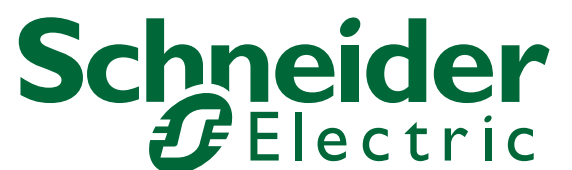


# ConneXium

TCSESM, TCSESM-E Managed Switch  
Web-based Interface Reference Manual

EIO0000000482.02

[www.schneider-electric.com](http://www.schneider-electric.com)





# Contents

	Safety Information	7
	About this Manual	9
	Key	13
	Opening the Web-based Interface	15
1	Basic Settings	19
1.1	System	20
1.2	Network	24
1.3	Software	26
	1.3.1 View the software versions present on the device	27
	1.3.2 TFTP Software Update	27
	1.3.3 HTTP Software Update	27
	1.3.4 Automatic software update by EAM	28
1.4	Port Configuration	29
1.5	Loading/Saving the Configuration	31
	1.5.1 Loading the configuration	32
	1.5.2 Saving the Configuration	32
	1.5.3 URL	34
	1.5.4 Deleting a configuration	34
	1.5.5 Using the Memory Backup Adaptor (EAM)	34
	1.5.6 Canceling a configuration change	36
1.6	Restart	37
2	Security	39
2.1	Password / SNMPv3 access	40
2.2	SNMPv1/v2 Access Settings	43
2.3	Telnet/Web Access	46
	2.3.1 Description of Telnet Access	47
	2.3.2 Description of Web Access	47
2.4	Port Security	48
3	Time	51

3.1	SNTP configuration	53
3.2	PTP (IEEE 1588)	57
4	Switching	59
4.1	Switching Global	60
4.2	Filters for MAC addresses	64
4.3	Rate Limiter	66
4.3.1	Rate Limiter settings	66
4.4	Multicasts	69
4.4.1	IGMP (Internet Group Management Protocol)	69
4.4.2	GMRP (GARP Multicast Registration Protocol)	76
4.5	VLAN	78
4.5.1	VLAN Global	78
4.5.2	Current VLAN	81
4.5.3	VLAN Static	83
4.5.4	VLAN Port	85
5	QoS/Priority	89
5.1	Global	90
5.2	Port Configuration	93
5.2.1	Entering the port priority	93
5.2.2	Selecting the trust mode	94
5.2.3	Displaying the untrusted traffic class	95
5.3	802.1D/p mapping	96
5.4	IP DSCP mapping	98
6	Redundancy	101
6.1	Ring Redundancy	102
6.1.1	Configuring the HIPER-Ring	104
6.1.2	Configuring the MRP-Ring	108
6.1.3	Configuring the Fast HIPER-Ring (TCSESM-E)	111
6.2	Sub-Ring (TCSESM-E)	114
6.2.1	Sub-Ring configuration	115
6.2.2	Sub-Ring - New Entry	118
6.3	Ring/Network Coupling	120
6.3.1	Preparing a Ring/Network Coupling	120
6.4	Spanning Tree	126

6.4.1	Global	129
6.4.2	Dual RSTP (TCSESM-E)	135
6.4.3	Port	147
7	Diagnostics	157
7.1	Syslog	158
7.2	Event Log	163
7.3	Ports	164
7.3.1	Statistics table	164
7.3.2	Utilization	165
7.3.3	SFP modules	166
7.4	Topology Discovery	167
7.5	Port Mirroring	169
7.6	Device Status	171
7.7	Signal contact	174
7.7.1	Manual setting	174
7.7.2	Function monitoring	174
7.7.3	Device status	176
7.7.4	Configuring traps	176
7.8	Alarms (Traps)	178
7.9	Report	180
7.10	IP address conflict detection	183
7.11	Self Test	185
8	Advanced	187
8.1	DHCP Relay Agent	188
8.2	EtherNet/IP	190
8.3	Command Line	191
A	Appendix	193
A.1	Technical Data	194
A.2	List of RFCs	195
A.3	Underlying IEEE Standards	197

## Contents

---

A.4	Underlying IEC Norms	198
A.5	Copyright of Integrated Software	199
A.5.1	Bouncy Castle Crypto APIs (Java)	199
A.5.2	Broadcom Corporation	200
B	Index	201

# Safety Information

## ■ Important Information

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



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



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

### **DANGER**

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

### **WARNING**

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

### **CAUTION**

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

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

© 2011 Schneider Electric. All Rights Reserved.



# About this Manual

## **Validity Note**

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

## **Product Related Information**

Schneider Electric assumes no responsibility for any errors that may appear in this document. If you have any suggestions for improvements or amendments or have found errors in this publication, please notify us.

No part of this document may be reproduced in any form or by any means, electronic or mechanical, including photocopying, without express written permission of Schneider Electric.

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

When devices are used for applications with technical safety requirements, please follow the relevant instructions.

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

Failure to observe this product related warning can result in injury or equipment damage.

## **User Comments**

We welcome your comments about this document. You can reach us by e-mail at [techpub@schneider-electric.com](mailto:techpub@schneider-electric.com)

### Related Documents

Title	Reference Number
ConneXium TCSESM, TCSESM-E Managed Switch Redundancy Configuration User Manual	31007126
ConneXium TCSESM, TCSESM-E Managed Switch Basic Configuration User Manual	31007122
ConneXium TCSESM, TCSESM-E Managed Switch Command Line Interface Reference Manual	31007130
ConneXium TCSESM, TCSESM-E Managed Switch Web-based Interface Reference Manual	EIO0000000482
ConneXium TCSESM Managed Switch Installation Manual	31007118
ConneXium TCSESM-E Extended Managed Switch Installation Manual	EIO0000000529

**Note:** The Glossary is located in the Reference Manual “Command Line Interface”.

The “Web-based Interface” reference manual contains detailed information on using the Web 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 contains the information you need to select a suitable redundancy procedure and configure that procedure.









# Key

The designations used in this manual have the following meanings:

	List
<input type="checkbox"/>	Work step
	Subheading
<a href="#">Link</a>	Indicates a cross-reference with a stored link
<b>Note:</b>	A note emphasizes an important fact or draws your attention to a dependency.
<i>Courier</i>	ASCII representation in user interface

Symbols used:

	WLAN access point
	Router with firewall
	Switch with firewall
	Router
	Switch
	Bridge

# Key

---



Hub



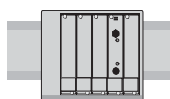
A random computer



Configuration Computer



Server



PLC -  
Programmable logic  
controller



I/O -  
Robot

---

# Opening the Web-based Interface

To open the Web-based interface, you need a Web browser (a program that can read hypertext), for example Mozilla Firefox version 1 or later, or Microsoft Internet Explorer version 6 or later.

**Note:** The Web-based interface uses Java software 6 (“Java™ Runtime Environment Version 1.6.x”).

Install the software from the enclosed CD-ROM. To do this, you go to the “ConneXium” directory on the CD-ROM, open the “Java” directory, and start the installation program.

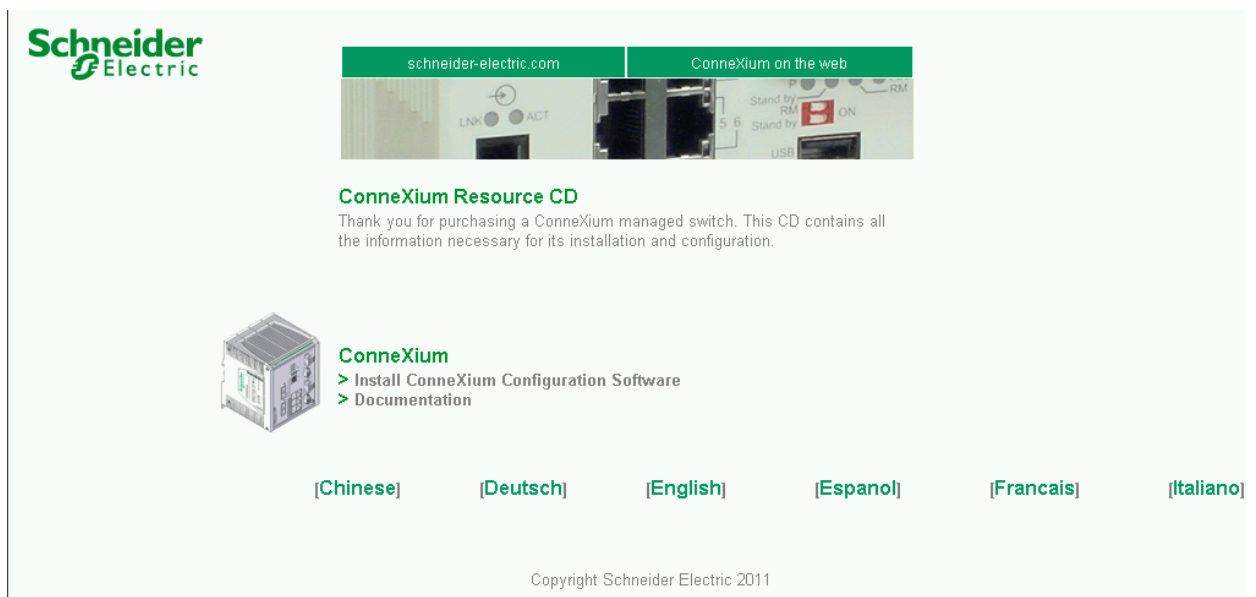


Figure 1: Installing Java

- Start your Web browser.
- Make sure that you have activated JavaScript and Java in the security settings of your browser.

- Establish the connection by entering the IP address of the device which you want to administer via the Web-based management in the address field of the Web browser. Enter the address in the following form:

`http://xxx.xxx.xxx.xxx`

The login window appears on the screen.

**Note:** Most properties of the TCSESM and TCSESM-E devices are identical. The supplement “(TCSESM-E)” indicates a difference between the TCSESM-E and the TCSESM.



Figure 2: Login window

- Select the desired language.
- In the drop-down menu “Login”, you select
  - user, to have read access, or
  - admin, to have read and write access



to the device.

- The password “public”, with which you have read access for the login “user”, is preset in the password field. If you wish to have write access to the device, use the login “admin”, select the contents of the password field and overwrite it with the password “private” (default setting).
- Click on OK.

The website of the device appears on the screen.

**Note:** The changes you make in the dialogs will be copied to the device when you click “Set”. Click “Reload” to update the display.

To save any changes made so that they will be retained after a power cycle or reboot of the device use the save option on the “Load/Save” dialog ([see page 31](#))

**Note:** If you enter an incorrect configuration, you may block access to your device.

Activating the function “Cancel configuration change” in the “Load/Save” dialog enables you to return automatically to the last configuration after a set time period has elapsed. This gives you back your access to the device.

## Opening the Web-based Interface

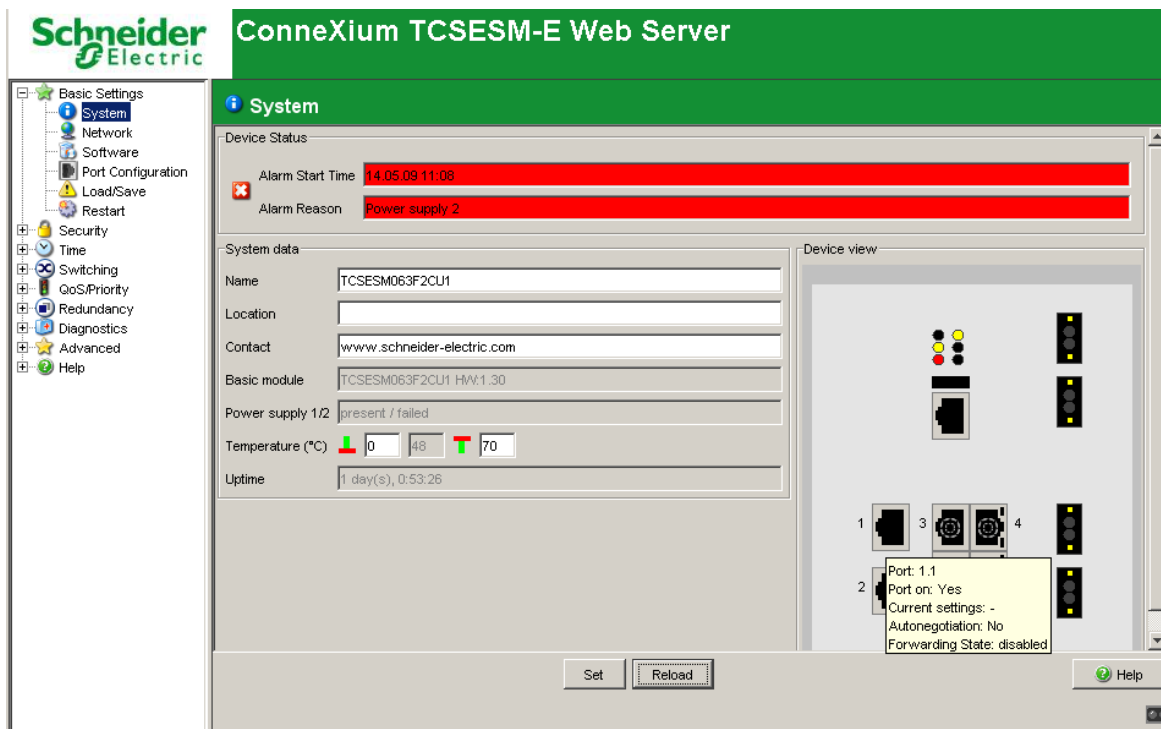
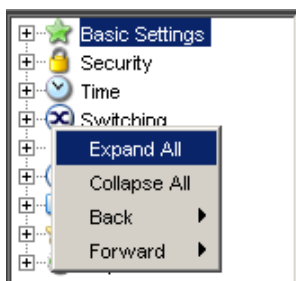


Figure 3: Website of the device with speech-bubble help

The menu section displays the menu items. By placing the mouse pointer in the menu section and clicking the alternate mouse button you can use “Back” to return to a menu item you have already selected, or “Forward” to jump to a menu item you have already selected.



# 1 Basic Settings

The Basic Settings menu contains the dialogs, displays and tables for the basic configuration:

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

# 1.1 System

The “System” submenu in the basic settings menu is structured as follows:

- ▶ Device Status
- ▶ System data
- ▶ Device view
- ▶ Reloading data

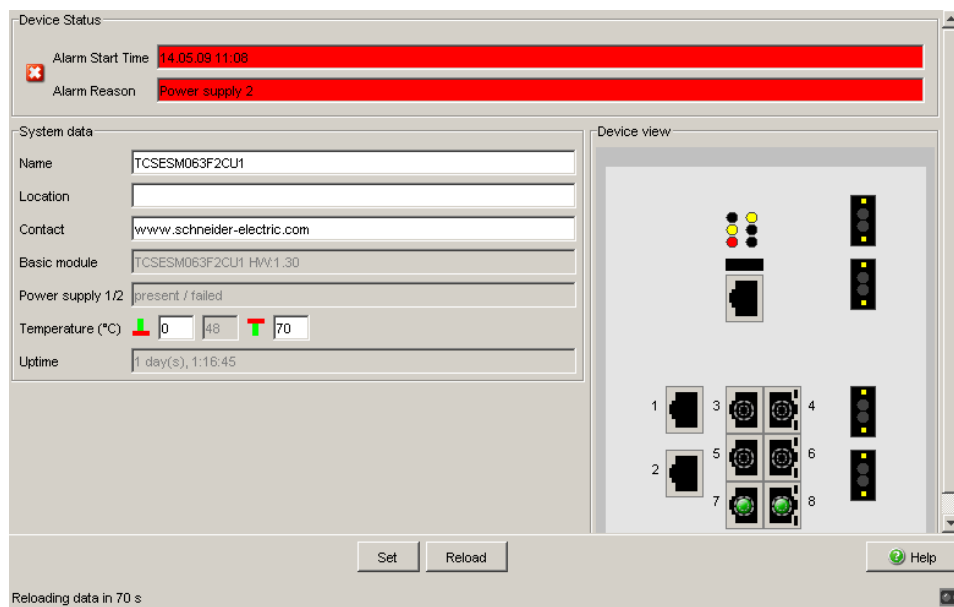
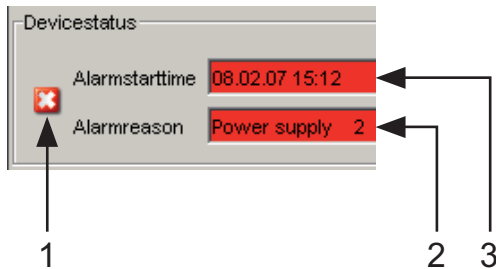


Figure 4: “System” Submenu

## ■ Device Status

This section of the website provides information on the device status and the alarm states the device has detected.



*Figure 5: Device status and display of detected alarms*  
 1 - Symbol indicates the Device Status  
 2 - Cause of the oldest existing alarm detected  
 3 - Time of the oldest existing alarm detected

### ■ System Data

This area of the website displays the system parameters of the device. Here you can change

- the system name,
- the location description,
- the name of the contact person for this device,
- the temperature threshold values.

Name	Meaning
Name	System name of this device
Location	Location of this device
Contact	The contact for this device
Basic module	Hardware version of the device
Power supply (P1/P2)	Status of power units (P1/P2)
Uptime	Time that has elapsed since this device was last restarted.
Temperature	Temperature of the device. Lower/upper temperature threshold values. If the temperature goes outside this range, the device generates an alarm.

*Table 1: System Data*

### ■ Device View

The device view shows the device with the current configuration. The status of the individual ports is indicated by one of the symbols listed below. You will get a full description of the port's status by positioning the mouse pointer over the port's symbol.

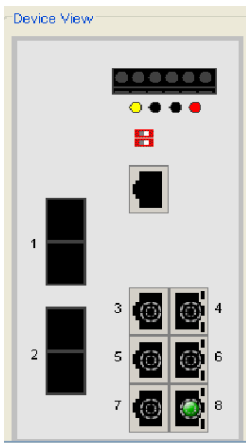








Figure 6: Device View

### Meaning of the symbols:

-  The port (10, 100 Mbit/s, 1 Gbit/s) is enabled and the connection is OK.
-  The port is disabled by the management and it has a connection.
-  The port is disabled by the management and it has no connection.
-  The port is in autonegotiation mode.
-  The port is in HDX mode.
-  The port (100 Mbit/s) is in the discarding mode of a redundancy protocol like e.g. Spanning Tree or HIPER-Ring.

### ■ Updating

This area of the website at the bottom left displays the countdown time until the applet requests the current data of this dialog again. Clicking the “Reload” button calls the current dialog information immediately. The applet polls the current data of the device automatically every 100 seconds.

Reloading data in 70 s

*Figure 7: Time until update*

## 1.2 Network

With the `Basic settings:Network` dialog you define the source from which the device gets its IP parameters after starting, and you assign the IP parameters and VLAN ID and configure the Ethernet Switch Configuration Software access.

The screenshot shows the 'Network parameters dialog' with the following configuration:

- Mode:** Local (selected)
- BOOTP /DHCP:** MAC Address: 00:80:63:97:50:00
- DHCP:** System name: TCSESM063F2CU1
- Local:** IP Address: 10.0.1.220, Netmask: 255.255.255.0, Gateway address: 10.0.1.1
- VLAN:** ID: 1
- Ethernet Switch Configurator Protocol:** Operation: On, Access: read-write

Figure 8: Network parameters dialog

- Under “Mode”, you enter where the device gets its IP parameters:
  - ▶ In the BOOTP mode, the configuration is via a BOOTP or DHCP server on the basis of the MAC address of the device ([see on page 31 “Loading/Saving the Configuration”](#)).
  - ▶ In the DHCP mode, the configuration is via a DHCP server on the basis of the MAC address or the name of the device ([see on page 31 “Loading/Saving the Configuration”](#)).
  - ▶ In the local mode the net parameters in the device memory are used.



**Note:** When you change the mode of the IP address, the device activates the new mode immediately after the “Set” button is pressed.

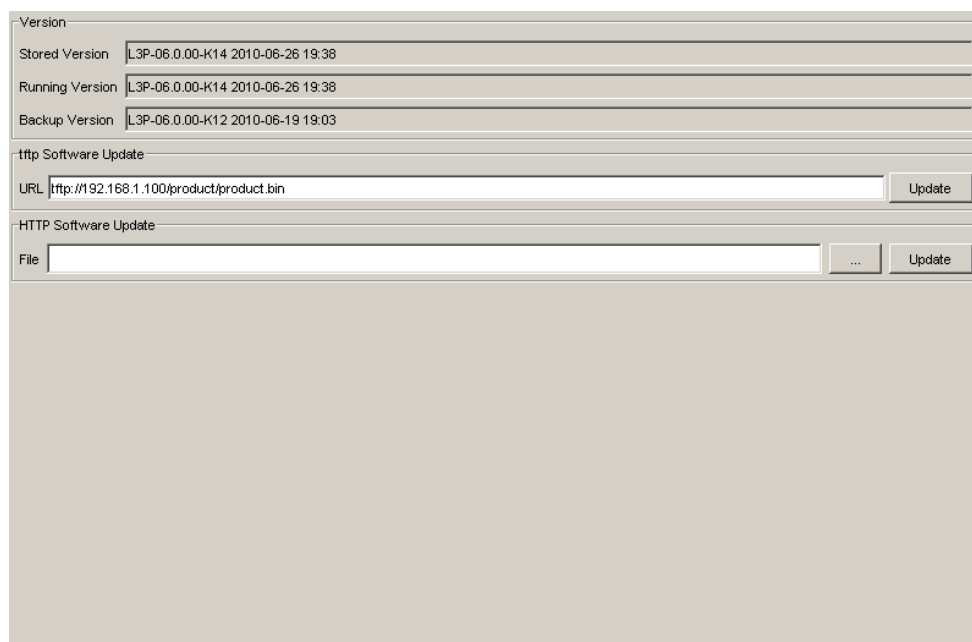
- Enter the parameters on the right according to the selected mode.
- You enter the name applicable to the DHCP protocol in the “Name” line in the system dialog of the Web-based interface.
- The “VLAN” frame enables you to assign a VLAN to the management CPU of the device. If you enter 0 here as the VLAN ID (not included in the VLAN standard version), the management CPU will then be accessible from all VLANs.
- The Ethernet Switch Configurator protocol allows you to allocate an IP address to the device on the basis of its MAC address. Activate the Ethernet Switch Configurator protocol if you want to allocate an IP address to the device from your PC with the enclosed Ethernet Switch Configurator protocol software (setting on delivery: operation “on”, access “read-write”).

**Note:** When you change the network mode from “Local” to “BOOTP” or “DHCP”, the server will assign a new IP address to the device. If the server does not respond, the IP address will be set to 0.0.0.0, and the BOOTP/ DHCP process will try to obtain an IP address again.

## 1.3 Software

The software dialog enables you to display the software versions in the device and to carry out a software update of the device via file selection, tftp or Memory Backup Adaptor (EAM).

**Note:** The TCSESM and TCSESM-E Managed Switches use the Memory Backup Adaptor TCSEAM0100.



The screenshot displays a software management dialog box with the following sections:

- Version:** A table showing three types of versions:

Stored Version	L3P-06.0.00-K14 2010-06-26 19:38
Running Version	L3P-06.0.00-K14 2010-06-26 19:38
Backup Version	L3P-06.0.00-K12 2010-06-19 19:03
- tftp Software Update:** A text input field containing the URL `ftp://192.168.1.100/product/product.bin` and an **Update** button.
- HTTP Software Update:** A text input field for a file path, followed by a browse button (**...**) and an **Update** button.

Figure 9: Software dialog

### 1.3.1 View the software versions present on the device

You can view:

- ▶ **Stored Version**  
The software version stored in the flash memory.
- ▶ **Running Version**  
The currently loaded software version.
- ▶ **Backup Version**  
The previous software version stored in the flash memory.

### 1.3.2 TFTP Software Update

For a tftp update you need a tftp server on which the software to be loaded is stored.

The URL identifies the path to the software stored on the tftp server. The URL is in the format

tftp://IP address of the tftp server/path name/file name

(e.g. tftp://192.168.1.1/device/device.bin).

Click “tftp Update” to load the software from the tftp server to the device.

To start the new software after loading, cold start the device ([see on page 37 “Restart”](#)).

### 1.3.3 HTTP Software Update

For an HTTP software update (via a file selection window), the device software must be on a data carrier that you can access from your workstation.

- In the file selection frame, click on "...".
- In the file selection window, select the device software (name type: \*.bin, e.g. device.bin) and click on "Open".
- Click on "Update" to transfer the software to the device.

The end of the update is indicated by one of the following messages:

- ▶ Update completed successfully.
  - ▶ Update failed. Reason: incorrect file.
  - ▶ Update failed. Reason: error when saving.
  - ▶ File not found (reason: file name not found or does not exist).
  - ▶ Connection error (reason: path without file name).
- After the update is completed successfully, you activate the new software: Select the `Basic settings: Restart` dialog and perform a cold start. In a cold start, the device reloads the software from the non-volatile memory, restarts, and performs a self-test.
  - In your browser, click on "Reload" so that you can access the device again after it is booted.

### 1.3.4 Automatic software update by EAM

The device also allows you to perform an automatic software update using the EAM. You will find the relevant details in the document "Basic Configuration User", chapter "Automatic Software Update by EAM".

---

## 1.4 Port Configuration

This configuration table allows you to configure each port of the device and also display each port's current mode of operation (link state, bit rate (speed) and duplex mode).

- ▶ In the “Name” column, you can enter a name for every port.
- ▶ In the “Ports on” column, you can switch on the port by selecting it here.
- ▶ In the “Propagate connection error” column, you can specify that a link alarm will be forwarded to the device status and/or the the signal contact is to be opened.
- ▶ In the “Automatic Configuration” column, you can activate the automatic selection of the the operating mode (Autonegotiation) and the automatic assigning of the connections (Auto cable crossing) of a TP port by selecting the appropriate field. After the autonegotiation has been switched on, it takes a few seconds for the operating mode to be set.
- ▶ In the “Manual Configuration” column, you set the operating mode for this port. The choice of operating modes depends on the media module. The possible operating modes are:
  - 10 Mbit/s half duplex (HDX)
  - 10 Mbit/s full duplex (FDX)
  - 100 Mbit/s half duplex (HDX)
  - 100 Mbit/s full duplex (FDX)
  - 1000 Mbit/s half duplex (HDX)
  - 1000 Mbit/s full duplex (FDX)
- ▶ The “Link/Current Operating Mode” column displays the current operating mode and thereby also an existing connection.
- ▶ In the “Cable Crossing (Auto. Conf. off)” column, you assign the connections of a TP port, if “Automatic Configuration” is deactivated for this port. The possible settings are:
  - enable: the device swaps the send and receive line pairs of the TP cable for this port (MDIX).
  - disable: the device does not swap the send and receive line pairs of the TP cable for this port (MDI).
  - unsupported: the port does not support this function (optical port, TP SFP port).
- ▶ In the “Flow Control” column, you checkmark this port to specify that flow control is active here. You also activate the global “Flow Control” switch ([see on page 60 “Switching Global”](#)).

**Note:** The active automatic configuration has priority over the manual configuration.

**Note:** When you are using a redundancy function, you deactivate the flow control on the participating ports. Default setting: flow control deactivated globally and activated on all ports.  
If the flow control and the redundancy function are active at the same time, the redundancy may not work as intended.

**Note:** The following settings are required for the ring ports in a HIPER-Ring:

Port Type	Bit Rate	Autonegotiation (Automatic Configuration)	Port Setting	Duplex Mode
Optical	all	off	on	full
TX	100 Mbit/s	off	on	full
TX	1000 Mbit/s	on	on	-

*Table 2: Port Settings for Ring Ports*

When you switch the DIP switch for the ring ports, the device sets the required settings for the ring ports in the configuration table. The port, which has been switched from a ring port to a normal port, is given the settings Autonegotiation (automatic configuration) on and Port on. The settings remain changeable for all ports.

## 1.5 Loading/Saving the Configuration

With this dialog you can:

- ▶ load a configuration,
- ▶ save a configuration,
- ▶ enter a URL,
- ▶ restore the delivery configuration,
- ▶ use the Memory Backup Adaptor TCSEAM0100 for loading/saving the configuration,
- ▶ cancel a configuration change.

The screenshot shows a software dialog box with the following sections and controls:

- Load:** Radio buttons for 'from Device' (selected), 'from URL', 'from URL & save to Device', and 'via PC'. A 'Restore' button is on the right.
- Save:** Radio buttons for 'to Device' (selected), 'to URL (binary)', 'to URL (script)', 'to PC (binary)', and 'to PC (script)'. A 'Save' button is on the right.
- URL:** A text input field containing 'http://192.168.1.100/product/product.cfg'.
- Delete:** Radio buttons for 'Current Configuration' (selected) and 'Current Configuration and from Device'. A 'Delete configuration' button is on the right.
- EAM:** A dropdown menu labeled 'Status' with 'notPresent' selected.
- Undo Modifications of Configuration:** A checkbox for 'Function' (unchecked), a text field for 'Period to undo while Connection is lost [s]' with '600', and a text field for 'Watchdog IP Address' with '0.0.0.0'.
- Bottom:** 'Set', 'Reload', and 'Help' buttons.

Figure 10: Load/Save dialog

### 1.5.1 Loading the configuration

In the “Load” frame, you have the option to

- ▶ load a configuration saved on the device,
- ▶ load a configuration stored under the specified URL,
- ▶ load a configuration stored on the specified URL and save it on the device,
- ▶ load a configuration saved on the PC in binary format.

If you change the current configuration (for example, by switching a port off), the Web-based interface changes the “load/save” symbol in the navigation tree from a disk symbol to a yellow triangle. After saving the configuration, the Web-based interface displays the “load/save” symbol as a disk again.

**Note:** Loading a configuration deactivates the ports while the configuration is being set up. Afterwards, the Switch sets the port status according to the new configuration.

### 1.5.2 Saving the Configuration

In the “Save” frame, you have the option to

- ▶ save the current configuration on the device,
- ▶ save the current configuration in binary form in a file under the specified URL, or as an editable and readable script,
- ▶ save the current configuration in binary form or as an editable and readable script on the PC.



**Note:** For script configuration files, consider the following characteristics:

- ▶ When you save the configuration to a binary file, the device will save all its configuration settings to the binary file. In contrast, when you save the configuration to a script file, it will only save those configuration settings to the configuration script file that are different from the default configuration.
- ▶ When you restore a configuration from a script file, first clear the configuration on the device so that the loaded script will properly overwrite the default configuration settings. Otherwise, loading a script file will result in a configuration that comprises the union of the non-default configuration settings from the previous configuration and the script file's contents. When you are using this feature, remember that loading a script will only set configuration items to a non-default state.
- ▶ To clear the configuration on a device, select the "Current Configuration" option from the "Delete" frame and click "Delete configuration". The device will delete its current configuration immediately ([see on page 34 "Deleting a configuration"](#)).

**Note:** The loading process started by DHCP/BOOTP (see ["Network" on page 24](#)) shows the selection of "from URL & save local" in the "Load" frame. If you get an error message when saving a configuration, this could be due to an active loading process. DHCP/BOOTP only finishes a loading process when a valid configuration has been loaded. If DHCP/BOOTP does not find a valid configuration, finish the loading process by loading the local configuration from the device in the "Load" frame.

If you change the current configuration (for example, by switching a port off), the Web-based interface changes the "load/save" symbol in the navigation tree from a disk symbol to a yellow triangle. After saving the configuration, the Web-based interface displays the "load/save" symbol as a disk again.

After you have successfully saved the configuration on the device, the device sends an alarm (trap) `saConfigurationSavedTrap` together with the information about the Memory Backup Adaptor (EAM), if one is connected. When you change the configuration for the first time after saving it, the device sends a trap `saConfigurationChangedTrap`.

### 1.5.3 URL

The URL identifies the path to the tftp server on which the configuration file is to be stored. The URL is in the format: tftp://IP address of the tftp server/path name/file name (e.g. tftp://192.168.1.100/device/config.dat).

The configuration file includes all configuration data, including the passwords for accessing the device. Therefore pay attention to the access rights on the tftp server.

### 1.5.4 Deleting a configuration

In the “Delete” frame, you have the option to

- ▶ Reset the current configuration to the state on delivery. The configuration saved on the device is retained.
- ▶ Reset the device to the state on delivery. After the next restart, the IP address is also in the state on delivery.

### 1.5.5 Using the Memory Backup Adaptor (EAM)

The EAMs are devices for loading/saving the configuration data of a device. An EAM enables the configuration data to be transferred easily by means of a substitute device of the same type.

**Note:** If you replace a device with DIP switches, check that the DIP switch settings to be sure that they are the same.

- Storing the current configuration data in the EAM:  
You have the option of transferring the current device configuration, including the SNMP password, to the EAM and the flash memory by using the “to device” option in the “Save” frame .
  
- Transferring the configuration data from the EAM:  
When you restart with the EAM connected, the device adopts the configuration data of the EAM and saves it permanently in the flash memory. If the connected EAM does not contain any valid data, for example, if the delivery state is unchanged, the device loads the data from the flash memory.

**Note:** Before loading the configuration data from the EAM, the device compares the password in the device with the password in the EAM configuration data.

The device loads the configuration data if

- ▶ the admin password matches or
- ▶ there is no password saved locally or
- ▶ the local password is the original default password or
- ▶ no configuration is saved locally.

Status	Meaning
notPresent	No EAM present
ok	The configuration data from the EAM and the device match.
removed	The EAM was removed after booting.
notInSync	- The configuration data of the EAM and the device do not match, or only one file exists <sup>a</sup> , or - no configuration file is present on the EAM or on the device <sup>b</sup> .
outOfMemory	The local configuration data is too extensive to be stored on the EAM.
wrongMachine	The configuration data in the EAM originates from a different device type and cannot be read or converted.
checksumErr	The configuration data is damaged.

*Table 3: EAM status*

<sup>a</sup> In these cases, the EAM status is identical to the status “EAM not in sync”, which sends “Not OK” to the signal contacts and the device status.,

<sup>b</sup> In this case, the EAM status (“notInSync”) deviates from the status “EAM not in sync”, which sends “OK” to the signal contacts, and the device status.

## 1.5.6 Canceling a configuration change

### ■ Function

If the function is activated and the connection to the device is interrupted for longer than the time specified in the field “Period to undo while connection is lost [s]”, the device then loads the last configuration saved.

Activate the function before you configure the device so that you will then be reconnected if an incorrect configuration interrupts your connection to the device.

Enter the “Period to undo while the connection is lost [s]” in seconds.  
Possible values: 10-600 seconds.  
Default setting: 600 seconds.

**Note:** Deactivate the function after you have successfully saved the configuration, so that the device does not reload the configuration after you close the web interface.

### ■ Watchdog IP address

“Watchdog IP address” shows you the IP address of the PC from which you have activated the (watchdog) function. The device monitors the link to the PC with this IP address, checking for interruptions.

## 1.6 Restart

With this dialog you can:

- ▶ initiate a cold start of the device. The device reloads the software from the non-volatile memory, restarts, and performs a self-test.  
In your browser, click on “Reload” so that you can access the device again after it is booted.
- ▶ initiate a warm start of the device. In this case the device checks the software in the volatile memory and restarts. If a warm start is not possible, the device automatically performs a cold start.
- ▶ reset the entries with the status “learned” in the filter table (MAC address table).
- ▶ reset the ARP table.  
The device maintains an ARP table internally.  
If, for example, you assign a new IP address to a computer and subsequently cannot set up a connection to the device, you then reset the ARP table.
- ▶ reset the port counters.
- ▶ delete the log file.

**Note:** During the restart, the device temporarily does not transfer any data, and it cannot be accessed via the Web-based interface or other management systems.

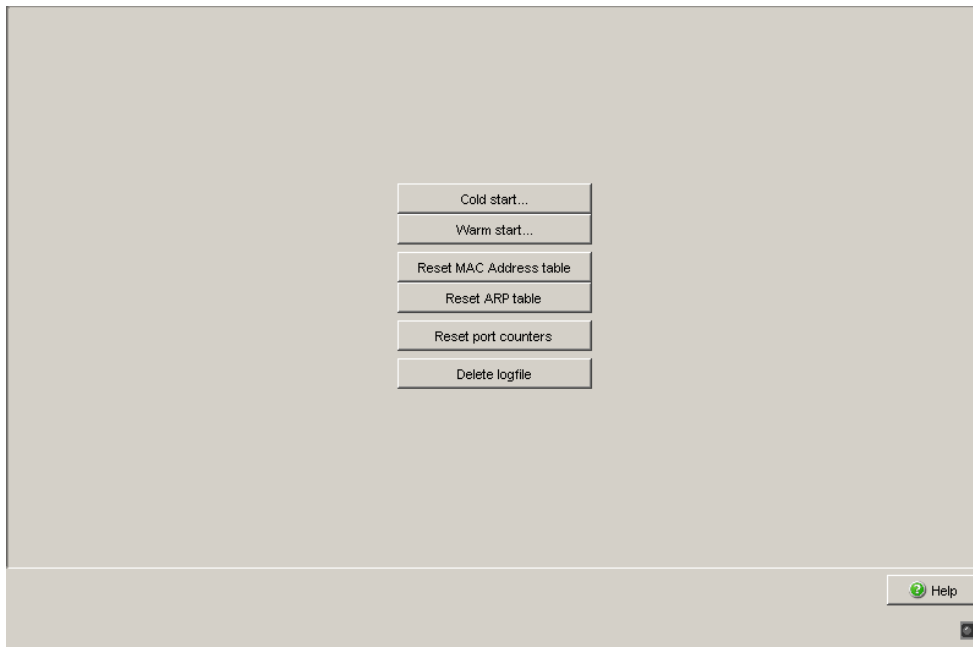


Figure 11: Restart Dialog

## 2 Security

The “Security” menu contains the dialogs, displays and tables for configuring the security settings:

- ▶ Password/SNMPv3 access
- ▶ SNMPv1/v2 access
- ▶ Telnet/Web access
- ▶ Restricted management access
- ▶ Port security

## 2.1 Password / SNMPv3 access

This dialog gives you the option of changing the read and read/write passwords for access to the device via the Web-based interface, via the CLI, and via SNMPv3 (SNMP version 3).

Set different passwords for the read password and the read/write password so that a user that only has read access (user name “user”) does not know, or cannot guess, the password for read/write access (user name “admin”). If you set identical passwords, when you attempt to write this data the device reports a general error.

The Web-based interface and the user interface (CLI) use the same passwords as SNMPv3 for the users “admin” and “user”.

**Note:** Passwords are case-sensitive.

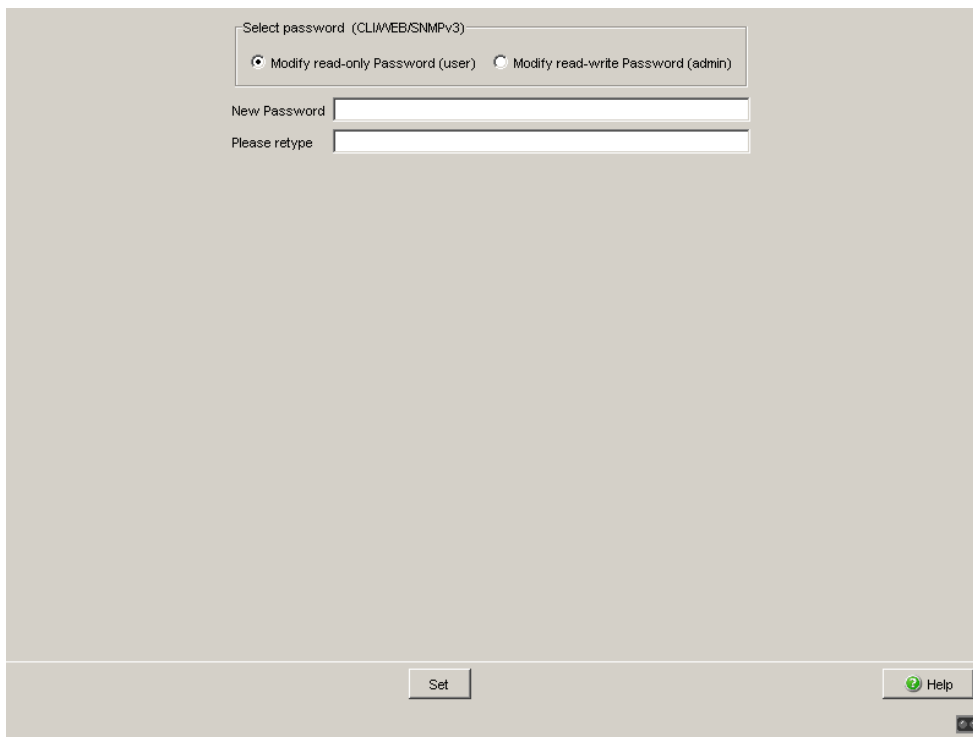
- Select “Modify read-only password (user)” to enter the read password.
- Enter the new read password in the “New password” line and repeat your entry in the “Please retype” line.
- Select “Modify read-write password (admin)” to enter the read/write password.
- Enter the read/write password and repeat your entry.
- The “Data encryption” function controls the encryption of the Web-based management data for the transfer between your PC and the device via SNMPv3.
  - When the data encryption is deactivated, the transfer of the configuration data is unencrypted, and is protected from corruption.
  - The Web-based interface always transfers the passwords securely.
  - The Web-based interface always transfers the user name in plain text.
  - The device allows you to set the function differently for the access with the read password and with the read/write password.



**Note:** When you change the SNMPv3 password for the read/write access, the device automatically synchronizes the readWrite community for the SNMPv1/v2 access to the same value. Similarly, when the read access password is changed, the device synchronizes the readOnly community for SNMPv1/v2 (see on page 43 “SNMPv1/v2 Access Settings”).

As the Web-based interface displays the communities readably in the dialog for SNMPv1/v2, this dialog can only be accessed by a user who has logged in with the user name “admin” and the correct read/write password.

**Note:** When you change the SNMPv3 password for the user name with which you have logged in to the Web-based interface, log in again so that you can access the Web-based interface of the device again. Otherwise you will get a general error message when you attempt to access it.



Select password (CLI/WEB/SNMPv3)

Modify read-only Password (user)  Modify read-write Password (admin)

New Password

Please retype

Set Help

Figure 12: Dialog Password/SNMP Access

**Note:** If you do not know a password with “read/write” access, you will not have write access to the device.

**Note:** For security reasons, the device does not display the passwords. Make a note of every change. You cannot access the device without a valid password.

**Note:** For security reasons, SNMPv3 encrypts the password. With the “SNMPv1” or “SNMPv2” setting in the dialog `Security:SNMPv1/v2 access`, the device transfers the password unencrypted, so that this can also be read.

**Note:** Use between 5 and 32 characters for the password in SNMPv3, since many applications do not accept shorter passwords.

Access at IP address level is restricted in a separate dialog ([see on page 43 “SNMPv1/v2 Access Settings”](#)).

## 2.2 SNMPv1/v2 Access Settings

With this dialog you can select access via SNMPv1 or SNMPv2. In the state on delivery, both protocols are activated.

You can thus use the device to communicate with earlier versions of SNMP.

**Note:** To be able to read and/or change the data in this dialog, log in to the Web-based interface with the user name “admin” and the relevant password.

- ▶ In the “Index” column, the device displays the access restriction’s sequential number.
- ▶ In the “Password” column, you enter the password with which a management station may access the device via SNMPv1/v2 from the specified address range.

**Note:** Passwords are case-sensitive.

- ▶ In the “IP Address” column, you enter the IP address which may access the device. No entry in this field, or the entry “0.0.0.0”, allows access to this device from computers with any IP address. In this case, the only access protection is the password.
- ▶ In the “IP Mask” column, much the same as with netmasks, you have the option of selecting a group of IP addresses.

Example:

255.255.255.255: a single IP address

255.255.255.240 with IP address = 172.168.23.20:

the IP addresses 172.168.23.16 to 172.168.23.31.

Binary notation of the mask 255.255.255.240:

```
1111 1111 1111 1111 1111 1111 1111 0000
                                |-----|
                                mask bits
```

Binary notation of the IP address 172.168.23.20:

```
1010 1100 1010 1000 0001 0111 0001 0100
```

The binary representation of the mask with the IP address yields an address range of:

```
1010 1100 1010 1000 0001 0111 0001 0000 bis
```

```
1010 1100 1010 1000 0001 0111 0001 1111
```

i.e.: 172.168.23.16 to 172.168.23.31

- ▶ In the “Access Mode” column, you specify whether this computer can access the device with the read password (access mode “readOnly”) or with the read/write password (access mode “readWrite”).

**Note:** The password for the “readOnly” access mode is the same as the SNMPv3 password for read access. The password for the “readWrite” access mode is the same as the SNMPv3 password for read/write access. When you change one of the passwords, the device automatically synchronizes the corresponding password for SNMPv3 ([see on page 40 “Password / SNMPv3 access”](#)).

- ▶ You can activate/deactivate this table entry in the “Active” column.

**Note:** If you have not activated any line, the device does not apply any access restriction with regard to the IP addresses.

- ▶ The “Create entry” button enables you to create a new row in the table.
- ▶ With “Delete entry” you delete selected rows in the table.

**Note:** The row with the password currently in use cannot be deleted or changed.

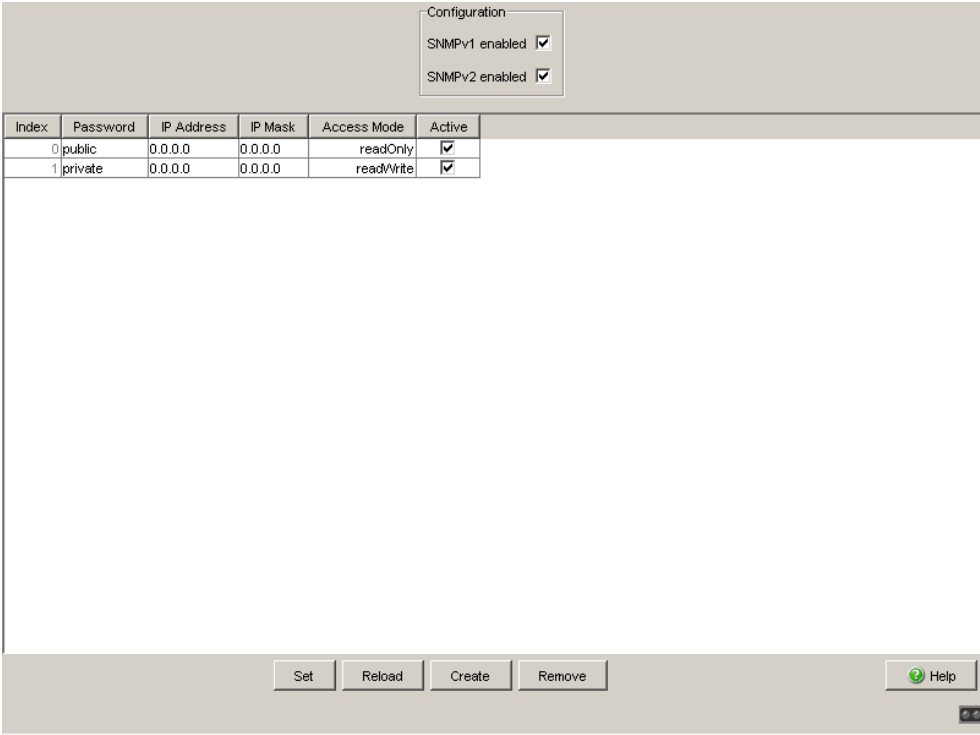
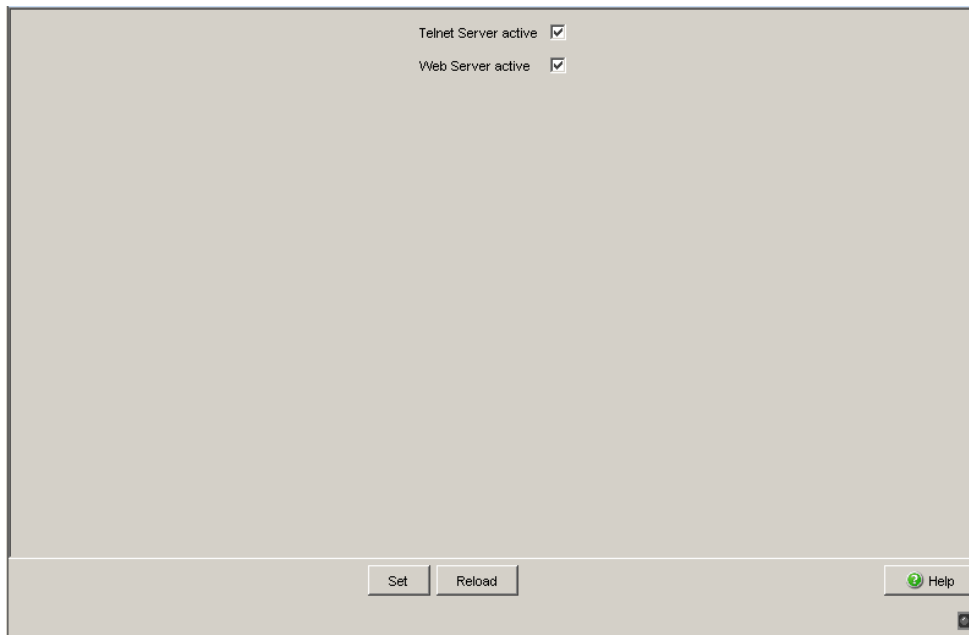


Figure 13: SNMPv1/v2 Access Dialog

## 2.3 Telnet/Web Access

This dialog allows you to switch off the Telnet server and the Web server on the device.



*Figure 14: Telnet/Web Access dialog*

### 2.3.1 Description of Telnet Access

The Telnet server of the device allows you to configure the device using the Command Line Interface (in-band). You can deactivate the Telnet server to disable Telnet access to the device.

The server is activated in the state on delivery.

After the Telnet server has been deactivated, you will no longer be able to access the device via a new Telnet connection. If a Telnet connection already exists, it is kept.

**Note:** The Command Line Interface (out-of-band) and the `Security:Telnet/Web access` dialog in the Web-based interface allow you to reactivate the Telnet server.

### 2.3.2 Description of Web Access

The Web server of the device allows you to configure the device by using the Web-based interface. Deactivate the Web server if you do not want the device to be accessed from the Web.

On delivery, the server is activated.

After the Web server has been switched off, it is no longer possible to log in via a Web browser. The login in the open browser window remains active.

**Note:** The Command Line Interface allows you to reactivate the Web server.

## 2.4 Port Security

The device allows you to configure each port to help prevent unauthorized access. Depending on your selection, the device checks the MAC address or the IP address of the connected device.

In the “Configuration” frame, you set whether the port security works with MAC or with IP addresses.

Name	Meaning
MAC-Based Port Security	Check source MAC address of the received data packet.
IP-Based Port Security	IP-Based Port Security internally relies on MAC-Based Port Security. Principle of operation: When you configure the function, the device translates the entered source IP address into the respective MAC address. In operation, it checks the source MAC address of the received data packet against the internally stored MAC address.

*Table 4: Configuration of port security globally for all ports*

Set the individual parameters for each port in the port table.

Name	Meaning
Module	Module of the device on which the port is located.
Port	Port to which this entry applies.
Port Status	enabled: Port is switched on and transmitting. disabled: Port is switched off and not transmitting. The port is switched on if - an authorized address accesses the port or - an unauthorized address attempts to access the port and trapOnly or none is selected under “Action”. The port is switched off if - an unauthorized address attempts to access the port and portDisable is selected under “Action”.

*Table 5: Configuration of port security for a single port*



Name	Meaning
Allowed MAC Addresses	<p>MAC addresses of the devices with which you allow data exchange at this port.</p> <p>The Web-based interface allows you to enter up to 10 MAC addresses, each separated by a space. After each MAC address you can enter a slash followed by a number identifying an address area. This number, between 2 and 47, indicates the number of relevant bits. Example:</p> <p>00:80:63:01:02:00/40 stands for 00:80:63:01:02:00 to 00:80:63:01:02:FF</p> <p>or</p> <p>00:80:63:00:00:00/24 stands for 00:80:63:00:00:00 to 00:80:63:FF:FF:FF</p> <p>If there is no entry, any number of devices can communicate via this port.</p>
Current MAC Address	<p>Shows the MAC address of the device from which the port last received data. The Web-based interface allows you to copy an entry from the “Current MAC Address” column into the “Allowed MAC Addresses” column by dragging and dropping with the mouse button.</p>
Allowed IP Addresses	<p>IP addresses of the devices with which you allow data exchange at this port.</p> <p>The Web-based interface allows you to enter up to 10 IP addresses, each separated by a space.</p> <p>If there is no entry, any number of devices can communicate via this port.</p>
Action	<p>Action performed by the device after an unauthorized access:</p> <ul style="list-style-type: none"> <li>– none: no action</li> <li>– trapOnly: send alarm</li> <li>– portDisable: disable the port with the corresponding entry in the port configuration table (<a href="#">see on page 29 “Port Configuration”</a>) and send an alarm.</li> </ul>

*Table 5: Configuration of port security for a single port*

**Note:** This entry in the port configuration table is part of the configuration ([see page 31](#)) and is saved together with the configuration.

**Note:** Prerequisites for the device to be able to send an alarm (trap) ([see on page 178 “Alarms \(Traps\)”](#)):

- You have entered at least one recipient
- You have selected at least one recipient in the “Active” column
- In the “Selection” frame, you have selected “Port Security”

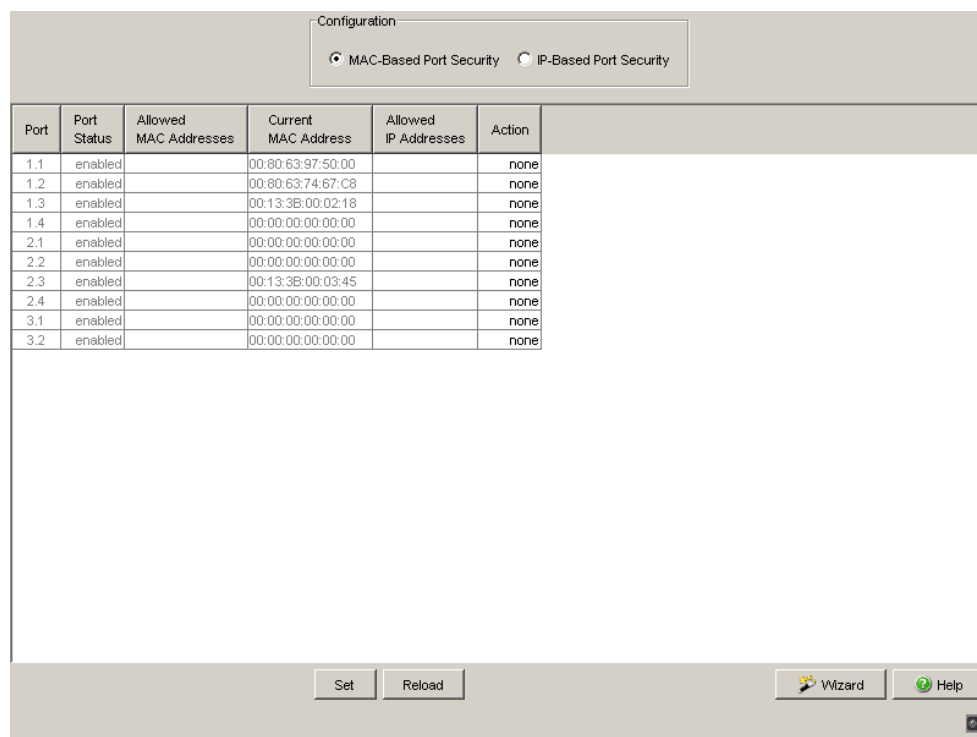


Figure 15: Port Security dialog

**Note:** The IP port security operates internally on layer 2. The device internally translates an allowed IP address into an allowed MAC address when you enter the IP address. An ARP request is used for this.

Prerequisites for the IP-based port security:

- The device with the allowed IP address supports ARP
- The device can be accessed while configuring IP port security
- The MAC address to which the IP address is assigned is unique and remains unchanged after the IP address is entered.

If you have entered a router interface as the allowed IP address, all the packets sent from this interface are considered allowed, since they contain the same MAC source address.

If a connected device sends packets with the allowed IP address but a different MAC address, it will not be allowed by the Switch. If you exchange the device with the allowed IP address for a different one with the same IP address, enter the IP address in the Switch again so that the Switch learns the new MAC address.

## 3 Time

With this dialog you can enter time-related settings independently of the time synchronization protocol selected.

- ▶ The “IEEE/SNTP time” displays the time with reference to Universal Time Coordinated (UTC).  
The time displayed is the same worldwide. Local time differences are not taken into account.
- ▶ The “System time” uses the “IEEE 1588 / SNTP time”, allowing for the local time difference from “IEEE 1588 / SNTP time”.  
“System time” = “IEEE 1588 / SNTP time” + “Local offset”.
- ▶ “Time source” displays the source of the following time data. The device automatically selects the source with the greatest accuracy.  
Possible sources are: `local` and `sntp`. The source is initially `local`. If SNTP is activated and if the device receives a valid SNTP packet, the device sets its time source to `sntp`.
- With “Set time from PC”, the device takes the PC time as the system time and calculates the IEEE 1588 / SNTP time using the local time difference.  
“IEEE 1588 / SNTP time” = “System time” - “Local offset”
- ▶ The “Local Offset” is for displaying/entering the time difference between the local time and the “IEEE 1588 / SNTP time”.
- With “Set offset from PC”, the device determines the time zone on your PC and uses it to calculate the local time difference.

**Note:** When setting the time in zones with summer and winter times, make an adjustment for the local offset, if applicable. The device can also get the SNTP server IP address and the local offset from a DHCP server.

## Interaction of PTP and SNTP

According to PTP (IEEE 1588) and SNTP, both protocols can exist in parallel in the same network. However, since both protocols affect the system time of the device, situations may occur in which the two protocols compete with each other.

The PTP reference clock gets its time either via SNTP or from its own clock. All other clocks favor the PTP time as the source.

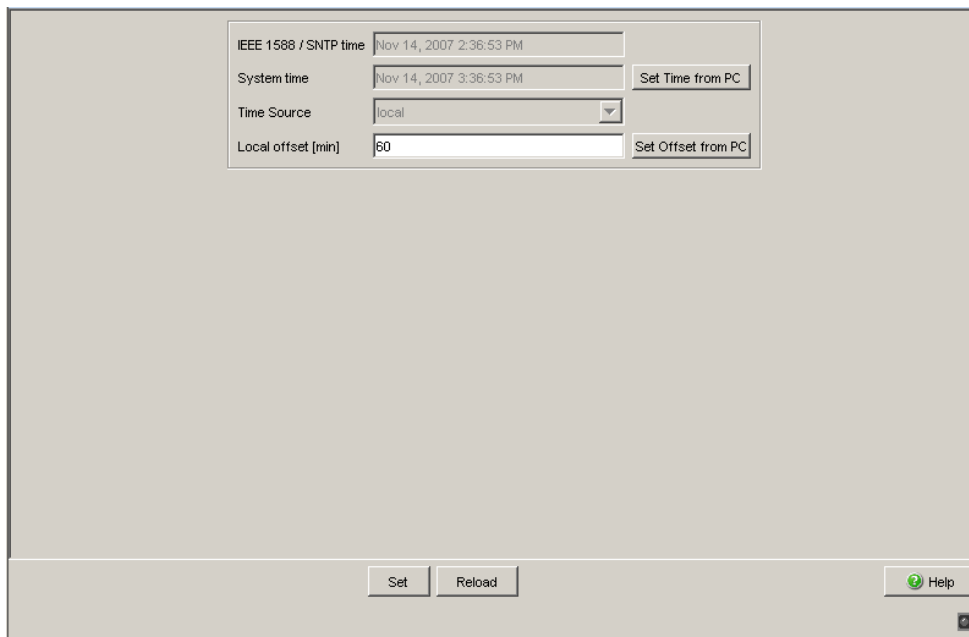


Figure 16: Time Dialog

## 3.1 SNTP configuration

The Simple Network Time Protocol (SNTP) enables you to synchronize the system time in your network.

The device supports the SNTP client and the SNTP server function.

The SNTP server makes the UTC (Universal Time Coordinated) available. UTC is the time relating to the coordinated world time measurement. The time displayed is the same worldwide. Local time differences are not taken into account.

SNTP uses the same packet format as NTP. In this way, an SNTP client can receive the time from an SNTP server as well as from an NTP server.

**Note:** For accurate system time distribution with cascaded SNTP servers and clients, use only network components (routers, switches, hubs) in the signal path between the SNTP server and the SNTP client which forward SNTP packets with a minimized delay.

Parameter	Meaning	Possible Values	Default Setting
Function	Switches the SNTP function on and off globally.	On, Off	Off

*Table 6: Switches SNTP on and off globally*

Parameter	Meaning	Possible Values	Default Setting
SNTP Status	Displays conditions such as "Server cannot be reached".	-	-

*Table 7: SNTP Status*

Parameter	Meaning	Possible Values	Default Setting
Client Status	Switches the SNTP client on and off.	On, Off	On
External server address	IP address of the SNTP server from which the device periodically requests the system time.	Valid IPv4 address	0.0.0.0
Redundant server address	IP address of the SNTP server from which the device periodically requests the system time if it does not receive a response to a request from the "External server address" within 0.5 seconds.	Valid IPv4 address	0.0.0.0
Server request interval	Time interval at which the device requests SNTP packets	1 s - 3,600 s	30 s
Accept SNTP Broadcasts	Specifies whether the device accepts the system time from SNTP Broadcast/Multicast packets that it receives.	On, Off	On
Threshold for obtaining the UTC [ms]	The device changes the time as soon as the deviation from the server time is above this threshold in milliseconds. This reduces the frequency of time changes.	0 - 2.147.483.647 (2 <sup>31</sup> -1)	0
Disable client after successful synchronization	Enable/disable further time synchronizations once the client, after its activation, has synchronized its time with the server.	On, Off	Off

*Table 8: Configuration SNTP Client*

**Note:** If you have enabled PTP at the same time, the SNTP client first collects 60 time stamps before it deactivates itself. The device thus determines the drift compensation for its PTP clock. With the preset server request interval, this takes about half an hour.

**Note:** If you are receiving the system time from an external/redundant server address, you do not accept any SNTP Broadcasts (see below). Otherwise you can never distinguish whether the device is displaying the time from the server entered, or that of an SNTP Broadcast packet.

Parameter	Meaning	Possible Values	Default Setting
Server status	Switches the SNTP server on and off.	On, Off	On
Anycast destination address	IP address, to which the SNTP server of the device sends the SNTP packets (see table 10).	Valid IPv4 address	0.0.0.0
VLAN ID	VLANs to which the device periodically sends SNTP packets.		1
Anycast send interval	Time interval at which the device sends SNTP packets.	1 - 3,600	120
Disable Server at local time source	Enables/disables the SNTP server function if the status of the time source is local (see Time dialog).	On, Off	Off

Table 9: Configuration SNTP Server

IP destination address	Send SNTP packet to
0.0.0.0	Nobody
Unicast address (0.0.0.1 - 223.255.255.254)	Unicast address
Multicast address (224.0.0.0 - 239.255.255.254), especially 224.0.1.1 (NTP address)	Multicast address
255.255.255.255	Broadcast address

Table 10: Destination address classes for SNTP and NTP packets

The image shows a configuration dialog box for SNTP. It is divided into several sections:

- Operation:** Contains radio buttons for 'On' and 'Off', with 'Off' selected.
- SNTP Status:** A text input field.
- Configuration SNTP Client:**
  - Client Status:** Radio buttons for 'On' and 'Off', with 'On' selected.
  - External Server Address:** Text input field with '0.0.0.0'.
  - Redundant Server Address:** Text input field with '0.0.0.0'.
  - Server Request Interval [s]:** Text input field with '30'.
  - Accept SNTP Broadcasts:** Checkmark is checked.
  - Threshold for obtaining the UTC [ms]:** Text input field with '0'.
  - Disable Client after successful Synchronization:** Checkmark is unchecked.
- Configuration SNTP Server:**
  - Server Status:** Radio buttons for 'On' and 'Off', with 'On' selected.
  - Anycast Destination Address:** Dropdown menu showing '0.0.0.0'.
  - VLAN ID:** Text input field with '1'.
  - Anycast Send Interval [s]:** Text input field with '120'.
  - Disable Server at local Time Source:** Checkmark is unchecked.

At the bottom of the dialog, there are three buttons: 'Set', 'Reload', and 'Help' (with a question mark icon).

Figure 17: SNTP Dialog



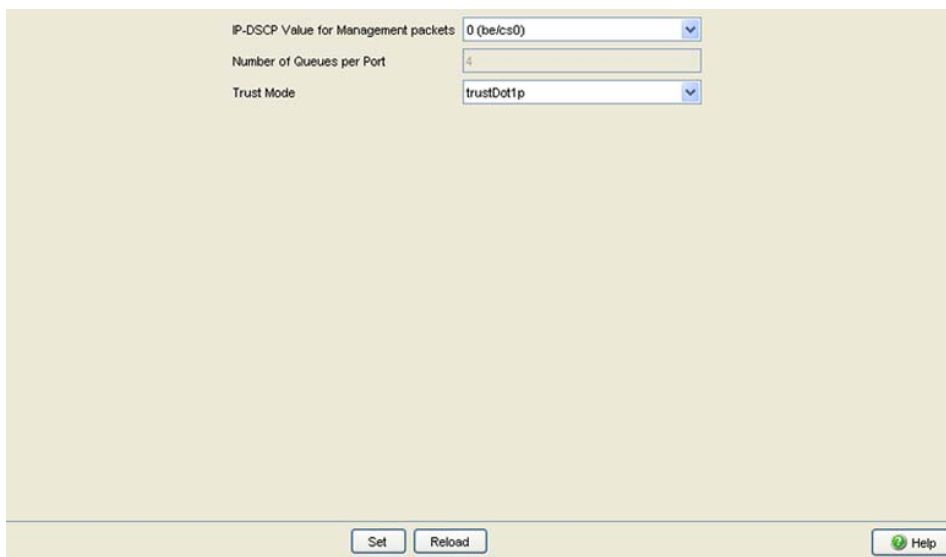
## 3.2 PTP (IEEE 1588)

Precise time management is required for running time-critical applications via a LAN.

The IEEE 1588 standard with the Precision Time Protocol (PTP) describes a procedure that determines the best master clock in a LAN and thus enables the precise synchronization of all clocks in this LAN.

For devices **without** a real-time (RT) module (module without timestamp unit):

- ▶ enable/disable the PTP function in the PTP dialog.
- ▶ select PTP mode in the PTP dialog.
  - Select `v1-simple-mode` if the reference clock uses PTP Version 1.
  - Select `v2-simple-mode` if the reference clock uses PTP Version 2.



IP-DSCP Value for Management packets: 0 (be/cso)

Number of Queues per Port: 4

Trust Mode: trustDot1p

Set Reload Help

Figure 18: Dialog PTP



## 4 Switching

The switching menu contains the dialogs, displays and tables for configuring the switching settings:

- ▶ Switching Global
- ▶ Filters for MAC Addresses
- ▶ Rate Limiter
- ▶ Multicasts
- ▶ VLAN

---

## 4.1 Switching Global

Variable	Meaning	Possible Values	
MAC address (read only)	Display the MAC address of the device		
Aging Time (s)	Enter the Aging Time in seconds for dynamic MAC address entries.	15-3.825	30
Flow control	Activate/deactivate the flow control	On, Off	Off

*Table 11: Switching:Global dialog*

**Note:** When you are using a redundancy function, you deactivate the flow control on the participating ports. Default setting: flow control deactivated globally and activated on all ports.

If the flow control and the redundancy function are active at the same time, the redundancy may not work as intended.

Variable	Meaning	Possible Values	
Learning addresses	Activate/deactivate the learning of MAC source addresses.	On, Off	On
Frame size	Set the maximum packet size (frame size) in bytes.	1522, 1632	1522
Activate Address Relearn Detection	Enable/disable whether the device detects whether it has repeatedly learned the same MAC source addresses at different ports. This process very probably indicates a loop situation in the network. If the device detects this process, it creates an entry in the log file and sends an alarm (trap).	On, Off	Off
Address Relearn Threshold	Number of MAC addresses that are learned at different ports within a checking interval, so that if this number is exceeded, the device sees this as a relevant event. The interval for this check is a few seconds.	1 - 1,024	1
Activate Duplex Mismatch Detection	Enable/disable whether the device reports a duplex problem at a port for specific error events. This means that the duplex mode of the port might not match that of the remote port. If the device detects a potential non-match, it creates an entry in the event log and sends an alarm (trap). To detect potential non-matches, the device evaluates the error counters of the port after the connection is set up, in the context of the port settings (see table 13).	On, Off	On

Table 12: Switching:Global dialog

The following table lists the duplex operating modes for TX ports together with the possible error events. The terms in the table mean:

- ▶ Collisions: In half-duplex mode, collisions mean normal operation.
- ▶ Duplex problem: Duplex modes do not match.
- ▶ EMI: Electromagnetic interference.
- ▶ Network extension: The network extension too great, or too many hubs are cascaded.

- ▶ Collisions, late collisions: In full-duplex mode, the port does not count collisions or late collisions.
- ▶ CRC error: The device only evaluates these errors as duplex mismatches in the manual full duplex mode.

No.	Autonegotiation	Current duplex mode	Detected error events ( $\geq 10$ )	Evaluation of duplex situation by device	Possible causes
1	On	Half duplex	None	OK	
2	On	Half duplex	Collisions	OK	
3	On	Half duplex	Late collisions	Duplex problem detected	Duplex problem, EMI, network extension
4	On	Half duplex	CRC error	OK	EMI
5	On	Full duplex	None	OK	
6	On	Full duplex	Collisions	OK	EMI
7	On	Full duplex	Late collisions	OK	EMI
8	On	Full duplex	CRC error	OK	EMI
9	Off	Half duplex	None	OK	
10	Off	Half duplex	Collisions	OK	
11	Off	Half duplex	Late collisions	Duplex problem detected	Duplex problem, EMI, network extension
12	Off	Half duplex	CRC error	OK	EMI
13	Off	Full duplex	None	OK	
14	Off	Full duplex	Collisions	OK	EMI
15	Off	Full duplex	Late collisions	OK	EMI
16	Off	Full duplex	CRC error	Duplex problem detected	Duplex problem, EMI

Table 13: Evaluation of non-matching of the duplex mode

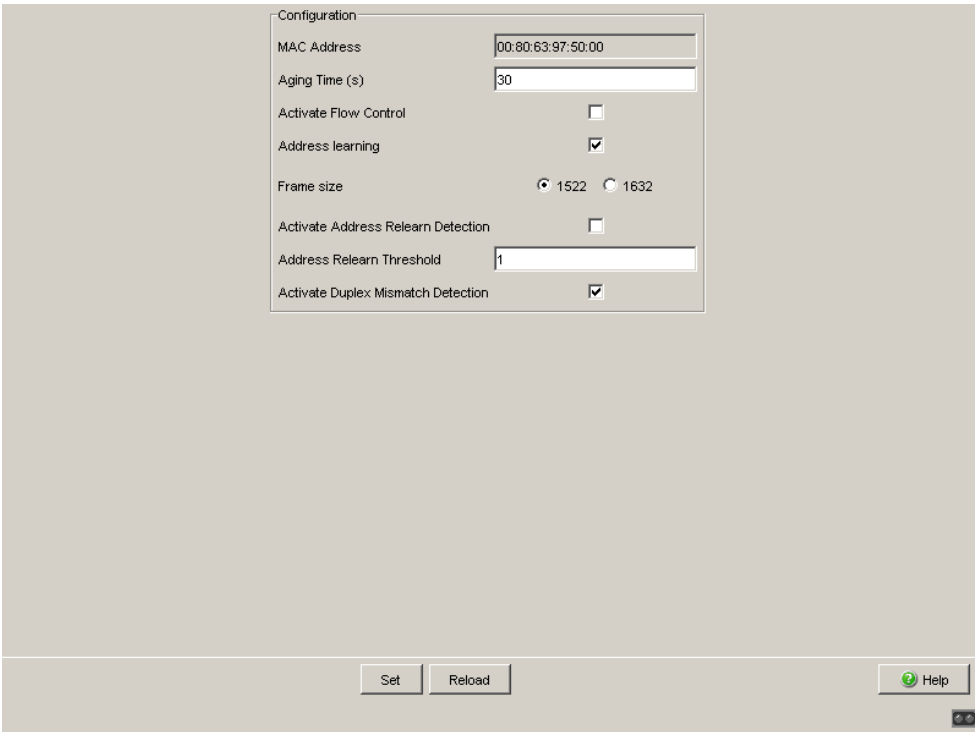


Figure 19: Dialog Switching Global

## 4.2 Filters for MAC addresses

The filter table for MAC addresses is used to display and edit filters. Each row represents one filter. Filters specify the way in which data packets are sent. They are set automatically by the device (learned status) or manually. Data packets whose destination address is entered in the table are sent from the receiving port to the ports marked in the table. Data packets whose destination address is not in the table are sent from the receiving port to all other ports. The following conditions are possible:

- ▶ **learned**: The filter was created automatically by the device.
- ▶ **invalid**: With this status you delete a manually created filter.
- ▶ **permanent**: The filter is stored permanently in the device or on the URL (see on page 31 “Loading/Saving the Configuration”).
- ▶ **igmp**: The filter was created by IGMP Snooping.

In the “Create” dialog (see buttons below), you can create new filters.

Address	Status	VLAN-ID	1.1	1.2	1.3	1.4	1.5	1.6	1.7	1.8	1.9	1.10	1.11	1.12	1.13	1.14
00 13 3b 00 00 ae	learned	1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
00 13 3b 00 00 fa	learned	1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
00 13 3b 00 01 5e	learned	1	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
00 80 63 1f 10 54	mgmt	1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
00 80 63 2f fb b8	learned	1	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
00 80 63 2f fb c6	learned	1	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
00 80 63 51 74 00	learned	1	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
00 80 63 57 4c 67	learned	1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
00 80 63 62 b0 ff	learned	1	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
00 80 63 74 67 c8	learned	1	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Buttons: Set, Reload, Create, Help

Figure 20: Filter Table dialog



**Note:** For Unicast addresses, the device allows you to include one or no ports in a filter entry. Do not include any ports if you want to create a discard filter entry.

**Note:** This filter table allows you to create up to 100 filter entries for Multicast addresses.

---

## 4.3 Rate Limiter

The device can limit the rate of message traffic during periods of heavy traffic flow.

Entering a limit rate for each port specifies the amount of traffic the device is permitted to transmit and receive.

If the data load transmitted at this port exceeds the maximum load entered, the device will discard the excess data at this port.

A global setting enables/disables the rate limiter function at all ports.

**Note:** The limiter functions work exclusively on layer 2 and serve the purpose of limiting the effects of storms of those frame types (typically broadcasts) that the Switch floods. The limiter function ignores any protocol information of higher layers like IP or TCP. This may affect e.g., TCP traffic.

You can minimize this effects by:

- ▶ applying the limiter function only to particular frame types (e.g., to broadcasts, multicasts and unicasts with an unlearned destination address) and excluding unicasts with a learned destination address from the limitation,
- ▶ using the egress limiter function instead of the ingress limiter function because the former cooperates slightly better with TCP's flow control (reason: frames buffered by the internal switching buffer),
- ▶ increasing the aging time for learned unicast destination addresses.

### 4.3.1 Rate Limiter settings

- ▶ “Ingress Limiter (kbit/s)” allows you to enable or disable the input limiting function for all ports.

- 
- ▶ “Egress Limiter (Pkt/s)” allows you to enable or disable the broadcast output limiter function at all ports.
  - ▶ “Egress Limiter (kbit/s)” allows you to enable or disable the output limiter function for all packet types at all ports.

Setting options per port:

- ▶ “Ingress Packet Types” allows you to select the packet type for which the limit is to apply:
  - ▶ All, limits the total inbound data volume at this port.
  - ▶ BC, limits the broadcast packets received at this port.
  - ▶ BC + MC, limits broadcast packets and Multicast packets received at this port.
  - ▶ BC + MC + uUC, limits broadcast packets, Multicast packets, and unknown Unicast packets received at this port.
- ▶ Ingress Limiter Rate for the inbound packet type selected:
  - ▶ = 0, no ingress limit at this port.
  - ▶ > 0, maximum inbound traffic rate in kbit/s that can be received at this port.
- ▶ Egress Limiter Rate for broadcast packets:
  - ▶ = 0, no rate limit for outbound broadcast packets at this port.
  - ▶ > 0, maximum number of outbound broadcasts per second that can be sent at this port.
- ▶ Egress Limiter Rate for the entire data stream:
  - ▶ = 0, no rate limit for outbound data stream at this port.
  - ▶ > 0, maximum outbound transmission rate in kbit/s sent at this port.

Ingress Limiter (kbit/s)

Function  On  Off

Egress Limiter (Pkt/s) Packet Type: BC

Function  On  Off

Egress Limiter (kbit/s) Packet Type: all

Function  On  Off

Module	Port	Ingress Packet Types	Ingress Limiter Rate (kbit/s)	Egress Limit (Pkt/s) Packet Type: BC	Egress Limit (kbit/s) Packet Type: all
1	2	BC	0	0	0
1	3	All	0	0	0
1	4	BC	0	0	0
1	5	BC + MC	0	0	0
1	6	BC + MC + uUC	0	0	0
1	7	BC	0	0	0
1	8	BC	0	0	0
1	9	BC	0	0	0
1	10	BC	0	0	0
1	11	BC	0	0	0
1	12	BC	0	0	0
1	13	BC	0	0	0
1	14	BC	0	0	0
1	15	BC	0	0	0
1	16	BC	0	0	0

Set
Reload

Help

Figure 21: Rate Limiter Dialog

## 4.4 Multicasts

### 4.4.1 IGMP (Internet Group Management Protocol)

With this dialog you can

- ▶ activate/deactivate the IGMP Snooping protocol,
- ▶ configure the IGMP Snooping protocol globally and per port.

Port	IGMP an	IGMP Forw. All	IGMP Automatic Query Port	Statischer Query Port	Gelernter Query Port
1.1	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	disable	<input type="checkbox"/>
1.2	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	disable	<input type="checkbox"/>
1.3	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	disable	<input type="checkbox"/>
1.4	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	disable	<input type="checkbox"/>
2.1	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	disable	<input type="checkbox"/>
2.2	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	disable	<input type="checkbox"/>
2.3	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	disable	<input type="checkbox"/>
2.4	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	disable	<input type="checkbox"/>
3.1	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	disable	<input type="checkbox"/>
3.2	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	disable	<input type="checkbox"/>

Figure 22: IGMP Snooping dialog

- Operation  
In this frame you can:

- ▶ activate/deactivate the IGMP Snooping protocol.

Parameter	Meaning	Value range	Default setting
Function	Activate/deactivate IGMP Snooping globally for the device. If IGMP Snooping is switched off: <ul style="list-style-type: none"> <li>▶ the device does not evaluate Query and Report packets received, and</li> <li>▶ it sends (floods) received data packets with a Multicast address as the destination address to all ports.</li> </ul>	On, Off	Off

*Table 14: IGMP Snooping, global function*

#### ■ IGMP Querier and IGMP Settings

With these frames you can enter global settings for the IGMP settings and the IGMP Querier function.

Prerequisite: The IGMP Snooping function is activated globally.

Parameter	Meaning	Value range	Default setting
<b>IGMP Querier</b>			
IGMP Querier enabled	Switch query function on/off	on/off	off
Protocol Version	Select IGMP version 1, 2 or 3.	1, 2, 3	2
Send Interval	Enter the interval at which the switch sends query packets. All IGMP-capable terminal devices respond to a query with a report message.	2-3599 s <sup>a</sup>	125 s
<b>IGMP settings</b>			
Current querier IP address	Display the IP address of the router/switch that contains the query function.		
Max. Response Time	Enter the time within which the Multicast group members respond to a query. The Multicast group members select random values within the response time for their response, so that all the Multicast group members do not respond to the query at the same time.	Protocol Version 10 s - 1,2: 1-25 s <sup>a</sup> - 3: 1-3598 s <sup>a</sup>	
Group Membership Interval	Enter the period for which a dynamic Multicast group remains entered in the device if it does not receive any report messages.	3-3600 s <sup>a</sup>	260 s

Table 15: IGMP Querier and IGMP settings

a.) Note the connection between the parameters Max. Response Time, Send Interval and Group Membership Interval, (see table 16)

The parameters

- Max. Response Time,
  - Send Interval and
  - Group Membership Interval
- have a relationship to each other:

**Max. Response Time < Send Interval < Group Membership Interval.**

If you enter values that contradict this relationship, the device then replaces these values with a default value or with the last valid values.

Parameter	Protocol Version	Value range	Default setting
Max. Response Time,	1, 2 3	1-25 seconds 1-3,598 seconds	10 seconds
Send Interval	1, 2, 3	2-3,599 seconds	125 seconds
Group Membership Interval	1, 2, 3	3-3,600 seconds	260 seconds

*Table 16: Value range for*

- *Max. Response Time*
- *Send Interval*
- *Group Membership Interval*

For “Send Interval” and “Max. Response Time”,

- select a large value if you want to reduce the load on your network and can accept the resulting longer switching times,
- select a small value if you require short switching times and can accept the resulting network load.

## ■ Multicasts

In this frame you specify how the device transmits packets with

- ▶ unknown MAC/IP Multicast address not learned with IGMP Snooping
- ▶ known MAC/IP Multicast address learned with IGMP Snooping.

Prerequisite: The IGMP Snooping function is activated globally.



Parameter	Meaning	Value range	Default setting
<b>Unknown Multicasts</b>			
	<ul style="list-style-type: none"> <li>▶ <b>Send to Query Ports:</b> The device sends the packets with an unknown MAC/IP Multicast address to all query ports.</li> <li>▶ <b>Send to All Ports:</b> The device sends the packets with an unknown MAC/IP Multicast address to all ports.</li> <li>▶ <b>Discard:</b> The device discards all packets with an unknown MAC/IP Multicast address.</li> </ul>	Send to Query Ports, Send to All Ports, Discard	Send to All Ports
<b>Known Multicasts</b>			
	<ul style="list-style-type: none"> <li>▶ <b>Send to query and registered ports:</b> The device sends the packets with a known MAC/IP Multicast address to all query ports and to registered ports. The advantage of this is that it works in many applications without any additional configuration. Application: “Flood and Prune” routing in PIM-DM.</li> <li>▶ <b>Send to registered ports:</b> The device sends the packets with a known MAC/IP Multicast address to registered ports. The advantage of this setting is that it uses the available bandwidth optimally through direct distribution. It requires additional port settings. Application: Routing protocol PIM-SM.</li> </ul>	Send to query and registered ports, send to registered ports	Send to registered ports

*Table 17: Known and unknown Multicasts*

**Note:** The way in which unlearned Multicast addresses are handled also applies to the reserved addresses from the “Local Network Control Block” (224.0.0.0 - 224.0.0.255). This can have an effect on higher-level routing protocols.

- Settings per Port (Table)

With this configuration table you can enter port-related IGMP settings.

Parameter	Meaning	Value range	Default setting
Port	Module and port numbers to which this entry applies.	-	-
IGMP Snooping on	Switch IGMP on/off for each port. Switching IGMP off at a port prevents registration for this port. Prerequisite: In the <code>Switching:Multicasts:IGMP</code> dialog, IGMP is enabled.	on, off	on
IGMP Forward All	Switch the IGMP Snooping function "Forward All" on/off. With the <code>IGMP Forward All</code> setting, the device sends to this port all data packets with a Multicast address in the destination address field. Prerequisite: In the <code>Switching:Multicasts:IGMP</code> dialog, IGMP is enabled.  <b>Note:</b> If a number of routers are connected to a subnetwork, you must use IGMP version 1 so that all the routers receive all the IGMP reports.  <b>Note:</b> If you use IGMP version 1 in a subnetwork, then you must also use IGMP version 1 in the entire network.	on, off	off
IGMP Automatic Query Port	Displays which ports the device has learned as query ports if <code>automatic</code> is selected in "Static Query Port". Prerequisite: The IGMP Snooping function is activated globally.	yes, no	-
Static Query Port	The device sends IGMP report messages to the ports at which it receives IGMP queries (default setting). This column allows you to also send IGMP report messages to: other selected ports (enable) or connected Schneider Electric devices (automatic). Prerequisite: The IGMP Snooping function is activated globally.	enable, disable, automatic	disable
Learned Query Port	Shows at which ports the device has received IGMP queries if "disable" is selected in "Static Query Port". Prerequisite: In the <code>Switching:Multicasts:IGMP</code> dialog, IGMP is enabled.	yes, no	-

*Table 18: Settings per port*

**Note:** If the device is incorporated into a HIPER-Ring, you can use the following settings to quickly reconfigure the network for data packets with registered Multicast destination addresses after the ring is switched:

- ▶ Switch on the IGMP Snooping on the ring ports and globally, and
- ▶ activate “IGMP Forward All” per port on the ring ports.

## 4.4.2 GMRP (GARP Multicast Registration Protocol)

With this dialog you can:

- ▶ activate/deactivate the GMRP function globally,
- ▶ configure the GMRP for each Port.

### ■ Operation

In this frame you can:

- ▶ activate/deactivate the GMRP function globally.

Parameter	Meaning	Default setting
GMRP	Activate GMRP globally for the entire device. If GMRP is switched off: <ul style="list-style-type: none"> <li>▶ the device does not generate any GMRP packets,</li> <li>▶ does not evaluate any GMRP packets received, and</li> <li>▶ sends (floods) received data packets to all ports.</li> </ul> The device is transparent for received GMRP packets, regardless of the GMRP setting.	Off

*Table 19: Global setting*

### ■ Settings per Port (Table)

With this configuration table you can enter port-related settings for:

Parameter	Meaning	Value range	Default setting
Port	Module and port numbers to which this entry applies.	-	-
GMRP	Switch GMRP on/off for each port. When you disable GMRP at a port, no registrations can be made for this port, and GMRP packets cannot be forwarded at this port. Prerequisite: In the <code>Switching:Multicasts:GMRP</code> dialog, GMRP is enabled.	On, Off	On
GMRP Service Requirement	Devices that do not support GMRP can be integrated into the Multicast addressing by means of <ul style="list-style-type: none"> <li>– a static filter address entry on the connecting port.</li> <li>– selecting “Forward all groups”.</li> </ul> The device enters ports with the selection “Forward all groups” in all Multicast filter entries learned via GMRP. Prerequisite: In the <code>Switching:Multicasts:GMRP</code> dialog, GMRP is enabled.	Forward all groups, Forward all unregistered groups	Forward all unregistered groups

*Table 20: GMRP settings per port*

**Note:** If the device is incorporated into a HIPER-Ring, you can use the following settings to quickly reconfigure the network for data packets with registered Multicast destination addresses after the ring is switched:

- ▶ Activate GMRP on the ring ports and globally, and
- ▶ activate “Forward all groups” on the ring ports.

---

## 4.5 VLAN

VLAN contains dialogs and attributes for configuring and monitoring the VLAN function in accordance with the IEEE 802.1Q standard.

### 4.5.1 VLAN Global

With this dialog you can:

- ▶ display VLAN parameters
- ▶ activate/deactivate the VLAN 0 transparent mode
- ▶ configure and display the learning mode
- ▶ reset the VLAN settings of the device to the original defaults.

Parameter	Meaning
Max. VLAN ID	Displays the largest possible VLAN ID ( <a href="#">see on page 83 “VLAN Static”</a> ).
Max. supported VLANs	Displays the maximum number of VLANs the device supports ( <a href="#">see on page 83 “VLAN Static”</a> ).
Number of VLANs	Displays the number of configured VLANs ( <a href="#">see on page 83 “VLAN Static”</a> ).

*Table 21: VLAN display*

**Note:** The device provides the VLAN with the ID 1. The VLAN with ID 1 is always present.

Parameter	Meaning	Value range	Default setting
VLAN 0 Transparent Mode	When the VLAN 0 Transparent Mode is activated, the device accepts a VLAN ID of 0 in the packet when it receives it, regardless of the setting for the port VLAN ID in the dialog ( <a href="#">see on page 85 “VLAN Port”</a> ). Activate “VLAN 0 Transparent Mode” to transmit packets with a priority TAG without VLAN membership, i.e. with a VLAN ID of 0.	On, Off	Off

Table 22: VLAN settings

**Note:** If you are using the GOOSE protocol in accordance with IEC61850-8-1, you activate the “VLAN 0 transparent mode”. Thus the prioritizing information remains in the data packet in accordance with IEEE802.1D/p even when the device forwards the data packet.

This also applies to other protocols that use this prioritizing in accordance with IEEE802.1D/p but that do not require any VLANs in accordance with IEEE802.1Q.

**Note:** When using the “Transparent Mode” in this way, note the following:

- ▶ In “Transparent mode”, the devices ignore the port VLAN ID set. Set the VLAN membership of the ports of VLAN 1 to  $\cup$  (Untagged) or  $\mathbb{T}$  (Tagged), ([see on page 83 “VLAN Static”](#)).

Parameter	Meaning	Value range	Default setting
Mode	<p>VLAN mode selection.</p> <p><b>“Independent VLAN”</b> subdivides the forwarding database (see on page 64 <a href="#">“Filters for MAC addresses”</a>) virtually into one independent forwarding database per VLAN. The device cannot assign data packets with a destination address in another VLAN, and so floods it to all ports of the VLAN.</p> <p><b>Application area:</b> Setting up identical networks that use the same MAC addresses.</p> <p><b>“Shared VLAN”</b> uses the same forwarding database for all VLANs (see on page 64 <a href="#">“Filters for MAC addresses”</a>). The device cannot assign data packets with a destination address in another VLAN, and so only forwards them to the destination port if the receiving port is also a member of the VLAN group of the destination port.</p> <p><b>Application area:</b> In the case of overlapping groups, the device can distribute directly across VLANs, as long as the ports involved belong to a VLAN that can be reached.</p> <p>Changes to the mode are only taken over after a warm start (see on page 37 <a href="#">“Restart”</a>) is performed on the device, and the changes are then displayed in the line below under <b>“Status”</b>.</p>	Independent VLAN, Shared VLAN	Independent VLAN
Status	<p>Displays the current status. After a warm start (see on page 37 <a href="#">“Restart”</a>) on the device, the device take the setting for the <b>“Mode”</b> into the status line.</p>	Independent VLAN, Shared VLAN	

Table 23: Settings and displays in the *“Learning”* frame



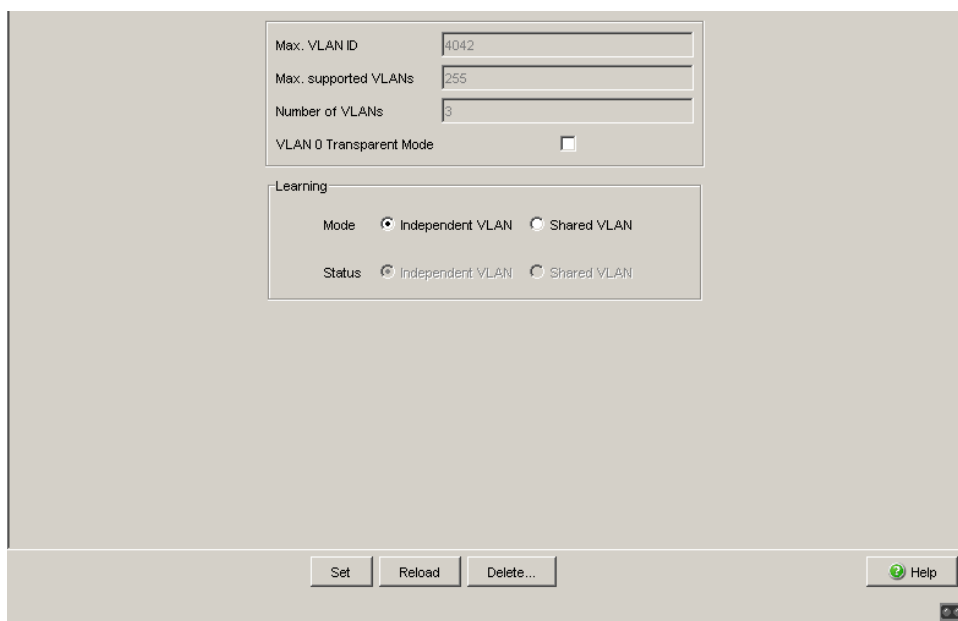


Figure 23: VLAN Global dialog

## 4.5.2 Current VLAN

With this dialog you can:

- ▶ display VLAN parameters

The Current VLAN table shows all

- manually configured VLANs
- VLANs configured via redundancy mechanisms

The Current VLAN table is only used for information purposes. You can make changes to the entries in the `VLAN:Static` dialog.

Parameter	Meaning	Value range
VLAN ID	Displays the ID of the VLAN.	
Status	Displays the VLAN status.	<p><b>other</b>: This entry solely appears for VLAN 1. The system provides VLAN 1. VLAN 1 is always present.</p> <p><b>permanent</b>: A static entry made by you. This entry is kept when the device is restarted.</p> <p><b>dynamic</b>: This VLAN was created dynamically via GVRP.</p>
Time created	Operating time (see “ <a href="#">System Data</a> ”) at which the VLAN was created.	
Ports x.x	VLAN membership of the relevant port and handling of the VLAN tag.	<p>– Currently not a member</p> <p>⊞ Member of VLAN; send data packets with tag.</p> <p>⊞ Member of the VLAN; send data packets without tag (untagged).</p> <p>⊞ Membership forbidden, so no entry possible via GVRP either.</p>

Table 24: Current VLAN

VLAN ID	Status	Creation Time	1.1	1.2	1.3	1.4	2.1	2.2	2.3	2.4	3.1	3.2
1	other	0 day(s), 0:00:06	U	U	U	U	U	U	U	U	U	U
222	permanent	0 day(s), 0:00:06	T	T	T	T	T	T	T	T	T	T
333	permanent	0 day(s), 0:00:06	-	-	-	-	-	-	-	-	-	-

Reload Help

Figure 24: Current VLAN dialog

### 4.5.3 VLAN Static

With this dialog you can:

- ▶ Create VLANs
- ▶ Assign names to VLANs
- ▶ Assign ports to VLANs and configure them
- ▶ Delete VLANs

Parameter	Meaning	Possible Values	Default Setting
VLAN ID	Displays the ID of up to 255 VLANs that are simultaneously possible.	1-4.042	
Name	Enter the name of your choice for this VLAN.	Maximum 32 characters	VLAN 1: default
Status	Displays the VLAN status.	active: Entry is activated notInService: Entry is deactivated	active
Ports x.x	Select the membership of the ports to the VLANs.	-: currently not a member. T: Member of the VLAN; send data packets with tag (tagged). U: Member of the VLAN; send data packets without tag (untagged). F: Membership forbidden.	VLAN 1: U, new VLANs: -

*Table 25: VLAN Static dialog*

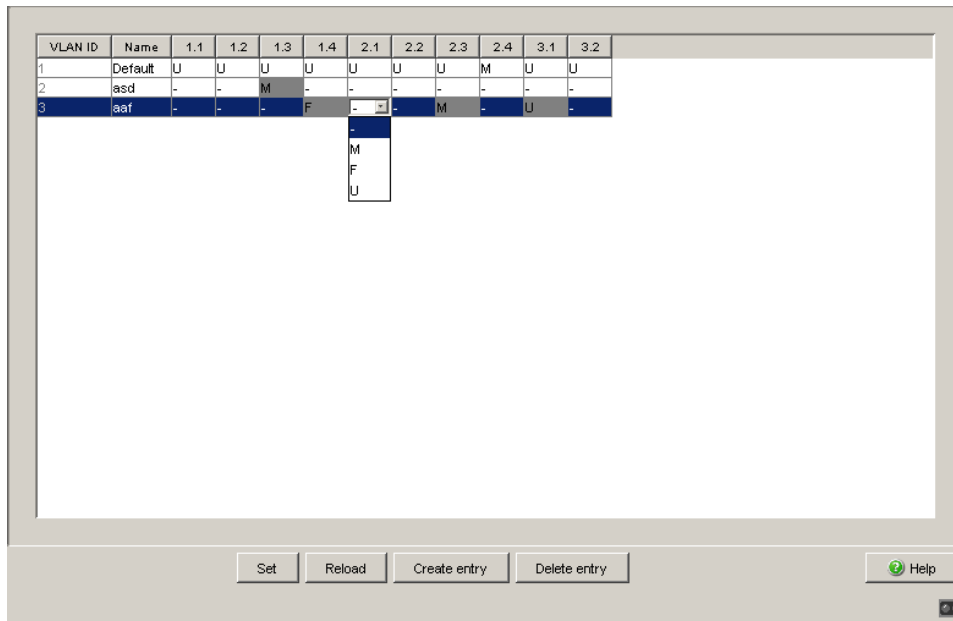


Figure 25: VLAN Static Dialog

**Note:** When configuring the VLAN, the management station must maintain access to the device after the VLAN configuration is saved. You achieve this by connecting the management station to a port with the VLAN ID 1. The device transmits the data of the management station in VLAN 1.

**Note:** The device automatically creates VLANs for MRP rings. The MRP ring function prevents the deletion of these VLANs.

Redundancy	VLAN membership
HIPER-Ring	VLAN 1 U
MRP-Ring	any
Ring/Network coupling	VLAN 1 U

*Table 26: Required VLAN settings for ports that are part of redundant Rings or Ring/Network coupling.*

#### 4.5.4 VLAN Port

With this dialog you can:

- ▶ assign ports to VLANs
- ▶ define the Acceptable Frame Type
- ▶ activate/deactivate Ingress Filtering

Parameter	Meaning	Possible Values	Default Setting
Module	Module of the device on which the port is located.		
Port	Port to which this entry applies.		
Port VLAN ID	Specifies the VLAN to which the port assigns a received untagged data packet.	All allowed VLAN IDs	1
Acceptable Frame Types	Specifies whether the port may also receive untagged data packets.	- admitAll - admitOnlyVlanTagged	admitAll
Ingress Filtering	Specifies whether the port evaluates the received tags.	on, off	off

*Table 27: VLAN Port dialog*

---

**Note:** Note the following:

- ▶ **HIPER-Ring**  
Select the port VLAN ID 1 for the ring ports and deactivate “Ingress Filtering”.
- ▶ **MRP-Ring**
  - If the MRP-Ring configuration ([see on page 108 “Configuring the MRP-Ring”](#)) is not assigned to a VLAN, select the port VLAN ID 1.
  - If the MRP-Ring configuration ([see on page 108 “Configuring the MRP-Ring”](#)) is assigned to a VLAN, the device automatically performs the VLAN configuration for this port.
- ▶ **Fast HIPER-Ring (TCSESM-E)**
  - If the Fast HIPER-Ring configuration ([see on page 111 “Configuring the Fast HIPER-Ring \(TCSESM-E\)”](#)) is not assigned to a VLAN, select the port VLAN ID 1.
  - If the Fast HIPER-Ring configuration ([see on page 111 “Configuring the Fast HIPER-Ring \(TCSESM-E\)”](#)) is assigned to a VLAN, the device automatically performs the VLAN configuration for this port.
- ▶ **Network/Ring coupling**  
Select the VLAN ID 1 for the coupling and partner coupling ports and deactivate “Ingress Filtering”.

The screenshot shows a dialog box titled "VLAN Port" with a table of configurations. The table has five columns: "Module", "Port", "Port VLAN ID", "Acceptable Frame Types", and "Ingress Filtering". Each row represents a port configuration, with "Module" set to 1, "Port" ranging from 1 to 16, "Port VLAN ID" set to 1, "Acceptable Frame Types" set to "admitAll", and "Ingress Filtering" set to an unchecked checkbox. Below the table are "Set" and "Reload" buttons, and a "Help" button with a question mark icon.

Module	Port	Port VLAN ID	Acceptable Frame Types	Ingress Filtering
1	1	1	admitAll	<input type="checkbox"/>
1	2	1	admitAll	<input type="checkbox"/>
1	3	1	admitAll	<input type="checkbox"/>
1	4	1	admitAll	<input type="checkbox"/>
1	5	1	admitAll	<input type="checkbox"/>
1	6	1	admitAll	<input type="checkbox"/>
1	7	1	admitAll	<input type="checkbox"/>
1	8	1	admitAll	<input type="checkbox"/>
1	9	1	admitAll	<input type="checkbox"/>
1	10	1	admitAll	<input type="checkbox"/>
1	11	1	admitAll	<input type="checkbox"/>
1	12	1	admitAll	<input type="checkbox"/>
1	13	1	admitAll	<input type="checkbox"/>
1	14	1	admitAll	<input type="checkbox"/>
1	15	1	admitAll	<input type="checkbox"/>
1	16	1	admitAll	<input type="checkbox"/>

Figure 26: VLAN Port dialog





## 5 QoS/Priority

The device enables you to set

- ▶ how it evaluates the QoS/prioritizing information of incoming data packets:
  - ▶ VLAN priority based on IEEE 802.1Q/ 802.1D (Layer 2)
  - ▶ Type of Service (ToS) or DiffServ (DSCP) for IP packets (Layer 3)
- ▶ which QoS/prioritizing information it writes to outgoing data packets (e.g. priority for management packets, port priority).

The QoS/Priority menu contains the dialogs, displays and tables for configuring the QoS/priority settings:

- ▶ Global
- ▶ Port configuration
- ▶ IEEE 802.1D/p mapping
- ▶ IP DSCP mapping

---

## 5.1 Global

With this dialog you can:

- ▶ enter the VLAN priority for management packets in the range 0 to 7 (default setting: 0).  
In order for you to have full access to the management of the device, even when there is a high network load, the device enables you to prioritize management packets.  
In prioritizing management packets (SNMP, Telnet, etc.), the device sends the management packets with priority information.  
Note the assignment of the VLAN priority to the traffic class ([see table 31](#)).
  - ▶ enter the IP-DSCP value for management packets in the range 0 to 63 (default setting: 0 (be/cs0)).  
In order for you to have full access to the management of the device, even when there is a high network load, the device enables you to prioritize management packets.  
In prioritizing management packets (SNMP, Telnet, etc.), the device sends the management packets with priority information.  
Note the assignment of the IP-DSCP value to the traffic class ([see table 32](#)).
- Note:** Certain DSCP values have DSCP names, such as be/cs0 to cs7 (class selector) or af11 to af43 (assured forwarding) and ef (expedited forwarding).
- ▶ display the maximum number of queues possible per port.  
The device supports 4 priority queues (traffic classes in compliance with IEEE 802.1D).
  - ▶ select the trust mode globally. You use this to specify how the device handles received data packets that contain priority information.
    - ▶ “untrusted”:  
The device ignores the priority information in the packet and always assigns the packets the port priority of the receiving port.

- ▶ “trustDot1p”:  
The device prioritizes received packets that contain VLAN tag information according to this information (assigning them to a traffic class - see [“802.1D/p mapping”](#)).  
The device prioritizes received packets that do not contain any tag information (assigning them to a traffic class - see [“Entering the port priority”](#)) according to the port priority of the receiving port .
- ▶ “trustIpDscp”:  
The device prioritizes received IP packets (assigning them to a traffic class - see [“IP DSCP mapping”](#)) according to their DSCP value.  
The device prioritizes received packets that are not IP packets (assigning them to a traffic class - see [“Entering the port priority”](#)) according to the port priority of the receiving port .  
For received IP packets:  
The device also performs VLAN priority remarking.  
In VLAN priority remarking, the device modifies the VLAN priority of the IP packets if the packets are to be sent with a VLAN tag ([see on page 83 “VLAN Static”](#)).  
Based on the traffic class to which the IP packet was assigned (see above), the device assigns the new VLAN priority to the IP packet in accordance with [table 28](#).  
Example: A received IP packet with a DSCP value of 32 (cs4) is assigned to traffic class 2 (default setting). The packet was received at a port with port priority 2. Based on [table 28](#), the VLAN priority is set to 4.

**Note:** Changing the global setting for „Trust Mode“ and clicking “Set“ will set all ports’ settings at once. You can then modify each port's settings individually.

Changing the global setting again will overwrite the individual port settings.

---

Traffic class	New VLAN priority when receiving port has an even port priority	New VLAN priority when receiving port has an odd port priority
0	0	1
1	2	3
<i>Table 28: VLAN priority remarking</i>		
2	4	5
3	6	7

---

## 5.2 Port Configuration

This dialog allows you to configure the ports. You can:

- ▶ assign a port priority to a port.

Parameter	Meaning
Module	Module of the device on which the port is located.
Port	Port to which this entry applies.
Port priority	Enter the port priority.

*Table 29: Port configuration table*

### 5.2.1 Entering the port priority

- Double-click a cell in the “Port priority” column and enter the priority (0-7). According to the priority entered, the device assigns the data packets that it receives at this port to a traffic class ([see table 30](#)).

Prerequisite:

setting in the `Global:Trust Mode dialog: untrusted` ([see on page 90 “Global”](#)) or

setting in the `Global:Trust Mode dialog:trustDot1p` ([see on page 90 “Global”](#)) and the data packets do not contain a VLAN tag or setting in `Global:Trust Mode dialog: trustIpDscp` ([see on page 90 “Global”](#)) and the data packets are not IP packets.

Port priority	Traffic class (default setting)	IEEE 802.1D traffic type
0	1	Best effort (default)
1	0	Background
2	0	Standard
3	1	Excellent effort (business critical)
4	2	Controlled load (streaming multimedia)
5	2	Video, < 100 ms of latency and jitter
6	3	Voice, < 10 ms of latency and jitter
7	3	Network control reserved traffic

Table 30: Assigning the port priority to the 4 traffic classes

## 5.2.2 Selecting the trust mode

The device provides 3 options for selecting how it handles received data packets that contain priority information. Click once on a cell in the “Trust mode” column to select one of the 3 options:

- ▶ “untrusted”:  
The device ignores the priority information in the packet and always assigns the packets the port priority of the receiving port.
- ▶ “trustDot1p”:  
The device prioritizes received packets that contain VLAN tag information according to this information (assigning them to a traffic class - see [“802.1D/p mapping”](#)).  
The device prioritizes received packets that do not contain any tag information (assigning them to a traffic class - see [“Entering the port priority”](#)) according to the port priority of the receiving port .
- ▶ “trustIpDscp”:  
The device prioritizes received IP packets (assigning them to a traffic class - see [“IP DSCP mapping”](#)) according to their DSCP value.  
The device prioritizes received packets that are not IP packets (assigning them to a traffic class - see [“Entering the port priority”](#)) according to the port priority of the receiving port .

For received IP packets:

The device also performs VLAN priority remarking.

In VLAN priority remarking, the device modifies the VLAN priority of the IP packets if the packets are to be sent with a VLAN tag ([see on page 83 “VLAN Static”](#)).

For received IP packets:

Based on the traffic class to which the IP packet was assigned (see above), the device assigns the new VLAN priority to the IP packet in accordance with [table 32](#).

Example: A received IP packet with a DSCP value of 16 (cs2) is assigned traffic class 1 (default setting). The packet is now assigned VLAN priority 2 in accordance with [table 32](#).

### 5.2.3 Displaying the untrusted traffic class

“Untrusted traffic class” shows you the traffic class that is used in the “untrusted” trust mode. When you change the port priority ([see on page 93 “Entering the port priority”](#)), the untrusted traffic class also changes ([see table 30](#)).

## 5.3 802.1D/p mapping

The 802.1D/p mapping dialog allows you to assign a traffic class to every VLAN priority.

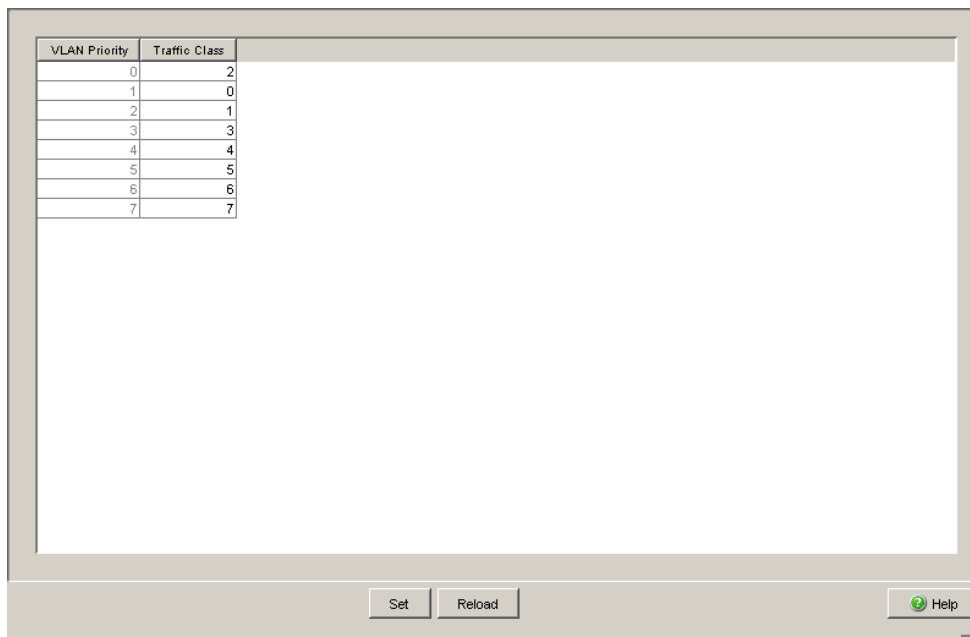


Figure 27: 802.1D/p Mapping dialog

- Enter the desired value from 0 to 3 in the Traffic Class field for every VLAN priority.



---

Port priority	Traffic class (default setting)	IEEE 802.1D traffic type
0	1	Best effort (default)
1	0	Background
2	0	Standard
3	1	Excellent effort (business critical)
4	2	Controlled load (streaming multimedia)
5	2	Video, < 100 ms of latency and jitter
6	3	Voice, < 10 ms of latency and jitter
7	3	Network control reserved traffic

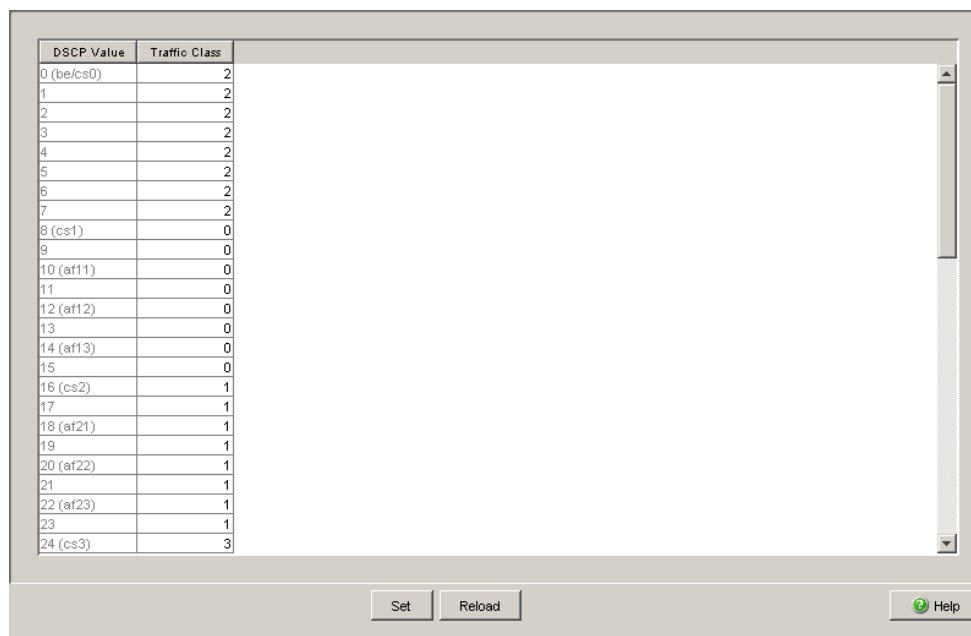
*Table 31: Assigning the VLAN priority to the 4 traffic classes*

**Note:** Network protocols and redundancy mechanisms use the highest traffic class 3. Therefore, select other traffic classes for application data.

## 5.4 IP DSCP mapping

The IP DSCP mapping table allows you to assign a traffic class to every DSCP value.

- Enter the desired value from 0 to 3 in the Traffic Class field for every DSCP value (0-63).



DSCP Value	Traffic Class
0 (be/cs0)	2
1	2
2	2
3	2
4	2
5	2
6	2
7	2
8 (cs1)	0
9	0
10 (af11)	0
11	0
12 (af12)	0
13	0
14 (af13)	0
15	0
16 (cs2)	1
17	1
18 (af21)	1
19	1
20 (af22)	1
21	1
22 (af23)	1
23	1
24 (cs3)	3

Figure 28: IP DSCP mapping table

The different DSCP values get the device to employ a different forwarding behavior, namely Per-Hop Behavior (PHB).

PHB classes:

- ▶ Class Selector (CS0-CS7): For reasons of compatibility to TOS/IP Precedence
- ▶ Expedited Forwarding (EF): Premium service. Reduced delay, jitter + packet loss (RFC 2598)

- ▶ Assured Forwarding (AF): Provides a differentiated schema for handling different data traffic (RFC 2597).
- ▶ Default Forwarding/Best Effort: No particular prioritizing.

DSCP value	DSCP name	Traffic class (default setting)
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

*Table 32: Mapping the DSCP values onto the traffic classes*



## 6 Redundancy

Under Redundancy you will find the dialogs and views for configuring and monitoring the redundancy functions:

- ▶ Ring Redundancy
- ▶ Sub-Ring
- ▶ Ring/Network coupling
- ▶ Spanning Tree

**Note:** The “Redundancy Configuration” user manual contains extensive information you need to select a suitable redundancy procedure and configure that procedure.

---

## 6.1 Ring Redundancy

The concept of the Ring Redundancy enables the construction of high-availability, ring-shaped network structures.

If a section is down, the ring structure of a

- ▶ HIPER-(**HIGH PERFORMANCE REDUNDANCY**) Ring with up to 50 devices typically transforms back to a line structure within 80 ms (possible settings: standard/accelerated).
- ▶ MRP (**Media Redundancy Protocol**) Ring (IEC 62439) of up to 50 devices typically transforms back to a line structure within 80 ms (adjustable to max. 200 ms/500 ms).
- ▶ Fast HIPER-Ring of up to 5 devices typically transforms back to a line structure within 5 ms (maximum 10 ms). With a larger number of devices, the reconfiguration time increases.

With the help of the **Ring Manager** (RM) function of a device, you can connect both ends of a backbone in a line structure to form a redundant ring.

- ▶ Within a HIPER-Ring, you can use any combination of the following devices:
  - TCSESM
  - TCSESM-E
- ▶ Within an MRP-Ring, you can use devices that support the MRP protocol based on IEC62439:
  - TCSESM
  - TCSESM-E
- ▶ Within a Fast HIPER-Ring, you can use the following device:
  - TCSESM-E

Depending on the device model, the Ring Redundancy dialog allows you to:

- ▶ Select one of the available Ring Redundancy versions, or change it.
- ▶ Display an overview of the current Ring Redundancy configuration.
- ▶ Create new Ring Redundancies.
- ▶ Configure existing Ring Redundancies.
- ▶ Enable/disable the Ring Manager function.
- ▶ Receive Ring information.
- ▶ Delete the Ring Redundancy.

---

**Note:** Enabled Ring Redundancy methods on a device are mutually exclusive at any one time. When changing to another Ring Redundancy method, deactivate the function for the time being.

Parameter	Meaning
Version	Select the Ring Redundancy version you want to use: HIPER-Ring MRP FAST HIPER-Ring (TCSESM-E) Default setting is HIPER-Ring
Ring port No.	In a ring, every device has 2 neighbors. Define 2 ports as ring ports to which the neighboring devices are connected.
Module	Module identifier of the ports used as ring ports
Port	Port identifier of the ports used as ring ports
Operation	Value depends on the Ring Redundancy version used. Described in the following sections for the corresponding Ring Redundancy version.

*Table 33: Ring Redundancy basic configuration*

### 6.1.1 Configuring the HIPER-Ring

For the ring ports, select the following basic settings in the `Basic Settings:Port Configuration` dialog:

Port Type	Bit Rate	Autonegotiation (Automatic Configuration)	Port Setting	Duplex Mode
Optical	all	off	on	full
TX	100 Mbit/s	off	on	full
TX	1000 Mbit/s	on	on	-

*Table 34: Port Settings for Ring Ports*



## WARNING

### RING LOOP HAZARD

To avoid loops during the configuration phase, configure all the devices of the HIPER-Ring individually. Before you connect the redundant line, you must complete the configuration of all the devices of the HIPER-Ring.

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

**Note:** As an alternative to using software to configure the HIPER-Ring, with device TCSESM you can also use DIP switches to enter a number of settings on the devices. You can also use a DIP switch to enter a setting for whether the configuration via DIP switch or the configuration via software has priority. The state on delivery is “Software Configuration”. You will find details on the DIP switches in the “Installation” user manual.



Parameter	Meaning
Ring port X.X operation	Display in "Operation" field: <i>active</i> : This port is switched on and has a link. <i>inactive</i> : This port is switched off or it has no link.
Redundancy Manager Mode (Ring Manager)	If there is exactly one device, you switch the Ring Manager function on at the ends of the line.
Ring Recovery	The settings in the "Ring Recovery" frame are only effective for devices that are ring managers. In the ring manager, select the desired value for the test packet timeout for which the ring manager waits after sending a test packet before it evaluates the test packet as lost. <ul style="list-style-type: none"> <li>▶ Standard: test packet timeout 480 ms</li> <li>▶ Accelerated: test packet timeout 280 ms</li> </ul> <p><b>Note:</b> The settings are especially meaningful if at least one line in the ring consists of a 1,000 MBit/s twisted pair line. The reconfiguration time after connection interruption existing due to the reaction characteristic of 1,000 MBit/s twisted pair ports can thus be accelerated considerably.</p>
Information	If the device is a ring manager: The displays in this frame mean: "Redundancy working": When a component of the ring is down, the redundant line takes over its function. "Configuration failure": You have configured the function incorrectly, or there is no ring port connection.

*Table 35: HIPER-Ring configuration*

The screenshot displays a configuration window for Hiper-Ring. At the top, the 'Version' section has three radio buttons: 'Hiper-Ring', 'MRP', and 'Fast Hiper-Ring', with 'Fast Hiper-Ring' selected. Below this are two columns for 'Ring Port 1' and 'Ring Port 2', each containing fields for 'Module', 'Port', and 'Operation'. The 'Redundancy Manager' section has a 'Mode' with 'On' and 'Off' radio buttons, where 'Off' is selected. The 'Operation' section also has 'On' and 'Off' radio buttons, with 'Off' selected. The 'Ring Information' section includes a 'Round Trip Delay' field. The 'VLAN' section has a 'VLAN ID' field. The 'Switches' section has a 'Number' field. At the bottom, there is an 'Information' field and a row of buttons: 'Set', 'Reload', 'Delete ring configuration', and 'Help'.

*Figure 29: Selecting Hiper-Ring version, entering ring ports, enabling/disabling ring manager and selecting ring recovery (TCSESM-E)*

**Note:** Deactivate the Spanning Tree protocol (STP) for the ports connected to the redundant ring, because the Spanning Tree and the Ring Redundancy work with different reaction times (Redundancy:Spanning Tree:Port).

**Note:** If you have configured VLANs, note the VLAN configuration of the ring ports.

In the configuration of the Hiper-Ring, you select for the ring ports

- VLAN ID 1 and
- VLAN membership Untagged in the static VLAN table.

**Note:** When activating the HIPER-Ring function via software or DIP switches, the device sets the corresponding settings for the pre-defined ring ports in the configuration table (transmission rate and mode). If you switch off the HIPER-Ring function, the ports, which are changed back into normal ports, keep the ring port settings. Independently of the DIP switch setting, you can still change the port settings via the software.

## 6.1.2 Configuring the MRP-Ring

To configure an MRP-Ring, you set up the network to meet your demands. For the ring ports, select the following basic settings in the `Basic Settings:Port Configuration` dialog:

Port Type	Bit Rate	Autonegotiation (Automatic Configuration)	Port Setting	Duplex Mode
Optical	all	off	on	full
TX	100 Mbit/s	off	on	full
TX	1000 Mbit/s	on	on	-

*Table 36: Port Settings for Ring Ports*



### WARNING

#### **RING LOOP HAZARD**

To avoid loops during the configuration phase, configure all the devices of the MRP-Ring individually. Before you connect the redundant line, you must complete the configuration of all the devices of the MRP-Ring.

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

Parameter	Meaning
Ring port X.X operation	Display in “Operation” field: <i>forwarding</i> : This port is switched on and has a link. <i>blocked</i> : This port is blocked and has a link. <i>disabled</i> : This port is switched off. <i>not connected</i> : This port has no link.
Configuration Redundancy Manager (Ring Manager)	Deactivate the advanced mode if a device in the ring does not support the advanced mode for fast switching times. Otherwise you activate the advanced mode.  <b>Note:</b> All TCSESM (from vers. 4.1), TCSESM-E and TCSESB devices that support the MRP-Ring also support the advanced mode.
Redundancy Manager Mode (Ring Manager)	If there is exactly one device, you switch the Ring Manager function on at the ends of the line.
Operation	When you have configured all the parameters for the MRP-Ring, you switch the operation on with this setting. When you have configured all the devices in the MRP-Ring, you close the redundant line.
Ring Recovery	For the device for which you have activated the ring manager, select the value 200 ms if the stability of the ring meets the requirements for your network. Otherwise select 500 ms. <b>Note:</b> Settings in the “Ring Recovery” frame are only effective for devices that are ring managers.
VLAN ID	If you have configured VLANs, you select <code>VLAN ID 0</code> here if you do not want to assign the MRP-Ring configuration to a VLAN. Note the VLAN configuration of the ring ports: Select for VLAN ID 1 and VLAN membership <code>U</code> in the static VLAN table for the ring ports. <code>VLAN ID &gt; 0</code> if you want to assign the MRP-Ring configuration to this VLAN. Select this VLAN ID in the MRP-Ring configuration for all devices in this MRP-Ring. Note the VLAN configuration of the ring ports: For all ring ports in this MRP-Ring, select this corresponding VLAN ID and the VLAN membership <code>T</code> in the static VLAN table.
Information	If the device is a ring manager: The displays in this frame mean: “Redundancy working”: When a component of the ring is down, the redundant line takes over its function. “Configuration failure”: You have configured the function incorrectly, or there is no ring port connection.

*Table 37: MRP-Ring configuration*

The screenshot shows a configuration window for Ring Redundancy. At the top, the 'Version' section has three radio buttons: 'HIPER-Ring', 'MRP' (which is selected), and 'Fast HIPER-Ring'. Below this are two columns for 'Ring Port 1' and 'Ring Port 2'. 'Ring Port 1' has 'Module' set to 1, 'Port' set to 1, and 'Operation' is empty. 'Ring Port 2' has 'Module' set to 1, 'Port' set to 2, and 'Operation' is empty. The 'Configuration Redundancy Manager' section has a checked checkbox for 'Advanced Mode'. The 'Redundancy Manager' section has a 'Mode' with 'On' selected and 'Off' unselected. The 'Operation' section has 'On' selected and 'Off' unselected. The 'Ring Recovery' section has '500ms' selected and '200ms' unselected. The 'VLAN' section has 'VLAN ID' set to 1. An 'Information' section is empty. At the bottom, there are buttons for 'Set', 'Reload', 'Delete ring configuration', and 'Help'.

Figure 30: Selecting MRP-Ring version, entering ring ports and enabling/disabling ring manager (TCSESM-E)

### 6.1.3 Configuring the Fast HIPER-Ring (TCSESM-E)

Within a Fast HIPER-Ring, you can use any combination of the following devices:

► TCSESM-E

To configure a Fast HIPER-Ring, you set up the network to meet your demands for the ring ports, select the following basic settings in the `Basic Settings:Port Configuration` dialog:

<b>Bit rate</b>	<b>100 Mbit/s</b>
Autonegotiation (automatic configuration)	off
Port	on
Duplex	Full

*Table 38: Port settings for ring ports*



## WARNING

### **RING LOOP HAZARD**

To avoid loops during the configuration phase, configure all the devices of the Fast HIPER-Ring individually. Before you connect the redundant line, you must complete the configuration of all the devices of the Fast HIPER-Ring.

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

Parameter	Meaning
Ring port X.X operation	Display in "Operation" field: <i>forwarding</i> : This port is switched on and has a link. <i>blocked</i> : This port is blocked and has a link. <i>disabled</i> : This port is switched off. <i>not connected</i> : This port has no link.
Redundancy Manager Mode (Ring Manager)	If there is exactly one device, you switch the Ring Manager function on at the ends of the line.
Operation	When you have configured all the parameters for the Fast HIPER-Ring, you switch the operation on here. When you have configured all the devices in the Fast HIPER-Ring, you close redundant lines.
Ring Information Round Trip Delay	<i>Round Trip Delay</i> : round-trip delay in $\mu\text{s}$ for test packets, measured by ring manager. The display begins with 100 $\mu\text{s}$ , in steps of 100 $\mu\text{s}$ . Values of 1000 $\mu\text{s}$ and greater indicate that the ring may become unstable. In this case, check that the number of devices in the "Switches" frame is correct (see below).
VLAN ID	If you have configured VLANs, you select <i>VLAN ID 0</i> here if you do not want to assign the Fast HIPER-Ring configuration to a VLAN. Note the VLAN configuration of the ring ports: Select for VLAN ID 1 and VLAN membership $\cup$ in the static VLAN table for the ring ports. <i>VLAN ID &gt; 0</i> if you want to assign the Fast HIPER-Ring configuration to this VLAN. Select the same VLAN ID in the Fast HIPER-Ring configuration for all devices in this ring. Note the VLAN configuration of the ring ports: For all ring ports in this Fast HIPER-Ring, select this corresponding VLAN ID and the VLAN membership $\tau$ in the static VLAN table.
Switches / Number	Enter the number of devices integrated in this Fast HIPER-Ring. This entry is used to optimize the reconfiguration time and the stability of the ring.
Information	If the device is a ring manager: The displays in this frame mean: "Redundancy working": When a component of the ring is down, the redundant line takes over its function. "Configuration failure": You have configured the function incorrectly, or there is no ring port connection.

Table 39: Fast HIPER-Ring configuration



The screenshot shows a configuration window for Fast HIPER-Ring. At the top, under 'Version', the 'Fast HIPER-Ring' radio button is selected. Below this, there are two columns for 'Ring Port 1' and 'Ring Port 2'. For Ring Port 1, the 'Module' is 1 and the 'Port' is 1. For Ring Port 2, the 'Module' is 1 and the 'Port' is 2. The 'Redundancy Manager' section has the 'Mode' set to 'On'. There are two 'Operation' sections, both with 'On' selected. The 'Ring Information' section has a 'Round Trip Delay' field. The 'VLAN' section has a 'VLAN ID' of 1. The 'Switches' section has a 'Number' of 3. At the bottom, there are buttons for 'Set', 'Reload', 'Delete ring configuration', and 'Help'.

Figure 31: Selecting and configuring Fast HIPER-Ring

**Note:** Deactivate the Spanning Tree protocol (STP) for the ports connected to the redundant ring, because the Spanning Tree and the Ring Redundancy work with different reaction times (Redundancy:Spanning Tree:Port).

---

## 6.2 Sub-Ring (TCSESM-E)

With this dialog you can:

- ▶ display an overview of all the connected Sub-Rings,
- ▶ create Sub-Rings,
- ▶ configure Sub-Rings, and
- ▶ Delete Sub-Rings.

**Note:** The following devices support the Sub-Ring Manager function:

- TCSESM-E

In a Sub-Ring, you can integrate as participants the devices that support MRP - the Sub-Ring Manager function is not required.



### WARNING

#### **RING LOOP HAZARD**

To avoid loops during the configuration phase, configure all the devices of the Sub-Ring individually. Before you connect the redundant line (close the Sub-Ring), you must complete the configuration of all the devices of the Sub-Ring.

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

**Note:** Sub-Rings use MRP. You can couple Sub-Rings to existing primary rings with the HIPER-Ring protocol, the Fast HIPER-Ring protocol and MRP. If you couple a Sub-Ring to a primary ring under MRP, configure both rings in different VLANs. You configure

- ▶ either the Sub-Ring Managers' Sub-Ring ports and the devices of the Sub-Ring in a separate VLAN. Here multiple Sub-Rings can use the same VLAN.

- ▶ or the devices of the primary ring including the Sub-Ring Managers' primary ring ports in a separate VLAN. This reduces the configuration effort when coupling multiple Sub-Rings to a primary ring.

**Note:** In the Sub-Ring, you configure the devices with the Sub-Ring Manager functions switched off as participants of an MRP-Ring (see on page 108 “Configuring the MRP-Ring”).

This means:

- ▶ Define different VLAN membership for the primary ring and the Sub-Ring even if the primary ring uses the MRP protocol; e.g., VLAN ID 1 for the primary ring and VLAN ID 2 for the Sub-Ring.
- ▶ Switch the MRP-Ring function on for all devices.
- ▶ Switch the Ring Manager function off for all devices.
- ▶ Switch RSTP off for the MRP-Ring ports used in the Sub-Ring.
- ▶ Assign the same MRP domain ID to all devices. If you are only using Schneider Electric SA devices, you do not have to change the default value for the MRP domain ID.

**Note:** Use the Command Line Interface (CLI) to assign devices without the Sub-Ring Manager function a different MRP domain name. For further information, see the Command Line Interface reference manual.

### 6.2.1 Sub-Ring configuration

Parameter	Meaning	Possible Values	Default Setting
Max. Table Entries	Number of Sub-Rings that can be managed by a Sub-Ring Manager at the same time.	4	4
Sub Ring ID	Unique name for this Sub-Ring.		

*Table 40: Sub-Ring basic configuration*

Parameter	Meaning	Possible Values	Default Setting
Function on/off	Activate the Sub-Ring only when the configuration has been completed, then close the Sub-Ring.	on off	off
Configuration State	A symbol displays the current state of the Sub-Ring.		
Redundancy exists	A symbol displays whether the redundancy exists.		
Module.Port	ID of the port that connects the device to the Sub-Ring.	All available ports that do not already belong to the ring redundancy of the base ring, in the form X.X. (module.port)	
Name	Optional name for the Sub-Ring		
SRM Mode	Target state: Define whether this SRM is to manage the redundant connection ( <code>Redundant Manager mode</code> ) or not. If you have set the same value for the SRM Mode for both SRMs, the SRM with the higher MAC address assumes the function of redundant manager. <code>SingleManager</code> describes the special state when you connect a Sub-Ring via 2 ports of a single device. In this case, the port with the higher port number manages the redundant connection.	Manager RedundantManager SingleManager	Manager
SRM State	Actual state: Shows whether this SRM manages the redundant connection ( <code>Redundant Manager mode</code> ) or not. If you have set the same value for the SRM Mode for both SRMs, the SRM with the higher MAC address assumes the function of redundant manager. <code>SingleManager</code> describes the special state when you connect a Sub-Ring via 2 ports of a single device. In this case, the port with the higher port number manages the redundant connection.	Manager RedundantManager SingleManager	Manager
Port Status	Connection status of the Sub-Ring port	forwarding disabled blocked not connected	

Table 40: Sub-Ring basic configuration

Parameter	Meaning	Possible Values	Default Setting
VLAN	VLAN to which this Sub-Ring is assigned. If no VLAN exists under the VLAN ID entered, the device automatically creates it. If you do not want to use a separate VLAN for this Sub-Ring, you leave the entry as "0".	Corresponds to the entries in the VLAN dialog	0
Partner MAC	Shows the MAC address of the Sub-Ring Manager at the other end of the Sub-Ring.	Valid MAC address	00 00 00 00 00 00
MRP Domain	Assign the same MRP domain name to all the members of a Sub-Ring. If you are only using Schneider Electric devices, you can use the default value for the MRP domain; otherwise adjust it if necessary. With multiple Sub-Rings, all the Sub-Rings can use the same MRP domain name.	All permitted MRP domain names	255.255.255. 255.255.255. 255.255.255. 255.255.255. 255.255.255. 255
Protocol		standardMRP	standardMRP

Table 40: Sub-Ring basic configuration

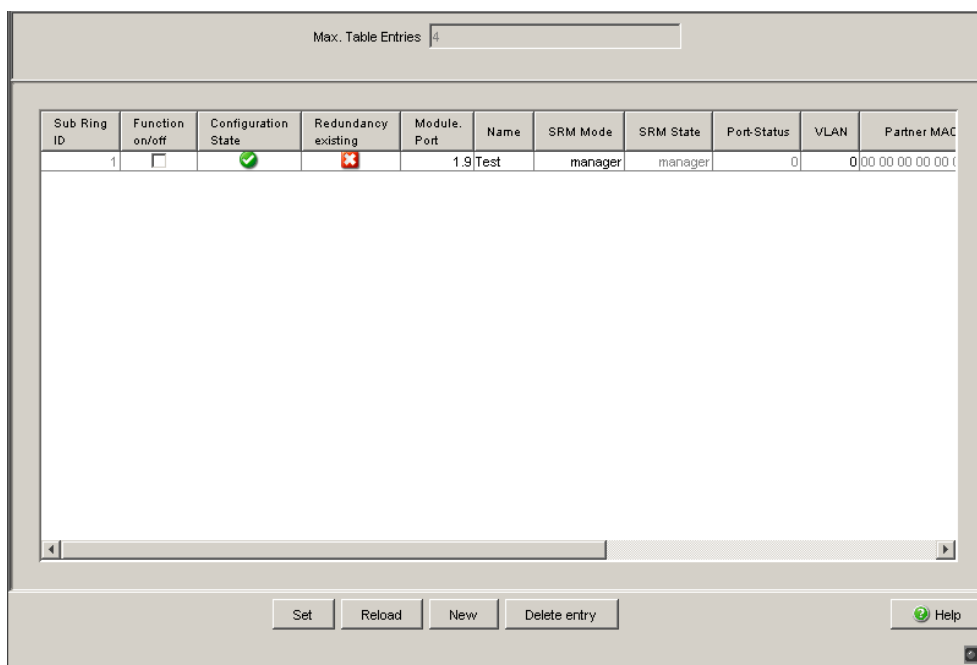


Figure 32: Sub-Ring basic configuration

## 6.2.2 Sub-Ring - New Entry

Parameter	Meaning	Possible Values	Default Setting
Sub Ring ID	Unique name for this Sub-Ring.		
Module.Port	ID of the port that connects the device to the Sub-Ring.	All available ports that do not already belong to the ring redundancy of the base ring, in the form X.X. (module.port)	
Name	Optional name for the Sub-Ring		
SRM Mode	Target state: Define whether this SRM is to manage the redundant connection ( <code>RedundantManager</code> mode) or not. If you have set the same value for the SRM Mode for both SRMs, the SRM with the higher MAC address assumes the function of redundant manager. <code>SingleManager</code> describes the special state when you connect a Sub-Ring via 2 ports of a single device. In this case, the port with the higher port number manages the redundant connection.	Manager RedundantManager SingleManager	Manager
VLAN	VLAN to which this Sub-Ring is assigned. If no VLAN exists under the VLAN ID entered, the device automatically creates it. If you do not want to use a separate VLAN for this Sub-Ring, you leave the entry as "0".	Corresponds to the entries in the VLAN dialog	0
MRP Domain	Assign the same MRP domain name to all the members of a Sub-Ring. If you are only using Schneider Electric devices, you can use the default value for the MRP domain; otherwise adjust it if necessary. With multiple Sub-Rings, all the Sub-Rings can use the same MRP domain name.	All permitted MRP domain names	255.255.255. 255.255.255. 255.255.255. 255.255.255. 255

Table 41: Sub-Ring - New Entry

**Note:** For one Sub-Ring in the `singleManager` mode, create 2 entries with different Sub-Ring IDs.

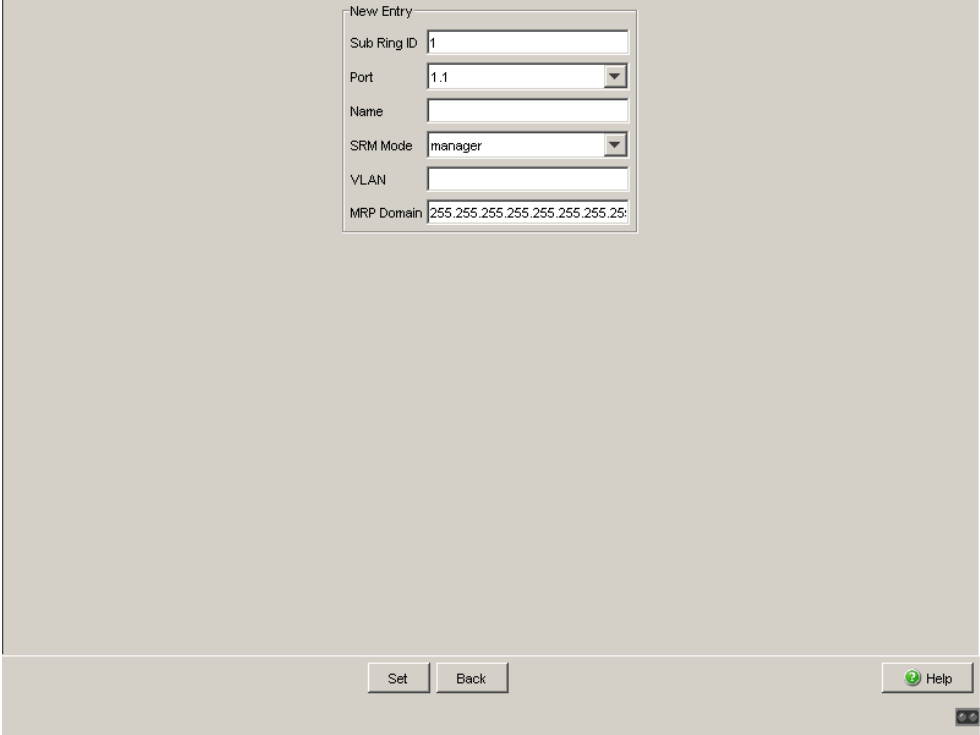


Figure 33: Sub-Ring - New Entry dialog

---

## 6.3 Ring/Network Coupling

With this dialog you can:

- ▶ display an overview of the existing Ring/Network coupling,
- ▶ configure a Ring/Network coupling,
- ▶ switch a Ring/Network coupling on/off,
- ▶ create a new Ring/Network coupling, and
- ▶ Delete Ring/Network couplings

### 6.3.1 Preparing a Ring/Network Coupling



#### WARNING

##### **RING-/NETWORK COUPLING LOOP HAZARD**

To avoid loops during the configuration phase, configure all the devices that participate actively in the Ring-/Network Coupling individually. Before you connect the redundant line, you must complete the configuration of all the devices that participate actively in the Ring-/Network Coupling.

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

#### ■ STAND-BY switch

All devices have a STAND-BY switch, with which you can define the role of the device within a Ring/Network coupling.



Depending on the device type, this switch is a DIP switch on the devices, or else it is exclusively a software setting (`Redundancy:Ring/Network Coupling` dialog). By setting this switch, you define whether the device has the main coupling or the redundant coupling role within a Ring/Network coupling. You will find details on the DIP switches in the “Installation” user manual.

**Note:** Depending on the model, the devices have a DIP switch, with which you can choose between the software configuration and the DIP switch configuration. When you set the DIP switches so that the software configuration is selected, the DIP switches are effectively deactivated.

Device type	STAND-BY switch type
TCSESM	Selectable: DIP switch and software setting
TCSESM-E	Software switch

*Table 42: Overview of the STAND-BY switch types*

Depending on the device and model, set the STAND-BY switch in accordance with the following table:

Device with	Choice of main coupling or redundant coupling
DIP switch	On “STAND-BY” DIP switch
DIP switch/software switch option	According to the option selected - on “STAND-BY” DIP switch or in the - <code>Redundancy:Ring/Network Coupling</code> dialog, by making selection in “Select configuration”. <b>Note:</b> These devices have a DIP switch, with which you can choose between the software configuration and the DIP switch configuration. You can find details on the DIP switches in the User Manual Installation.
Software switch	In the <code>Redundancy:Ring/Network Coupling</code> dialog

*Table 43: Setting the STAND-BY switch*

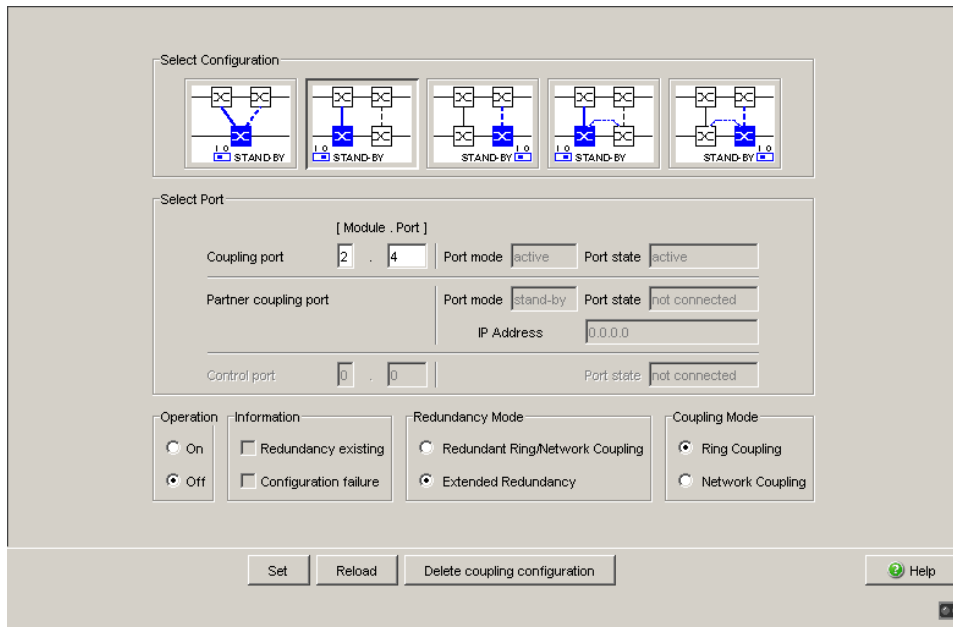


Figure 34: Software configuration of the STAND-BY switch (TCSESM-E)

Depending on the STAND-BY DIP switch position, the dialog displays those configurations that are not possible as grayed-out. If you want to select one of these grayed-out configurations, change the STAND-BY DIP switch on the device to the other position.

#### One-Switch coupling

On the device set the 'STAND BY' dip switch to the ON position or use the software configuration to assign the redundancy function to it.

#### Two-Switch coupling

Assign the device in the redundant line the DIP switch setting “STAND-BY”, or use the software configuration to assign the redundancy function to it.

**Note:** For reasons of redundancy reliability, do not use Rapid Spanning Tree and Ring/Network Coupling in combination.

## ■ Ring/Network Coupling dialog

Parameter	Meaning
Selecting the configuration	<p>Depending on your local conditions, select “One-Switch coupling”, “Two-Switch coupling, Slave”, “Two-Switch coupling, Master”, “Two-Switch coupling with control line, Slave” or “Two-Switch coupling with control line, Master”. These options are presented as buttons from left to right.</p> <p>Depending on the device type (see table 42), you make this setting:</p> <ul style="list-style-type: none"> <li>– only using software</li> <li>– using DIP switch and software</li> </ul> <p>You will find details on the DIP switches on the devices in the “Installation” user manual.</p> <ul style="list-style-type: none"> <li>– For devices without DIP switches, you only use the software to make settings. You can select the configuration using the buttons.</li> <li>– For devices that can be configured using DIP switches and software, you can activate or deactivate the DIP switches. If you have activated the DIP switches, you cannot overwrite the DIP switch settings using the software - settings that cannot be selected using the software are grayed-out in the dialog.</li> </ul> <p>To configure using the software, select the relevant Ring/Network coupling constellation by pressing the corresponding button.</p>
Coupling port	<p>This is the port to which you have connected a redundant connection.</p> <p><b>Note:</b> Configure the coupling port and the ring ports, if there are any ring ports, on different ports.</p> <p><b>Note:</b> To avoid continuous loops, the device sets the port status of the coupling port to “off” if you switch off the function or change the configuration while the connections are operating at these ports.</p>
Port mode	<ul style="list-style-type: none"> <li>- active You have switched the port on.</li> <li>- stand-by The port is in stand-by mode.</li> </ul>
Port state	<ul style="list-style-type: none"> <li>- active: You have switched the port on.</li> <li>- stand-by: The port is in stand-by mode.</li> <li>- not connected: You have not connected the port.</li> </ul>
Partner coupling port	<p>This is the port at which the partner has made its connection. It is only possible and necessary to enter a port if “One-Switch coupling” is being set up.</p> <p><b>Note:</b> Configure the partner coupling port and the ring ports, if there are any ring ports, on different ports.</p>
IP address	<p>If you have selected “Two-Switch coupling”, the device displays the IP address of the partner here, once you have already started operating the partner in the network.</p>
Control port	<p>This is the port to which you connect the control line.</p>
Operation	<p>Here you switch the Ring/Network coupling for this device on or off</p>

Table 44: Ring/Network Coupling dialog

Parameter	Meaning
Information	If the device is a ring manager: The displays in this frame mean: “Redundancy working”: When a component of the ring is down, the redundant line takes over its function. “Configuration failure”: You have configured the function incorrectly, or there is no ring port connection.
Redundancy Mode	With the “Redundant Ring/Network Coupling” setting, either the main line or the redundant line is active. Both lines are never active simultaneously. With the “Extended Redundancy” setting, the main line and the redundant line are simultaneously active if a problem is detected in the connection line between the devices in the connected (i.e., the remote) network. During the reconfiguration period, package duplications may possibly occur. Therefore, only select this setting if your application detects package duplications.
Coupling Mode	Here you define whether the constellation you are configuring is a coupling of redundancy rings (HIPER-Ring, MRP-Ring or Fast HIPER-Ring), or network segments.

*Table 44: Ring/Network Coupling dialog*

The following tables show the selection options and default settings for the ports used in the Ring/Network coupling.

Device	Partner coupling port	Coupling port
TCSESM	All ports (default setting: port 1.3)	All ports (default setting: port 1.4)
TCSESM-E	All ports (default setting: port 1.3)	All ports (default setting: port 1.4)

*Table 45: Port assignment for one-Switch coupling*

Device	Coupling port
TCSESM	Adjustable for all ports (default setting: port 1.4)
TCSESM-E	Adjustable for all ports (default setting: port 1.4)

*Table 46: Port assignment for the redundant coupling (two-Switch coupling)*

Device	Coupling port	Control port
TCSESM	Adjustable for all ports (default setting: port 1.4)	Adjustable for all ports (default setting: port 1.3)
TCSESM-E	Adjustable for all ports (default setting: port 1.4)	Adjustable for all ports (default setting: port 1.3)

*Table 47: Port assignment for the redundant coupling (two-Switch coupling with control line)*

**Note:** For the coupling ports, select the following settings in the `Basic Settings:Port Configuration` dialog:

- Port: on
- Automatic configuration (autonegotiation):  
on for twisted-pair connections
- Manual configuration: 100 Mbit/s FDX or 1 Gbit/s FDX for glass fiber connections, depending on the port's capabilities

**Note:** If you have configured VLANs, note the VLAN configuration of the coupling and partner coupling ports.

In the Ring/Network Coupling configuration, select for the coupling and partner coupling ports

- VLAN ID 1 and “Ingress Filtering” disabled in the port table and
- VLAN membership U in the static VLAN table.

**Note:** If you are operating the Ring Manager and two-Switch coupling functions at the same time, there is the possibility of creating a loop.

## 6.4 Spanning Tree

Under Spanning Tree you will find the dialogs and views for configuring and monitoring the Spanning Tree function in accordance with the IEEE 802.1w (Rapid Spanning Tree, RSTP) standard, and also the Dual RSTP function.

**Note:** The Spanning Tree Protocol is a protocol for MAC bridges. For this reason, the following description uses the term bridge for Switch.

### Introduction

Local networks are getting bigger and bigger. This applies to both the geographical expansion and the number of network participants. Therefore, it is advantageous to use multiple bridges, for example:

- ▶ to reduce the network load in sub-areas,
- ▶ to set up redundant connections and
- ▶ to overcome distance limitations.

However, using multiple bridges with multiple redundant connections between the subnetworks can lead to loops and thus loss of communication across of the network. In order to help avoid this, you can use Spanning Tree. Spanning Tree enables loop-free switching through the systematic deactivation of redundant connections. Redundancy enables the systematic reactivation of individual connections as needed.

### Rapid Spanning Tree Protocol (RSTP)

RSTP is a further development of the Spanning Tree Protocol (STP) and is compatible with it. If a connection or a bridge becomes inoperable, the STP required a maximum of 30 seconds to reconfigure. This is no longer acceptable in time-sensitive applications. RSTP achieves average reconfiguration times of less than a second. When you use RSTP in a ring topology with 10 to 20 devices, you can even achieve reconfiguration times in the order of milliseconds.

**Note:** RSTP reduces a layer 2 network topology with redundant paths into a tree structure (Spanning Tree) that does not contain any more redundant paths. One of the Switches takes over the role of the root bridge here. The maximum number of devices permitted in an active branch (from the root bridge to the tip of the branch) is specified by the variable `Max Age` for the current root bridge. The preset value for `Max Age` is 20, which can be increased up to 40.

If the device working as the root is inoperable and another device takes over its function, the `Max Age` setting of the new root bridge determines the maximum number of devices allowed in a branch.

**Note:** You have the option of coupling RSTP network segments to an MRP-Ring. For this, you activate the MRP compatibility. This enables you to operate RSTP via an MRP-Ring.

If the root bridge is within the MRP-Ring, the devices in the MRP-Ring count as a single device when calculating the length of the branch. A device that is connected to a random Ring bridge receives such RSTP information as if it were directly connected to the root bridge.

**Note:** The RSTP standard dictates that all the devices within a network work with the (Rapid) Spanning Tree Algorithm. If STP and RSTP are used at the same time, the advantages of faster reconfiguration with RSTP are lost in the network segments that are operated in combination.

A device that only supports RSTP works together with MSTP devices by not assigning an MST region to itself, but rather the CST (Common Spanning Tree).

**Note:** By changing the IEEE 802.1D-2004 standard for RSTP, the Standards Commission reduced the maximum value for the “Hello Time” from 10 s to 2 s. When you update the Switch software from a release before 5.0 to release 5.0 or higher, the new software release automatically reduces the locally entered “Hello Time” values that are greater than 2 s to 2 s.

If the device is not the RSTP root, “Hello Time” values greater than 2 s can remain valid, depending on the software release of the root device.

**Dual Rapid Spanning Tree Protocol, Dual RSTP/DRSTP (TCSESM-E)**

Dual RSTP is an extension of the Rapid Spanning Tree Protocol, used to achieve fast switching times for a defined subnetwork, even in a worst case scenario in a network with a large diameter. One application case, for example, is a small ring that is connected to a ring with many bridges.

Dual RSTP allows you to:

- ▶ define 2 RSTP instances in such a network,
- ▶ configure each RSTP instance with individual parameters, and
- ▶ couple these RSTP instances redundantly.

These instances are called primary and secondary instances. Each instance prevents loops and provides redundancy if a network component becomes inoperable. The instances work independently of each other. You can configure the instances with different values for the bridge priority, forward delay and max age.

2 bridges perform the task of coupling the two instances. What is known as the Dual RSTP Master transmits between the two instances in the normal state, and the Dual RSTP Slave performs this task if the master or the connection lines becomes inoperable. Each of these bridges knows the ports that are responsible for the primary and secondary instances.

The two bridges are coupled with each other for each instance via what are known as the “inner ports”. The complimentary ports that close the ring for an instance are called “outer ports”.

**Note:** Directly couple the inner ports of both bridges with each other. Otherwise, connections interruptions may occur that exceed the maximum time specified for Dual RSTP.

**Note:** The following text uses the term Spanning Tree (STP) to describe settings or behavior that applies to STP, RSTP or Dual RSTP (for the device TCSESM-E).



### 6.4.1 Global

With this dialog you can:

- ▶ switch the Rapid Spanning Tree Protocol on/off,
- ▶ display bridge-related information on the Spanning Tree Protocol,
- ▶ configure bridge-related parameters of the Spanning Tree Protocol,
- ▶ set bridge-related additional functions,
- ▶ display the parameters of the root bridge and
- ▶ display bridge-related topology information.

**Note:** Rapid Spanning Tree is activated on the device by default, and it automatically begins to resolve the existing topology into a tree structure. If you have deactivated RSTP on individual devices, you avoid loops during the configuration phase.



## WARNING

### **RSTP LOOP HAZARD**

To avoid loops during the configuration phase, configure all the devices of the RSTP configuration individually. Before you connect the redundant lines, you must complete the configuration of all devices in the RSTP configuration.

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

The following tables show the selection options and default settings, and information on the global Spanning Tree settings for the bridge.

Parameter	Meaning	Possible Values	Default Setting
<b>Frame „Function“</b>	Switches the Spanning Tree function for this device “On” or “Off”. If you switch off the Spanning Tree for a device globally, the device floods the Spanning Tree packets received like normal Multicast packets to the ports. Thus the device behaves transparently with regard to Spanning Tree packets.	On, Off	On
<b>Frame „Protocol Version“</b>	The protocol version is always RSTP (IEEE 802.1w) in a shared instance.	RSTP (IEEE 802.1w)	RSTP (IEEE 802.1w)

Table 48: Global Spanning Tree settings, basic function

In the “Protocol Configuration / Information” frame you can configure the following values and read information.

In the context of Dual RSTP (for the device TCSESM-E), these are the settings for the Dual RSTP Primary Ring.

Parameter	Meaning	Possible Values	Default Setting
<b>Column „Bridge“</b>	<b>Information and configuration parameters of the local device</b>		
Bridge ID (read only)	The local Bridge ID, made up of the local priority and its own MAC address. The format is ppppp / mm mm mm mm mm mm, with: ppppp: priority (decimal) and mm: the respective byte of the MAC address (hexadecimal).		

Table 49: Global Spanning Tree settings, local bridge parameters

Parameter	Meaning	Possible Values	Default Setting
Priority	Sets the local bridge priority. The bridge priority and its own MAC address make up this separate Bridge ID. The device with the best (numerically lowest) priority assumes the role of the root bridge. Define the root device by assigning the device the best priority in the Bridge ID among all the devices in the network. Enter the value as a multiple of 4,096.	$0 \leq n \cdot 4096 \leq 61440$	32,768
Hello Time	Sets the Hello Time. The local Hello Time is the time in seconds between the sending of two configuration messages (Hello packets). If the local device has the root function, the other devices in the entire network take over this value. Otherwise the local device uses the value of the root bridge in the "Root" column on the right.	1 - 2	2
Forward Delay	Sets the Forward Delay parameter. In the previous STP protocol, the Forward Delay parameter was used to delay the status change between the statuses disabled, discarding, learning, forwarding. Since the introduction of RSTP, this parameter has a subordinate role, because the RSTP bridges negotiate the status change without any specified delay. If the local device is the root, the other devices in the entire network take over this value. Otherwise the local device uses the value of the root bridge in the "Root" column on the right.	4 - 30 s See the note following this table.	15 s
Max Age	Sets the Max Age parameter. In the previous STP protocol, the Max Age parameter was used to specify the validity of STP BPDUs in seconds. For RSTP, Max Age signifies the maximum permissible branch length (number of devices to the root bridge). If the local device is the root, the other devices in the entire network take over this value. Otherwise the local device uses the value of the root bridge in the "Root" column on the right.	6 - 40 s See the note following this table.	20 s

*Table 49: Global Spanning Tree settings, local bridge parameters*

Parameter	Meaning	Possible Values	Default Setting
Tx Hold Count	Sets the Tx Hold Count parameter. If the device sends a BPDU, it increments a counter at this port. When the counter reaches the value of the Tx Hold Count, the port stops sending any more BPDUs. The counter is decremented by 1 every second. The device sends a maximum of 1 new BPDU in the following second.	1 - 40 (based on RSTP standard: 1 - 10)	10
MRP compatibility	Switches the MRP compatibility on/off. MRP compatibility enables RSTP to be used within an MRP-Ring and when coupling RSTP segments to an MRP-Ring. The prerequisite is that all devices in the MRP-Ring must support MRP compatibility.  <b>Note:</b> If you combine RSTP with an MRP-Ring, you must give the devices in the MRP-Ring a better (i.e. numerically lower) RSTP bridge priority than the devices in the connected RSTP network. You thus help avoid a connection interruption for devices outside the Ring.	On, Off	Off
BPDU Guard	Switches the BPDU Guard function on/off. If BPDU Guard is switched on, the device automatically activates the function for edge ports (with the setting "Admin Edge Port" true). When such a port receives any STP-BPDU, the device sets the port status "BPDU Guard Effect" to true and the transmission status of the port to discarding(see table 62). Thus the device helps protect your network at terminal device ports from incorrect configurations or attacks with STP-BPDUs that try to change the topology.	On, Off	Off

Table 49: Global Spanning Tree settings, local bridge parameters

**Note:** The parameters `Forward Delay` and `Max Age` have the following relationship:

$$\text{Forward Delay} \geq (\text{Max Age}/2) + 1$$

If you enter values that contradict this relationship, the device then replaces these values with the last valid values or the default value.

Parameter	Meaning	Possible Values	Default Setting
<b>Column „Root“</b>	<b>Information on the device that is currently the root bridge</b>		
Bridge ID	The <code>Bridge ID</code> of the current root bridge. The format is ppppp / mm mm mm mm mm mm, with: ppppp: priority (decimal) and mm: the respective byte of the MAC address (hexadecimal).		
Priority	The <code>Priority</code> of the current root bridge.	$0 \leq n \leq 4096 \leq 61440$	32768
Hello Time	The <code>Hello Time</code> of the current root bridge.	1 - 2	2
Forward Delay	The <code>Forward Delay</code> of the current root bridge.	4 - 30 s	30 s
Max Age	The <code>Max Age</code> of the current root bridge.	6 - 40 s	20 s

*Table 50: Global Spanning Tree settings, root bridge information*

Parameter	Meaning	Value range
<b>Column „Topology“</b>	<b>Spanning Tree topology information</b>	
Bridge is root	If the local device is currently the root bridge, the device displays this box as selected, and otherwise as empty.	Selected, not selected.
Root Port	The port of the device from which the current path leads to the root bridge. 0: the local bridge is the root.	Valid port ID or 0.
Root path costs	Path costs from the root port of the device to the current root bridge of the entire layer 2 network. 0: the local bridge is the root.	0-200,000,000
Topology changes	Counts how often the device has put a port into the <code>Forwarding</code> status via Spanning Tree since it was started.	
Time since last change	Time since the last topology change.	

*Table 51: Global Spanning Tree settings, topology information*

If you have activated the “MRP Compatibility” function, the device displays the “Information” frame with additional information on MRP compatibility:

Parameter	Meaning	Possible Values	Default Setting
Information	If you have activated the MRP compatibility (RSTP over MRP) and one of the participating devices has detected a configuration problem, the device displays “Conflict with bridge pppp / mm mm mm mm mm”. During normal operation, this field is empty.	Message with bridge ID or empty.	-

Table 52: Global Spanning Tree settings, Information frame

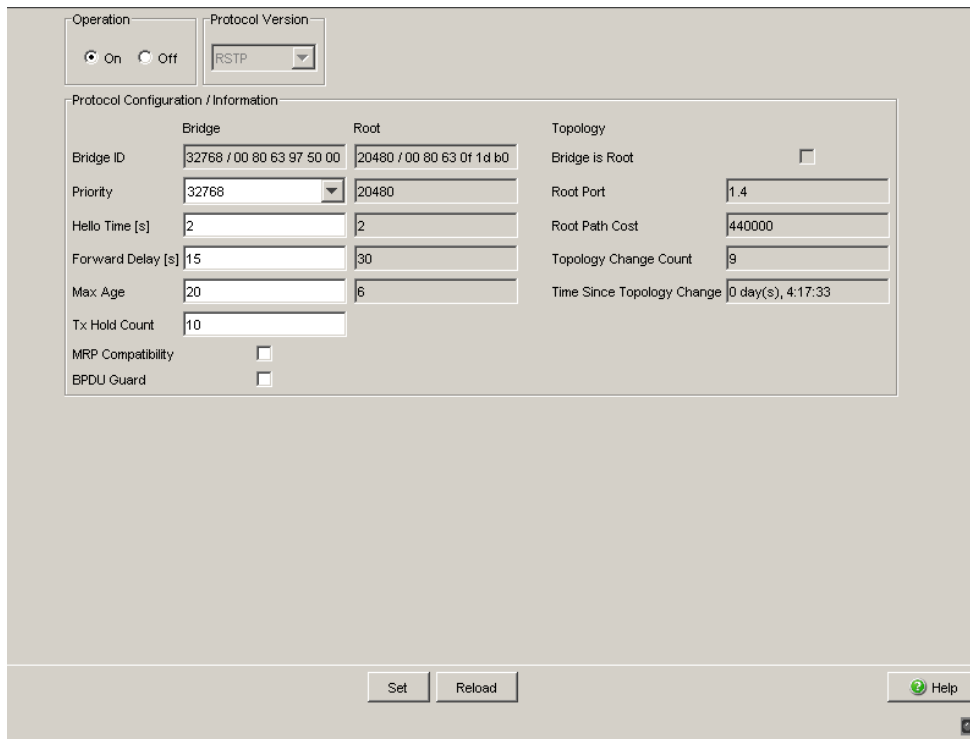


Figure 35: Dialog Spanning Tree, Global

## 6.4.2 Dual RSTP (TCSESM-E)

With this dialog you can:

- ▶ activate/deactivate Dual RSTP,
- ▶ display bridge-related information on Dual RSTP,
- ▶ configure bridge-related parameters of Dual RSTP,
- ▶ set bridge-related additional functions,
- ▶ display the parameters of the root bridge and
- ▶ display bridge-related topology information,
- ▶ configure the coupling ports for the primary and secondary Dual RSTP instances (rings),
- ▶ configure the Dual RSTP coupling and display coupling information.

**Note:** Exclude the use of Dual RSTP in combination with the following redundancy procedures and settings:

- ▶ RSTP in the MRP compatibility mode (RSTP over MRP)

**Note:** On the ports of the Dual RSTP Primary Ring, exclude a combination with the following redundancy procedures and settings:

- ▶ Sub-Ring
- ▶ Network/Ring coupling

For details of how you can configure this exclusion with maximum protocol inter-operability ([see on page 147 “Port”](#)).

**Note:** Only use Dual RSTP together with one of the following redundancy procedures if both ports of the Dual RSTP Primary Ring are identical to the ring ports of the other redundancy procedure:

- ▶ HIPER-Ring
- ▶ MRP-Ring
- ▶ Fast HIPER-Ring

**Note:** On the ports of the Dual RSTP Secondary Ring, exclude a combination with other redundancy procedures and settings.

**Note:** If you configure Dual RSTP in a network and the configuration is still incomplete, it is possible that the devices will temporarily not provide any connection between the Secondary and Primary Rings.

In this case, the management of the Dual RSTP bridges cannot be reached from the Secondary Ring.

During this configuration phase, connect your administration PC to the Primary Ring.

**Note:** Only those ports of a Dual RSTP Bridge that are configured as the secondary ring's outer or inner ring ports belong to the secondary RSTP instance.

All other ports belong to the Dual RSTP Bridge's primary instance.



## WARNING

### DUAL RSTP LOOP HAZARD

- ▶ Configure all the devices of the Dual RSTP configuration individually. Before you connect the redundant lines, you must complete the configuration of all the devices of the Dual RSTP configuration.
- ▶ Configure the timeout in the Dual RSTP coupling configuration longer than the longest assumable interruption time for the faster instance of the redundancy protocol.
- ▶ In a topology with 2 coupling bridges, configure the coupling roles of the two devices only as Master, Slave or Auto.
- ▶ Couple the primary and the secondary instance only by means of 1 Dual RSTP Bridge (for a topology with 1 Dual RSTP Bridge) or by means of 2 Dual RSTP Bridges (for a topology with 2 Dual RSTP Bridges). Keep all ports of the primary instance separated from all ports of all secondary instances.
- ▶ Only activate the "Admin Edge Port" setting at a port when a terminal device is connected to the port.

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



The following tables show the selection options, default settings and information for the Dual RSTP Secondary Ring.

Parameter	Meaning	Possible Values	Default Setting
<b>Frame “Operation“</b>	Switches the Dual RSTP function for this device “On” or “Off”.	On, Off	Off

*Table 53: Dual RSTP settings, basic function*

**Note:** If you have activated Dual RSTP, the device displays the parameters of the Primary and Secondary Rings in the following dialogs:

- ▶ Dual RSTP Primary Ring:
  - Display in the Redundancy:Spanning Tree:Global dialog, in the “Protocol Configuration/Information” frame
- ▶ Dual RSTP Secondary Ring:
  - Display in the Redundancy:Spanning Tree: Dual RSTP dialog, in the “Protocol Configuration/Information” frame

In the “Protocol Configuration / Information” frame you can configure the following values and read information.

Parameter	Meaning	Possible Values	Default Setting
<b>Column „Bridge“</b>	<b>Information and configuration parameters of the local device</b>		
Bridge ID (read only)	The local Bridge ID, made up of the local priority and its own MAC address. The format is ppppp / mm mm mm mm mm mm, with: ppppp: priority (decimal) and mm: the respective byte of the MAC address (hexadecimal).		
Priority	Sets the local bridge priority. The bridge priority and its own MAC address make up this separate Bridge ID. The device with the best (numerically lowest) priority assumes the role of the root bridge. Define the root device by assigning the device the best priority in the Bridge ID among all the devices in the network. Enter the value as a multiple of 4,096.	$0 \leq n \cdot 4096 \leq 61440$	32,768
Hello Time	Sets the Hello Time. The local Hello Time is the time in seconds between the sending of two configuration messages (Hello packets). If the local device has the root function, the other devices in the entire network take over this value. Otherwise the local device uses the value of the root bridge in the “Root” column on the right.	1 - 2	2

Table 54: Dual RSTP settings, local bridge parameters

Parameter	Meaning	Possible Values	Default Setting
Forward Delay	<p>Sets the Forward Delay parameter.</p> <p>In the previous STP protocol, the Forward Delay parameter was used to delay the status change between the statuses disabled, discarding, learning, forwarding. Since the introduction of RSTP, this parameter has a subordinate role, because the RSTP bridges negotiate the status change without any specified delay.</p> <p>If the local device is the root, the other devices in the entire network take over this value. Otherwise the local device uses the value of the root bridge in the "Root" column on the right.</p>	<p>4 - 30 s</p> <p>See the note following this table.</p>	15 s
Max Age	<p>Sets the Max Age parameter.</p> <p>In the previous STP protocol, the Max Age parameter was used to specify the validity of STP BPDUs in seconds. For RSTP, Max Age signifies the maximum permissible branch length (number of devices to the root bridge).</p> <p>If the local device is the root, the other devices in the entire network take over this value. Otherwise the local device uses the value of the root bridge in the "Root" column on the right.</p>	<p>6 - 40 s</p> <p>See the note following this table.</p>	20 s

*Table 54: Dual RSTP settings, local bridge parameters*

Parameter	Meaning	Possible Values	Default Setting
Tx Hold Count	Sets the Tx Hold Count parameter. If the device sends a BPDU, it increments a counter at this port. When the counter reaches the value of the Tx Hold Count, the port stops sending any more BPDUs. The counter is decremented by 1 every second. The device sends a maximum of 1 new BPDU in the following second.	1 - 40 (based on RSTP standard: 1 - 10)	10
BPDU Guard	Switches the BPDU Guard function on/off. If BPDU Guard is switched on, the device automatically activates the function for edge ports (with the setting "Admin Edge Port" true). When such a port receives any STP-BPDU, the device sets the port status "BPDU Guard Effect" to true and the transmission status of the port to discarding (see table 62). Thus the device helps protect your network at terminal device ports from incorrect configurations or attacks with STP-BPDUs that try to change the topology.	On, Off	Off

Table 54: Dual RSTP settings, local bridge parameters

**Note:** The parameters `Forward Delay` and `Max Age` have the following relationship:

$$\text{Forward Delay} \geq (\text{Max Age}/2) + 1$$

If you enter values that contradict this relationship, the device then replaces these values with the last valid values or the default value.

Parameter	Meaning	Possible Values	Default Setting
<b>Column „Root“</b>	<b>Information on the device that is currently the root bridge</b>		
Bridge ID	The <code>Bridge ID</code> of the current root bridge. The format is <code>ppppp / mm mm mm mm mm mm</code> , with: <code>ppppp</code> : priority (decimal) and <code>mm</code> : the respective byte of the MAC address (hexadecimal).		
Priority	The <code>Priority</code> of the current root bridge.	$0 \leq n \cdot 4096 \leq 61440$	32768
Hello Time	The <code>Hello Time</code> of the current root bridge.	1 - 2	2
Forward Delay	The <code>Forward Delay</code> of the current root bridge.	4 - 30 s	30 s
Max Age	The <code>Max Age</code> of the current root bridge.	6 - 40 s	20 s

*Table 55: Dual RSTP settings, root bridge information*

Parameter	Meaning	Value range
<b>Column „Topology“</b>	<b>Spanning Tree topology information</b>	
Bridge is root	If the local device is currently the root bridge, the device displays this box as selected, and otherwise as empty.	Selected, not selected.
Root Port	The port of the device from which the current path leads to the root bridge. 0: the local bridge is the root.	Valid port ID or 0.
Root path costs	Path costs from the root port of the device to the current root bridge of the entire layer 2 network. 0: the local bridge is the root.	0-200,000,000
Topology changes	Counts how often the device has put a port into the <code>Forwarding</code> status via Spanning Tree since it was started.	
Time since last change	Time since the last topology change.	

*Table 56: Dual RSTP settings, topology information*

## ■ Dual RSTP Ring Ports

You define the Dual RSTP Ring ports in the “Dual RSTP Primary Ring” and “Dual RSTP Secondary Ring” frames.

Parameter	Meaning	Possible Values	Default Setting
Frame „Dual RSTP Primary Ring“	<p><b>Note:</b> On the ports of the Dual RSTP Primary Ring, exclude a combination with the following redundancy procedures and settings:</p> <ul style="list-style-type: none"> <li>▶ Sub-Ring</li> <li>▶ Network/Ring coupling</li> </ul> <p>For details of how you can configure this exclusion with maximum protocol interoperability (<a href="#">see on page 147 “Port”</a>).</p> <p><b>Note:</b> Only use Dual RSTP together with one of the following redundancy procedures if both ports of the Dual RSTP Primary Ring are identical to the ring ports of the other redundancy procedure:</p> <ul style="list-style-type: none"> <li>▶ HIPER-Ring</li> <li>▶ MRP-Ring</li> <li>▶ Fast HIPER-Ring</li> </ul>		
Inner Port	Port for the Dual RSTP Primary instance that is directly connected with the Dual RSTP partner (master or slave).	Valid port	0.0 (no port)
Outer Port	<p>The complimentary port to the inner port for the Dual RSTP Primary Instance that closes the ring for the instance.</p> <p><b>Note:</b> The functions of the inner and outer ports only differ if there are 2 coupling bridges in the instance. For a device in the single mode, the functions of the inner and outer ports are identical.</p>	Valid port	0.0 (no port)

Table 57: Dual RSTP settings, Primary Ring ports

Parameter	Meaning	Possible Values	Default Setting
<b>Frame „Dual RSTP Secondary Ring“</b>	<b>Note:</b> On the ports of the Dual RSTP Secondary Ring, exclude a combination with other redundancy procedures and settings.		
Inner Port	Port of the Dual RSTP Secondary instance that is directly connected with the Dual RSTP partner.	Valid port	0.0 (no port)
Outer Port	The complementary port to the inner port for the Dual RSTP Secondary Instance that closes the ring for the instance.  <b>Note:</b> The functions of the inner and outer ports only differ if there are 2 coupling bridges in the instance. For a device in the single mode, the functions of the inner and outer ports are identical.	Valid port	0.0 (no port)

*Table 58: Dual RSTP settings, Secondary Ring ports*

#### ■ Dual RSTP coupling configuration

You configure the coupling of the two rings in the “Dual RSTP Coupler Configuration” frame.

Parameter	Meaning	Possible Values	Default Setting
Role	<p>The configured Dual RSTP role of the local device for both Dual RSTP instances.</p> <p><b>Note:</b> Only configure the single role if you are coupling the instances via 1 bridge, as otherwise loops can result.</p> <p><b>Note:</b> Only configure the auto role if you are coupling the instances via 2 bridges. If both partner bridges are configured as auto, the partner bridge that is currently coupling the instances takes the master role, and the other bridge takes the slave role.</p> <p><b>Note:</b> The configuration of the auto role has the following features:</p> <ul style="list-style-type: none"> <li>▶ Advantage: If a partner bridge that had temporarily become inoperable and that was previously the master participates in the protocol again, it always remains the slave. The protocol thus avoids an unnecessary switching back into the static master role.</li> <li>▶ Disadvantage: The role distribution is not foreseeable in normal operation, but rather depends dynamically on the initialization of the protocol and any failures.</li> </ul>	master, slave, single, auto	master

*Table 59: Dual RSTP settings, Coupling Configuration*



Parameter	Meaning	Possible Values	Default Setting
Current role (read only)	<p>The actual current Dual RSTP role of the local device.</p> <p>It can differ from the configured role:</p> <ul style="list-style-type: none"> <li>▶ If you have configured both partner bridges as <code>auto</code>, the partner bridge that is currently coupling the instances takes the <code>master</code> role, and the other bridge takes the <code>slave</code> role.</li> <li>▶ If both partner bridges are configured as <code>master</code> or both as <code>slave</code>, the partner bridge with the smaller base MAC address takes the <code>master</code> role, and the other bridge takes the <code>slave</code> role.</li> <li>▶ When the protocol is started, if the partner bridge cannot be found for a bridge in the configured role <code>master</code>, <code>slave</code> or <code>auto</code>, it sets its own role to <code>listening</code></li> <li>▶ If the device detects a configuration problem, e.g. if the inner Ring ports are connected crosswise, the device sets its role to <code>error</code>.</li> <li>▶ If you have deactivated Dual RSTP for the device, it sets its role to <code>disabled</code>.</li> </ul>	<code>master</code> , <code>slave</code> , <code>single</code> , <code>listening</code> , <code>error</code> , <code>disabled</code>	-
Timeout [ms]	<p>Maximum time during which the slave bridge waits for test packets from the master bridge at the outer ports before it takes over the coupling.</p> <p>This only applies in the state in which both inner ports of the slave bridge have lost the connection to the master bridge.</p> <p><b>Note:</b> Configure this timeout longer than the longest assumable interruption time for the redundancy protocol of the faster instance. Otherwise, loops can occur.</p>	5 - 60,000 ms	45 ms
Partner MAC (read only)	The base MAC address of the Dual RSTP partner device	MAC address (in <code>single</code> mode 00:00:00:00:00:00)	-

*Table 60: Dual RSTP settings, Coupling Configuration*

Parameter	Meaning	Possible Values	Default Setting
Partner IP (read only)	The IP address of the Dual RSTP partner device	IPv4 address (in single mode 0.0.0.0)	-
Coupling status (read only)	Displays the coupling status of the local device	forwarding, blocking	-
Redundancy status (read only)	Specifies whether a redundancy reserve is available (with a correct configuration and in normal operation) or not (with configuration problems or a failure). For a master-slave configuration, both bridges display this information.	Redundancy available, redundancy not available	-

Table 60: Dual RSTP settings, Coupling Configuration

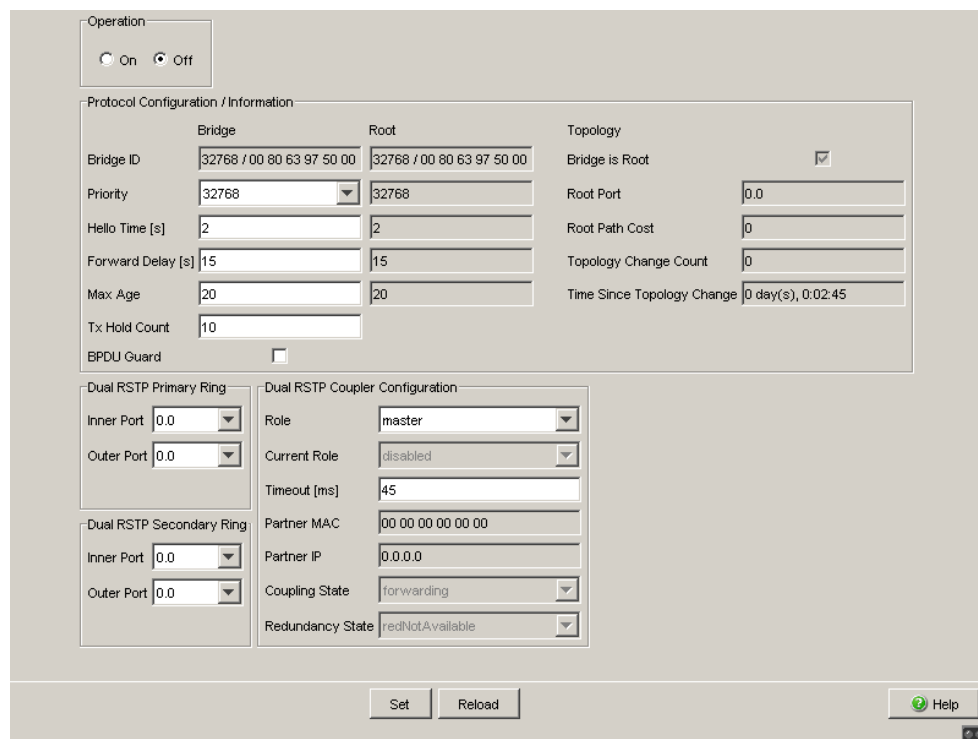


Figure 36: Dual RSTP dialog

### 6.4.3 Port

**Note:** Deactivate the Spanning Tree protocol for the ports connected to a HIPER-Ring, Fast HIPER-Ring, or Ring/Network coupling, because Spanning Tree and Ring Redundancy or Ring/Network coupling affect each other.

Activate the MRP compatibility in an MRP-Ring if you want to use RSTP and MRP in combination.

If you combine RSTP with an MRP-Ring, you must give the devices in the MRP-Ring a better (i.e. numerically lower) RSTP bridge priority than the devices in the connected RSTP network. You thus help avoid a connection interruption for devices outside the Ring.

If you are using the device in a Multiple Spanning Tree (MSTP) environment, the device only participates in the Common Spanning Tree (CST) instance. This chapter of the manual also uses the term Global MST instance to describe this general case.

Parameter	Meaning	Possible Values	Default Setting
<b>Tab „CIST“</b>	Port configuration and information on the global MSTI (IST) and the CST.		
STP active	Here you can switch Spanning Tree on or off for this port. If Spanning Tree is activated globally and switched off at one port, this port does not send STP-BPDUs and drops any STP-BPDUs received.	On, Off	On
	<p><b>Note:</b> If you want to use other layer 2 redundancy protocols such as HIPER-Ring or Ring/Network coupling in parallel with Spanning Tree, make sure you switch off the ports participating in these protocols in this dialog for Spanning Tree. Otherwise the redundancy may not operate as intended or loops can result.</p>		
Dual RSTP active (for TCSESM-E)	Specifies that the port belongs to the Dual RSTP Secondary Ring - that is, it is configured as an inner or outer port of the Secondary Ring in the Redundancy:Spanning Tree: Dual RSTP dialog.	On (selected), Off (not selected)	Off
	<p><b>Note:</b> You will find the ports that belong to the Dual RSTP Primary Ring in the dialog Redundancy:Spanning Tree: Dual RSTP, in the “Dual RSTP Primary Ring” frame (inner and outer port).</p>		
Port status (read only)	Displays the STP port status with regard to the global MSTI (IST).	discarding, learning, forwarding, disabled, manualForwarding, notParticipate	-
Port role (read only)	Displays the STP port role with regard to the global MSTI (IST).	root, alternate, designated, backup, disabled	-

Table 61: Port-related STP settings and displays, CIST

Parameter	Meaning	Possible Values	Default Setting
Port path costs	Enter the path costs with regard to the global MSTI (IST) to indicate preference for redundant paths. If the value is 0, the Switch automatically calculates the path costs for the global MSTI (IST) depending on the transmission rate.	0 - 200,000,000	0 (automatically)
Port priority	Here you enter the port priority (the four highest bits of the port ID) with regard to the global MSTI (IST) as a decimal number of the highest byte of the port ID.	$16 \leq n \cdot 16 \leq 240$	128
Received bridge ID (read only)	Displays the remote bridge ID from which this port last received an STP-BPDU. <sup>a</sup>	Bridge identification (format ppppp / mm mm mm mm mm mm)	-
Received port ID (read only)	Displays the port ID at the remote bridge from which this port last received an STP-BPDU. <sup>a</sup>	Port ID, format pn nn, with p: port priority / 16, nnn: port No., (both hexadecimal)	-
Received path costs (read only)	Displays the path costs of the remote bridge from its root port to the CIST root bridge. <sup>a</sup>	0-200,000,000	-
Admin Edge Port	Activate this setting only if a terminal device is connected to the port. Then the port immediately transitions to the forwarding status after a link is set up, without first going through the STP statuses. If the port still receives an STP-BPDU, the device blocks the port and clarifies the port's STP port role. In the process, the port can switch to a different status, e.g. forwarding, discarding, learning. Deactivate the setting when the port is connected to a bridge. After a link is set up, the port then goes through the STP statuses first before taking on the forwarding status, if applicable. This setting applies to all MSTIs.	active (box selected), inactive (box empty)	inactive

Table 61: Port-related STP settings and displays, CIST

Parameter	Meaning	Possible Values	Default Setting
Auto Edge Port	The device only considers the Auto Edge Port setting when the Admin Edge Port parameter is deactivated. If Auto Edge Port is active, after a link is set up the device sets the port to the forwarding status after $1.5 \cdot \text{Hello Time}$ (in the default setting 3 s). If Auto Edge Port is deactivated, the device waits for the <code>Max Age</code> instead (in the default setting 20 s). This setting applies to all MSTIs.	<code>active</code> (box selected), <code>inactive</code> (box empty)	<code>active</code>
Oper Edge Port (read only)	The device sets “Oper Edge Port” condition to <code>true</code> if no STP-BPDUs have been received, i.e., a terminal device is connected. It sets the state to <code>false</code> if STP-BPDUs have been received, i.e., a bridge is connected. This condition applies to all MSTIs.	<code>true</code> , <code>false</code>	-
Actual point-to-point (read only)	The device sets the “Actual point-to-point” condition to <code>true</code> if this port has a full duplex condition to an STP device. Otherwise it sets the condition to <code>false</code> (e.g. if a hub is connected). The point-to-point connection makes a direct connection between 2 RSTP devices. The direct, decentralized communication between the two bridges results in a short reconfiguration time. This condition applies to all MSTIs.	<code>true</code> , <code>false</code> The device determines this condition from the duplex mode: FDX: <code>true</code> HDX: <code>false</code>	

Table 61: Port-related STP settings and displays, CIST

- <sup>a</sup> These columns show you more detailed information than that available up to now:  
For designated ports, the device displays the information for the STP-BPDU last received by the port. This helps with the diagnosis of possible STP problems in the network.  
For alternative, back-up and root ports, is in the stationary condition (static topology) this information is identical to the designated information.  
If a port has no link, or if it has not received any STP-BPDUs yet, the device displays the values that the port would send as a designated port.

CIST		Guards							
Port	Stp active	Dual RSTP active	Port State	Port Role	Port Pathcost	Port Priority	Received Bridge ID	Received Port ID	Received Path Cost
1.1	<input checked="" type="checkbox"/>	<input type="checkbox"/>	disabled	disabled	0	128	32768 / 00 80 63 97 50 00	00 00	0
1.2	<input checked="" type="checkbox"/>	<input type="checkbox"/>	disabled	disabled	0	128	32768 / 00 80 63 97 50 00	00 00	0
1.3	<input checked="" type="checkbox"/>	<input type="checkbox"/>	disabled	disabled	0	128	32768 / 00 80 63 97 50 00	00 00	0
1.4	<input checked="" type="checkbox"/>	<input type="checkbox"/>	forwarding	root	200000	128	32768 / 00 80 63 51 74 00	80 07	240000
1.5	<input checked="" type="checkbox"/>	<input type="checkbox"/>	disabled	disabled	0	128	32768 / 00 80 63 97 50 00	00 00	0
1.6	<input checked="" type="checkbox"/>	<input type="checkbox"/>	disabled	disabled	0	128	32768 / 00 80 63 97 50 00	00 00	0
1.7	<input checked="" type="checkbox"/>	<input type="checkbox"/>	forwarding	designated	200000	128	32768 / 00 80 63 b2 42 18	80 08	440000
1.8	<input checked="" type="checkbox"/>	<input type="checkbox"/>	disabled	disabled	0	128	32768 / 00 80 63 97 50 00	00 00	0

Figure 37: Multiple Spanning Tree dialog, Port, CIST tab

Parameter	Meaning	Possible Values	Default Setting
<b>Tab „Guards“</b> Protective settings for the ports.			
Root Guard	<p>The “Root Guard” setting is only relevant for ports with the STP role <code>designated</code>. If such a port receives an STP-BPDU with better path information on the root than what the device knows, the device discards the BPDU and sets the port status to <code>discarding</code>, instead of assigning the port the STP port role <code>root</code>. Thus the device helps protect your network from attacks with STP-BPDUs that try to change the topology, and from incorrect configurations. If there are no STP-BPDUs with better path information on the root, the device resets the transmission status of the port according to the port role.</p> <p><b>Note:</b> The “Root Guard” and “Loop Guard” settings are mutually exclusive. If you activate one setting when the other is already active, the device switches off the other one.</p>	<p><code>active</code> (box selected), <code>inactive</code> (box empty)</p>	<code>inactive</code>
TCN Guard	<p>If the “TCN Guard” setting is active (TCN: Topology Change Notification) the port ignores the topology change flag in the STP-BPDUs received that is reporting a topology change. Thus the device helps protect your network from attacks with STP-BPDUs that try to change the topology. If the “TCN Guard” setting is inactive, the device follows the protocol in reacting to the STP-BPDUs received: it deletes its address table and forwards the TCN information.</p> <p><b>Note:</b> If the received BPDU contains other information apart from the topology change flag that causes a topology change, the device processes the BPDU even if the TCN guard is activated. Example: the device receives better path information for the root than that already known.</p>	<p><code>active</code> (box selected), <code>inactive</code> (box empty)</p>	<code>inactive</code>

Table 62: Port-related STP settings and displays, guards



Parameter	Meaning	Possible Values	Default Setting
Loop Guard	<p>The “Loop Guard” setting is only meaningful for ports with the STP role <code>alternate</code>, <code>backup</code> or <code>root</code>. If the “Loop Guard” setting is active and the port has not received any STP-BPDUs for a while, the device sets the port to the <code>discarding</code> condition (port sends no more data).</p> <p>The device also sets the port to what is known as the “loop inconsistent status” and displays this in the “Loop Status” column.</p> <p>The device prevents a potential loop if no more STP-BPDUs are received if, for example, you switch STP off on the remote device, or the link only becomes inoperable in the receiving direction.</p> <p>When the port receives BPDUs again, the device resets the loop status of the port to <code>false</code>, and the transmission status of the port according to the port role.</p> <p>If the “Loop Guard” setting is inactive, however, the device sets the port to the <code>forwarding</code> status when STP-BPDUs have not been received.</p>	<code>active</code> (box selected), <code>inactive</code> (box empty)	<code>inactive</code>
	<p><b>Note:</b> The “Root Guard” and “Loop Guard” settings are mutually exclusive. If you activate one setting when the other is already active, the device switches off the other one.</p>		
Loop Status (read only)	<p>Display the status of the Loop Status.</p> <p>The device sets the loop status of the port to <code>true</code> if the “Loop Guard” setting is active at the port and the port is not receiving any more STP-BPDUs.</p> <p>Here the device leaves the port in the <code>discarding</code> transmission status, to help prevent a potential loop.</p> <p>When the port receives STP-BPDUs again, the device resets the loop status to <code>false</code>.</p>	<code>true</code> , <code>false</code>	-
Transitions to Loop Status (read only)	Counts how often the device has set the port to the loop status (“Loop Status” column <code>true</code> ).	0 - 4,294,967,295 ( $2^{32}-1$ )	0

*Table 62: Port-related STP settings and displays, guards*

Parameter	Meaning	Possible Values	Default Setting
Transitions from Loop Status	Counts how often the device has set the port out of the loop status (“Loop Status” column <code>true</code> ).	0 - 4,294,967,295 ( $2^{32}-1$ )	0
BPDU Guard Effect (read only)	<p>The “BPDU Guard Effect” status is only relevant for edge ports (ports with the “Admin Edge Port” status <code>true</code>), and only if the “BPDU Guard” global function is active (see <a href="#">table 49</a>).</p> <p>When such a port receives any random STP-BPDU, the device sets the port’s “BPDU Guard Effect” status to <code>true</code> and its transmission status to <code>discarding</code>.</p> <p>Thus the device helps protect your network at terminal device ports from incorrect configurations or attacks with STP-BPDUs that try to change the topology.</p> <p>To return the port to a normal transmitting status from the locked status, break and reconnect the link, or switch the “Admin Edge Port” port setting off and on again.</p>	<code>true</code> , <code>false</code>	-

*Table 62: Port-related STP settings and displays, guards*

Port	Root Guard	TCN Guard	Loop Guard	Loop State	Trans. into Loop	Trans. out of Loop	BPDU Guard Effect
1.1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	false	0	0	disable
1.2	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	false	0	0	disable
1.3	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	false	0	0	disable
1.4	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	false	0	0	disable
1.5	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	false	0	0	disable
1.6	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	false	0	0	disable
1.7	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	false	0	0	disable
1.8	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	false	0	0	disable

Set Reload Help

Figure 38: Multiple Spanning Tree dialog, Port, Guards tab



## 7 Diagnostics

The diagnosis menu contains the following tables and dialogs:

- ▶ Syslog
- ▶ Event Log
- ▶ Ports (statistics, utilization, SFP modules)
- ▶ Topology Discovery
- ▶ Port Mirroring
- ▶ Device Status
- ▶ Signal Contact
- ▶ Alarms (Traps)
- ▶ Report (log file, system information)
- ▶ IP Address Conflict Detection
- ▶ Self Test

In service situations, they provide the technician with the necessary information for diagnosis.

## 7.1 Syslog

The “Syslog” dialog enables you to additionally send to one or more syslog servers, the events that the device writes to its event log. You can switch the function on or off, and you can manage a list of up to 8 syslog server entries. You also have the option to specify that the device informs various syslog servers, depending on the minimum “level to report” of the event.

Additionally, you can also send the SNMP requests to the device as events to one or more syslog servers. Here you have the option of treating GET and SET requests separately, and of assigning a “level to report” to the requests to be logged.

**Note:** You will find the actual events that the device has logged in the “Event Log” dialog ([see on page 163 “Event Log”](#)) and in the log file ([see on page 180 “Report”](#)), a HTML page with the title “Event Log”.

The device evaluates SNMP requests as events if you have activated “Log SNMP Set/Get Request” ([see table 64](#)).

Parameter	Meaning	Possible Values	Default Setting
<b>Frame „Function“</b>	Switches the syslog function for this device “On” or “Off”	On, Off	Off
<b>Frame „SNMP Logging“</b>	Settings for sending SNMP requests to the device as events to the list of syslog servers.		
Log SNMP Get Requests.	Creates events for the syslog for SNMP Get requests with the specified “level to report”.	active, inactive	inactive
Level to Report (for logs of SNMP Get Requests)	Specifies the level for which the device creates the event “SNMP Get Request received” for the list of the syslog servers.	debug, informational, notice, warning, error, critical, alert, emergency	notice

*Table 63: Syslog and SNMP Logging settings*

Log SNMP Set Requests.	Creates events for the syslog for SNMP Set requests with the specified “level to report”.	active, inactive	inactive
Level to Report (for logs of SNMP Set Requests)	Specifies the level for which the device creates the event “SNMP Set Request received” for the list of the syslog servers.	debug, informational, notice, warning, error, critical, alert, emergency	notice

Parameter	Meaning	Possible Values	Default Setting
<b>Syslog server entries</b>			
Index	Sequential number of the syslog server entry in the table. When you delete an entry, this leaves a gap in the numbering. When you create a new entry, the device fills the first gap.	1 - 8	-
IP address	Address of a syslog server to which the device sends its log entries.	Valid IPv4 address	0.0.0.0
Port	UDP port at which your syslog server receives entries.	1 - 65.535	514
Minimum level to report	Minimum level to report for an event for the device to sent a log entry for it to this syslog server.	debug, informational, notice, warning, error, critical, alert, emergency	critical
Active	Activate or deactivate the current syslog server entry in the table.	active (box selected), inactive (box empty)	active

Table 64: Syslog server entries

Parameter	Meaning	Possible Values	Default Setting
<b>Buttons</b>			
"Set" button	Click on "Write" to temporarily save the data.	-	
	<b>Note:</b> If you have entered an IP address different to 0.0.0.0 for a newly created syslog server entry, after the entry is written the device activates it automatically. Click on "Load" for the device to update the display.		
"Create" button	Creates a new syslog server entry in the list.	-	
"Remove" button	Deletes the selected syslog server entry/entries from the list.	-	

Table 65: Syslog entries, buttons



**Note:** When you activate the logging of SNMP requests, the device sends these as events with the preset level to report `notice` to the list of syslog servers. The preset minimum level to report 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 level to report for which the device creates SNMP requests as events to `warning` or `error` and change the minimum level to report 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.
- ▶ Only set the level to report for SNMP requests to `critical` or higher. The device then sends SNMP requests as events with the level to report `critical` or higher to the syslog servers.
- ▶ Only set the minimum level to report for one or more syslog server entries to `notice` or lower. Then it may happen that the device sends a large number of events to the syslog servers.

Operation:  On  Off

SNMP Logging

Log SNMP Get Request  Severity: notice

Log SNMP Set Request  Severity: notice

Index	IP-Address	Port	Minimum Severity	Active
1	0.0.0.0	514	critical	<input type="checkbox"/>
2	0.0.0.0	514	critical	<input type="checkbox"/>
3	10.0.1.1	514	critical	<input checked="" type="checkbox"/>

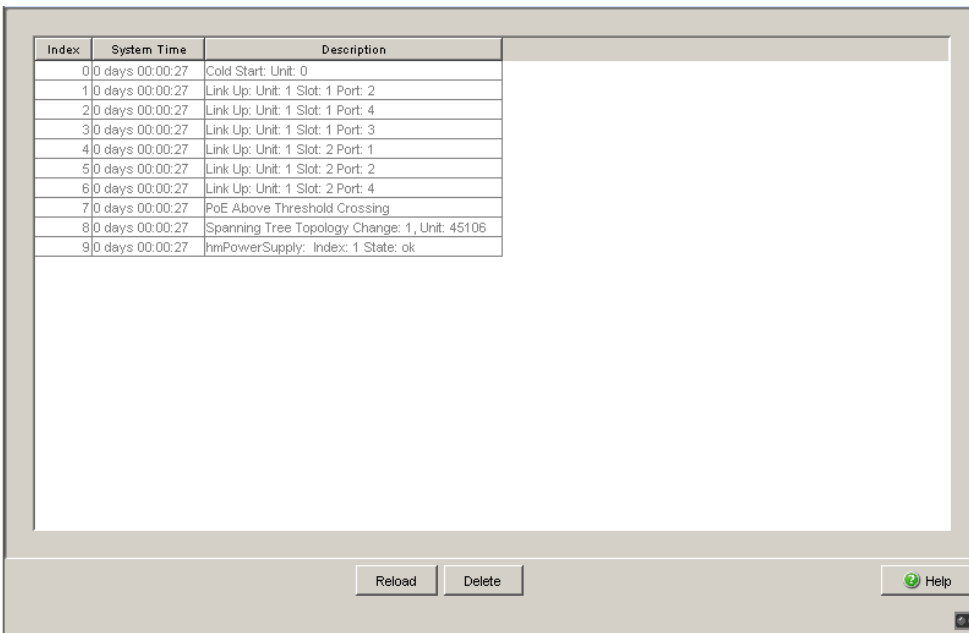
Set Reload Create Remove Help

Figure 39: Syslog dialog

## 7.2 Event Log

The table lists the logged events with a time stamp.

The “Reload” button allows you to update the content of the event log, and with the “Delete” button you delete the content of the event log.



Index	System Time	Description
0	0 days 00:00:27	Cold Start: Unit: 0
1	0 days 00:00:27	Link Up: Unit: 1 Slot: 1 Port: 2
2	0 days 00:00:27	Link Up: Unit: 1 Slot: 1 Port: 4
3	0 days 00:00:27	Link Up: Unit: 1 Slot: 1 Port: 3
4	0 days 00:00:27	Link Up: Unit: 1 Slot: 2 Port: 1
5	0 days 00:00:27	Link Up: Unit: 1 Slot: 2 Port: 2
6	0 days 00:00:27	Link Up: Unit: 1 Slot: 2 Port: 4
7	0 days 00:00:27	PoE: Above Threshold Crossing
8	0 days 00:00:27	Spanning Tree Topology Change: 1, Unit: 45106
9	0 days 00:00:27	hmiPowerSupply: Index: 1 State: ok

Figure 40: Event log table

You have the option to also send the logged events to one or more syslog servers ([see on page 158 “Syslog”](#)).

## 7.3 Ports

The port menu contains displays and tables for the individual ports:

- ▶ Statistics table
- ▶ Utilization
- ▶ SFP Modules

### 7.3.1 Statistics table

This table shows you the contents of various event counters. In the Restart menu item, you can reset all the event counters to zero using “Warm start”, “Cold start” or “Reset port counter”.

The packet counters add up the events sent and the events received.

Module	Port	Transmitted Unicast Packets	Received Packets	Received Octets	Received Fragments	Detected CRC errors	Detected Collisions	Packets 64 bytes	Packets 65 to 127 bytes	Packets 128 to 255 bytes
1	1	0	0	0	0	0	0	0	0	
1	2	1493	1601	433624	0	0	0	12	2217	
1	3	1493	1603	459246	0	0	0	13	2218	
1	4	1635	5591	664808	0	0	0	3998	2365	
2	1	1493	537	94484	0	0	0	3991	2216	
2	2	1493	0	0	0	0	0	3984	2216	
2	3	0	0	0	0	0	0	0	0	
2	4	2317	4938	716317	0	0	0	4061	2399	40
3	1	0	0	0	0	0	0	0	0	
3	2	0	0	0	0	0	0	0	0	
8	1	0	0	0	0	0	0	0	0	
8	2	0	0	0	0	0	0	0	0	

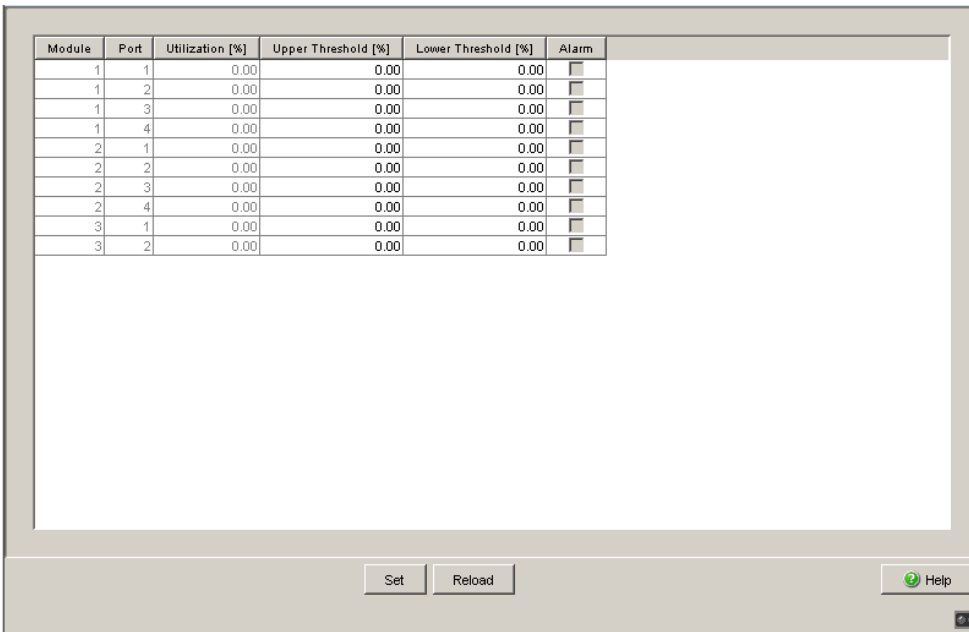
Figure 41: Port statistics table

### 7.3.2 Utilization

This table displays the network load of the individual ports.

In the “Upper Threshold[%]” column you enter the upper threshold value for network load. If this threshold value is exceeded, the device sets a check mark in the “Alarm” field.

In the “Lower Threshold [%]” column you enter the lower threshold value for network load. If the current load falls below this threshold value, the device removes the check mark previously set.



The screenshot shows a dialog window titled "Network load dialog" with a table of port utilization data. The table has six columns: Module, Port, Utilization [%], Upper Threshold [%], Lower Threshold [%], and Alarm. The data is as follows:

Module	Port	Utilization [%]	Upper Threshold [%]	Lower Threshold [%]	Alarm
1	1	0.00	0.00	0.00	<input type="checkbox"/>
1	2	0.00	0.00	0.00	<input type="checkbox"/>
1	3	0.00	0.00	0.00	<input type="checkbox"/>
1	4	0.00	0.00	0.00	<input type="checkbox"/>
2	1	0.00	0.00	0.00	<input type="checkbox"/>
2	2	0.00	0.00	0.00	<input type="checkbox"/>
2	3	0.00	0.00	0.00	<input type="checkbox"/>
2	4	0.00	0.00	0.00	<input type="checkbox"/>
3	1	0.00	0.00	0.00	<input type="checkbox"/>
3	2	0.00	0.00	0.00	<input type="checkbox"/>

At the bottom of the dialog, there are three buttons: "Set", "Reload", and "Help".

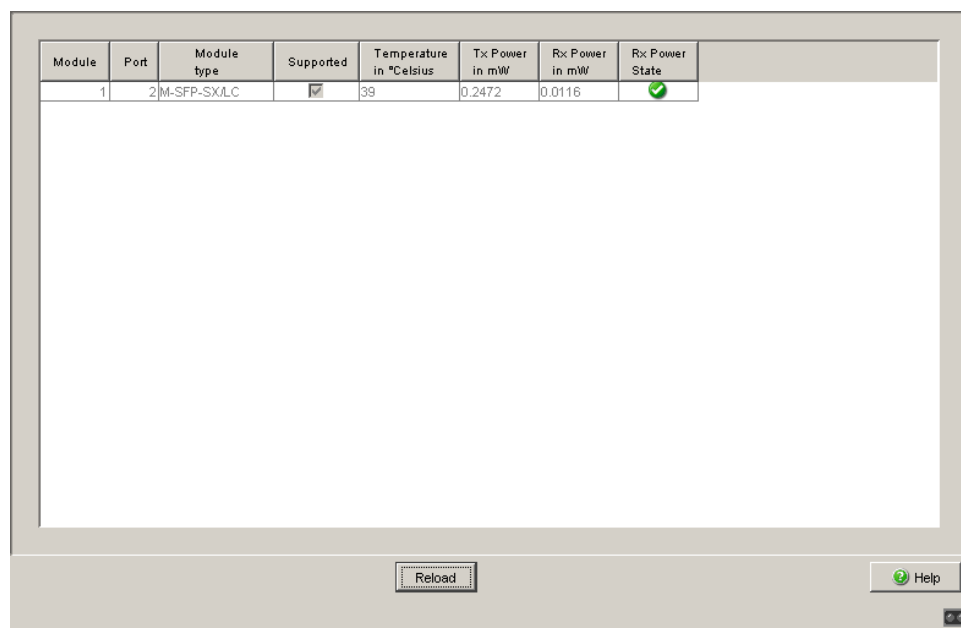
Figure 42: Network load dialog

### 7.3.3 SFP modules

The SFP status display allows you to look at the current SFP module connections and their properties. The properties include:

Parameter	Meaning
Module	Module of the device on which the port is located.
Port	Port to which this entry applies.
Module type	Type of SFP module, e.g. M-SFP-SX/LC
Supported	Shows whether the media module supports the SFP module.
Temperature in Celsius	Shows the operating temperature of the SFP
Tx Power in mW	Shows the transmission power in mW
Rx Power in mW	Shows the receiver power in mW
Receiver power status	Shows the power level of the received signal. - good receiver power - limited receiver power - insufficient receiver power

Table 66: SFP Modules dialog



Module	Port	Module type	Supported	Temperature in °Celsius	Tx Power in mW	Rx Power in mW	Rx Power State
1	2	M-SFP-SX/LC	<input checked="" type="checkbox"/>	39	0.2472	0.0116	✓

Reload Help

Figure 43: SFP Modules dialog

## 7.4 Topology Discovery

This dialog allows you to switch on/off the topology discovery function (LLDP). The topology table shows you the collected information for neighboring devices. This information enables the network management station to map the structure of your network.

The option “Show LLDP entries exclusively” allows you to reduce the number of table entries. In this case, the topology table hides entries from devices without active LLDP support.

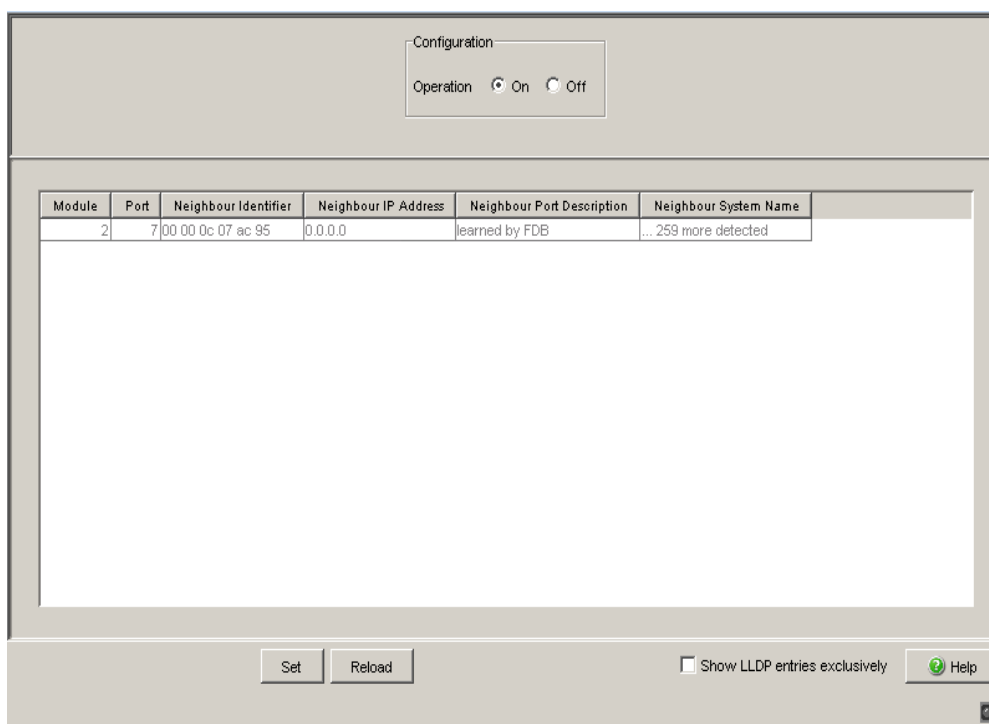


Figure 44: Topology discovery

If several devices are connected to one port, for example via a hub, the table will contain one line for each connected device.

When devices both with and without an active topology discovery function are connected to a port, the topology table hides the devices without active topology discovery.

If only devices without active topology discovery are connected to a port, the table will contain one line for this port to represent all devices. This line contains the number of connected devices.

MAC addresses of devices that the topology table hides for the sake of clarity, are located in the address table (FDB), ([see page 64 “Filters for MAC addresses”](#)).



---

## 7.5 Port Mirroring

The port mirroring function enables you to review the data traffic at up to 8 ports of the device for diagnostic purposes. The device additionally forwards (mirrors) the data for these ports to another port. This process is also called port mirroring.

The ports to be reviewed are known as source ports. The port to which the data to be reviewed is copied is called the destination port. You can only use physical ports as source or destination ports.

In port mirroring, the device copies valid incoming **and** outgoing data packets of the source port to the destination port. The device does not affect the data traffic at the source ports during port mirroring.

A management tool connected at the destination port, e.g. an RMON probe, can thus monitor the data traffic of the source ports in the sending and receiving directions.

The destination port forwards both data to be sent and received data.

- Select the source ports whose data traffic you want to review from the list of physical ports by checkmarking the relevant boxes.  
You can select a maximum of 8 source ports. Ports that cannot be selected are displayed as inactive by the device, e.g. the port currently being used as the destination port, or if you have already selected 8 ports.  
Default setting: no source ports.
- Select the destination port to which you have connected your management tool from the list element in the “Destination Port” frame.  
The device does not display ports that cannot be selected in the list, e.g. the ports currently being used as source ports. Default setting: port 0.0 (no destination port).
- Select “On” in the “Function” frame to switch on the function. Default setting: “Off”.

The “Reset configuration” button in the dialog allows you to reset all the port mirroring settings of the device to the state on delivery.

**Note:** When port mirroring is active, the specified destination port is used solely for reviewing, and does not participate in the normal data traffic.

Operation:  On  Off

Destination Port:

Source Port	Enabled
1.1	<input checked="" type="checkbox"/>
1.2	<input type="checkbox"/>
1.3	<input type="checkbox"/>
1.4	<input checked="" type="checkbox"/>
1.5	<input type="checkbox"/>
1.6	<input type="checkbox"/>
1.7	<input type="checkbox"/>
1.8	<input type="checkbox"/>

Set   Reload   Reset Config   Help

Figure 45: Dialog Port Mirroring

## 7.6 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.

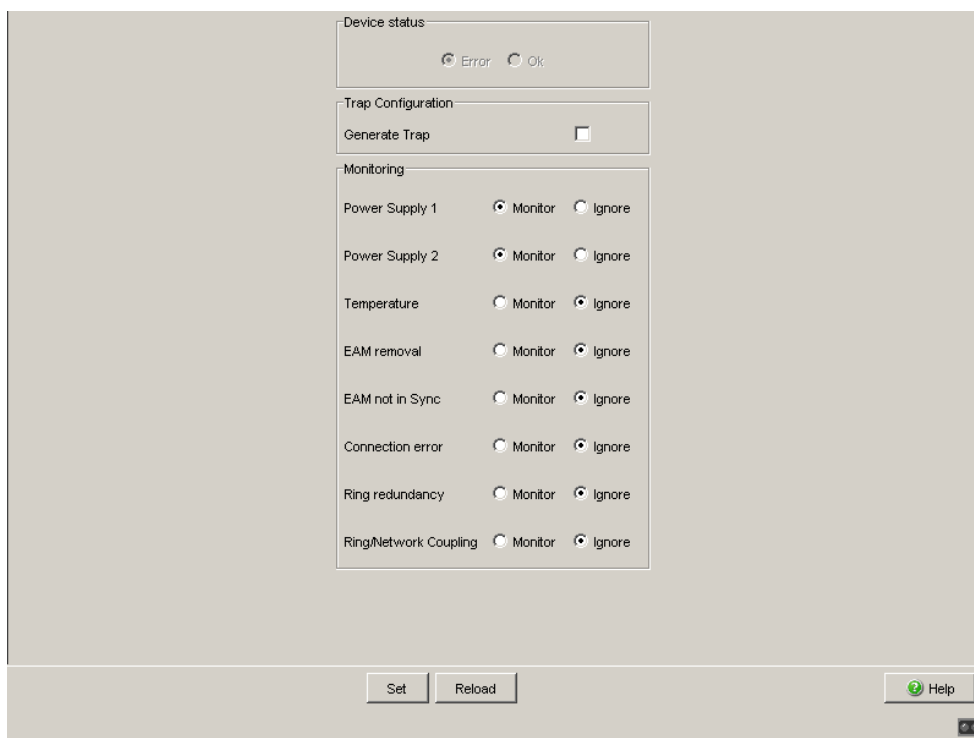


Figure 46: Device Status Dialog

- In the “Monitoring” field, you select the events you want to monitor.
- To monitor the temperature, you set the temperature thresholds in the `Basics: System` dialog at the end of the system data.

The events which can be selected are:

Name	Meaning
Power supply ...	Monitor/ignore supply voltage(s).
Temperature	Monitor/ignore temperature thresholds set ( <a href="#">see on page 20 “System”</a> ) for temperatures that are too high/too low
EAM removal	Monitor/ignore the removal of the EAM.
EAM not in sync	Monitor/ignore the non-matching of the configuration in the device and on the EAM <sup>a</sup>
Connection error	Monitor/ignore the link status (Ok or inoperable) of at least one port. The reporting of the link status can be masked for each port by the management ( <a href="#">see on page 29 “Port Configuration”</a> ). Link status is not monitored in the state on delivery.
Ring Redundancy	Monitor/ignore the ring redundancy (for the HIPER-Ring, only in ring manager operation). On delivery, ring redundancy is not monitored.

**Note:** If the device is a normal ring member and not a ring manager, it doesn't report anything for the HIPER-Ring; for the Fast HIPER-Ring and for MRP it only reports detected errors in the local configuration.

Ring/Network coupling	Monitor/ignore the redundant coupling operation. On delivery, no monitoring of the redundant coupling is set. For two-Switch coupling with control line, the slave additionally reports the following conditions: <ul style="list-style-type: none"> <li>– Incorrect link status of the control line</li> <li>– Partner device is also a slave (in standby mode).</li> </ul>
-----------------------	--

**Note:** In two-Switch coupling, both Switches must have found their respective partners.

*Table 67: Device Status*

- a. The configurations are non-matching if only one file exists or the two files do not have the same content.

- Select “Generate Trap” in the “Trap Configuration” field to activate the sending of a trap if the device state changes.

**Note:** With a non-redundant voltage supply, the device reports the absence of a supply voltage. If you do not want this message to be displayed, feed the supply voltage over both inputs or switch off the monitoring ([see on page 174](#) “Signal contact”).

## 7.7 Signal contact

The signal contacts are used for

- ▶ controlling external devices by manually setting the signal contacts,
- ▶ monitoring the functions of the device,
- ▶ reporting the device state of the device.

### 7.7.1 Manual setting

- Select the tab page “Alarm 1” or “Alarm 2” (for devices with two signal contacts).
- In the “Signal contact mode” field, you select the “Manual setting” mode. With this mode you can control this signal contact remotely.
- Select “Opened” in the “Manual setting” frame to open the contact.
- Select “Closed” in the “Manual setting” frame to close the contact.

Application options:

- ▶ Simulation of an error during SPS monitoring.
- ▶ Remote control of a device via SNMP, such as switching on a camera.

### 7.7.2 Function monitoring

- Select the tab “Signal contact 1” or “Signal contact 2” (for devices with two signal contacts).

- In the “Mode Signal contact” box, you select the “Monitoring correct operation” mode. In this mode, the signal contacts monitor the functions of the device, thus enabling remote diagnosis.  
A break in contact is reported via the potential-free signal contact (relay contact, closed circuit).
- ▶ Loss of the supply voltage 1/2 (either of the external voltage supply or of the internal voltage). Select “Monitor” for the respective power supply if the signal contact shall report the loss of the power supply voltage, or of the internal voltage that is generated from the external power supply.
- ▶ One of the temperature thresholds has been exceeded ([see on page 21 “System Data”](#)). Select “Monitor” for the temperature if the signal contact should report an impermissible temperature.
- ▶ Removing a module. Select “Monitor” for removing modules if the signal contact is to report the removal of a module (for modular devices).
- ▶ The removal of the EAM. Select “Monitor” for EAM removal if the signal contact is to report the removal of an EAM (for devices which support the EAM).
- ▶ Non-matching of the configuration in the device and on the EAM<sup>1</sup>. Select “Monitor” EAM not in sync if the signal contact is to report the non-matching of the configuration (for devices which support EAM).
- ▶ The inoperable link status of at least one port. The reporting of the link status can be masked via the management for each port in the device. Link status is not monitored in the state on delivery. Select “Monitor” for bad connections if the signal contact is to report an inoperative link status for at least one port.
- ▶ If the device is part of a redundant ring: the elimination of the reserve redundancy (i.e. the redundancy function did actually switch on), ([see on page 102 “Ring Redundancy”](#)). Select “Monitor” for the ring redundancy if the signal contact is to report the elimination of the reserve redundancy in the redundant ring.  
Default setting: no monitoring.

**Note:** If the device is a normal ring member and not a ring manager, it doesn't report anything for the HIPER-Ring; for the Fast HIPER-Ring and for MRP it only reports detected errors in the local configuration.

1. The configurations are non-matching if only one file exists or the two files do not have the same content.

- ▶ The elimination of the reserve redundancy for the ring/network coupling (i.e. the redundancy function did actually switch on). Select “Monitor” for the ring/network coupling if the signal contact is to report the elimination of the reserve redundancy for the ring/network coupling ([see on page 120 “Preparing a Ring/Network Coupling”](#)).  
Default setting: no monitoring.

**Note:** In two-Switch coupling, both Switches must have found their respective partners.

### 7.7.3 Device status

- Select the tab page “Alarm 1” or “Alarm 2” (for devices with two signal contacts).
- In the “Mode Signal Contact” field, you select the “Device status” mode. In this mode, the signal contact monitors the device status ([see on page 171 “Device Status”](#)) and thereby offers remote diagnosis. The device status “Error detected” ([see on page 171 “Device Status”](#)) is reported by means of a break in the contact via the potential-free signal contact (relay contact, closed circuit).

### 7.7.4 Configuring traps

- Select `generate Trap`, if the device is to create a trap as soon as the position of a signal contact changes when function monitoring is active.



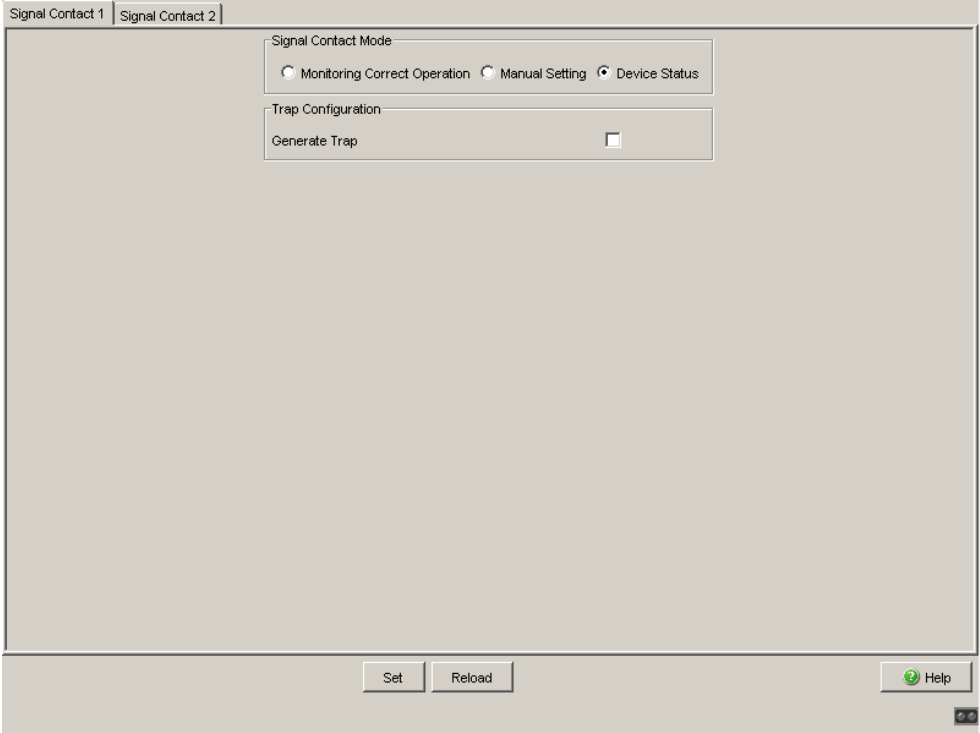


Figure 47: Signal contact dialog

## 7.8 Alarms (Traps)

This dialog allows you to determine which events trigger an alarm (trap) and where these alarms should be sent.

- Select “Create entry“.
- In the “Address” column, enter the IP address of the management station to which the traps should be sent.
- In the “Enabled” column, you mark the entries which should be taken into account when traps are sent.
- In the column “Password”, enter the community name that the device uses to identify itself as the trap's source.
- In the “Selection” frame, select the trap categories from which you want to send traps.

The events which can be selected are:

Name	Meaning
Authentication	The device has rejected an unauthorized access attempt ( <a href="#">see on page 43 “SNMPv1/v2 Access Settings”</a> ).
Link Up/Down	At one port of the device, the link to another device has been established/interrupted.
Spanning Tree	The topology of the Rapid Spanning Tree has changed.
Chassis	Summarizes the following events: <ul style="list-style-type: none"> <li>– The status of a supply voltage has changed (see the <i>System</i> dialog).</li> <li>– The status of the signal contact has changed.</li> </ul> To take this event into account, you activate “Create trap when status changes” in the <i>Diagnostics:Signal Contact 1/2</i> dialog. <ul style="list-style-type: none"> <li>– The receiver power status of a port with an SFP module has changed (see dialog <i>Diagnostics:Ports:SFP Modules</i>).</li> <li>– The configuration has been successfully saved in the device and in the Memory Backup Adaptor (EAM), if present.</li> <li>– The configuration has been changed for the first time after being saved in the device.</li> </ul>
Redundancy	The redundancy status of the ring redundancy (redundant line active/inactive) or (for devices that support redundant ring/network coupling) the redundant ring/network coupling (redundancy exists) has changed.
Port security	On one port a data packet has been received from an unauthorized terminal device (see the <i>Port Security</i> dialog).

*Table 68: Trap categories*

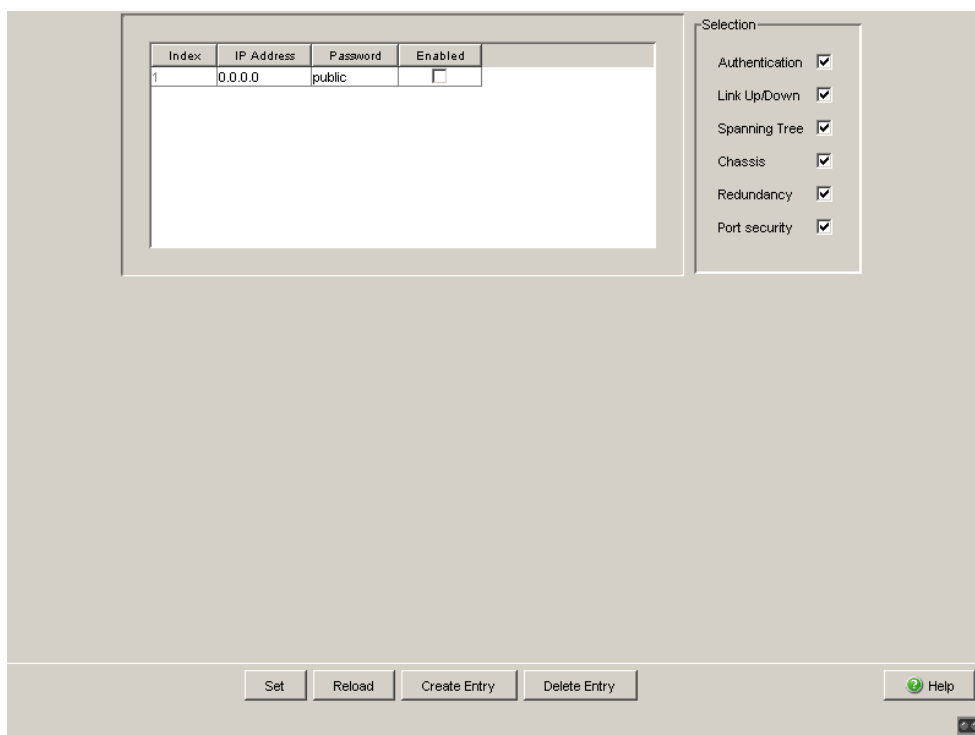


Figure 48: Alarms Dialog

---

## 7.9 Report

The following reports are available for the diagnostics:

- ▶ [Log file](#).  
The log file is an HTML file in which the device writes important device-internal events.
- ▶ [System information](#).  
The system information is an HTML file containing system-relevant data.

**Note:** You have the option to also send the logged events to one or more syslog servers ([see on page 158 “Syslog”](#)).

The following buttons are available:

- ▶ **Download Switch-Dump.**  
This button allows you to download system information as files in a ZIP archive ([see table 69](#)).
  - Select the directory in which you want to save the switch dump.
  - Click “Save”.

The device creates the file name of the switch dumps automatically in the format <IP address>\_<system name>.zip, e.g. for a device of the type TCSESM-E: “10.0.1.112\_TCSESM063F2CU1.zip”.
- ▶ **Download JAR file.**  
This button allows you to download the applet of the Web-based interface as a JAR file. Afterwards you have the option to start the applet outside a browser.  
This enables you to administer the device even when you have deactivated its Web server for security reasons.
  - Select the directory in which you want to save the applet.
  - Click “Save”.

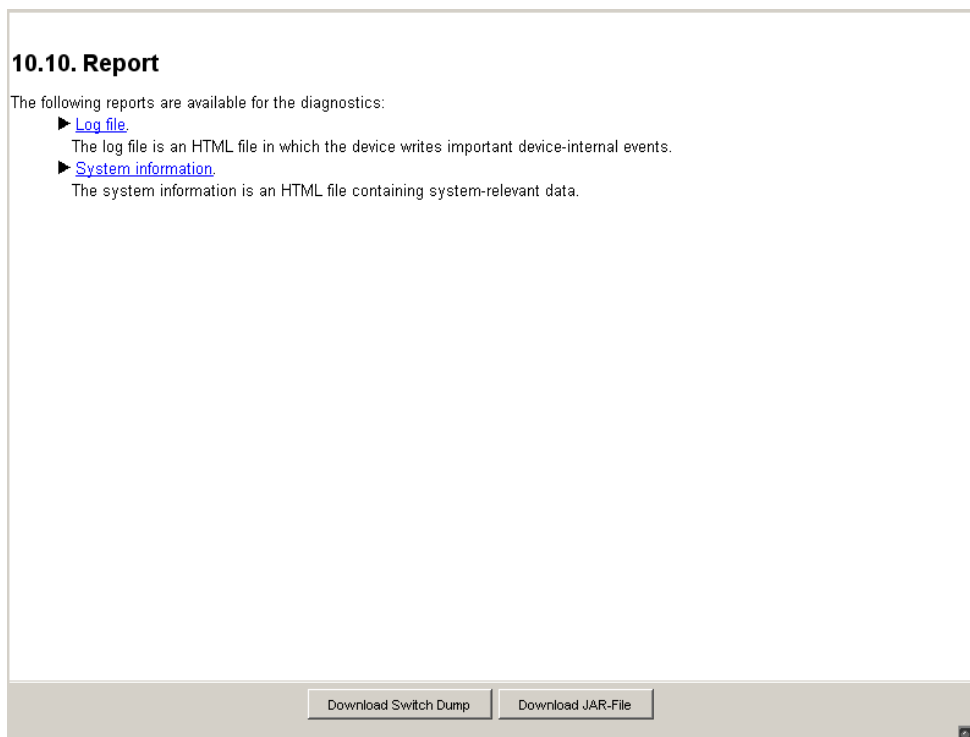
The device creates the file name of the applet automatically in the format <device type><software version>\_<software revision of applet>.jar, e.g. for a device of type TCSESM-E: "tcsesm\_e06000\_00.jar".

File	Name	Format	Comments
Log file	event_log.html	HTML	
System information	systemInfo.html	HTML	
Event log	traplog.txt	Text	
Device configuration (binary)	switch.cfg	Binary	
Device configuration (as script)	switch.cli	Script	
Internal memory extract for the manufacturer to improve the product	dump.hmd	Binary	
Exception log	exception_log.html	HTML	
Output of CLI commands <sup>a</sup> : – show running-config <sup>b</sup> – show port all – show sysinfo – show mac-address-table – show mac-filter-table – igmpsnooping	clicommands.txt	Text	

*Table 69: Files in switch dump archive*

*a: Prerequisite: a Telnet connection is available.*

*b: Prerequisite: you are logged in as a user with write access.*



*Figure 49: Report dialog*

## 7.10 IP address conflict detection

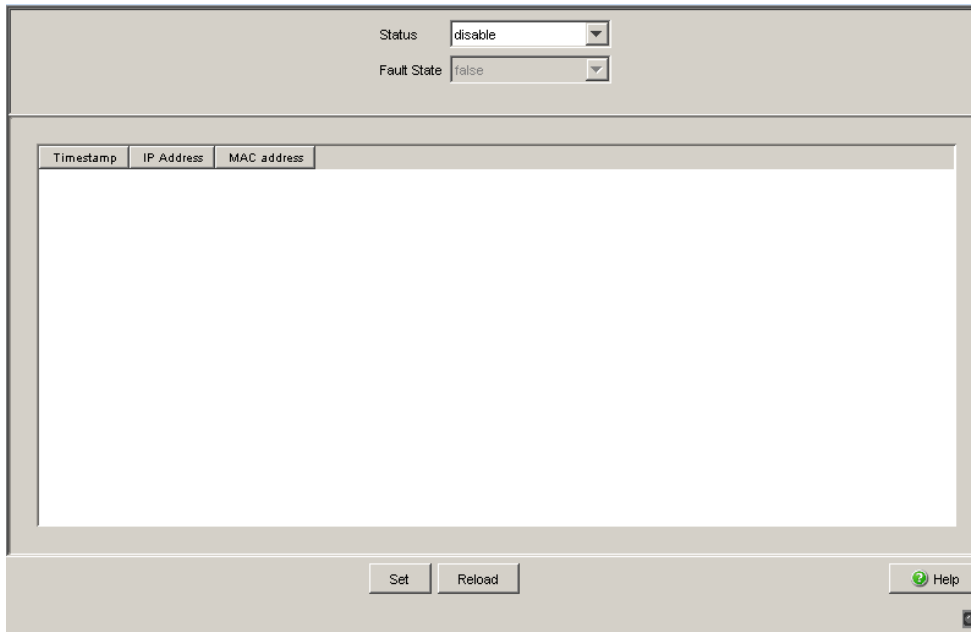
This dialog allows you to detect address conflicts the device is having with its own IP address and rectify them (Address Conflict Detection, ACD).

- Select IP address conflict detection on/off under “Status” or select the mode ([see table 70](#)).

Mode	Meaning
enable	Enables active and passive detection.
disable	Disables the function
activeDetectionOnly	Enables active detection only. After connecting to a network or after an IP address has been configured, the device immediately checks whether its IP address already exists within the network. If the IP address already exists, the device will return to the previous configuration, if possible, and make another attempt after 15 seconds. The device therefore avoids to participate in the network traffic with a duplicate IP address.
passiveOnly	Enables passive detection only. The device listens passively on the network to determine whether its IP address already exists. If it detects a duplicate IP address, it will initially defend its address by employing the ACD mechanism and sending out gratuitous ARPs. If the remote device does not disconnect from the network, the management interface of the local device will then disconnect from the network. Every 15 seconds, it will poll the network to determine if there is still an address conflict. If there isn't, it will connect back to the network.

*Table 70: Possible address conflict operation modes*

- ▶ In the table the device logs IP address conflicts with its IP address.  
For each conflict the device logs:
  - ▶ the time
  - ▶ the conflicting IP address
  - ▶ the MAC address of the device with which the IP address conflicted.
 For each IP address, the device logs a line with the last conflict that occurred.
- You can delete this table by restarting the device.



*Figure 50: IP Address Conflict Detection dialog*

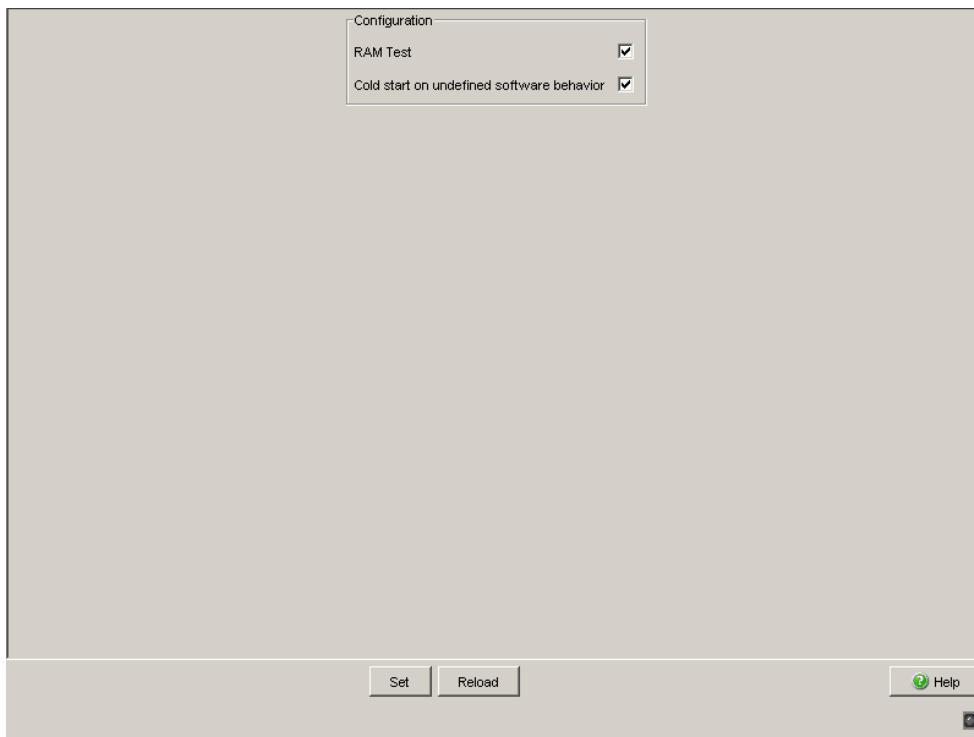


---

## 7.11 Self Test

With this dialog you can:

- ▶ activate/deactivate the RAM test for a cold start of the device.  
Deactivating the RAM test reduces the boot-up time for a cold start of the device.
- ▶ allow or disable a restart due to an undefined software or hardware state.



*Figure 51: Self-test dialog*




## 8 Advanced

The menu contains the dialogs, displays and tables for:

- ▶ DHCP Relay Agent
- ▶ Ethernet/IP
- ▶ Command Line

## 8.1 DHCP Relay Agent

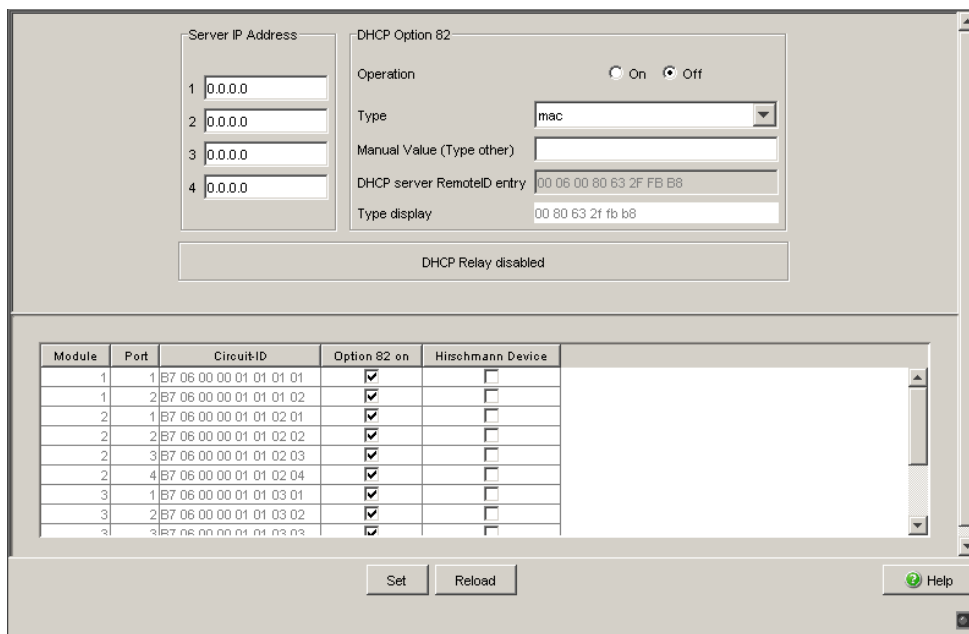
On the device's front panel you will find the following hazard message.


WARNING

**UNINTENDED OPERATION**

Do not change cable positions if DHCP Option 82 is enabled. Check the Basic Configuration user manual before servicing (refer to DHCP OPTION 82 topic).

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



Module	Port	Circuit-ID	Option 82 on	Hirschmann Device
1	1	B7 06 00 00 01 01 01 01	<input checked="" type="checkbox"/>	<input type="checkbox"/>
1	2	B7 06 00 00 01 01 01 02	<input checked="" type="checkbox"/>	<input type="checkbox"/>
2	1	B7 06 00 00 01 01 02 01	<input checked="" type="checkbox"/>	<input type="checkbox"/>
2	2	B7 06 00 00 01 01 02 02	<input checked="" type="checkbox"/>	<input type="checkbox"/>
2	3	B7 06 00 00 01 01 02 03	<input checked="" type="checkbox"/>	<input type="checkbox"/>
2	4	B7 06 00 00 01 01 02 04	<input checked="" type="checkbox"/>	<input type="checkbox"/>
3	1	B7 06 00 00 01 01 03 01	<input checked="" type="checkbox"/>	<input type="checkbox"/>
3	2	B7 06 00 00 01 01 03 02	<input checked="" type="checkbox"/>	<input type="checkbox"/>
3	3	B7 06 00 00 01 01 03 03	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Figure 52: DHCP Relay Agent dialog

This dialog allows you to configure the DHCP relay agent.

- Enter the DHCP server IP address.  
If one DHCP server is not available, you can enter up to 3 additional DHCP server IP addresses so that the device can change to another DHCP server.
- With Option 82, a DHCP relay agent which receives a DHCP request adds an “Option 82” field to the request, as long as the request received does not already have such a field.  
When the function is switched off, the device will forward attached “Option 82” fields, but it will not add any on. Under “Type”, you specify the format in which the device recognition of this device is entered in the “Option 82” field by the DHCP relay agent.  
The options are:
  - IP address
  - MAC Address (state on delivery)
  - System name (client ID)
  - Other (freely definable ID, which you can specify in the following rows). “Remote ID entry for DHCP server” shows you the value which you enter when configuring your DHCP server. “Type display” shows the device recognition in the selected form.
- ▶ The “Circuit ID” column shows you the value which you enter when configuring your DHCP server. The “Circuit ID” contains the port number and the ID of the VLAN from which the DHCP has been received.

Example of a configuration of your DHCP server:

Type: mac

DHCP server for Remote ID entry: 00 06 00 80 63 00 06 1E

Circuit ID: B3 06 00 00 01 00 01 01

This results in the entry for the “Hardware address” in the DHCP server:

B306000001000101000600806300061E

- In the “Option 82 on” column, you can switch this function on/off for each port.
- In the “Schneider Electric Device” column, you mark the ports to which a Schneider Electric device is connected.

## 8.2 EtherNet/IP

The EtherNet/IP menu allows you to

- ▶ activate and deactivate the EtherNet/IP protocol and
- ▶ download the EDS file for this device to your PC to configure the PLC.

### **General settings:**

- In the `Switching:Multicasts:IGMP` dialog, check whether IGMP Snooping is activated ([see on page 69 “IGMP \(Internet Group Management Protocol\)”](#)).

### **Global EtherNet/IP settings:**

- Activate the function in the “EtherNet/IP” frame; the default setting is off.
- Click on “Download EDS File” to load the EDS file onto your PC.

## 8.3 Command Line

This window enables you to access the Command Line Interface (CLI) using the Web interface.

You will find detailed information on CLI in the “Command Line Interface” reference manual.





# A Appendix

---

## A.1 Technical Data

<b>Switching</b>	
Size of MAC address table (incl. static filters)	8.000
Max. number of statically configured MAC address filters	100
Max. number of MAC address filters learnable via GMRP/IGMP Snooping	512
Max. length of over-long packets (from rel. 03.0.00)	1,632 bytes

<b>VLAN</b>	
VLAN ID	1 to 4,042
Number of VLANs	max. 255 simultaneously per device max. 255 simultaneously per port
Number of VLANs in GMRP in VLAN 1	max. 255 simultaneously per device max. 255 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 1769	(SNTP)
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 1907	(Management Information Base for SNMP v2)
RFC 1908	(Coexistence between SNMP v1 and 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 2271	(SNMP Framework MIB)
RFC 2346	(AES Ciphersuites for Transport Layer Security)
RFC 2365	(Administratively Scoped Boundaries)
RFC 2570	(Introduction to SNMP v3)
RFC 2571	(Architecture for Describing SNMP Management Frameworks)
RFC 2572	(Message Processing and Dispatching for SNMP)
RFC 2573	(SNMP v3 Applications)

---

---

RFC 2574	(User Based Security Model for SNMP v3)
RFC 2575	(View Based Access Control Model for SNMP)
RFC 2576	(Coexistence between SNMP v1, v2 & v3)
RFC 2578	(SMI v2)
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 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)

---

## A.3 Underlying IEEE Standards

IEEE 802.1AB	Topology Discovery (LLDP)
IEEE 802.1af	Power over Ethernet
IEEE 802.1D	Switching, GARP, GMRP, Spanning Tree (Supported via 802.1S implementation)
IEEE 802.1D-1998, IEEE 802.1D-2004	Media access control (MAC) bridges (includes IEEE 802.1p Priority and Dynamic Multicast Filtering, GARP, GMRP, Spanning Tree)
IEEE 802.1w-2001	Rapid Reconfiguration (RSTP)
IEEE 802.1X	Port Authentication
IEEE 802.3-2002	Ethernet
IEEE 802.3ac	VLAN Tagging
IEEE 802.3x	Flow Control

## A.4 Underlying IEC Norms

---

IEC 62439	High availability automation networks; especially: Chap. 5, MRP – Media Redundancy Protocol based on a ring topology
-----------	---

---

## A.5 Copyright of Integrated Software

### A.5.1 Bouncy Castle Crypto APIs (Java)

The Legion Of The Bouncy Castle  
Copyright (c) 2000 - 2004 The Legion Of The Bouncy Castle  
(<http://www.bouncycastle.org>)

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR 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.

## A.5.2 Broadcom Corporation

(c) Copyright 1999-2007 Broadcom Corporation. All Rights Reserved.



# B Index

8			
802.1D/p mapping		96	
<b>A</b>			
Accept SNMP Broadcast		54	
Acceptable Frame Types		85	
Access with Web-based interface, password		40	
ACD		183	
Address Conflict Detection		183	
Advanced		187	
AF		99	
Aging Time		60	
Alarm		178	
Assured Forwarding		99	
<b>B</b>			
BPDU Guard	132, 140		
Broadcast Limiter Settings		66	
<b>C</b>			
Cable crossing		29	
Class Selector		98	
CLI		191	
CLI access, password		40	
Clock		57	
Cold start (after software update)		27	
Coldstart		37	
Command Line Interface		191	
Configuring Fast HIPER-Ring		111	
Configuring the MRP-Ring		108	
Current VLAN dialog		81	
<b>D</b>			
Device status		171	
DHCP Option 82		189	
DHCP Relay Agent		188	
Diagnose		157	
DiffServ		89	
DIP switch		104	
DSCP		89	
Dual RSTP		126	
<b>E</b>			
EAM	31, 178		
EF		98	
EtherNet/IP		190	
Event log		163	
Expedited Forwarding		98	
<b>F</b>			
Fast HIPER-Ring (port VLAN ID)		86	
Fast HIPER-Ring, Configuration		111	
Filters for MAC addresses		64	
Firmware update		26	
Forward Delay		131, 133, 139, 141	
<b>G</b>			
General		19	
<b>H</b>			
Hello Time		131, 133, 138, 141	
HIPER-Ring		11, 85, 101, 135, 142	
HIPER-Ring (source for alarms)		178	
<b>I</b>			
IGMP Querier		70	
IGMP settings		70	
IGMP Snooping		70	
Independent VLAN		80	
Ingress Filtering		85	
IP DSCP mapping		89, 98	
IP-DSCP value		90	
<b>J</b>			
Java Runtime Environment		15	
JavaScript		15	
<b>L</b>			
Link State (Port)		29	
LLDP		167	
Login		16	
<b>M</b>			
Max Age		131, 133, 139, 141	
Message URL <a href="http://myHostName/base/system/event_log.html">http://myHostName/base/system/event_log.html</a>		180	
Message URL <a href="http://myHostName/base/system/systemInfo.html">http://myHostName/base/system/systemInfo.html</a>		180	
MRP		11, 101	
MRP Domain		117, 118	
Multicasts		69	
<b>N</b>			
Network load		126, 165	
Network management station		167	
NTP		53	

# Index

---

O		Ring Manager	102
One-Switch coupling	122	Ring Redundancy	101
Option 82	189	Ring Redundancy basic configuration	103
P		Ring structure	102
Password	17, 42	Ring/Network Coupling	11, 101, 120
Password for access with Web-based interface	40	Ring/Network coupling	85, 101, 172
Password for CLI access	40	Ring/Network coupling (source for alarms)	178
Password for SNMPv3 access	40	Ringport	104
Per-Hop-Behavior (PHB)	98	RM function	102
Port configuration	29, 93	RMON probe	169
Port configuration (QoS/priority)	93	Root bridge	127
Port Mirroring	169	RSTP	126
Port priority	93, 93	S	
Port security (IP-/MAC-based)	48	Security	39
Port security (source for alarms)	49	Self-test	185
Port State (Link)	29	Set	17
Port Statistics	164	SFP Module (source for alarms)	178
Port VLAN ID	85	SFP Modules	166
Ports	164	SFP status display	166
Precedence	98	Shared VLAN	80
Precision Time Protocol	57	Signal contact	174
Priority Queue	90	Signal contact (source for alarm)	178
PTP	57	SNMP logging	158
Q		SNMPv1/v2 access settings	43
QoS/Priority	89	SNMPv3 access, password	40
R		SNTP	53
RAM test	185	SNTP Broadcast	54
Rapid Spanning Tree	126	SNTP client	53
Rapid Spanning Tree Port Protocol	147	SNTP server	53
Rate Limiter	66	Software update	26
Rate Limiter Settings	66	Spanning Tree	126
Read access	17	Statistics table	164
Reboot	37	STP	126
Receiver power status	166	Sub-Ring - New Entry dialog	118
Receiver power status (source for alarms)	178	Sub-Ring configuration	115
Redundancy	11, 101	Supply voltage	178
Redundancy functions	101	Switching	59
Redundancy Manager	102	Switching Global Dialog	60
Redundant	102	Symbol	13
Redundant connections	126	Syslog	158
Redundant coupling	85, 85, 101, 135, 142, 172	System time	54
Report	180	T	
Request interval (SNTP)	54, 54	Telnet Access	46
Restart	37	Temperature (device)	21
Restore default settings	31	Temperature (SFPs)	166
Restore state on delivery	31	Time	51
RFC	195	Time management	57
Ring	102	Timestamp unit	57
		Topology	167
		ToS	89
		Trap	178

## Index

---

Trust mode	90, 94
TrustDot1p (global trust mode)	91, 94
TrustIpDscp	91, 95
TrustIpDscp (global trust mode)	91, 94
Two-switch coupling	122
Two-Switch coupling with control line	122
TX Hold Count	132, 140
Type of Service	89
U	
Untrusted (global trust mode)	90, 94
Untrusted traffic class	95
V	
VLAN	78
VLAN (HIPER-Ring settings)	106
VLAN and GOOSE Protocol	79
VLAN and redundancy rings	86
VLAN Global dialog	78
VLAN ID (network parameter of the device)	24
VLAN Mapping	89
VLAN mode	80
VLAN Port dialog	85
VLAN priority	89
VLAN priority	90
VLAN Static dialog	83
W	
Web Access	46
Web-based interface	15
Web-based management	16
Website	17
Write access	17

