the device and applies them. 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 "Select" button. ☐ Click the "Save" button.
Reload	Updates the fields with the values that are saved in the volatile memory (`RAM`) of the device.
Help	Opens the online help.

5.19 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

5.19.1 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 determines 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	Activates/deactivates the periodic state machine on the device. Possible values: ▶ `On` With MVRP "Operation" enabled globally, the device transmits MVRP periodic events in 1 second intervals, on MVRP participating ports. ▶ `Off` (default setting) Disables the periodic state machine on the device.

Table

Parameters	Meaning
Port	Displays the number of the device port.
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

Button	Meaning
Set	Transfers the changes to the volatile memory (`RAM`) of the device and applies them. 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 "Select" button. ☐ Click the "Save" button.
Reload	Updates the fields with the values that are saved in the volatile memory (`RAM`) of the device.
Help	Opens the online help.

5.19.2 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 number of the device port.
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

Button	Meaning
Reset	Resets the port statistics counters and the "Last Received MAC Address" field.
Set	Transfers the changes to the volatile memory (`RAM`) of the device and applies them. 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 "Select" button. ☐ Click the "Save" button.
Reload	Updates the fields with the values that are saved in the volatile memory (`RAM`) of the device.
Help	Opens the online help.

5.20 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 terminal 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, e.g. 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

5.21 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.
Max. supported VLANs	Displays the maximum number of VLANs possible. See the `Switching > VLAN > Configuration` dialog.
Number of VLANs	Number of VLANs currently configured in the device. See the `Switching > VLAN > Configuration` dialog. The VLAN ID 1 is always present in the device.

Buttons

Button	Meaning
Reload	Updates the fields with the values that are saved in the volatile memory (`RAM`) of the device.
Clear...	Resets the VLAN settings of the device to the default setting. Caution: You block your access to the device if you have changed in the `Basic Settings > Network` dialog the VLAN ID for the management functions of the device.
Help	Opens the online help.

5.22 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 device 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 16 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 user or by the "MRP" function, see the `Switching > L2-Redundancy > MRP` dialog. VLANs with this setting remain set up also after a restart. ▶ `dynamicMvrp` VLAN set up by the "Multiple VLAN Registration Protocol" function, see the `Switching > MRP-IEEE > MMRP` 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
<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. ▶ `F` = Forbidden The port is not a member of the VLAN and does not transmit data packets of this VLAN. Additionally, the device prevents the port from becoming a VLAN member through the "Multiple VLAN Registration Protocol" 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 device ports.

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. To access the management functions is possible solely using the CLI through the V.24 interface of the device.

■ Buttons

Button	Meaning
Set	Transfers the changes to the volatile memory (`RAM`) of the device and applies them. 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 "Select" button. ☐ Click the "Save" button.
Reload	Updates the fields with the values that are saved in the volatile memory (`RAM`) of the device.
Create	Opens the "Create" dialog to add a new entry to the table. In the "VLAN ID" field, you specify the ID of the VLAN.
Remove	Removes the highlighted table entry.
Help	Opens the online help.

5.23 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 device ports and thus specify the port VLAN ID.
Additionally, you also specify for each device port how the device transmits data packets when the VLAN Unaware mode is switched off 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 number of the device port.
Port-VLAN ID	Specifies the ID of the VLAN which the devices assigns to data packets without a VLAN tag. Prerequisite is that you specify in the "Acceptable Frame Types" field 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.

Parameters	Meaning
Acceptable Frame 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	Specifies whether the port transmits or discards received data packets with a VLAN tag. Possible values: ▶ `marked` 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 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

Button	Meaning
Set	Transfers the changes to the volatile memory (`RAM`) of the device and applies them. 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 "Select" button. □ Click the "Save" button.
Reload	Updates the fields with the values that are saved in the volatile memory (`RAM`) of the device.
Help	Opens the online help.

5.24 L2-Redundancy

This menu allows you to specify and monitor the settings for redundancy mechanisms.
The “Redundancy Configuration User Manual” document contains detailed information that you require to select the suitable redundancy procedure and configure it.

The menu contains the following dialogs:

- MRP
- PRP
- HSR
- Spanning Tree
- Link Aggregation
- Link Backup

5.25 MRP

The MRP (Media Redundancy Protocol) 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 switching 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: The devices with hardware for enhanced redundancy functions offer the delay times `30ms` and `10ms`. To use the short delay times, load the device software with Fast MRP support.

Note: Spanning Tree and Ring Redundancy affect each other. Deactivate the Spanning Tree protocol for the ports connected to the MRP ring.

■ Operation

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

Ring Port 1/Ring Port 2

Parameters	Meaning
Port	Number of the device port that is operating as a ring port.
Operation	Displays the operating status of the ring port. Possible values: ▶ `forwarding` Port is switched on, connection exists. ▶ `blocked` Port is blocked, connection exists. ▶ `disabled` Port is disabled. ▶ `not connected` No connection exists.

Configuration

Parameters	Meaning
Ring Manager	Specifies whether the device is operating as a ring manager. Possible values: ▶ `Off` (default setting) Device is operating as a ring client. ▶ `On` Device is operating as a ring manager. If there is one device at each end of the line, you activate this function.
Advanced Mode	Enables/disables the advanced mode for fast switching 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.

Parameters	Meaning
Ring Recovery	Specifies the maximum switching time in milliseconds for reconfiguration of the ring. This setting is effective if the device is operating as a ring manager. Possible values: ▶ `500ms` ▶ `200ms` (default setting) ▶ `30ms` ▶ `10ms` The switching times `30ms` and `10ms` are only available to you for devices with hardware support for redundancy. To use the short failover times, load the device software with Fast MRP support. You load the device software in the `Basic Settings > Software` dialog. Set the switching time to `10ms` only when you use up to 20 devices in the ring that support this switching time. If you use more than 20 of these devices, set the switching time to at least `30ms`. 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 switching 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 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: Ring port link error` Error in the cabling of the ring ports. The following messages are possible if the device is operating as a ring manager: ▶ `Configuration error: Packet of other ring manager received` Another device exists in the ring that is operating as the ring manager. Enable the "Ring Manager" function if there is exactly one device in the ring. ▶ `Configuration error: Connection in ring is connected to incorrect 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

Button	Meaning
Set	Transfers the changes to the volatile memory (`RAM`) of the device and applies them. 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 "Select" button. □ Click the "Save" button.
Reload	Updates the fields with the values that are saved in the volatile memory (`RAM`) of the device.
Delete ring configuration	Disables the redundancy function and resets the settings in the dialog to the default setting.
Help	Opens the online help.

5.26 PRP

PRP uses 2 independent LANs with arbitrary ring, mesh, star, and bus topologies resulting in a high availability of network connection. The device connects to the PRP network with 100 Mbit/s optical SFPs or 100 Mbit/s FDX twisted pair interfaces installed in specially marked dedicated ports A and B for the LAN links. The International Standard IEC 62439-3 describes the Parallel Redundancy Protocol (PRP).

The main advantage of PRP is that the destination node receives packets from the source as long as 1 LAN is available. The absence of the second LAN due to repairs or maintenance has no impact on the packet transmission.

The network device which connects the end devices to the network implements the PRP protocol. The Ethernet switches in both LANs are standard switches that are oblivious to PRP. A Double Attached Node implementing PRP (DANP) is a network device with PRP functionality and has 1 connection into each independent LAN. A Single Attached Node (SAN) is a standard Ethernet device with a single LAN interface directly connected to one of the redundant LANs. For this reason, a SAN is unable to use the redundant LAN.

A Redundancy Box (RedBox) is a network device which implements the PRP functionality for standard ethernet devices. A standard ethernet device when connected to a PRP network via a RedBox is a virtual DANP (VDAN). Many applications and devices used for signal and control functions or VoIP, for example, need an integrated dual PRP interface which delivers packets without interruption.

Note: PRP is available for devices with hardware for enhanced redundancy functions. In order to use the PRP functions, load the PRP device software.

Note: If the inter-frame gap is shorter than the latency between the 2 LANs, a frame-ordering mismatch can occur. Frame-ordering mismatch is a phenomenon of the PRP protocol. The only solution for avoiding a frame-ordering mismatch is to verify that the inter-frame gap is greater than the latency between the LANs.

The menu contains the following dialogs:

- PRP Configuration
- DAN/VDAN Table
- Proxy Node Table
- Statistics

5.27 PRP Configuration

With this dialog you switch the Parallel Redundancy Protocol function on/off, and manage PRP supervision packet transmission and reception.

MRP and STP cannot operate on the same ports as PRP. Deactivate or choose different ports for MRP and deactivate STP on the PRP ports.

Note: If PRP is active, it uses the interfaces 1/1 and 1/2. As seen in the `Switching > VLAN`, `Switching > Rate Limiter` and `Switching > Filter for MAC Addresses` dialogs, the PRP function replaces the interfaces 1/1 and 1/2 with the interface prp/1. Configure the VLAN membership, the rate limiting, and the MAC filtering for the interface prp/1.

■ Operation

Parameters	Meaning
Operation	Enables/disables the PRP function globally. Possible values: ▶ `On` The device processes the traffic according to the configured functions when this function is active. ▶ `Off` (default setting) **Note:** Proceed as follows to avoid network loops: Deactivate port A or B before deactivating the PRP operation globally.

■ Port A/Port B

Parameters	Meaning
Port A	The textbox displays the number of the port which the device uses as the PRP port A. Using the radio buttons you enable/disable the PRP function on the port. Possible values: ▶ `On` (default setting) PRP function on the port is enabled. ▶ `Off` PRP function on the port is disabled.
Port B	The textbox displays the number of the port which the device uses as the PRP port B. Using the radio buttons you enable/disable the PRP function on the port. Possible values: ▶ `On` (default setting) PRP function on the port is enabled. ▶ `Off` PRP function on the port is disabled.

■ Supervision Packet Receiver

Parameters	Meaning
Evaluate Supervision Packets	Activates/deactivates the analysis of the supervision packets. Possible values: ▶ `marked` (default setting) The analysis of the supervision packets is active. The device receives supervision frames and analyzes them. ▶ `unmarked` The analysis of the supervision packets is inactive. The device still receives supervision frames, but without analyzing them.

■ Supervision Packet Transmitter

Parameters	Meaning
Active	Enables/disables the transmission of supervision packets. Possible values: ▶ `On` (default setting) The transmission of supervision packets is enabled. The RedBox transmits its own supervision packets. ▶ `Off` The transmission of supervision packets is disabled.
Send VDAN Packets	Activates/deactivates the transmission of VDAN supervision packets. Prerequisite is that you activate the "Supervision Packet Transmitter" first. Possible values: ▶ `marked` (default setting) The transmission of VDAN supervision packets is active. The RedBox transmits both its own supervision packets and the supervision packets for the VDANs listed in the "Proxy Node Table". ▶ `unmarked` The transmission of VDAN supervision packets is inactive.

■ Buttons

Button	Meaning
Set	Transfers the changes to the volatile memory (`RAM`) of the device and applies them. 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 "Select" button. □ Click the "Save" button.
Reload	Updates the fields with the values that are saved in the volatile memory (`RAM`) of the device.
Help	Opens the online help.

5.28 DAN/VDAN Table

The "DAN/VDAN Table" (Double Attached Node / Virtual Double Attached Node) dialog helps to analyze the LANs. For example, when the "Last Seen …" counter of 1 port continually increases while the other remains the same. This condition indicates a loss of LAN connection.

Table

Parameters	Meaning
Index	Displays a sequential number for the node to which the table entry refers. The device automatically defines this number.
MAC Address	Displays the MAC address of the node.
Last Seen A	Displays the time between received first packets for this node on LAN A. When the counter threshold reaches 497 days, it restarts from 0.
Last Seen B	Displays the time between received first packets for this node on LAN B. When the counter threshold reaches 497 days, it restarts from 0.
Remote Node Type	Displays the type of node. Possible values: ▶ `RedBoxp` Management ▶ `vdanp` Client

Buttons

Button	Meaning
Reset	Resets the entire table.
Reload	Updates the fields with the values that are saved in the volatile memory (`RAM`) of the device.
Help	Opens the online help.

5.29 Proxy Node Table

This dialog informs you of the connected devices for which this device provides PRP redundancy.

Note: The Redbox supports up to 128 hosts. When attempt to support more than 128 with the Redbox, then device drops packets.

■ Table

Parameters	Meaning
Index	Displays a sequential number to which the table entry relates. The device automatically defines this number. Possible values: ▶ `0..128`
MAC Address	Displays the MAC address of the connected devices for which this device implements PRP redundancy.

■ Buttons

Button	Meaning
Reset	Resets the entire table.
Reload	Updates the fields with the values that are saved in the volatile memory (`RAM`) of the device.
Help	Opens the online help.

5.30 Statistics

This dialog lists receive events for various MIB Managed Objects. Each entry represents link degradation for the MIB Managed Objects listed in the description column. The table lists how often the event occurred for each path through the device. The Port A entries for example, specify the path between the transceiver, through the Link Redundancy Entity (LRE) to the UDP and TCP layers.

■ Table

Parameters	Meaning
Description	Displays the MIB Managed Objects description to which the Port and Interlink entries refer.
Port A	Displays the number of MIB Managed Objects events on port A. The device examines the traffic as it passes from receive transceiver A to the LRE.
Port B	Displays the number of MIB Managed Objects events on port B. The device examines the traffic as it passes from receive transceiver B to the LRE.
Interlink	Displays the number of MIB Managed Objects events on the interlink. The counters are active for the MIB Managed Objects that pertain to the interlink. The other counters remain empty. A sample is made of the traffic as it passes from the LRE to the switch.
CPU Port	Displays the number of MIB Managed Objects events on the CPU Port. There is one MIB Managed Object that pertains to the CPU Port. The other counters remain empty. A sample is made of the traffic as it passes from receive transceiver to the CPU.

■ Buttons

Button	Meaning
Reset	Resets the entire table.
Reload	Updates the fields with the values that are saved in the volatile memory (`RAM`) of the device.
Help	Opens the online help.

5.31 HSR

As with PRP, an HSR-based ring also offers zero recovery time (HSR = High-availability Seamless Redundancy). HSR is suited for applications that demand high availability and short reaction times. For example, protection applications for electrical station automation and controllers for synchronized drives which require constant connection.

HSR Redundancy Boxes (RedBox) use 2 Ethernet ports operating in parallel to connect to a ring. An HSR RedBox operating in this configuration is a Doubly Attached Node implementing the HSR protocol (DANH). A standard ethernet device connected to the HSR ring through an HSR RedBox is a Virtual DANH (VDANH).

As with PRP, the transmitting HSR node or HSR RedBox sends twin frames, 1 in each direction, on the ring. For identification, the HSR node injects the twin frames with an HSR tag. The HSR tag consists of a port identifier, the length of the payload and a sequence number. In a normal operating ring, the destination HSR node or RedBox receives both frames within a certain time skew. An HSR node forwards the first frame to arrive to the upper layers and discards the second frame when it arrives. A RedBox on the other hand forwards the first frame to the VDANHs and discards the second frame when it arrives.

The device performs a specific role in the network. Configure a device as an HSR RedBox connecting standard ethernet devices to an HSR ring, or as an HSR node connecting a PRP LAN to an HSR ring.

A single HSR ring accommodates up to 7 PRP LANs. Configure the device to identify and tag the traffic addressed for the connected PRP LAN.

Limit the maximum number of nodes in an HSR ring to 10, so that a DAN or Redbox receives these packets within a specific time frame.

Note: HSR is available for devices with hardware for enhanced redundancy functions. In order to use the HSR functions, load the HSR device software.

The menu contains the following dialogs:

- HSR Configuration
- DAN/VDAN Table
- Proxy Node Table
- Statistics

5.32 HSR Configuration

With this dialog you activate or deactivate the HSR Protocol, manage HSR supervision packets, and configure the device for a specific network role.

MRP and STP cannot operate on the same ports as HSR. Deactivate or choose different ports for MRP and deactivate STP on the HSR ports.

Note: If HSR is active, it uses the interfaces 1/1 and 1/2. As seen in the `Switching > Rate Limiter` and `Switching > Filter for MAC Addresses` dialogs, the HSR function replaces the interfaces 1/1 and 1/2 with the interface hsr/1. Set up the VLAN membership and the rate limiting for the interface hsr/1.

■ Operation

Parameters	Meaning
Operation	Enables/disables the HSR function globally. Possible values: ▶ `On` The device processes the traffic according to the set up when this function is active. ▶ `Off` (default setting)

■ Port A/Port B

Parameters	Meaning
Port A	The textbox displays the number of the port which the device uses as the HSR port A. Using the radio buttons you enable/disable the HSR function on the port. Possible values: ▶ `On` (default setting) HSR function on the port is enabled. ▶ `Off` HSR function on the port is disabled.
Port B	The textbox displays the number of the port which the device uses as the HSR port B. Using the radio buttons you enable/disable the HSR function on the port. Possible values: ▶ `On` (default setting) HSR function on the port is enabled. ▶ `Off` HSR function on the port is disabled.

■ Supervision Packet Receiver

Parameters	Meaning
Evaluate Supervision Packets	Activates/deactivates the supervision packet analysis. Possible values: ▶ `marked` (default setting) Supervision packet analysis is active. The device receives supervision data packets and analyzes them. ▶ `unmarked` Supervision packet analysis is inactive. The device receives supervision data packets without analyzing them.

Supervision Packet Transmitter

Parameters	Meaning
Active	Enables/disables the transmission of supervision packets. Possible values: ▶ `On` (default setting) The transmission of supervision packets is enabled. The RedBox transmits its own supervision packets. ▶ `Off` The transmission of supervision packets is disabled.
Send VDAN Packets	Activates/deactivates the transmission of VDAN supervision packets. Prerequisite is that you enable the transmission of supervision packets, see the "Active" field. Possible values: ▶ `marked` The transmission of VDAN supervision packets is active. The RedBox transmits both its own supervision packets and the supervision packets for the VDANs listed in the "Proxy Node Table". ▶ `unmarked` (default setting) The transmission of VDAN supervision packets is inactive.

■ HSR Parameter

Parameters	Meaning
HSR Mode	Specifies the forwarding capacity of the device for unicast traffic. Possible values: ▶ `modeh` (default setting) If the host functions as a proxy for a destination device, it removes unicast traffic from the ring and forwards it to the destination address. ▶ `modeu` If the host operates as a proxy for a destination device, it forwards unicast traffic around the ring and forwards it to the destination address. When the frames return to the source node it discards the unicast traffic.

Parameters	Meaning
Switching Node Type	Specifies the function that the device executes in the HSR ring. Possible values: ▶ `hsrredboxsan` (default setting) You use this setting if you connect SANs to the device within a HSR ring. ▶ `hsrredboxprpa` You use this setting to connect the corresponding device with PRP LAN A. Furthermore, set the "Redbox Identity" parameter for the corresponding network connection. ▶ `hsrredboxprpb` You use this setting to connect the corresponding device with PRP LAN B. Furthermore, set the "Redbox Identity" parameter for the corresponding network connection.
Redbox Identity	Specifies the tags for the PRP LAN traffic. The parameter identifies and tags the data traffic for the PRP LAN that you connect to this device. The device identifies the traffic for up to 7 PRP LANs that you connect to the HSR ring. Prerequisite is that you set the "Switching Node Type" parameter to `hsrredboxprpa` or to `hsrredboxprpb`. Possible values: ▶ `id1a` (default setting) Use this value to handle the HSR data traffic for LAN A in PRP network 1. ▶ `id1b` Use this value to handle the HSR data traffic for LAN B in PRP network 1. ▶ `id2a` Use this value to handle the HSR data traffic for LAN A in PRP network 2. ▶ `id2b` Use this value to handle the HSR data traffic for LAN B in PRP network 2. ▶ `id7a` Use this value to handle the HSR data traffic for LAN A in PRP network 7. ▶ `id7b` Use this value to handle the HSR data traffic for LAN B in PRP network 7.

■ Buttons

Button	Meaning
Set	Transfers the changes to the volatile memory (`RAM`) of the device and applies them. 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 "Select" button. □ Click the "Save" button.
Reload	Updates the fields with the values that are saved in the volatile memory (`RAM`) of the device.
Help	Opens the online help.

5.33 DAN/VDAN Table

The "DAN/VDAN Table" (Double Attached Node / Virtual Double Attached Node) dialog helps to analyze the LANs. For example, when the "Last Seen …" counter of 1 port continually increases while the other remains the same. This condition indicates a loss of LAN connection.

■ Table

Parameters	Meaning
Index	Displays a sequential number for the node to which the table entry refers. The device automatically defines this number.
MAC Address	Displays the MAC address of the node.
Last Seen A	Displays the time between received first packets for this node on LAN A. When the counter threshold reaches 497 days, it restarts from 0.
Last Seen B	Displays the time between received first packets for this node on LAN B. When the counter threshold reaches 497 days, it restarts from 0.
Remote Node Type	Displays the type of node. Possible values: ▶ `RedBoxh` Management ▶ `vdanh` Client

■ Buttons

Button	Meaning
Reset	Resets the entire table.
Reload	Updates the fields with the values that are saved in the volatile memory (`RAM`) of the device.
Help	Opens the online help.

5.34 Proxy Node Table

This dialog informs you of the connected devices for which this device provides HSR redundancy.

■ Table

Parameters	Meaning
Index	Displays a sequential number to which the table entry relates. The device automatically defines this number. Possible values: ▶ `0..128`
MAC Address	Displays the MAC addresses of the connected devices for which this device implements HSR redundancy.

■ Buttons

Button	Meaning
Reset	Resets the entire table.
Reload	Updates the fields with the values that are saved in the volatile memory (`RAM`) of the device.
Help	Opens the online help.

5.35 Statistics

This dialog lists receive events for various MIB Managed Objects. Each entry represents link degradation for the MIB Managed Objects listed in the description column. The table lists how often the event occurred for each path through the device. The Port A entries for example, specify the path between the transceiver, through the Link Redundancy Entity (LRE) to the UDP and TCP layers.

■ Table

Parameters	Meaning
Description	Displays the MIB Managed Objects description to which the Port and Interlink entries refer.
Port A	Displays the number of MIB Managed Objects events on port A. The device examines the traffic as it passes from receive transceiver A to the LRE.
Port B	Displays the number of MIB Managed Objects events on port B. The device examines the traffic as it passes from receive transceiver B to the LRE.
Interlink	Displays the number of MIB Managed Objects events on the interlink. The counters are active for the MIB Managed Objects that pertain to the interlink. The other counters remain empty. A sample is made of the traffic as it passes from the LRE to the switch.
CPU Port	Displays the number of MIB Managed Objects events on the CPU Port. There is one MIB Managed Object that pertains to the CPU Port. The other counters remain empty. A sample is made of the traffic as it passes from receive transceiver to the CPU.

■ Buttons

Button	Meaning
Reset	Resets the entire table.
Reload	Updates the fields with the values that are saved in the volatile memory (`RAM`) of the device.
Help	Opens the online help.

5.36 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 device supports the Rapid Spanning Tree Protocol (RSTP) defined in standard IEEE 802.1D-2004. This protocol is a further development of the Spanning Tree Protocol (STP) and is compatible with it.

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

5.37 Spanning Tree - Global

With this dialog, you enable/disable the Spanning Tree function, view current values relating to the root bridge, 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 device ports.

■ Protocol Version

Parameters	Meaning
Protocol Version	Displays the protocol used for the Spanning Tree function: With `RSTP` (IEEE 802.1Q-2005) the Spanning Tree function is effective in all the configured VLANs.

■ Protocol Configuration / Information

Parameters	Meaning
Bridge	
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>`

Parameters	Meaning
Priority	Specifies the bridge priority of the device. Possible values: ▶ 0..61440 in steps of 4096 (default setting: 32,768) 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" column. Due to the interaction with the "Tx Hold Count" 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" column. In the RSTP protocol, the bridges negotiate a status change without a specified delay. The STP protocol uses the parameter to delay the status change between the statuses disabled, discarding, learning, forwarding.
The parameters "Forward Delay" and "Max Age" have the following relationship: Forward Delay ≥ (Max Age/2) + 1 If you enter a value in the field 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" column. The STP protocol uses the parameter to specify the validity of STP-BPDUs in seconds.

Parameters	Meaning
Tx Hold Count	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 device port. When the counter reaches the value specified here, the device port stops sending BPDUs. On the one hand, this reduces the load generated by RSTP, and on the other a loop 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.
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: ▶ `unmarked` (default setting) The BPDU Guard function is inactive. ▶ `marked` The BPDU Guard function is active. – The device activates the function for manually specified edge ports (end device ports). In the "CIST" tab, the checkbox for these device ports in the "Admin Edge Port" column is `marked`. – If an edge port receives an STP-BPDU, the device deactivates the port. In the "Configuration" tab of the `Basic Settings >` Port-dialog, the checkbox for these device ports in the "Port on" column is `marked`. To reset the status of the device port to the value `forwarding`, you proceed as follows: ☐ If the device 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 device port, proceed as follows: – Open the `Basic Settings > Port` dialog, "Configuration" tab. – Mark the checkbox in the "Port on" column.

Parameters	Meaning
Root	
Bridge ID	Displays the bridge ID of the current root bridge. Possible values: ▶ `<Bridge priority> / <MAC address>` The bridge ID is made up of the bridge priority and the MAC address.

Parameters	Meaning
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" column.
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" column. In the RSTP protocol, the bridges negotiate a status change without a specified delay. The STP 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 STP protocol uses the parameter to specify the validity of STP-BPDUs in seconds.

Parameters	Meaning
Topology	
Bridge is Root	Displays whether the device currently has the role of the root bridge. Possible values: ▶ `unmarked` Another device currently has the role of the root bridge. ▶ `marked` The device currently has the role of the root bridge.
Root Port	Displays the number of the device 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.

Parameters	Meaning
Topology Change Count	Displays how often the device has put a device 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

Button	Meaning
Set	Transfers the changes to the volatile memory (`RAM`) of the device and applies them. 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 "Select" button. ☐ Click the "Save" button.
Reload	Updates the fields with the values that are saved in the volatile memory (`RAM`) of the device.
Help	Opens the online help.

5.38 Spanning Tree - Port

With this dialog you can switch the Spanning Tree function on/off on the device ports, specify edge ports, and specify the settings for various protection functions.

The dialog contains the following tabs:

- CIST
- Guards

5.38.1 CIST

On this tab page you can switch the Spanning Tree function on/off on the device ports individually, specify the settings for edge ports, and view the current values. The abbreviation CIST stands for Common and Internal Spanning Tree.

Note: If you are using other layer 2 redundancy protocols parallel to Spanning Tree on the device: Switch off the Spanning Tree function on the device ports that are participating in other redundancy protocols. Otherwise the redundancy may operate differently to the way intended. This can cause loops.

■ Table

Parameters	Meaning
Port	Displays the number of the device port to which the table entry relates.
Stp active	Activates/deactivates the Spanning Tree function on the device port. Possible values: ▶ `marked` (default setting) ▶ `unmarked` If the Spanning Tree is active in the device and inactive on the device port, the port does not send STP-BPDUs and drops any STP-BPDUs received.
Port State	Displays the transmission status of the device port. Possible values: ▶ `discarding` The device port is blocked and forwards STP-BPDUs exclusively. ▶ `learning` The device port is blocked, but it learns the MAC addresses of received data packets. ▶ `forwarding` The device port forwards data packets. ▶ `disabled` The device port is disabled. See the `Basic Settings > Port` dialog, tab "Configuration". ▶ `manualFwd` The Spanning Tree function is inactive on the device port. The device port forwards STP-BPDUs. ▶ `notParticipate` The device port is not participating in STP.

Parameters	Meaning
Port Role	Displays the current role of the device port in CIST. Possible values: ▶ `root` Device port with the cheapest path to the root bridge. ▶ `alternate` Device port with the alternative path to the root bridge (currently interrupted). ▶ `designated` Device port for the side of the tree averted from the root bridge. ▶ `backup` Device port receives STP-BPDUs from its own device. ▶ `disabled` The device port is inactive. See the `Basic Settings > Port` dialog, tab "Configuration".
Port Pathcost	Specifies the path costs of the device 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 device port.
Port Priority	Specifies the priority of the device port. Possible values: ▶ `16..240` in steps of 16 (default setting: `128`) This value represents the first 4 bits of the port ID.
Received Bridge ID	Displays the bridge ID of the device from which this device port last received an STP-BPDU. Possible values: ▶ For device 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 device port has no connection, or if it has not received any STP-BDPUs yet, the device displays the values that the device port would send with the `designated` role.

Parameters	Meaning
Received Port ID	Displays the port ID of the device from which this device port last received an STP-BPDU. Possible values: ▶ For device 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 device port has no connection, or if it has not received any STP-BDPUs yet, the device displays the values that the device 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 device 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 device port has no connection, or if it has not received any STP-BDPUs yet, the device displays the values that the device port would send with the `designated` role.
Admin Edge Port	Specifies whether a end device is connected to the device port. Possible values: ▶ `unmarked` (default setting) An STP bridge is connected to the device port. After the connection is set up, the device port changes to the `learning` status before changing to the `forwarding` status, if applicable. ▶ `marked` A end device is connected to the device port. – After the connection is set up, the device port changes to the `forwarding` status without changing to the `learning` status beforehand. – If the device port receives an STP-BPDU, the device deactivates the port if the BPDU Guard function is inactive in the `Switching >` L2-Redundancy `> Spanning Tree > Global` dialog.

Parameters	Meaning
Auto Edge Port	Activates/deactivates the automatic detection of whether you connect an end device to the port. This setting is effective if you unmark the checkbox in the "Admin Edge Port" field. Possible values: ▶ `marked` (default setting) 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` 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 a terminal device or an STP bridge is connected to the device port. Possible values: ▶ `enable` A terminal device is connected to the device port. The device port does not receive any STP-BPDUs. ▶ `disable` An STP bridge is connected to the device port. The device port receives STP-BPDUs.
Oper PointToPoint	Displays whether the port is connected to an STP device via a direct full-duplex link. Possible values: ▶ `true` The device 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 device port is connected in another way, e.g. via a half-duplex link or via a hub.

■ Buttons

Button	Meaning
Set	Transfers the changes to the volatile memory (`RAM`) of the device and applies them. 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 "Select" button. ☐ Click the "Save" button.
Reload	Updates the fields with the values that are saved in the volatile memory (`RAM`) of the device.
Help	Opens the online help.

5.38.2 Guards

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

■ Table

Parameters	Meaning
Port	Displays the number of the device port to which the table entry relates.
Root Guard	Activates/deactivates the monitoring of STP-BPDUs on the device port. 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 device ports with the STP role `designated`. Possible values: ▶ `unmarked` (default setting) The monitoring of STP-BPDUs is inactive. ▶ `marked` The monitoring of STP-BPDUs is active. – If the device 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 device 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 device port after 2 × "Hello Time [s]". If you activate the "Root Guard" function while the "Loop Guard" function is active, the device deactivates the "Loop Guard" function.
TCN Guard	Activates/deactivates the monitoring of "Topology Change Notifications" on the device port. With this setting the device helps you protect your network from attacks with STP-BPDUs that try to change the topology. Possible values: ▶ `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 (FDB) of the device port and forwards the Topology Change Notifications. ▶ `marked` The monitoring of "Topology Change Notifications" is enabled. – The device 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.

Parameters	Meaning
Loop Guard	Activates/deactivates the monitoring of loops on the device port. With this setting the device prevents loops if the device port does not receive any more STP-BPDUs. Use this setting solely for device ports with the STP role `alternate`, `backup` or `root`. Possible values: ▶ `unmarked` (default setting) The monitoring of loops is inactive. If the device port does not receive any STP-BPDUs for a while, the device sets the status of the port to the value `forwarding`. ▶ `marked` The monitoring of loops is active. This prevents 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 device 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" field to `true`. – If the device 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" field to `false`. If you activate the "Loop Guard" function while the "Root Guard" function is active, the device deactivates the "Root Guard" function.
Loop Status	Displays whether the loop state of the device port is inconsistent. Possible values: ▶ `true` The loop state of the device port is inconsistent: – The device port is not receiving any STP-BPDUs and the “Root Guard” function is switched on. – The device sets the state of the device port to the value `discarding`. The device thus prevents any potential loops. ▶ `false` The loop state of the device port is consistent: The device port receives STP-BPDUs.
Trans. into Loop	Displays how often the device has set the value in the "Loop State" field from `false` to `true`.

Parameters	Meaning
Trans. out of Loop	Displays how often the device has set the value in the "Loop State" field from `true` to `false`.
BPDU Guard Effect	Displays whether the device port received an STP-BPDU as an edge port (end device port). Prerequisite: – The device port is a manually specified edge port (end device 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 enabled. Possible values: ▶ `disable` The device port is an edge port (end device port) and has not received any STP-BPDUs, or the device port is not an edge port. ▶ `enable` The device port is an edge port (end device port) and received an STP-BPDU. The device deactivates the port. In the `Basic Settings > Port` dialog, "Configuration" tab, the checkbox for this port in the "Port on" column is `unmarked`. To reset the status of the device port to the value `forwarding`, you proceed as follows: □ If the device port is still receiving BPDUs: – In the "CIST" tab, remove the selection from the checkbox in the "Admin Edge Port" column. or – In the `Switching > L2-Redundancy > Spanning Tree > Global` dialog, remove the selection in the "BPDU Guard" checkbox. □ To activate the device port, proceed as follows: – Open the `Basic Settings > Port` dialog, "Configuration" tab. – Mark the checkbox in the "Port on" column.

Buttons

Button	Meaning
Set	Transfers the changes to the volatile memory (`RAM`) of the device and applies them. 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 "Select" button. □ Click the "Save" button.

Button	Meaning
Reload	Updates the fields with the values that are saved in the volatile memory (`RAM`) of the device.
Help	Opens the online help.

5.39 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: ▶ Alphanumerical ASCII 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.

Parameters	Meaning
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.
Min. Active Ports	Specifies the minimum number of active LAG interfaces for the Link Aggregation group. Possible values: ▶ `1..2` (default setting: `1`)
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.
Link Trap	Activates/deactivates link state SNMP trap for the port. Possible values: ▶ `marked` (default setting) The device sends an SNMP trap to the network management station when the link state changes for the LAG port. ▶ `unmarked` Deactivates SNMP trap transmission. 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 SNMP manager.

Parameters	Meaning
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. The pull down menu provides you with the following variations of selectable values allowing you to have administrative control over the LACPDU parameters: – LACP Activity: This parameter determines 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. – LACP Timeout: 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 time-out. – Aggregation: This parameter determines whether the port is a potential candidate for aggregation or is an individual link. When selected you set the parameter to aggregatable. Possible values: ▶ `lacpActivity`, `lacpTimeout`, `aggregation` ▶ `lacpActivity`, `lacpTimeout` ▶ `lacpTimeout`, `aggregation` ▶ `lacpActivity`, `aggregation` ▶ `lacpActivity` ▶ `lacpTimeout` ▶ `aggregation` ▶ `-` The parameter is unspecified. When the parameter is unspecified the device displays the following values for the LACPDU parameters: ▶ `synchronization` When displayed, the system considers this link as 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` When displayed, 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` When displayed, distribution is currently disabled and remains disabled in the absence of administrative changes or changes in received protocol information. ▶ `defaulted` When displayed, the LACPDUs received by the actor is using the statically configured partner information. ▶ `expired` When displayed, the LACPDUs received by the actor is in the expired state.

Parameters	Meaning
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. To manage the partner ports, you use the "LACP Partner Port Admin Key" parameter in conjunction with "LACP Partner Admin Sys Priority", "LACP Partner Admin SysID", "LACP Partner Admin Port", and "LACP Partner Admin Port Priority". 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.

Parameters	Meaning
LACP Partner Admin State	Specifies the partner administrative state values. The following selectable values provide administrative control over the LACPDU parameters: – LACP Activity - this parameter determines 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. – LACP Timeout - 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 time out. – Aggregation - this parameter determines whether the port is a potential candidate for aggregation or as an individual link. When selected you set the parameter to aggregateable. Possible values: ▶ `lacpActivity`, `lacpTimeout`, `aggregation` ▶ `lacpActivity`, `lacpTimeout` ▶ `lacpTimeout`, `aggregation` ▶ `lacpActivity`, `aggregation` ▶ `lacpActivity` ▶ `lacpTimeout` ▶ `aggregation` ▶ `-` The "LACP Partner Admin State" parameter is unspecified. ▶ synchronization When displayed, 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 When displayed, 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 When displayed, distribution is currently disabled and remains disabled in the absence of administrative changes or changes in received protocol information. ▶ defaulted When displayed, the LACPDUs recieved by the actor is using the statically configured partner information. ▶ expired When displayed, the LACPDUs recieved by the partner is in the expired state.

Parameters	Meaning
LACP Partner Admin Port	Specifies the port number of the partner port. To manage the partner ports, you use the "LACP Partner Admin Port" parameter in conjunction with "LACP Partner Admin Sys Priority", "LACP Partner Admin SysID", "LACP Partner Port Admin Key", and "LACP Partner Admin Port Priority". Possible values: ▶ `0..65535` (default setting: `0`)
LACP Partner Admin Port Priority	Specifies the port priority for the partner port. To manage the partner ports, you use the "LACP Partner Admin Port Priority" parameter in conjunction with "LACP Partner Admin Sys Priority", "LACP Partner Admin SysID", "LACP Partner Port Admin Key", and "LACP Partner Admin Port" Possible values: ▶ `0..65535` (default setting: `0`) The port with the lower value has the higher priority.
LACP Partner Admin SysID	Specifies a MAC Address value representing the Partner System ID. To manage the partner ports, you use the "LACP Partner Admin SysID" parameter in conjunction with "LACP Partner Admin Sys Priority", "LACP Partner Port Admin Key", "LACP Partner Admin Port", and "LACP Partner Admin Port Priority". Possible values: ▶ valid MAC address (default setting: `00:00:00:00:00:00`)
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. To manage the partner ports, you use the "LACP Partner Admin Sys Priority" parameter in conjunction with "LACP Partner Admin SysID", "LACP Partner Port Admin Key", "LACP Partner Admin Port", and "LACP Partner Admin Port Priority". Possible values: ▶ `0..65535` (default setting: `0`) The port with the lower value has the higher priority.

■ Buttons

Button	Meaning
Set	Transfers the changes to the volatile memory (`RAM`) of the device and applies them. 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 "Select" button. □ Click the "Save" button.
Reload	Updates the fields with the values that are saved in the volatile memory (`RAM`) of the device.
Create	Opens the "Create", dialog to add a new entry to the table. In the "Lag Index" field you specify the port number of the Link Aggregation Group trunk.
Remove	Removes the highlighted table entry.
Add Ports	Opens the "Select Ports to add" window. This window allows you to assign available ports to the interface.
Help	Opens the online help.

5.40 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: ▶ Alphanumerical ASCII string with 0..255 characters

Parameters	Meaning
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.
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 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 Active	Enables/disables the automatic fail back function. Possible values: ▶ `marked` (default setting) The fail back function is enabled. The backup port changes to `blocking` and the primary port changes to `forwarding` after the delay timer expires. ▶ `unmarked` The fail back function is disabled. 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`.

Parameters	Meaning
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.

■ 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.

Buttons

Button	Meaning
Set	Transfers the changes to the volatile memory (`RAM`) of the device and applies them. 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 "Select" button. □ Click the "Save" button.
Reload	Updates the fields with the values that are saved in the volatile memory (`RAM`) of the device.
Create	Adds a new table entry.
Remove	Removes the highlighted table entry.
Help	Opens the online help.

6 Diagnostics

The dialogs in this menu display information on the operating status of the device and registered events. In service cases, this information helps our support to diagnose the situation.

The menu contains the following dialogs:

6.1 Status Configuration

In the dialogs of this menu, you specify which functions, statuses, and events the device monitors and registers.

The menu contains the following dialogs:

- Device Status
- Security Status
- Alarms (Traps)

6.2 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 the detected faults in the "Device Status" frame of the `Basic Settings > System` dialog for the monitored functions. When the device indicates more than 1 detected errors in the "Device Status" text box, use the arrow buttons to view the other detected faults. The device sorts the detected faults in the order in which they occur.

The dialog contains the following tabs:

- Global
- Port
- Status

6.2.1 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`

■ Trap Configuration

Parameters	Meaning
Generate Trap	Specifies whether the device sends a SNMP trap when it detects a change in the monitored functions. Possible values: ▶ `marked` The device sends a SNMP trap. ▶ `unmarked` (default setting) The device does not send a 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 SNMP manager.

■ Table

Parameters	Meaning
Ring redundancy	Specifies whether the device monitors the ring redundancy. Possible values: ▶ `unmarked` (default setting) The device ignores this parameter. ▶ `marked` 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.
Connection error	Specifies whether the device monitors the link status of the device ports. Possible values: ▶ `unmarked` (default setting) The device ignores this parameter. ▶ `marked` When the link on a device port is interrupted, the "Device status" changes to `Error`. Select the ports to monitor in the "Port" tab. You have the option of selecting the device ports to be monitored individually.

■ Buttons

Button	Meaning
Set	Transfers the changes to the volatile memory (`RAM`) of the device and applies them. 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 "Select" button. □ Click the "Save" button.
Reload	Updates the fields with the values that are saved in the volatile memory (`RAM`) of the device.
Help	Opens the online help.

6.2.2 Port

■ Table

Parameters	Meaning
Propagate Connection Error	Specifies whether the device monitors the link status of the port. Possible values: ▶ `marked` When the link on this port is interrupted, the "Device status" changes to `Error`. ▶ `unmarked` (default setting) The "Device status" remains unchanged if the link on this port is interrupted. This setting is effective when you select the "Connection error" checkbox in the "Global" tab of the `Diagnostics > Status Configuration > Device Status` dialog.

■ Buttons

Button	Meaning
Set	Transfers the changes to the volatile memory (`RAM`) of the device and applies them. 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 "Select" button. □ Click the "Save" button.
Reload	Updates the fields with the values that are saved in the volatile memory (`RAM`) of the device.
Help	Opens the online help.

6.2.3 Status

■ Table

Parameters	Meaning
Timestamp	Displays the date and time of the event.
Cause	Displays the event which caused the SNMP trap.

■ Buttons

Button	Meaning
Set	Transfers the changes to the volatile memory (`RAM`) of the device and applies them. 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 "Select" button. ☐ Click the "Save" button.
Reload	Updates the fields with the values that are saved in the volatile memory (`RAM`) of the device.
Help	Opens the online help.

6.3 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 the detected faults in the "Security Status" frame of the `Basic Settings > System` dialog for the monitored functions. When the device indicates more than 1 detected fault in the "Alarm Counter" text box, use the arrow buttons to view the other detected faults. The device sorts the detected faults in the order in which they occur.

The dialog contains the following tabs:

- Global
- Port
- Status

6.3.1 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`

■ Trap Configuration

Parameters	Meaning
Generate Trap	Specifies whether the device sends a SNMP trap when it detects a change in the monitored functions. Possible values: ▶ `marked` The device sends a SNMP trap. ▶ `unmarked` (default setting) The device does not send a 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 SNMP manager.

■ Table

Parameters	Meaning
Password default settings unchanged	Specifies whether the device monitors the password for the locally set up user accounts `user` and `admin`. Possible values: ▶ `unmarked` The device ignores this parameter. ▶ `marked` (default setting) When the password for the `user` or `admin` user accounts is the default setting, the "Security Status" changes to `Error`. You set the password in the `Device Security > User Management` dialog.
Minimum Password Length < 8	Specifies whether the device monitors the policy "Minimum Password Length". Possible values: ▶ `unmarked` The device ignores this parameter. ▶ `marked` (default setting) When the value for the password policy is less than `8`, the "Security Status" changes to `Error`. You specify the "Minimum Password Length" policy in the `Device Security > User Management` dialog in the "Configuration" frame.
Password Policy settings deactivated	Specifies whether the device monitors the Password policies settings. Possible values: ▶ `unmarked` The device ignores this parameter. ▶ `marked` (default setting) When the value for at least one of the following policies is `0`, the "Security Status" changes to `Error`: – Minimum Upper Cases – Minimum Lower Cases – Minimum Numbers – Minimum Special Characters You specify the policy settings in the `Device Security > User Management` dialog in the "Password Policy" frame.
User account password Policy Check deactivated	Specifies whether the device monitors the status of the function "Policy Check". Possible values: ▶ `unmarked` (default setting) The device ignores this parameter. ▶ `marked` When the function "Policy Check" is deactivated for at least 1 user account, the "Security Status" changes to `Error`. You activate the "Policy Check" function in the `Device Security > User Management` dialog.

Parameters	**Meaning**
Telnet server active	Specifies whether the device monitors the status of the Telnet server. Possible values: ▶ unmarked The device ignores this parameter. ▶ marked (default setting) When the Telnet server is enabled, the "Security Status" changes to Error. You enable/disable the Telnet server in the Device Security > Management Access > Server dialog, on the "Telnet" tab page.
HTTP server active	Specifies whether the device monitors the status of the HTTP server. Possible values: ▶ unmarked The device ignores this parameter. ▶ marked (default setting) When the HTTP server is enabled, the "Security Status" changes to Error. You enable/disable the HTTP server in the Device Security > Management Access > Server dialog, on the "HTTP" tab page.
SNMP unencrypted	Specifies whether the device monitors the status of the SNMP agent. Possible values: ▶ unmarked The device ignores this parameter. ▶ marked (default setting) When at least one of the following conditions applies, the "Security Status" changes to Error: – The "SNMPv1 enabled" function is enabled. – The "SNMPv2 enabled" 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. You specify the settings for the SNMP agent in the Device Security > Management Access > Server dialog, on the "SNMP" tab page.
Access to System Monitor with V.24 possible	Specifies whether the device monitors the option to switch to the system monitor. Possible values: ▶ unmarked (default setting) The device ignores this parameter. ▶ marked When the access to the system monitor is possible, the "Security Status" changes to Error. When the device boots up, the user has the possibility to open the system monitor via a V.24 connection. You enable/disable the system monitor in the Diagnostics > System > Selftest dialog.

Parameters	Meaning
Link interrupted on enabled device ports	Specifies whether the device monitors the link status of the enabled device ports. Possible values: ▶ `unmarked` (default setting) The device ignores this parameter. ▶ `marked` When the link on an enabled device port is interrupted, the "Security Status" changes to `Error`. Select the ports to monitor in the "Port" tab. You have the option of selecting the device ports to be monitored individually.
Write access using HiDiscovery possible	Specifies whether the device monitors the status of HiDiscovery. Possible values: ▶ `unmarked` The device ignores this parameter. ▶ `marked` (default setting) When "Operation" for the HiDiscovery Protocol is "On" and "Access" is `readWrite`, the "Security Status" changes to `Error`. You enable/disable the HiDiscovery Protocol in the `Basic Settings >` Network dialog, "HiDiscovery Protocol" frame.
IEC61850-MMS active	Specifies whether the device monitors the activation of the IEC61850 MMS protocol. Possible values: ▶ `unmarked` The device ignores this parameter. ▶ `marked` (default setting) When you activate the IEC61850-MMS protocol, the "Security Status" changes to `Error`. You activate the protocol in the "Operation" frame located in the `Industrial Protocols > IEC61850-MMS` dialog.
Self-signed HTTPS certificate present	Specifies whether the device monitors the HTTPS certificate. Possible values: ▶ `unmarked` The device ignores this parameter. ▶ `marked` (default setting) When the HTTPS server uses a self-created digital certificate, the "Security Status" changes to `Error`.

Buttons

Button	Meaning
Set	Transfers the changes to the volatile memory (RAM) of the device and applies them. 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 "Select" button. ☐ Click the "Save" button.
Reload	Updates the fields with the values that are saved in the volatile memory (RAM) of the device.
Help	Opens the online help.

6.3.2 Port

■ Table

Parameters	Meaning
Link interrupted on enabled device ports	Specifies whether the device monitors the link status of an enabled port. Possible values: ▶ `marked` When the port is enabled on (dialog `Basic Settings > Port`, "Configuration" tab, checkbox "Port on" is marked) and the link is down on the port, the "Security Status" changes to `Error`. ▶ `unmarked` (default setting) The security status remains unchanged if someone sets up a connection via the port. This setting takes effect when you select the "Link interrupted on enabled device ports" checkbox in the `Diagnostics > Status Configuration >` Security Status dialog, "Global" tab.

■ Buttons

Button	Meaning
Set	Transfers the changes to the volatile memory (`RAM`) of the device and applies them. 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 "Select" button. □ Click the "Save" button.
Reload	Updates the fields with the values that are saved in the volatile memory (`RAM`) of the device.
Help	Opens the online help.

6.3.3 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

Button	Meaning
Set	Transfers the changes to the volatile memory (`RAM`) of the device and applies them. 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 "Select" button. □ Click the "Save" button.
Reload	Updates the fields with the values that are saved in the volatile memory (`RAM`) of the device.
Help	Opens the online help.

6.4 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 SNMP managers 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	Specifies whether the device sends SNMP traps to the SNMP managers. Possible values: ▶ `On` (default setting) The device sends SNMP traps to the specified SNMP managers. ▶ `Off` The device does not send any SNMP traps.

Table

Parameters	Meaning
Name	Specifies the name of the SNMP manager. Possible values: ▶ Alphanumeric ASCII character string with 1..32 characters
Address	Specifies the IP address and the port number of the SNMP manager. Possible values: ▶ `<Valid IPv4 address>:<port number>`
Active	Specifies whether the device sends SNMP traps to this SNMP manager. Possible values: ▶ `marked` (default setting) The device sends SNMP traps to this SNMP manager. ▶ `unmarked` The device does not send SNMP traps to this SNMP manager.

■ Buttons

Button	Meaning
Set	Transfers the changes to the volatile memory (`RAM`) of the device and applies them. 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 "Select" button. □ Click the "Save" button.
Reload	Updates the fields with the values that are saved in the volatile memory (`RAM`) of the device.
Create	Opens the "Create" dialog to add a new entry to the table. ▶ In the "Name" field you specify a name for the SNMP manager. ▶ In the "Address" field you specify the IP address and the port number of the SNMP manager. If you choose not to enter a port number, the device automatically adds the port number `162`.
Remove	Removes the highlighted table entry.
Help	Opens the online help.

6.5 System

The dialogs in this menu allow you to display the current operating parameters of the device to check the congruence of the settings with the network environment and to control the starting behavior of the device.

The menu contains the following dialogs:

- System Information
- Hardware State
- Configuration Check
- IP Address Conflict Detection
- ARP Table
- Selftest

6.6 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.

The dialog allows you to search the page for search terms and save them in HTML format on your PC.

■ Buttons

Button	Meaning
Reload	Updates the fields with the values that are saved in the volatile memory (`RAM`) of the device.
Search	Opens the "Search" dialog. The dialog allows you to search the log file for search terms or regular expressions.
Save	Opens the "Save" dialog. The dialog allows you to save the log file in HTML format on your PC.
Help	Opens the online help.

6.7 Hardware State

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

Information

Parameters	Meaning
Operating Time	Displays the total operating time of the device since it was delivered. Possible values: ▶ `day(s), hh:mm:ss`

Table

Parameters	Meaning
Flash Region	Displays the name of the respective memory area.
Description	Displays a description of what the memory uses the memory area for.
Flash Sectors	Displays how many sectors are assigned to the memory area.
Number of Sector Erase Operations	Displays how often the device has overwritten the sectors of the memory area.

Buttons

Button	Meaning
Reload	Updates the fields with the values that are saved in the volatile memory (`RAM`) of the device.
Help	Opens the online help.

6.8 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 "Reload" 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

Parameters	Meaning
Number of Errors	Displays the number of errors that the device detected during the configuration check.
Number of Warnings	Displays the number of warnings that the device detected during the configuration check.
Amount of Information	Displays the amount of information that the device detected during the configuration check.

You will also find this information in the status bar above the menu.

Table

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

Parameters	Meaning
Rule ID	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 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	The dialog specifies more precisely the information, warnings and errors having occurred.

Note: A neighboring device without LLDP support, which forwards LLDP packets, may be the cause of equivocal messages in the dialog. This occurs if the neighboring device is a hub or a switch without management, which ignores the IEEE 802.1D-2004 standard.
In this case, the dialog displays the devices recognized and connected to the neighboring device as connected to the switch port, even though they are connected to the neighboring device.

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

Buttons

Button	Meaning
Reload	Updates the fields with the values that are saved in the volatile memory (RAM) of the device.
Help	Opens the online help.

6.9 IP Address Conflict Detection

The device allows you to detect whether another device in the network is using its own IP address.

In this dialog you specify the procedure with which the device detects address conflicts and specify the required settings for this. In the table the device logs instances of another device in the network using its own IP address.

■ Operation

Parameters	Meaning
Operation	When the function is switched on, the device detects whether another device in the network is using its own IP address. Possible values: ▶ `On` (default setting) The address conflict detection is switched on. ▶ `Off` The address conflict detection is switched off.

■ 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 switched off. – 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 gratuituous ARP data packets. The device repeats this procedure for the number of times specified in the "Number of 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`)
Number of Address Protections	Specifies how often 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	Specifies whether the device sends an SNMP trap when it detects during the periodic address conflict detection an address conflict. Possible values: ▶ `marked` The device sends an SNMP trap. ▶ `unmarked` (default setting) The device does not send an SNMP trap. The prerequisite for sending SNMP traps is that you enable the function in the `Diagnostics > Status Configuration > Alarms (Traps)` dialog and at least 1 SNMP manager is specified.

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
Time Stamp	Displays the time at which the device detected an address conflict.
Port	Displays the number of the device 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

Button	Meaning
Set	Transfers the changes to the volatile memory (`RAM`) of the device and applies them. 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 "Select" button. ☐ Click the "Save" button.
Reload	Updates the fields with the values that are saved in the volatile memory (`RAM`) of the device.
Help	Opens the online help.

6.10 ARP Table

This dialog allows you to display the MAC and IP addresses of the neighboring devices connected to the device. The device determines these addresses using the Address Resolution Protocol (ARP) before the connection to the corresponding neighboring device is set up for the first time.

■ Table

Parameters	Meaning
Port	Number of the device port to which the table entry relates.
MAC Address	Displays the MAC address of a device that responded to an ARP query to this device port.
IP Address	Displays the IP address of a device that responded to an ARP query to this device port.
Type	Displays the type of the address entry. Possible values: ▶ `static` Static ARP entry. This entry is kept when the ARP table is deleted. ▶ `dynamic` Dynamic entry. The device deletes this entry when the “Aging Time” has been exceeded, if the device does not receive any data from this device during this time.

To empty the table, click "Reset ARP table" in the `Basic Settings >` Restart dialog.

■ Buttons

Button	Meaning
Reload	Updates the fields with the values that are saved in the volatile memory (`RAM`) of the device.
Reset ARP Table	Removes the dynamically set up addresses from the ARP table.
Help	Opens the online help.

6.11 Selftest

This dialog allows you to do the following:

- Activate/deactivate the RAM test when the device is being started.
- Enable/disable the switch to the system monitor when the device is being started.
- Specifies how the device behaves in the case of an error.

Configuration

Parameters	Meaning
RAM Test	Specifies whether the device tests the RAM memory during the restart. Possible values: - `marked` (default setting) The device tests the RAM memory during the restart. - `unmarked` The device skips the memory test during the restart. This shortens the start time for the device.
Activate SysMon1	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 delivery settings if the device does not detect any readable configuration profile when it is restarting. Possible values: - `marked` (default setting) The device loads the delivery settings (default configuration). - `unmarked` The device interrupts the restart and stops. To access the management functions is possible solely using the CLI through the V.24 interface of the device. To regain the access to the device through the network, open the system monitor and reset the settings. Upon restart, the device loads the delivery settings (default configuration).

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.

- "Activate SysMon1" 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, e.g. if a task terminates or is not available. ▶ `resource` The device detects errors in the resources available, e.g. if the memory is becoming scarce. ▶ `software` The device detects software errors, e.g. error in the consistency check. ▶ `hardware` The device detects hardware errors, e.g. 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 (system log). ▶ `sendTrap` The device sends an SNMP trap. Prerequisite for sending SNMP traps is that you enable the function in the `Diagnostics > Status Configuration > Alarms (Traps)` dialog and at least 1 SNMP manager is specified.

Buttons

Button	Meaning
Set	Transfers the changes to the volatile memory (`RAM`) of the device and applies them. 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 "Select" button. ☐ Click the "Save" button.
Reload	Updates the fields with the values that are saved in the volatile memory (`RAM`) of the device.
Help	Opens the online help.

6.12 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	When the function is switched on, the device sends the events specified in the table to the specified syslog servers. Possible values: ▶ `On` ▶ `Off` (default setting)

■ Table

Parameters	Meaning
Index	Displays a sequential number to which the table entry relates. The device automatically defines 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. Possible values: ▶ `1..8`
IP address	Specifies the IP address of the syslog server. Possible values: ▶ Valid IP address (default setting: `0.0.0.0`)
Port	Specifies the UDP Port on which the syslog server expects the log entries. Possible values: ▶ `1..65535` (default setting `514`)

Parameters	Meaning
Minimum 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

Button	Meaning
Set	Transfers the changes to the volatile memory (`RAM`) of the device and applies them. 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 "Select" button. □ Click the "Save" button.
Reload	Updates the fields with the values that are saved in the volatile memory (`RAM`) of the device.
Create	Adds a new table entry.
Remove	Removes the highlighted table entry.
Help	Opens the online help.

6.13 Ports

The device allows you with the functions in this menu to monitor the operation of the device ports.

The menu contains the following dialogs:

- SFP
- Port Monitor
- Auto Disable
- Port Mirroring

6.14 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 number of the device port to which the table entry relates.
Module Type	Type of the SFP transceiver, e.g. M-SFP-SX/LC.
Serial Number	Serial number of the SFP module.
Supported	Displays whether the media module supports the SFP transceiver.
Temperature in °Celsius	Operating temperature of the SFP transceiver in °Celsius.
Tx Power in mW	Transmission power of the SFP transceiver in mW.
Rx Power in mW	Receiving power of the SFP transceiver in mW.
Tx Power in dBm	Transmission power of the SFP transceiver in dBm.
Rx Power in dBm	Receiving power of the SFP transceiver in dBm.
Rx Power State	Power level of the signal received: The threshold values are specified by the SFP transceiver. ✓ Signal strength is OK. ⚠ Signal strength is lower than the SFP manufacturer recommendation. The signal can still be used. ⊗ No signal or signal strength too low.

Buttons

Button	Meaning
Reload	Updates the fields with the values that are saved in the volatile memory (RAM) of the device.
Help	Opens the online help.

6.15 Port Monitor

In this dialog, you specify whether the device deactivates the respective device port or sends an SNMP trap when it recognizes link flaps, CRC/fragment errors, or duplex conflicts.

Procedure:
☐ Enable the port monitor globally.
☐ Configure the conditions on a port.
☐ Configure an action to perform on that port when the condition occurs:

The dialog contains the following tabs:
- ▶ Global
- ▶ Link Flap
- ▶ CRC/Fragments

6.15.1 Global

In this tab, you specify the settings individually for every device port. Specify whether the device deactivates the device port or sends an SNMP trap when it recognizes link flaps, CRC/fragment errors or duplex conflicts.

■ Operation

Parameters	Meaning
Operation	Enables or disables the port monitoring function globally. Possible values: ▶ `On` ▶ `Off` (default setting)

■ Table

Parameters	Meaning
Port	Displays the number of the device port to which the table entry relates.
Link Flap on	Specifies whether the device monitors link flaps on the port. Possible values: ▶ `unmarked` (default setting) The port monitoring is disabled. ▶ `marked` The device monitors link flaps on the port. If the device detects too many link flaps on the port, the device executes the action specified in the "Action" column. You specify the criteria to be monitored in the "Link Flap" tab.
CRC/Fragments on	Specifies whether the device monitors CRC/fragment errors on the port. Possible values: ▶ `unmarked` (default setting) The port monitoring is disabled. ▶ `marked` The device monitors CRC/fragment errors on the port. If the device detects too many CRC/fragment errors on the port, the device executes the action specified in the "Action" column. You specify the criteria to be monitored in the "CRC/Fragments" tab.

Parameters	Meaning
Duplex Mismatch Detection active	Specifies whether the device monitors duplex mismatches on the port. Possible values: ▶ `unmarked` (default setting) The port monitoring is disabled. ▶ `marked` The device monitors duplex mismatches on the port. If the device detects a duplex mismatch on the port, the device executes the action specified in the "Action" column.
Active Condition	Displays which configured condition caused an action to occur. Possible values: ▶ `-` ▶ `Link Flap` ▶ `CRC/Fragments` ▶ `Duplex Mismatch`
Action	Specifies the action that the device executes if it detects on a port a duplex mismatch or too many link flaps or CRC/fragment errors. Possible values: ▶ Disable port (default setting) The device disables the port. – If the device disabled the port, the `Diagnostics > Ports > Auto Disable` dialog displays the cause. – The "Auto Disable" function allows you to re-enable the port automatically. Alternatively, mark in the table the desired port and click the "Reset" button to re-enable the port. ▶ Send trap The device sends an SNMP trap. Prerequisite for sending SNMP traps is that you enable the function in the `Diagnostics > Status Configuration > Alarms (Traps)` dialog and at least 1 SNMP manager is specified.
Port Status	Displays the operating status of the port. Possible values: ▶ `up` The device port is active. ▶ `down` The device port is inactive. ▶ `notPresent` Physical device port unavailable.

■ Buttons

Button	Meaning
Set	Transfers the changes to the volatile memory (`RAM`) of the device and applies them. 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 "Select" button. ☐ Click the "Save" button.
Reload	Updates the fields with the values that are saved in the volatile memory (`RAM`) of the device.
Reset	Resets the port monitor function for the selected interface and enables the port when disabled by the Port Monitor function.
Help	Opens the online help.

6.15.2 Link Flap

In this tab, you specify the settings for link flaps individually for every device port. If link flaps occur, the link status changes between active and inactive.

■ Table

Parameters	Meaning
Port	Displays the number of the device port to which the table entry relates.
Sampling Interval [s]	Specifies the period in seconds within which the device detects link changes for this entry. Possible values: ▶ `1..180` (default setting `10`)
Link Flap Count	Specifies the counter for link flaps. When the number of link flaps reaches this value, the device executes the action specified in the "Global" tab. Prerequisite is that in the "Global" tab you mark the "Link Flap on" checkbox as `marked`. Possible values: ▶ `1..100` (default setting: `5`)
Last Sampling Interval	Displays the link flap count that occurred during the last interval.
Total	Displays the total link flap count since the last reset.

■ Buttons

Button	Meaning
Set	Transfers the changes to the volatile memory (`RAM`) of the device and applies them. 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 "Select" button. □ Click the "Save" button.
Reload	Updates the fields with the values that are saved in the volatile memory (`RAM`) of the device.
Reset	Resets the port monitor function for the selected interface and enables the port when disabled by the Port Monitor function.
Help	Opens the online help.

6.15.3 CRC/Fragments

In this tab, you specify the settings for each port individually for CRC/fragment error monitoring.

- Based on the checksum the device detects data packets modified during the transmission.
- Fragmentation occurs when the maximum transmission unit (MTU) of the port is smaller than the packet size. In those cases, the sending device splits the data packet into smaller segments before sending them. The receiving device reassembles the fragments in the right order to the original data packet. The device always recognizes data packets with less than 64 Bytes as fragments.

The device monitors both criteria if you enable the function in the "Global" tab. If the number of occurred CRC/fragment errors exceeds the specified threshold, the device executes the user-specified action.

Table

Parameters	Meaning
Port	Displays the number of the device port to which the table entry relates.
Sampling Interval [s]	Specifies the period in seconds within which the device detects CRC/fragment errors. Possible values: ▶ `5..180` (default setting: `10`)
CRC/Fragments count [ppm]	Specifies threshold for CRC/fragment errors. If the number of CRC/fragment errors on this port reaches this value, the device executes the action specified in the "Global" tab. Prerequisite is that in the "Global" tab you mark the checkbox in the "CRC/Fragments on" field. Possible values: ▶ `1..1000000` (default setting: `1000`)
Last active Interval [ppm]	Displays the number of CRC/fragment errors occurred during the last interval.
Total [ppm]	Displays the total number of CRC/fragment errors occurred since the last reset

■ Buttons

Button	Meaning
Set	Transfers the changes to the volatile memory (`RAM`) of the device and applies them. 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 "Select" button. □ Click the "Save" button.
Reload	Updates the fields with the values that are saved in the volatile memory (`RAM`) of the device.
Reset	Resets the port monitor function for the selected interface and enables the port when disabled by the Port Monitor function.
Help	Opens the online help.

6.16 Auto Disable

If the configuration displays a port as enabled, but the device detects an error, the software shuts down that port. In other words, the device software disables the port because of a detected error condition.

The auto-deactivation of a port causes the device to disable the respective port so that it blocks traffic. The port LED blinks green 1 time per period and identifies the cause of the deactivation. In addition, the device creates a log file entry which lists the causes of the deactivation. In addition, the device sends an SNMP trap with the interface number, the port status, and the cause to the administrator. When you re-enable a port after its auto-deactivation, the device sends an SNMP trap with the interface number, but without a value for the "Reason" parameter.

This feature provides a recovery function which re-enables a port disabled through the auto-deactivation after a user-specified time. When this function enables a port, the device sends an SNMP trap with the interface number, but without a value for the "Reason" parameter.

The auto-disable function serves 2 purposes:

- It assists the administrator in port analysis.
- It excludes the possibility that the corresponding port causes the deactivation of the other ports of the module (respectively of the complete module).

■ Configuration

Parameters	Meaning
Link Flap	Specifies whether the device re-enables a port after the device disabled the port because of too many link flaps. Possible values: ▶ `unmarked` (default setting) The port remains disabled. ▶ `marked` The device re-enables the port after the time specified in the "Reset Timer [s]" field has expired. In the `Diagnostics > Ports > Port Monitor` dialog you specify whether the device disables the port in case of too many link flaps.
CRC Error	Specifies whether the device re-enables a port after the device disabled the port because of too many CRC/fragment errors. Possible values: ▶ `unmarked` (default setting) The port remains disabled. ▶ `marked` The device re-enables the port after the time specified in the "Reset Timer [s]" field has expired. In the `Diagnostics > Ports > Port Monitor` dialog you specify whether the device disables the port in case of too many CRC/fragment errors.
Duplex Mismatch	Specifies whether the device re-enables a port after the device disabled the port because of a duplex mismatch. Possible values: ▶ `unmarked` (default setting) The port remains disabled. ▶ `marked` The device re-enables the port after the time specified in the "Reset Timer [s]" field has expired. In the `Diagnostics > Ports > Port Monitor` dialog you specify whether the device disables the port in case of a duplex mismatch.

Parameters	Meaning
BPDU Rate	Specifies whether the device monitors the "BPDU Rate" on the ports. Possible values: ▶ `unmarked` (default setting) No port monitoring. ▶ `marked` The device monitors the "BPDU Rate" on the ports. – The device disables the port if the "BPDU Rate" on the port is higher than 15 pps for more than 3 seconds. – The device re-enables the port after the time specified in the "Reset Timer [s]" field has expired.
Port Security	Specifies whether the device enables a port after a "Port Security" condition produces a disable port action. Possible values: ▶ `unmarked` (default setting) No port monitoring. ▶ `marked` The device monitors the MAC address of the connected end devices on the ports. – The device disables a port if the port registers undesired source MAC addresses or more source MAC addresses than specified in the `Network Security > Port Security` port, "Dynamic Limit" field. In the `Network Security > Port Security` dialog, you specify the sources/end devices desired on a port and the number of sources/end devices automatically recorded on the port. – The device re-enables the port after the time specified in the "Reset Timer [s]" field has expired.

■ Table

Parameters	Meaning
Port	Displays the number of the device port.
Reset Timer [s]	Timeout period in seconds after which the device activates a deactivated port again. Possible values: ▶ `30...4294967295` ▶ `0` (default setting) The value 0 deactivates the timer.
Error Time	Displays the local system time when the error occurred.
Remaining Time [s]	Remaining time in seconds until the reactivation of the port.
Component	Displays the name of the component that caused the port to disable itself.

Parameters	Meaning
Reason	Displays the cause for the auto-deactivation of the port.
Active	Displays the operating state of the function for the relevant port. Possible values: ▶ `marked` The Auto Disable function disables the port. ▶ `unmarked` (default setting) The Auto Disable function is inactive for this port.

■ Buttons

Button	Meaning
Set	Transfers the changes to the volatile memory (`RAM`) of the device and applies them. 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 "Select" button. □ Click the "Save" button.
Reload	Updates the fields with the values that are saved in the volatile memory (`RAM`) of the device.
Reset	Enables the port when disabled by the Port Monitor function.
Help	Opens the online help.

6.17 Port Mirroring

The Port Mirroring function allows you to copy received and sent data packets from selected device 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 at the source ports.

■ Operation

Parameters	Meaning
Operation	When the function is switched on, the device copies the data packets for the select source ports to the destination port. Possible values: ▶ `On` ▶ `Off` (default setting)

■ Destination port

Parameters	Meaning
Destination port	Specifies the destination port. Every device port that is not specified as source port can be a destination port. 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 device port. **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 at the destination port.

Table

Parameters	Meaning
Source Port	Number of the device port to which the table entry relates. Possible values: ▶ `<Port number>`
Enabled	Enables/disables the copying of the data packets from this source port to the destination port. Possible values: ▶ `unmarked` (default setting) The copying of the data packets is disabled. ▶ `marked` The copying of the data packets is enabled. The port is specified as a source port. ▶ `inactive` It is not possible to copy the data packets for this port. Possible causes: – The port is specified as a destination port. – The port is a logical port, not a physical port. **Note:** The device allows you to activate every device 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 sends and receives. **Note:** With the `txrx` setting the device copies sent 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.

■ Buttons

Button	Meaning
Set	Transfers the changes to the volatile memory (`RAM`) of the device and applies them. 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 "Select" button. □ Click the "Save" button.
Reload	Updates the fields with the values that are saved in the volatile memory (`RAM`) of the device.
Reset Config	Resets the settings in the dialog to the default settings and transfers the changes to the volatile memory of the device (`RAM`).
Help	Opens the online help.

6.18 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:

- Configuration
- Topology Discovery

6.19 Configuration

This dialog allows you to configure the topology discovery for every device port.

■ Operation

Parameters	Meaning
Operation	If the function is switched on, the topology discovery with LLDP is activated on the device. Possible values: ▶ `On` (default setting) ▶ `Off`

■ 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 device port. Possible values: ▶ `1..10` (default setting `2`) If the value for a device port in the "Operation" field is `Off`, the device tries to reinitialize the port after the time specified here has elapsed.

Parameters	Meaning
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 number of the device port.
Admin Status	Specifies whether the device port transmits and receives LLDP data packets. Possible values: ▶ Transmit The device port transmits LLDP data packets but does not save any information about neighboring devices. ▶ Receive The device port receives LLDP data packets but does not transmit any information to neighboring devices. ▶ Receive and Transmit (default setting) The device port transmits LLDP data packets and saves information about neighboring devices. ▶ Disabled The device port does not transmit LLDP data packets and does not save information about neighboring devices.
Notification Enabled	Specifies whether LLDP notifications are enabled on this device port. Possible values: ▶ `marked` LLDP notifications are enabled on this device port. ▶ `unmarked` (default setting) LLDP notifications are disabled on this device port.

Parameters	**Meaning**
Transmit Port Description	Specifies whether the device transmits a TLV (Type Length Value) with the port description. Possible values: ▶ `marked` (default setting) The device transmits a TLV with the port description. ▶ `unmarked` The device does not transmit a TLV with the port description.
Transmit System Name	Specifies whether the device transmits a TLV (Type Length Value) with the device name. Possible values: ▶ `marked` (default setting) The device transmits a TLV with the device name. ▶ `unmarked` The device does not transmit a TLV with the device name.
Transmit System Description	Specifies whether the device transmits a TLV (Type Length Value) with the system description. Possible values: ▶ `marked` (default setting) The device transmits a TLV with the system description. ▶ `unmarked` The device does not transmit a TLV with the system description.
Transmit System Capabilities	Specifies whether the device transmits a TLV (Type Length Value) with the system capabilities (performance data). Possible values: ▶ `marked` (default setting) The device transmits a TLV with the system capabilities. ▶ `unmarked` The device transmits a TLV with the system capabilities.

Parameters	Meaning
Max Neighbors	Limits the number of neighboring devices to be recorded for this port. Possible values: ▶ `1..50` (default setting: `10`)
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

Button	Meaning
Set	Transfers the changes to the volatile memory (`RAM`) of the device and applies them. 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 "Select" button. □ Click the "Save" button.
Reload	Updates the fields with the values that are saved in the volatile memory (`RAM`) of the device.
Help	Opens the online help.

6.20 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 tabs of this dialog allow 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 the 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 device port, the topology table hides the devices without active topology discovery.

When devices without active topology discovery are connected to a device port exclusively, the table will contain one line for this port to represent all devices. 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 number of the device port.
Neighbor Identifier	Displays the chassis ID of the neighboring device. This can be the basis MAC address of the neighboring device, for example.
Neighbor IP Address	Displays the IP address with which the management functions of the neighboring device can be reached.
Neighbor Port Description	Displays a description for the device port of the neighboring device.
Neighbor System Name	Displays the device name of the neighboring device.

Parameters	Meaning
Neighbor System Description	Displays a description for the neighboring device.
Port ID	Displays the ID of the device port through which the neighboring device is connected to the device.
Autonegotiation Supported	Displays whether the device port of the neighboring device supports autonegotiation.
Autonegotiation Enabled	Displays whether autonegotiation is enabled on the device port of the neighboring device.
PoE Supported	Displays whether the device port of the neighboring device supports Power over Ethernet (PoE).
PoE Enabled	Displays whether Power over Ethernet (PoE) is enabled on the device port of the neighboring device.

■ Display FDB Entries

Parameters	Meaning
Display FDB Entries	Adds entries to the table for devices without active LLDP support. Possible values: ▶ `unmarked` (default setting) The table displays entries for devices with LLDP support. ▶ `marked` The table displays entries for devices with and without LLDP support. Here the device uses information from its address table (FDB, Forwarding Database).

■ Buttons

Button	Meaning
Reload	Updates the fields with the values that are saved in the volatile memory (`RAM`) of the device.
Help	Opens the online help.

6.21 Report

The device allows you to register events and user actions. In this menu, you specify the settings for the logging.

The menu contains the following dialogs:
- Global
- System Log
- Audit Trail

6.22 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	When the function is switched on, the device logs the events on the console. Possible values: ▶ `On` ▶ `Off` (default setting)
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	Specifies whether the device registers SNMP Get requests as events in the syslog. In the "Severity Get Request" field, you specify the severity for this event. Possible values: ▶ `On` The device registers SNMP Get requests as events in the syslog. ▶ `Off` (default setting) Logging is deactivated.
Log SNMP Set Request	Specifies whether the device registers SNMP Set requests as events in the syslog. In the "Severity Set Request" field, you specify the severity for this event. Possible values: ▶ `On` The device registers SNMP Set requests as events in the syslog. ▶ `Off` (default setting) Logging is deactivated.

Parameters	Meaning
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 activate 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	If the function is switched on, the device logs all commands received via the Command Line Interface (CLI). Possible values: ▶ `On` ▶ `Off` (default setting)

■ Buttons

Button	Meaning
Set	Transfers the changes to the volatile memory (`RAM`) of the device and applies them. 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 "Select" button. □ Click the "Save" button.
Reload	Updates the fields with the values that are saved in the volatile memory (`RAM`) of the device.

Button	Meaning
Download Support Information	Opens the "Save" dialog. This dialog allows you to save a ZIP archive on your PC that contains system information about the device. The device generates the file name of the ZIP archive automatically based on the format `<IP address>_<device name>.zip`. You will find an explanation of the files contained in the ZIP archive in the following section.
Help	Opens the online help.

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.
CLICommands.txt	Text	Contains the output of CLI commands: ▶ show port all ▶ show system info ▶ show mac-addr-table ▶ show mac-filter-table igmp-snooping The prerequisite is that you enable the SSH server in the device, see the `Device Security > Management Access > Server` dialog.
defaultconfig.xml	XML	Contains the configuration profile with the default settings of the device.
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
`error`	Error status
`warning`	Warning
`notice`	Significant, normal status
`informational`	Informal message
`debug`	Debug message

6.23 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 search the log file for search terms and save them in HTML format on your PC.

The log file is kept until a restart is performed on the device. After the restart the device creates the file again.
To delete the logged events from the log file, click "Delete Log File" in the `Basic Settings > Restart` dialog.

■ Buttons

Button	Meaning
Reload	Updates the fields with the values that are saved in the volatile memory (`RAM`) of the device.
Search	Opens the "Search" dialog. The dialog allows you to search the log file for search terms or regular expressions.
Save	Opens the "Save" dialog. The dialog allows you to save the log file in HTML format on your PC.
Delete Log File	Removes the logged events from the log file.
Help	Opens the online help.

6.24 Audit Trail

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 logged entries are write-protected and remain saved in the device after a restart.

This dialog displays the log file (audit trail). The dialog allows you to search the log file for search terms and save them in HTML format on your PC.

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

Buttons

Button	Meaning
Reload	Updates the fields with the values that are saved in the volatile memory (`RAM`) of the device.
Search	Opens the "Search" dialog. The dialog allows you to search the log file for search terms or regular expressions.
Save	Opens the "Save" dialog. The dialog allows you to save the log file in HTML format on your PC.
Help	Opens the online help.

7 Advanced

This menu allows you to specify advanced settings.

The menu contains the following dialogs:

- Industrial Protocols
- Command Line Interface

7.1 Industrial Protocols

The "Industrial Protocols" menu allows you to set the following protocols:
- ▶ IEC61850-MMS

Detailed information on industrial protocols and PLC configuration is contained in the User Manual "Industrial Protocols“.

7.2 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 (e.g. 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 write access to the MMS server
- The MMS server TCP Port
- The maximum number of MMS server sessions

Operation

Parameters	Meaning
Operation	Activates/deactivates the MMS server. Possible values: ▶ `On` Enables the MMS server functionality on this device. ▶ `Off` (default setting) Disables the MMS server, but the IEC 61850 MIBs are accessible.

Configuration

Parameters	Meaning
Write Access	Activates/deactivates the write access to the MMS server. Possible values: ▶ `unmarked` (default setting) The write access to the MMS server is deactivated. The MMS server is accessible as read-only. ▶ `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.
Technical Key	Specifies the IED name. The IED name is eligible independently of the system name. Possible values: ▶ `0..9` `a..z` `A..Z` (default setting: `KEY`) To get the MMS server to use the IED name, click the "Set" button and restart the MMS server. The connection to connected clients is then interrupted.
TCP Port	Specifies TCP port for MMS server access. Possible values: ▶ Valid TCP port (default setting: `102`) **Note:** The server restarts automatically after you change the port. In the process, the device terminates open connections to the server.
Max. Number of Sessions	Specifies the maximum number of MMS server connections. Possible values: ▶ `1..15` (default setting: `5`)

ICD File

Parameters	Meaning
Download	This button copies the ICD file to your PC.

Buttons

Button	Meaning
Set	Transfers the changes to the volatile memory (`RAM`) of the device and applies them. 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 "Select" button. □ Click the "Save" button.
Reload	Updates the fields with the values that are saved in the volatile memory (`RAM`) of the device.
Help	Opens the online help.

7.3 Command Line Interface

This dialog allows you to access the device through the Command Line Interface. Prerequisite is that you enable the SSH server in the device, see the `Device Security > Management Access > Server` dialog, tab "SSH".

For detailed information on CLI commands, review the “Command Line Interface” reference manual.

■ Buttons

Button	Meaning
Help	Opens the online help.

A Appendix

A.1 Technical Data

Switching	
Size of MAC address table (incl. static filters)	2048 (2k)
Max. number of statically configured MAC address filters	100
Max. number of MAC address filters learnable through IGMP Snooping	256
MTU (max. length of over-long packets)	2000 bytes
Latency (of 64-byte data packets) 100 Mbit/s 10 Mbit/s	 Layer 2: typ. 3.4 µs Layer 2: typ. 7.8 µs
Number of priority queues	4 queues
Port priorities that can be set	0..3

VLAN	
VLAN-ID	1..4042
Number of VLANs	max. 16 simultaneously per device max. 16 simultaneously per port

A.2 List of RFCs

RFC 768	UDP
RFC 783	TFTP
RFC 791	IP
RFC 792	ICMP
RFC 793	TCP
RFC 826	ARP
RFC 854	Telnet
RFC 855	Telnet Option
RFC 951	BOOTP
RFC 1112	IGMPv1
RFC 1157	SNMPv1
RFC 1155	SMIv1
RFC 1212	Concise MIB Definitions
RFC 1213	MIB2
RFC 1493	Dot1d
RFC 1542	BOOTP-Extensions
RFC 1643	Ethernet-like -MIB
RFC 1757	RMON
RFC 1867	Form-Based File Upload in HTML
RFC 1901	Community based SNMP v2
RFC 1905	Protocol Operations for SNMP v2
RFC 1906	Transport Mappings for SNMP v2
RFC 1945	HTTP/1.0
RFC 2068	HTTP/1.1 protocol as updated by draft-ietf-http-v11-spec-rev-03
RFC 2131	DHCP
RFC 2132	DHCP-Options
RFC 2233	The Interfaces Group MIB using SMI v2
RFC 2236	IGMPv2
RFC 2246	The TLS Protocol, Version 1.0
RFC 2346	AES Ciphersuites for Transport Layer Security
RFC 2365	Administratively Scoped IP Multicast
RFC 2474	Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers
RFC 2475	An Architecture for Differentiated Service
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)

A.3 Underlying IEEE Standards

IEEE 802.1AB	Station and Media Access Control Connectivity Discovery
IEEE 802.1D	MAC Bridges (switching function)
IEEE 802.1Q	Virtual LANs (VLANs, MRP, Spanning Tree)
IEEE 802.1X	Port Authentication
IEEE 802.3	Ethernet
IEEE 802.3ac	VLAN Tagging
IEEE 802.3x	Flow Control
IEEE 802.3af	Power over Ethernet

A.4 Underlying IEC Norms

IEC 62439	High availability automation networks HSR – High-availability Seamless Redundancy MRP – Media Redundancy Protocol based on a ring topology PRP – Parallel Redundancy Protocol

A.5 Underlying ANSI Norms

ANSI/TIA-1057	Link Layer Discovery Protocol for Media Endpoint Devices, April 2006

A.6 Maintenance

Hirschmann are 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 (http://www.hirschmann.com).

A.7 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

- Hirschmann “Installation” user manual

- Hirschmann “Basic Configuration” user manual

- Hirschmann “Redundancy Configuration” user manual

- Hirschmann “Routing Configuration” user manual

- Hirschmann “GUI Graphical User Interface” reference manual

- Hirschmann “Command Line Interface” reference manual

- Hirschmann User Guide “Industry Protocol”

- Hirschmann Manual “Network Management System Industrial HiVision”

A.8 Copyright of Integrated Software

A.8.1 lighttpd

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- Neither the name of the 'incremental' nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE

A.8.2 Expat

A.8.3 libcurl

A.8.4 libssh2

A.8.5 OpenSSH

The licences which components of this software fall under are as follows. First, we will summarize and say that all components are under a BSD licence, or a licence more free than that.

OpenSSH contains no GPL code.

1)

```
 * Copyright (c) 1995 Tatu Ylonen <ylo@cs.hut.fi>, Espoo, Finland
 * All rights reserved
 *
 * As far as I am concerned, the code I have written for this software
 * can be used freely for any purpose.  Any derived versions of this
 * software must be clearly marked as such, and if the derived work is
 * incompatible with the protocol description in the RFC file, it must be
 * called by a name other than "ssh" or "Secure Shell".
```

[Tatu continues]

```
 *  However, I am not implying to give any licenses to any patents or
 * copyrights held by third parties, and the software includes parts that
 * are not under my direct control.  As far as I know, all included
 * source code is used in accordance with the relevant license agreements
 * and can be used freely for any purpose (the GNU license being the most
 * restrictive); see below for details.
```

[However, none of that term is relevant at this point in time. All of these restrictively licenced software components which he talks about have been removed from OpenSSH, i.e.,

– RSA is no longer included, found in the OpenSSL library
– IDEA is no longer included, its use is deprecated
– DES is now external, in the OpenSSL library
– GMP is no longer used, and instead we call BN code from OpenSSL
– Zlib is now external, in a library
– The make-ssh-known-hosts script is no longer included
– TSS has been removed
– MD5 is now external, in the OpenSSL library
– RC4 support has been replaced with ARC4 support from OpenSSL
– Blowfish is now external, in the OpenSSL library

[The licence continues]

Note that any information and cryptographic algorithms used in this software are publicly available on the Internet and at any major bookstore, scientific library, and patent office worldwide. More information can be found e.g. at "http://www.cs.hut.fi/crypto".

The legal status of this program is some combination of all these permissions and restrictions. Use only at your own responsibility. You will be responsible for any legal consequences yourself; I am not making any claims whether possessing or using this is legal or not in your country, and I am not taking any responsibility on your behalf.NO WARRANTY

BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

2)

The 32-bit CRC compensation attack detector in deattack.c was contributed by CORE SDI S.A. under a BSD-style license.

3)

ssh-keyscan was contributed by David Mazieres under a BSD-style license.

4)

The Rijndael implementation by Vincent Rijmen, Antoon Bosselaers and Paulo Barreto is in the public domain and distributed with the following license:

5)

One component of the ssh source code is under a 3-clause BSD license, held by the University of California, since we pulled these parts from original Berkeley code.

```
 * Copyright (c) 1983, 1990, 1992, 1993, 1995
 *      The Regents of the University of California.  All rights reserved.
 *
 * Redistribution and use in source and binary forms, with or without
 * modification, are permitted provided that the following conditions
 * are met:
 * 1. Redistributions of source code must retain the above copyright
 *    notice, this list of conditions and the following disclaimer.
 * 2. Redistributions in binary form must reproduce the above copyright
 *    notice, this list of conditions and the following disclaimer in the
 *    documentation and/or other materials provided with the distribution.
 * 3. Neither the name of the University nor the names of its contributors
 *    may be used to endorse or promote products derived from this
 *    software without specific prior written permission.
 *
 * THIS SOFTWARE IS PROVIDED BY THE REGENTS AND
 * CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED
 * WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
 * IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR
 * A PARTICULAR PURPOSE ARE DISCLAIMED.  IN NO EVENT SHALL
 * THE REGENTS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT,
 * INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR
 * CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO,
 * PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS
 * OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
 * HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY,
 * WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT
 * (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY
 * OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE
 * POSSIBILITY OF SUCH DAMAGE.
```

6)

Remaining components of the software are provided under a standard 2-term BSD licence with the following names as copyright holders:

Markus Friedl
Theo de Raadt
Niels Provos
Dug Song
Aaron Campbell
Damien Miller
Kevin Steves
Daniel Kouril
Wesley Griffin
Per Allansson
Nils Nordman
Simon Wilkinson

Portable OpenSSH additionally includes code from the following copyright holders, also under the 2-term BSD license:

Ben Lindstrom
Tim Rice
Andre Lucas
Chris Adams
Corinna Vinschen
Cray Inc.
Denis Parker
Gert Doering
Jakob Schlyter
Jason Downs
Juha Yrjölä
Michael Stone
Networks Associates Technology, Inc.
Solar Designer
Todd C. Miller
Wayne Schroeder
William Jones
Darren Tucker
Sun Microsystems
The SCO Group
Daniel Walsh
Red Hat, Inc

8) Portable OpenSSH contains the following additional licenses:

a) md5crypt.c, md5crypt.h

b) snprintf replacement

c) Compatibility code (openbsd-compat)

Apart from the previously mentioned licenses, various pieces of code in the openbsd-compat/ subdirectory are licensed as follows:

Some code is licensed under a 3-term BSD license, to the following copyright holders:

Todd C. Miller
Theo de Raadt
Damien Miller
Eric P. Allman
The Regents of the University of California
Constantin S. Svintsoff

```
* Redistribution and use in source and binary forms, with or without
* modification, are permitted provided that the following conditions
* are met:
* 1. Redistributions of source code must retain the above copyright
*    notice, this list of conditions and the following disclaimer.
* 2. Redistributions in binary form must reproduce the above copyright
*    notice, this list of conditions and the following disclaimer in the
*    documentation and/or other materials provided with the distribution.
* 3. Neither the name of the University nor the names of its contributors
*    may be used to endorse or promote products derived from this software
*    without specific prior written permission.
*
* THIS SOFTWARE IS PROVIDED BY THE REGENTS AND
* CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED
* WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED
* WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A
* PARTICULAR PURPOSE ARE DISCLAIMED.  IN NO EVENT SHALL THE
* REGENTS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT,
* INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR
* CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO,
* PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF
* USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
* HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER
* IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING
* NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE
* USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF
* SUCH DAMAGE.
```

Some code is licensed under an ISC-style license, to the following copyright holders:

Internet Software Consortium.
Todd C. Miller
Reyk Floeter
Chad Mynhier

Some code is licensed under a MIT-style license to the following copyright holders:

Free Software Foundation, Inc.

* IN NO EVENT SHALL THE ABOVE COPYRIGHT HOLDERS BE LIABLE
* FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN
* ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT
* OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR
* OTHER DEALINGS IN THE SOFTWARE.* * Except as contained in this notice, the name(s) of the above copyright
* holders shall not be used in advertising or otherwise to promote the
* sale, use or other dealings in this Software without prior written
* authorization.
***/

A.8.6 OpenSSL

```
* Copyright (c) 1998-2008 The OpenSSL Project.  All rights reserved.
*
* Redistribution and use in source and binary forms, with or without
* modification, are permitted provided that the following conditions
* are met:
*
* 1. Redistributions of source code must retain the above copyright
*    notice, this list of conditions and the following disclaimer.
*
* 2. Redistributions in binary form must reproduce the above copyright
*    notice, this list of conditions and the following disclaimer in
*    the documentation and/or other materials provided with the
*    distribution.
*
* 3. All advertising materials mentioning features or use of this
*    software must display the following acknowledgment:
*    "This product includes software developed by the OpenSSL Project
*    for use in the OpenSSL Toolkit. (http://www.openssl.org/)"
*
* 4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used
*    to endorse or promote products derived from this software without
*    prior written permission. For written permission, please contact
*    openssl-core@openssl.org.
*
* 5. Products derived from this software may not be called "OpenSSL"
*    nor may "OpenSSL" appear in their names without prior written
*    permission of the OpenSSL Project.
*
* 6. Redistributions of any form whatsoever must retain the following
*    acknowledgment:
*    "This product includes software developed by the OpenSSL Project
*    for use in the OpenSSL Toolkit (http://www.openssl.org/)"
*
* THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS''
* AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT
* NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY
* AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED.
* IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS
* CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT,
* INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL
* DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF
* SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR
* PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND
* ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT
* LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE)
* ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN
* IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.
* ==================================================
*
* This product includes cryptographic software written by Eric Young
* (eay@cryptsoft.com).  This product includes software written by Tim
* Hudson (tjh@cryptsoft.com).
*
*/
```

Original SSLeay License

```
 ------------------------------

/* Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com)
 * All rights reserved.
 *
 * This package is an SSL implementation written
 * by Eric Young (eay@cryptsoft.com).
 * The implementation was written so as to conform with Netscapes SSL.
 *
 * This library is free for commercial and non-commercial use as long as
 * the following conditions are aheared to.  The following conditions
 * apply to all code found in this distribution, be it the RC4, RSA,
 * lhash, DES, etc., code; not just the SSL code.  The SSL documentation
 * included with this distribution is covered by the same copyright terms
 * except that the holder is Tim Hudson (tjh@cryptsoft.com).
 *
 * Copyright remains Eric Young's, and as such any Copyright notices in
 * the code are not to be removed.
 * If this package is used in a product, Eric Young should be given attribution
 * as the author of the parts of the library used.
 * This can be in the form of a textual message at program startup or
 * in documentation (online or textual) provided with the package.
 *
```

```
* Redistribution and use in source and binary forms, with or without
* modification, are permitted provided that the following conditions
* are met:
* 1. Redistributions of source code must retain the copyright
*    notice, this list of conditions and the following disclaimer.
* 2. Redistributions in binary form must reproduce the above copyright
*    notice, this list of conditions and the following disclaimer in the
*    documentation and/or other materials provided with the distribution.
* 3. All advertising materials mentioning features or use of this software
*    must display the following acknowledgement:
*    "This product includes cryptographic software written by
*     Eric Young (eay@cryptsoft.com)"
*    The word 'cryptographic' can be left out if the rouines from the library
*    being used are not cryptographic related :-).
* 4. If you include any Windows specific code (or a derivative thereof) from
*    the apps directory (application code) you must include an
*    acknowledgement: "This product includes software written
*    by Tim Hudson (tjh@cryptsoft.com)"
*
* THIS SOFTWARE IS PROVIDED BY ERIC YOUNG ``AS IS'' AND
* ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT
* LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND
* FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED.  IN NO
* EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE
* FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY,
* OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO,
* PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF
* USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER
* CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN
* CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE
* OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS
* SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH
* DAMAGE.
*
* The licence and distribution terms for any publically available version or
* derivative of this code cannot be changed.  i.e. this code cannot simply be
* copied and put under another distribution licence
* [including the GNU Public Licence.]
*/
```

A.8.7 Parts of the FreeBSD IP stack

B Index

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?

Readers' Comments

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

D 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

HIRSCHMANN

A BELDEN BRAND