ConneXium

TCSESB Basic Managed Switch
Web-based Interface Reference Manual

S1A78429.00

www.schneider-electric.com

Schneider Electric

Contents

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.

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

Related Documents

Title of Documentation	Reference-Number
ConneXium TCSESB Basic Managed Switch Redundancy Configuration User Manual	S1A78418
ConneXium TCSESB Managed Switch Basic Configuration User Manual	S1A78213
ConneXium TCSESB Basic Managed Switch Command Line Interface Reference Manual	S1A78426
ConneXium TCSESB Basic Managed Switch Web-based Interface Reference Manual	S1A78429
ConneXium TCSESB Basic Managed Switch Installation Manual	S1A78204

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.

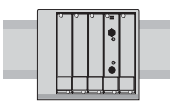
Key

The designations used in this manual have the following meanings:

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

Symbols used:

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

	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.

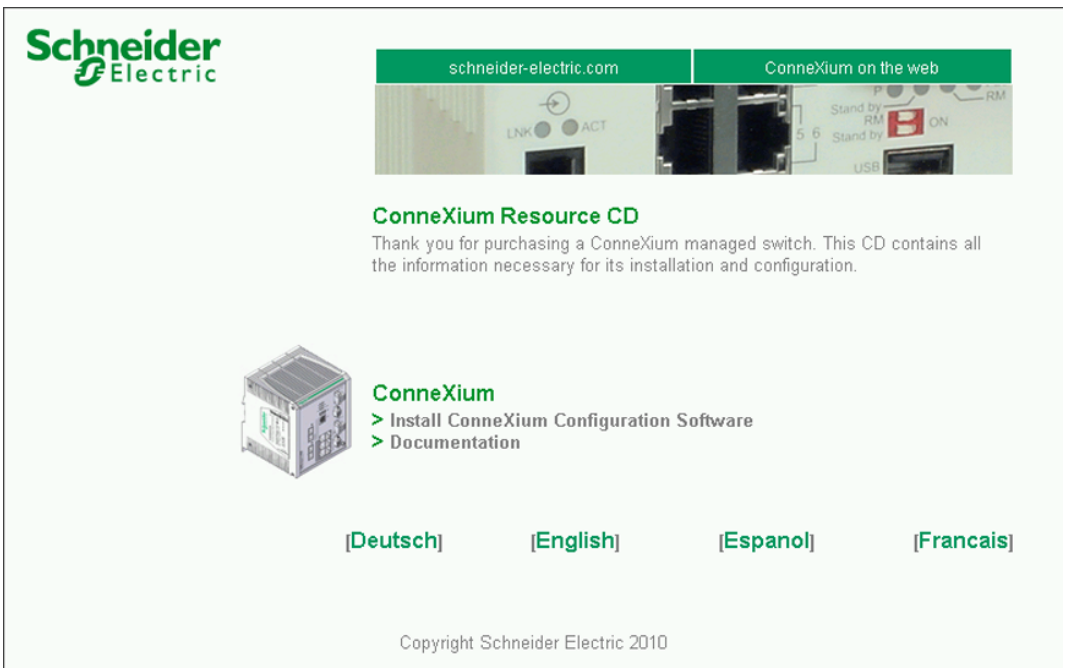


Figure 1: Installing Java

☐ 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.

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 „Loading/Saving the Configuration“)

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.

You can also launch the website for a device via the program. Refer to the "TCSESB Managed Switch Basic Configuration User Manual" for additional information.
Proceed as follows:
☐ Start the program.
☐ Select the device by clicking on the corresponding device line.
☐ Click in the menu bar on ”Edit“ and select the menu item ”Start Web Interface“, or click on the button bar on the ”WWW“ symbol.

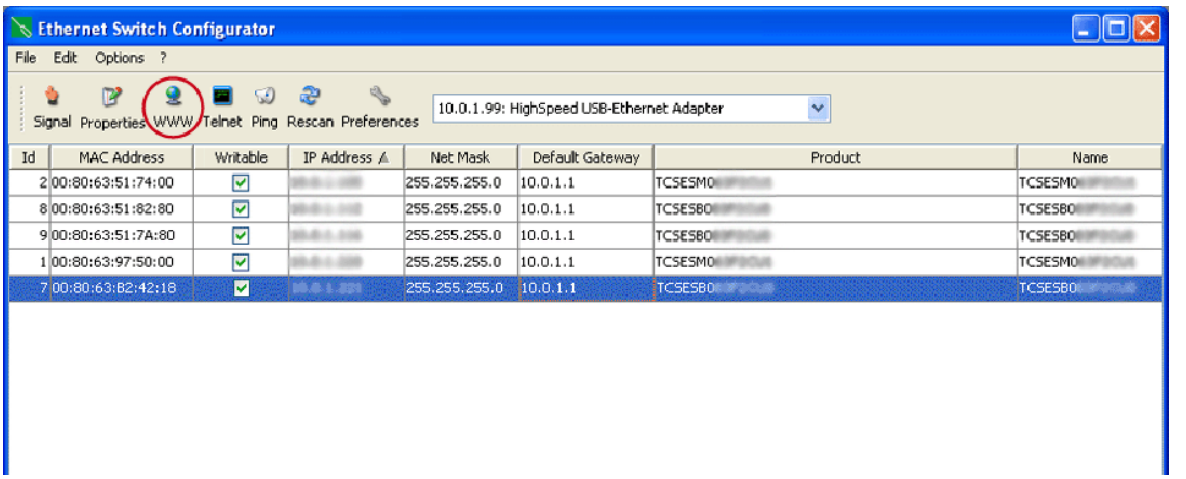


Figure 3: Launching the device website via Ethernet Switch Configuration Adapter

The website of the device appears on the screen.

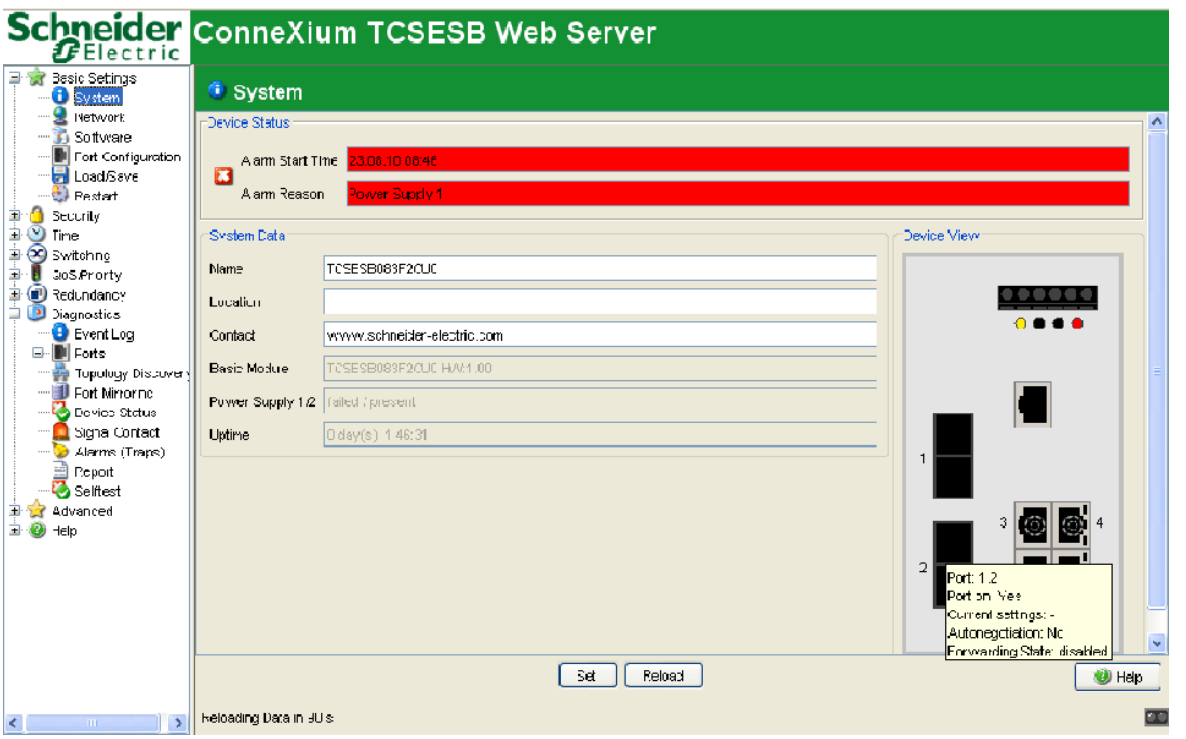
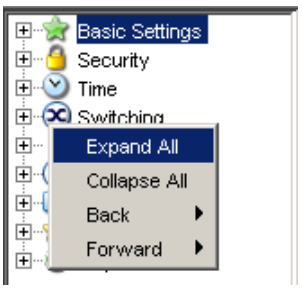


Figure 4: Website of the device with speech-bubble help

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

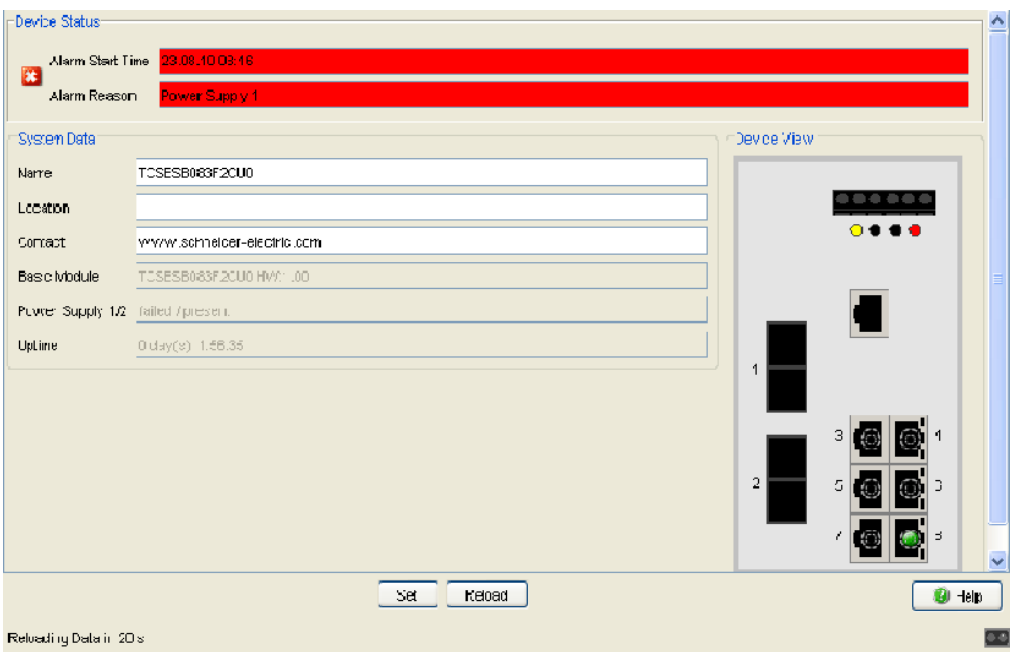


Figure 5: "System" Submenu

Device Status

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

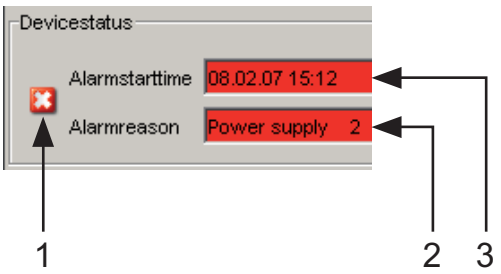


Figure 6: Device status and display of detected alarms
1 - Symbol indicates the Device Status
2 - Cause of the oldest existing alarm detected
3 - Time of the oldest existing alarm detected

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,

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.

Table 1: System Data

Device View

The device view shows the device with the current configuration. The symbols underneath the device view represent the status of the individual ports.

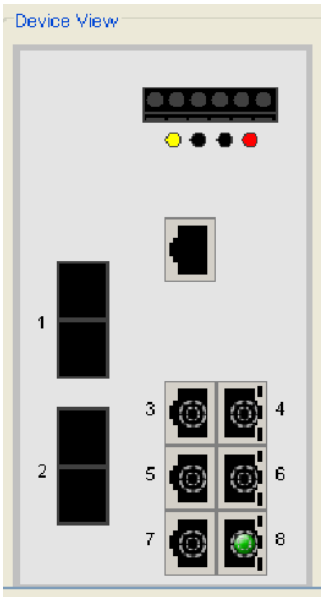


Figure 7: Device View

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.

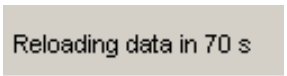


Figure 8: Time until update

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 configure the access.

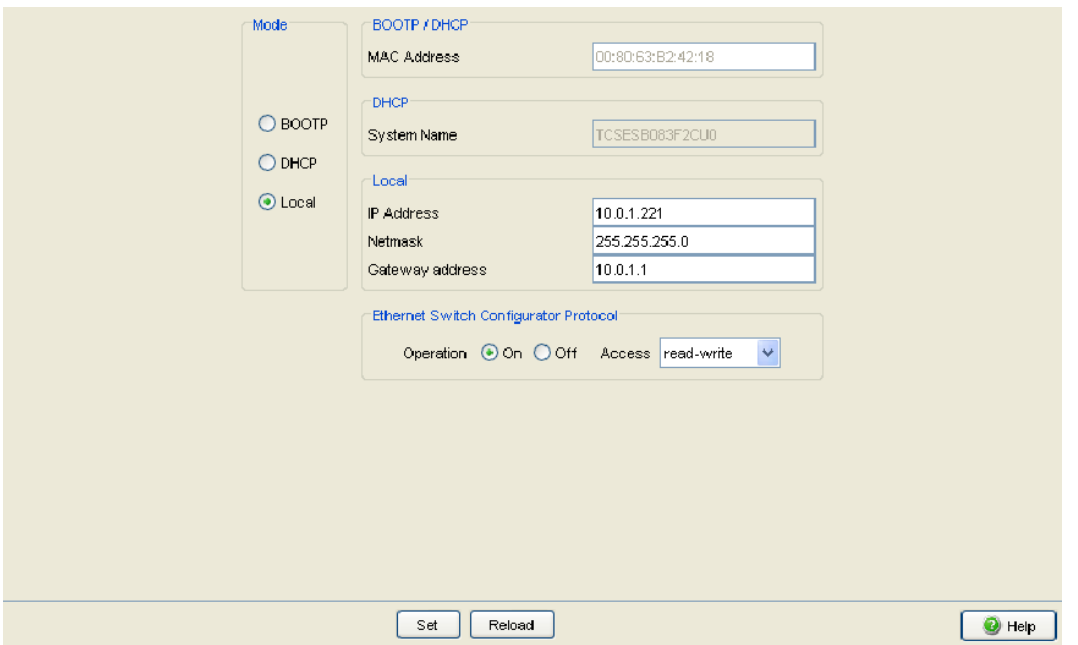


Figure 9: Network parameters dialog

☐ 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.

☐ 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 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 display the software versions in the device and to carry out a software update of the device via file selection.

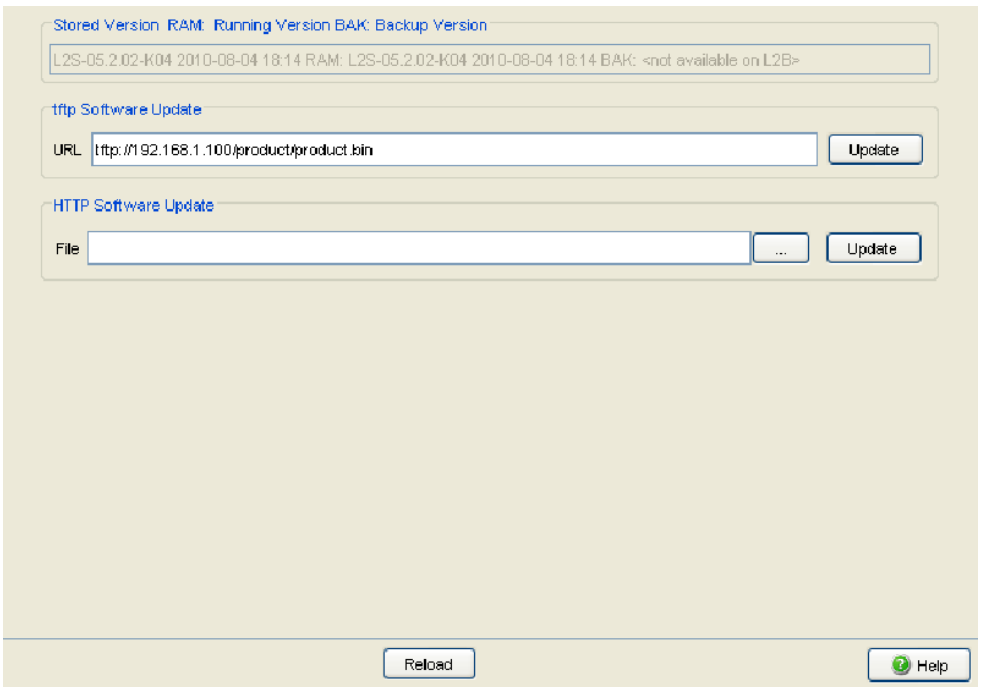


Figure 10: Software dialog

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.

1.4 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)
- 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).

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

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

Table 2: Port Settings for Ring Ports

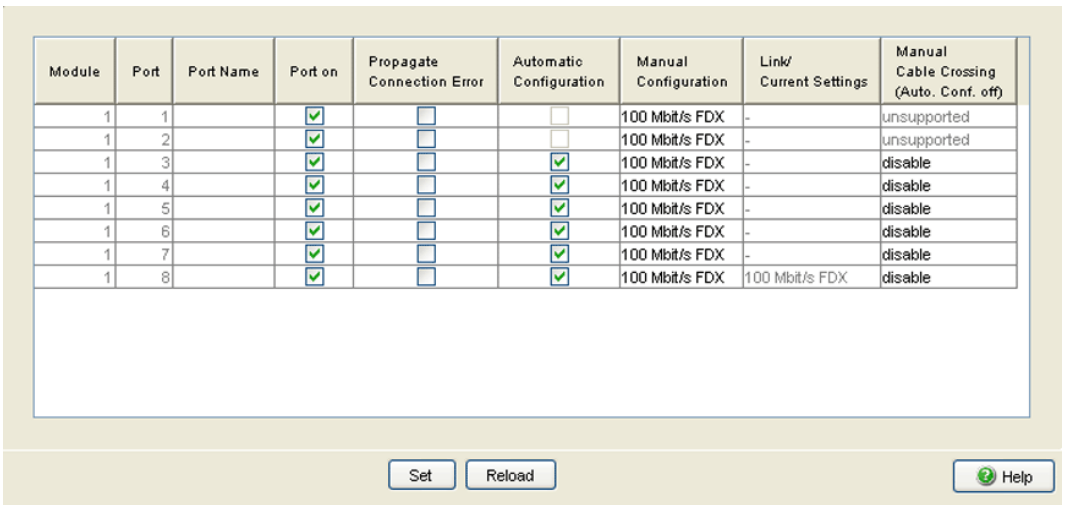


Figure 11: Port Configuration Table Dialog

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 TCSEAM0200 for loading/saving the configuration,
- cancel a configuration change.

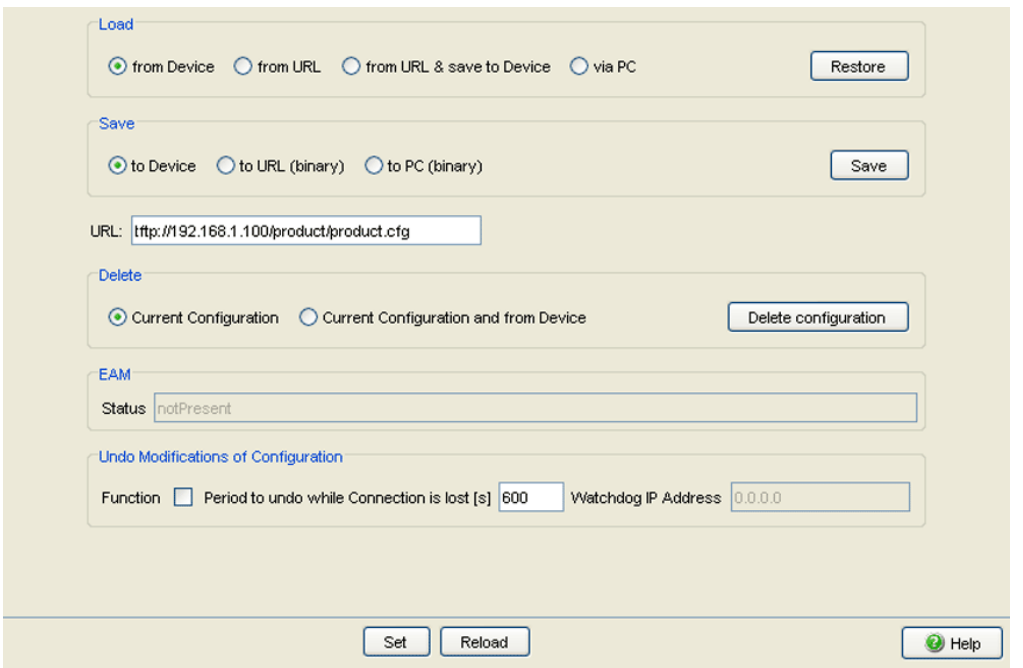


Figure 12: Load/Save dialog

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,
- save the current configuration in binary form on the PC,

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.

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 Adapter (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: TCESEB Basic switches use Memory Backup Adapter: TCSEAM0200.

- 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[a], or - no configuration file is present on the EAM or on the device[b].
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

[a] 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.,
[b] 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.

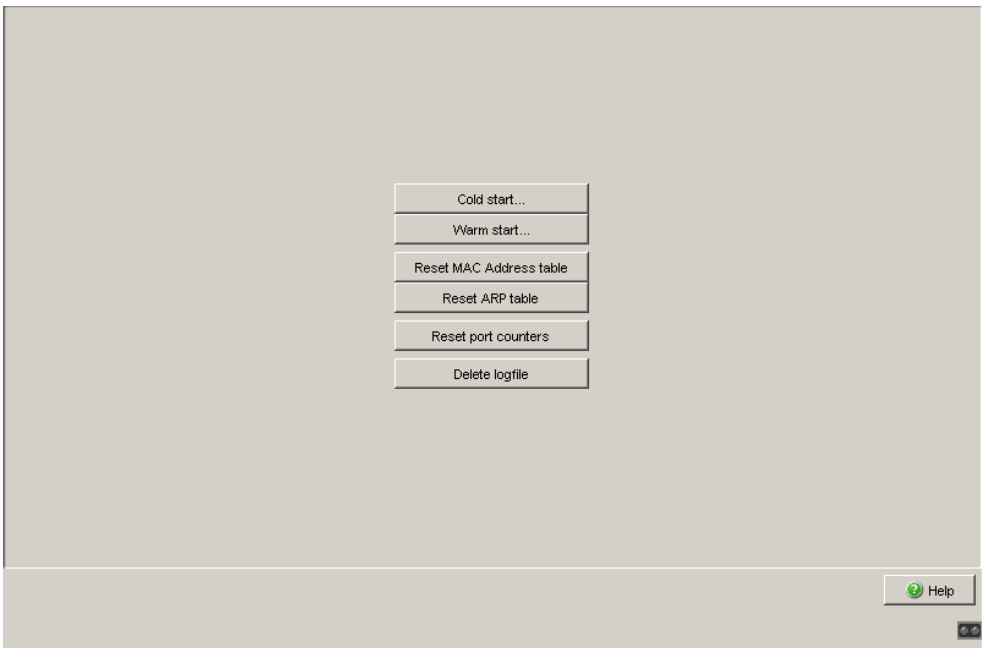


Figure 13: Restart Dialog

2 Security

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

- Password/SNMPv3 access
- SNMPv1/v2 access
- Web access

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). Please note that passwords are case-sensitive.
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”.

☐ 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.

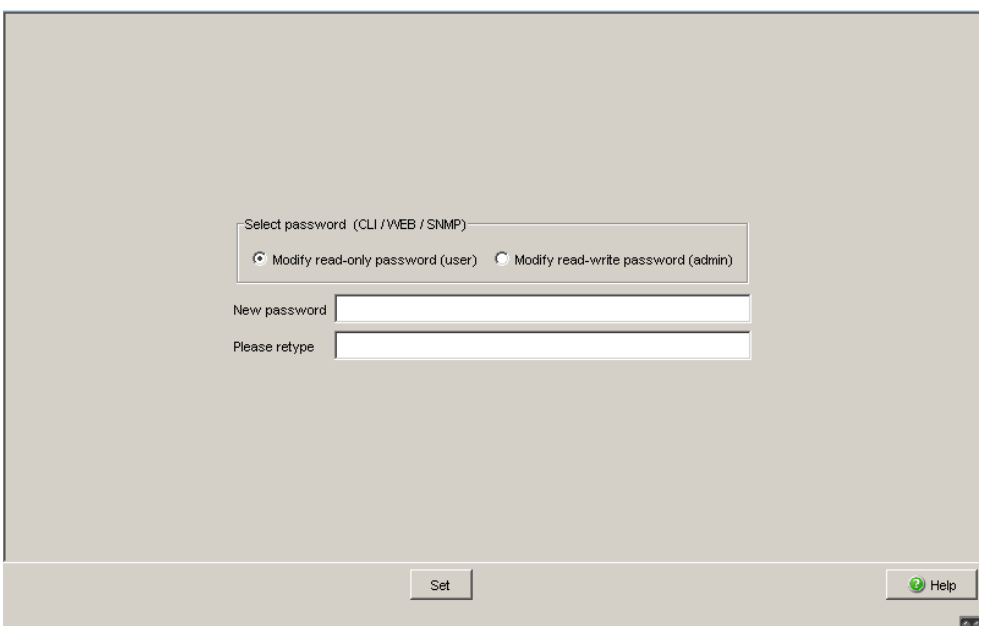


Figure 14: Dialog Password/SNMP Access

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 via a Web browser can be blocked in a separate dialog (see on page 45 „Web Access“).

Access at IP address level is restricted in a separate dialog (see on page 42 „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, you enter the sequential number to which the access restriction applies.
- 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. Please note that 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.

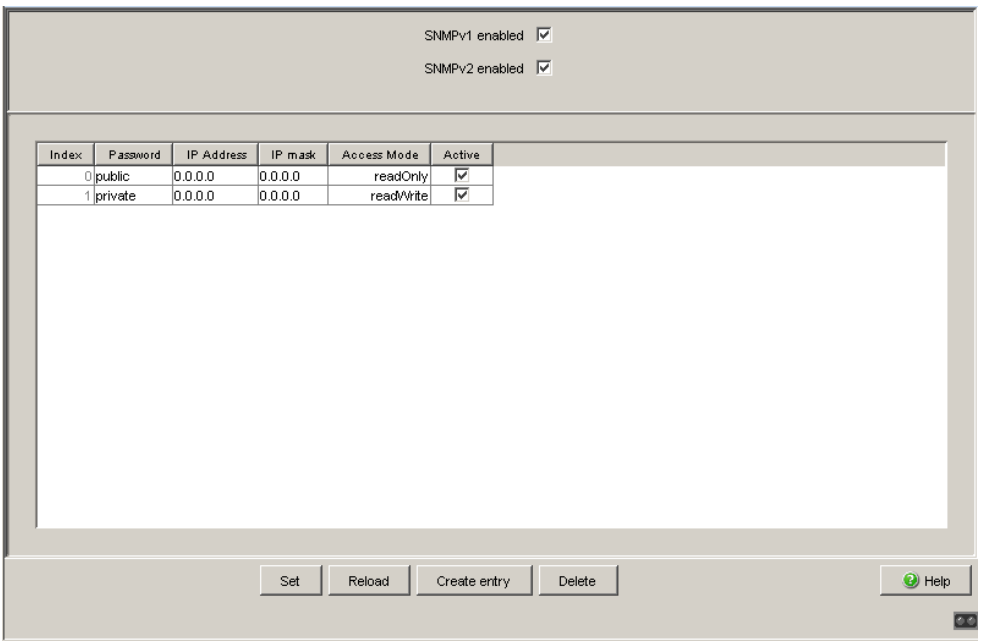


Figure 15: SNMPv1/v2 Access Dialog

2.3 Web Access

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

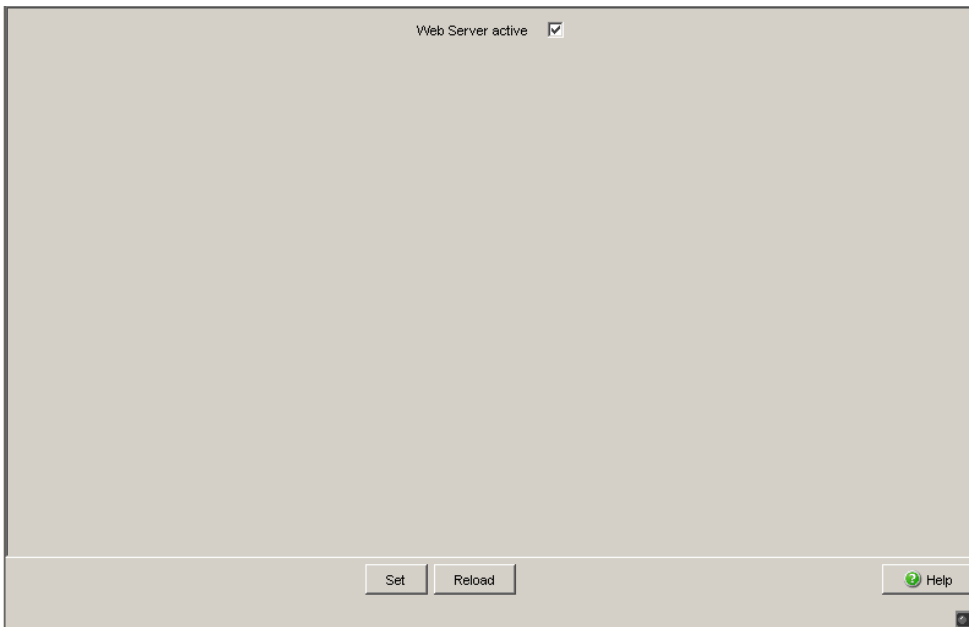


Figure 16: Web Access dialog

2.3.1 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.

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.

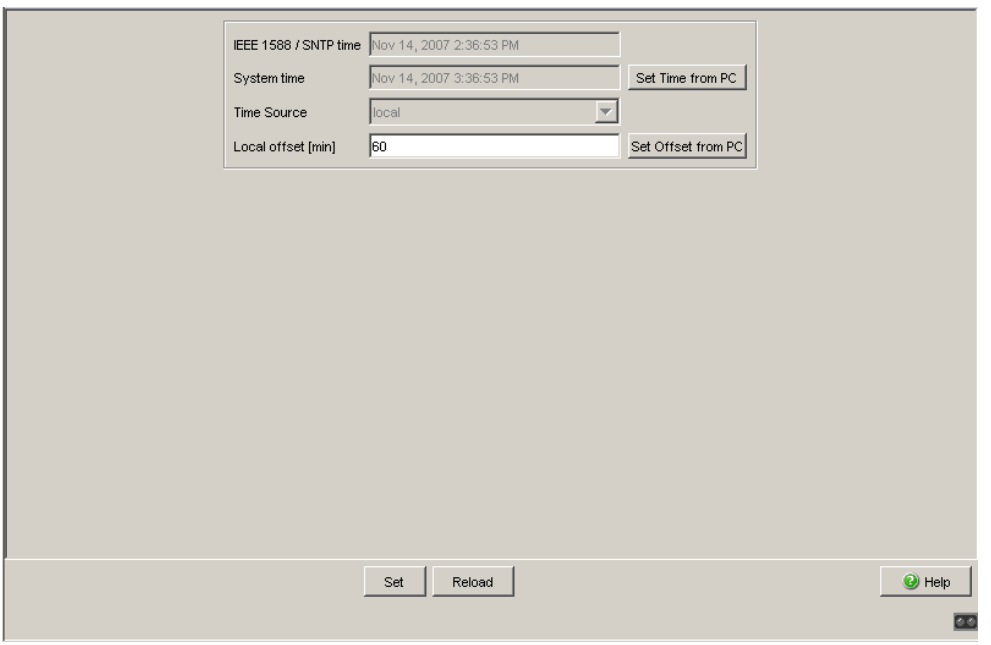


Figure 17: Time Dialog

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 very 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
Function	Switch the SNTP function on and off In this frame you switch the SNTP function on/off. When it is switched off, the SNTP server does not send any SNTP packets or respond to any SNTP requests. The SNTP client does not send any SNTP requests or evaluate any SNTP Broadcast/Multicast packets.

Table 4: Configuration SNTP Client and Server

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

Table 5: SNTP Status

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 7).	Valid IPv4 address	0.0.0.0
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 6: Configuration SNTP Server

IP destination address	Send SNTP packets periodically to
0.0.0.0	Nobody
Unicast	Unicast
224.0.1.1	Multicast
255.255.255.255	Broadcast

Table 7: Periodic sending of SNTP packets

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^{31}-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.

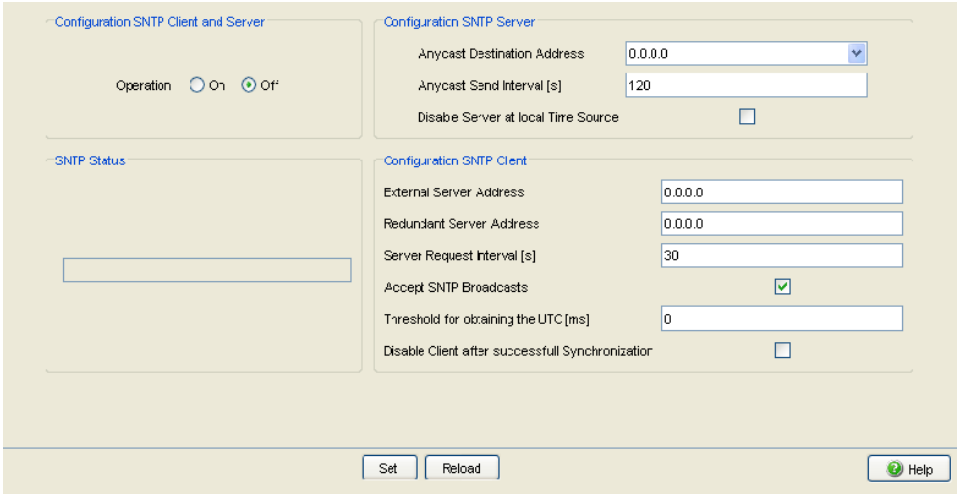


Figure 18: SNTP Dialog

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 assumes one clock is the most accurate and thus enables precise synchronization of all clocks in a 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.

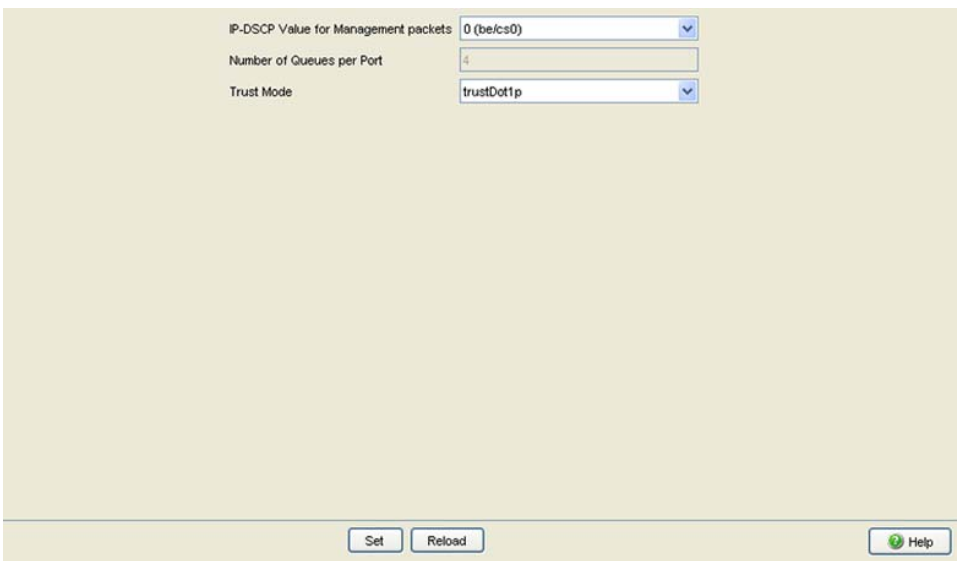


Figure 19: Dialog PTP

4 Switching

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

- Switching Global
- Filters for MAC Addresses
- Multicasts

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

Table 9: Switching:Global dialog

Figure 20: 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 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.

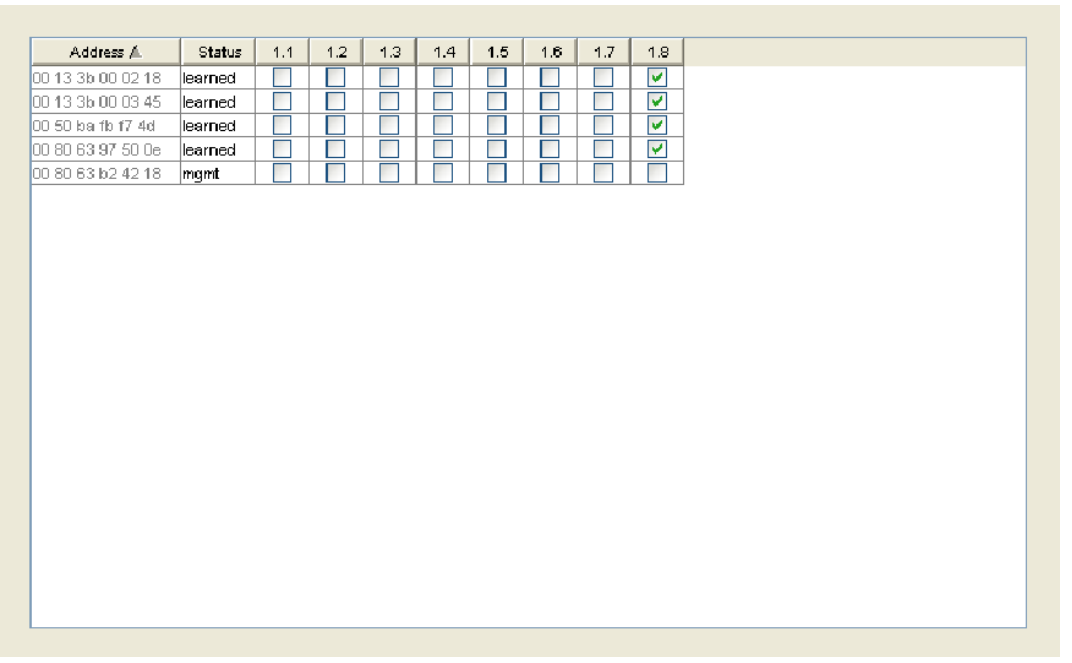


Figure 21: Filter Table dialog

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

4.3 Multicasts

With this dialog you can:
- activate/deactivate the IGMP Snooping protocol,
- configure the IGMP Snooping protocol globally and per port.

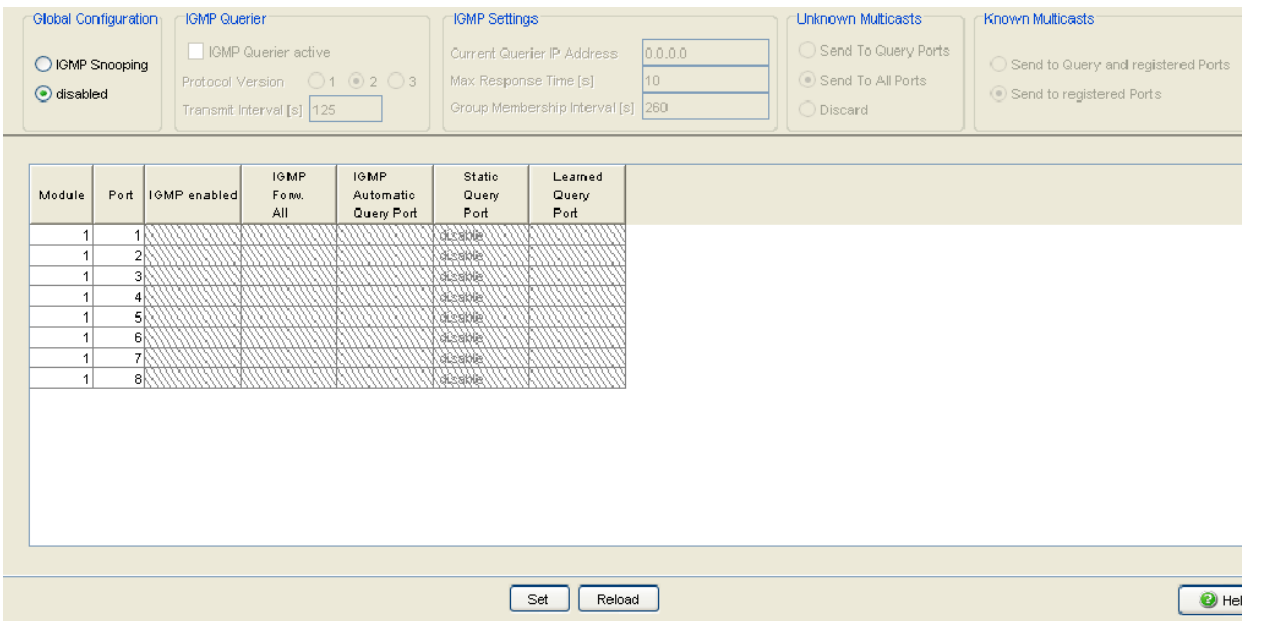


Figure 22: Multicasts dialog

4.3.1 Global Configuration

In this frame you can:
- activate/deactivate the IGMP Snooping protocol.

Parameter	Meaning	Default setting
IGMP Snooping	Activate IGMP Snooping globally for the entire device.	deselected
disabled	Deactivate IGMP Snooping globally for the entire device. If IGMP Snooping is switched off: ▶ the device does not evaluate Query and Report packets received, and ▶ it sends (floods) received data packets with a Multicast address as the destination address to all ports.	selected

Table 10: Global setting

4.3.2 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
IGMP Querier			
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, thus generating a network load.	2-3599 s[a]	125 s
IGMP settings			
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 - 1,2: 1-25 s[a] - 3: 1-3598 s[a]	10 s
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[a]	260 s

Table 11: IGMP Querier and IGMP settings

a.) Note the connection between the parameters Max. Response Time, Send Interval and Group Membership Interval, (see table 12)

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 12: 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.

4.3.3 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
Unknown Multicasts			
	▶ Send to Query Ports: The device sends the packets with an unknown MAC/IP Multicast address to all query ports. ▶ Send to All Ports: The device sends the packets with an unknown MAC/IP Multicast address to all ports. ▶ Discard: The device discards all packets with an unknown MAC/IP Multicast address.	Send to Query Ports, Send to All Ports, Discard	Send to All Ports
Known Multicasts			
	▶ Send to query and registered ports: 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. ▶ Send to registered ports: 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.	Send to query and registered ports, send to registered ports	Send to registered ports

Table 13: 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.

4.3.4 Settings per Port (Table)

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

- IGMP

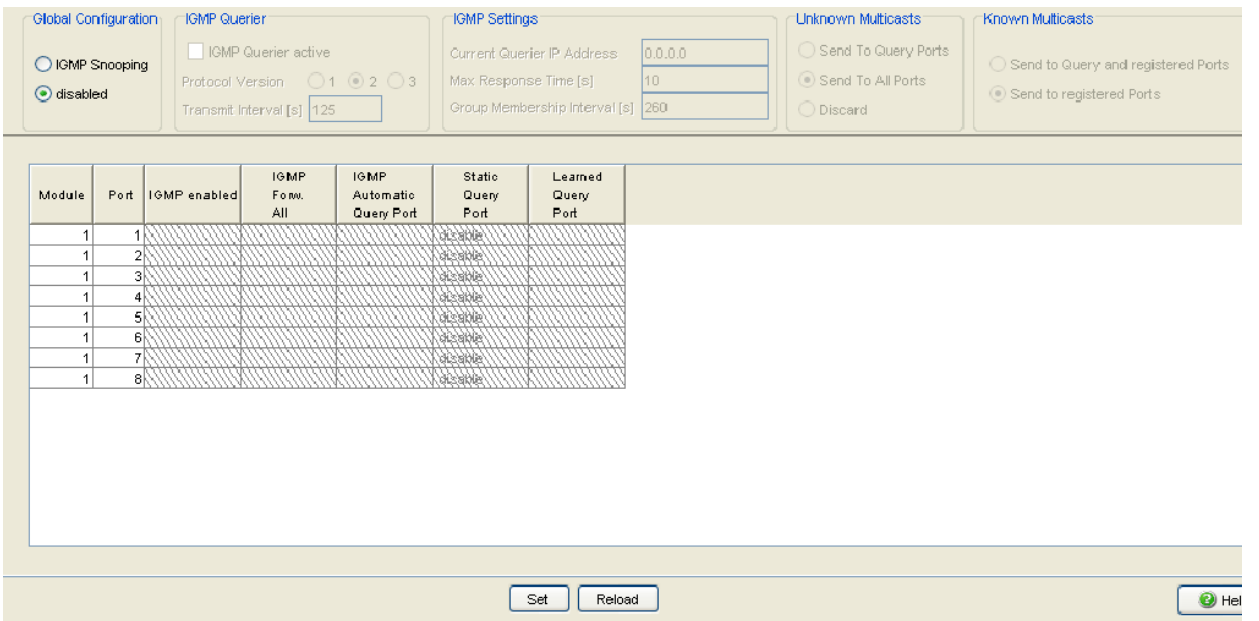


Figure 23: Port-related settings

Parameter	Meaning	Value range	Default setting
Module	Module number for modular devices, otherwise 1.		
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 `Switching:Multicasts:IGMP` dialog, IGMP is enabled.	`on`, `off`	`on`
IGMP Forward All	Switch the IGMP Snooping function “Forward All” on/off. With the `IGMP Forward All` setting, the device sends to this port all data packets with a Multicast address in the destination address field. Prerequisite: In the `Switching:Multicasts:IGMP` dialog, IGMP is enabled. **Note:** 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. **Note:** 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 “automatic” is selected in “Static Query Port”. Prerequisite: In the `Switching:Multicasts:Global Setting` dialog, the `IGMP Snooping` mode is selected.	`yes`, `no`	-

Table 14: Settings per port

Parameter	Meaning	Value range	Default setting
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: In the `Switching:Multicasts:Global Setting` dialog, the `IGMP Snooping` mode is selected.	`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 `Switching:Multicasts:IGMP` dialog, IGMP is enabled.	`yes`, `no`	-

Table 14: 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.

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 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 19).

  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 .

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
2	4	5
3	6	7

Table 15: VLAN priority remarking

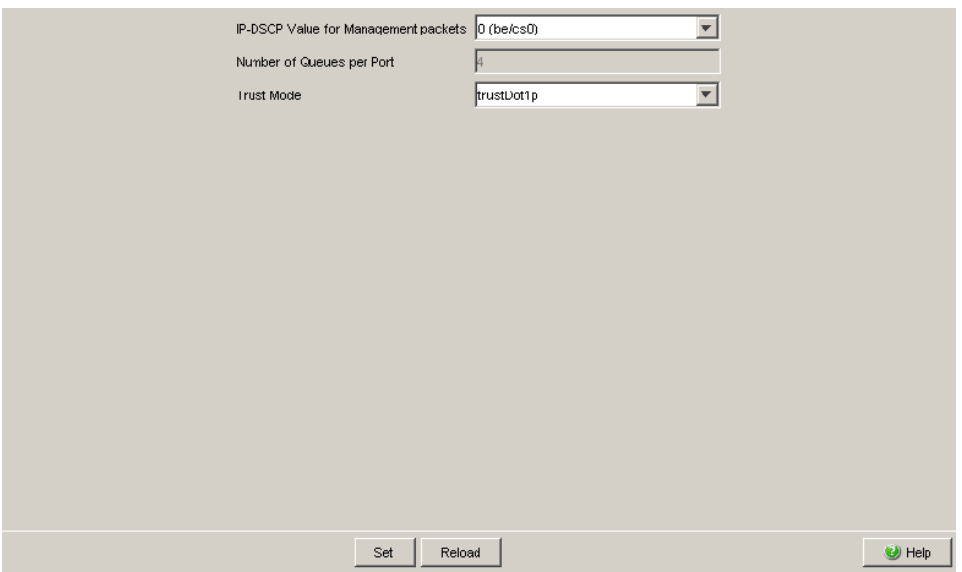


Figure 24: Global dialog

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 16: Port configuration table

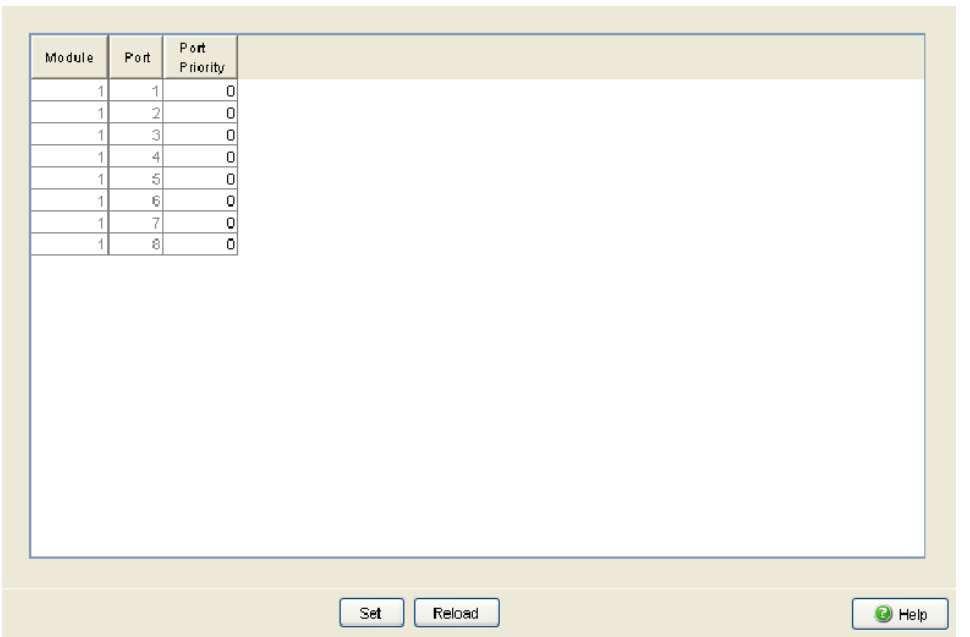


Figure 25: Port configuration dialog

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 17).
Prerequisite:
setting in the `Global:Trust Mode dialog: untrusted` (see on page 68 „Global“) or
setting in the `Global:Trust Mode dialog:trustDot1p`(see on page 68 „Global“) and the data packets do not contain a VLAN tag or
setting in `Global:Trust Mode dialog: trustIpDscp`(see on page 68 „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 17: Assigning the port priority to the 4 traffic classes

5.3 802.1D/p mapping

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

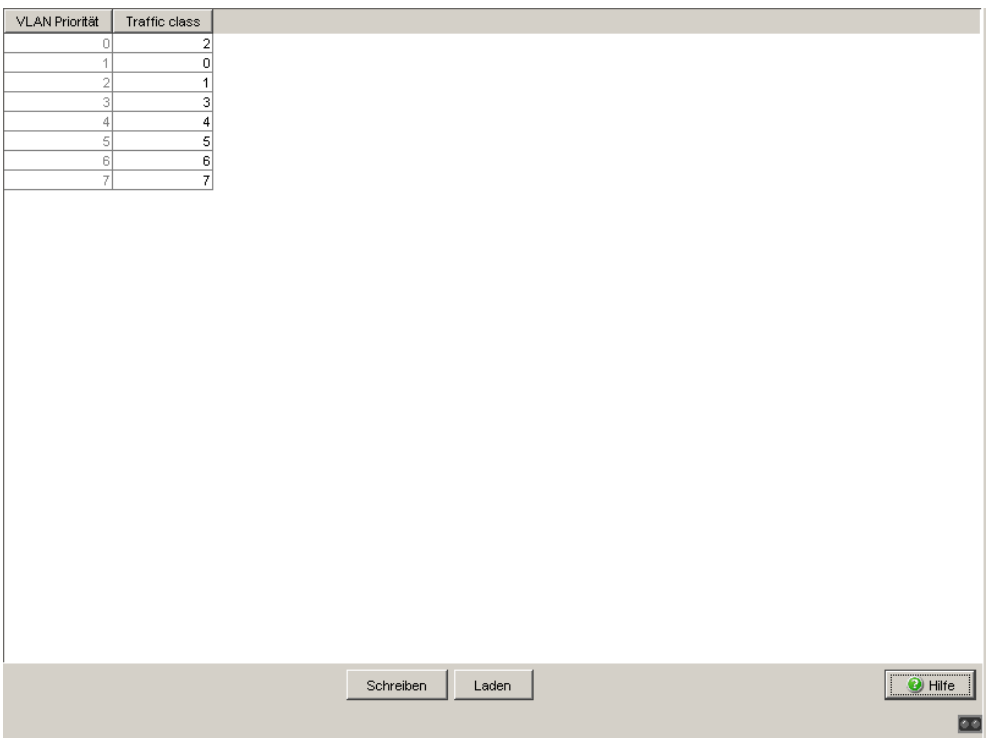


Figure 26: 802.1D/p Mapping dialog

☐ 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 18: 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).

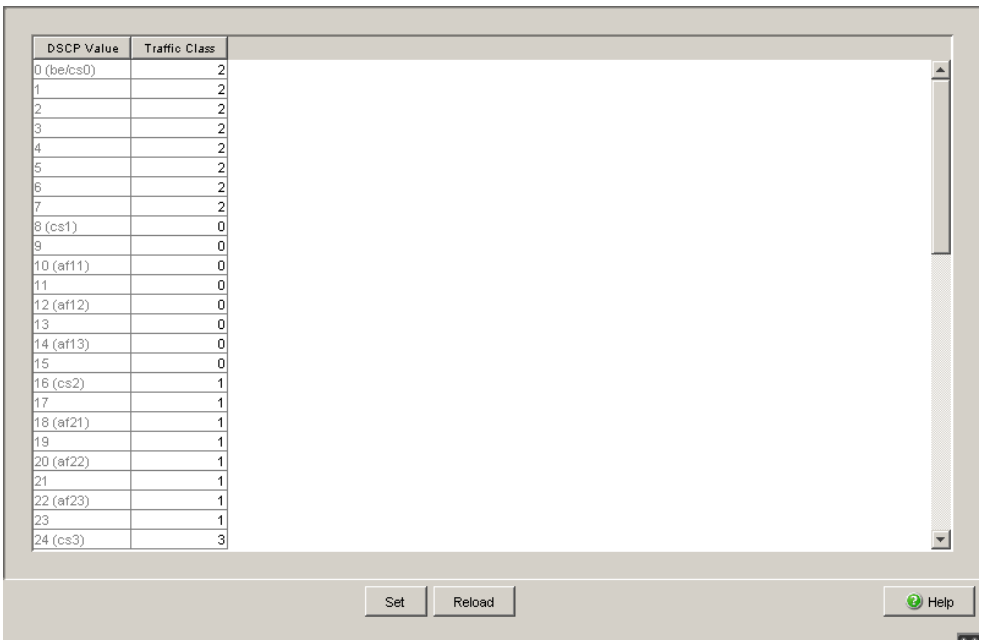


Figure 27: IP DSCP mapping table

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 19: 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
- Rapid Spanning Tree Protocol (RSTP)

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-(**HI**GH **PE**RFORMANCE **R**EDUNDANCY) Ring with up to 50 devices typically transforms back to a line structure within 80 ms (possible settings: standard/accelerated).
- MRP (**M**edia **R**edundancy **P**rotocol) 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).

With the help of the **R**ing **M**anager (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
  - TCSESB
- Within an MRP-Ring, you can use devices that support the MRP protocol based on IEC62439.
  - TCSESM
  - TCSESM-E
  - TCSESB

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`
	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 20: 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

Table 21: 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 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: `active:` This port is switched on and has a link. `inactive:` This port is switched off or it has no link.
Redundancy Manager Status (Ring Manager)	Status information, no input possible: `Active (redundant line)`: the redundant line was closed because a data line or a network component within the ring is down. `Inactive:` the redundant ring is open, and all data lines and network components are working.
Redundancy Manager Mode (Ring Manager)	If there is exactly one device, you switch the Ring Manager function on at the ends of the line.

Table 22: HIPER-Ring configuration

Parameter	Meaning
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. ▶ `Standard`: test packet timeout 480 ms ▶ `Accelerated`: test packet timeout 280 ms **Note:** 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.
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 22: HIPER-Ring configuration

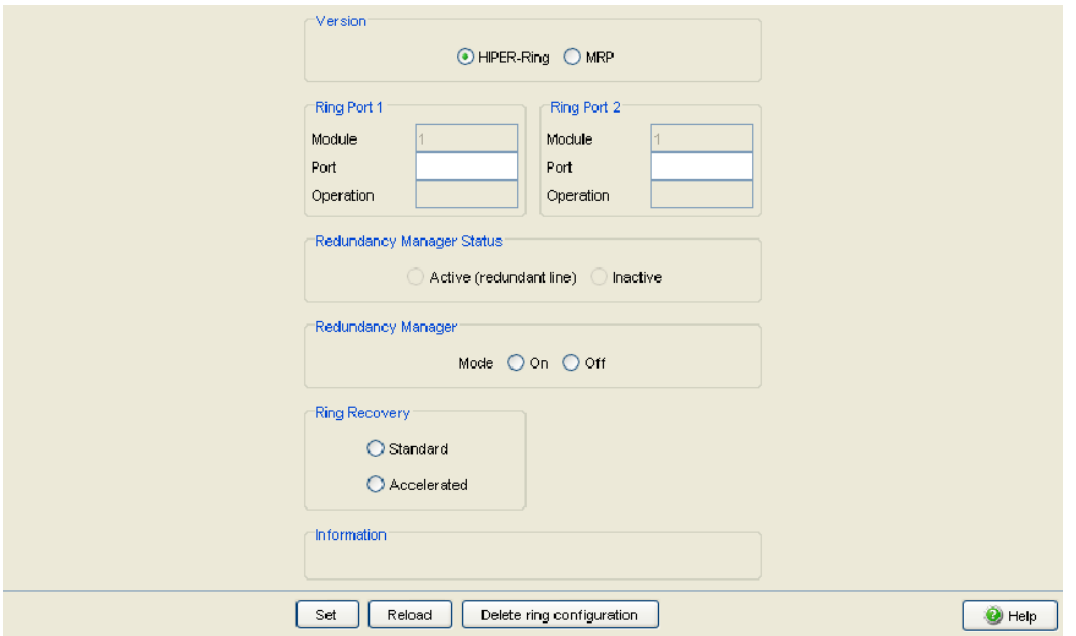


Figure 28: Selecting ring redundancy, entering ring ports, enabling/disabling ring manager and selecting ring recovery.

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

Note: When activating the HIPER-Ring function, 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.

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

Table 23: 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 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: `forwarding:` This port is switched on and has a link. `blocked:` This port is blocked and has a link. `disabled:` This port is switched off. `not connected:` 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. **Note:** 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. `Note:` Settings in the “Ring Recovery” frame are only effective for devices that are ring managers.
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 24: MRP-Ring configuration

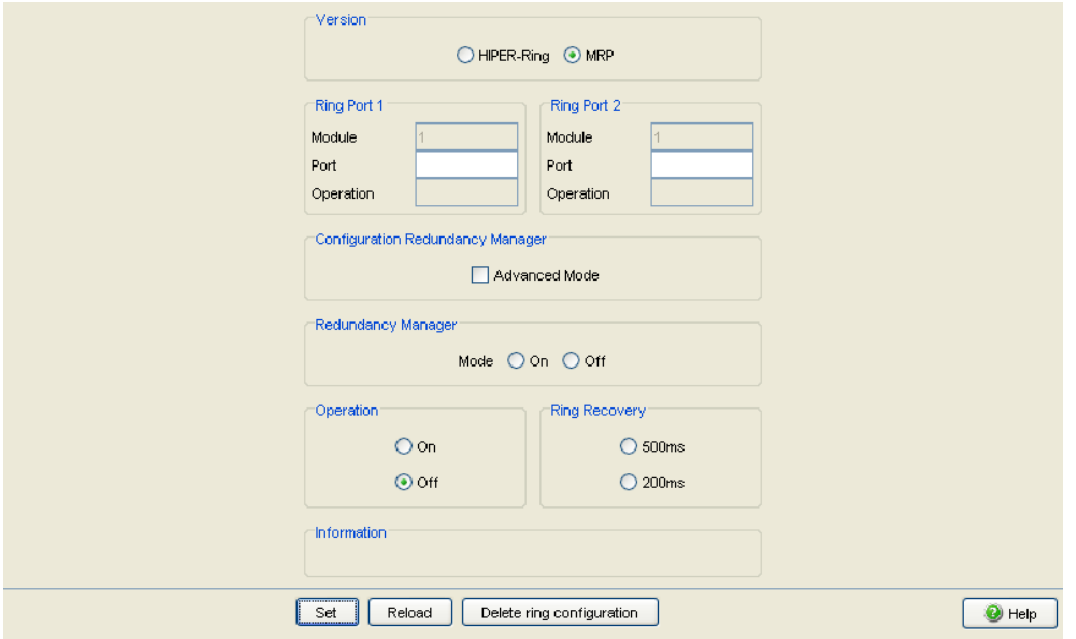


Figure 29: Selecting MRP-Ring version, entering ring ports and enabling/disabling ring manager

Note: For all devices in an MRP-Ring, activate the MRP compatibility in the `Redundancy:Spanning Tree:Global` dialog if you want to use RSTP in the MRP-Ring. If this is not possible, perhaps because individual devices do not support the MRP compatibility, you deactivate the Spanning Tree protocol at the ports connected to the MRP-Ring. Spanning Tree and Ring Redundancy affect each other.

Note: 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 avoid a connection interruption for devices outside the Ring.

6.2 Rapid Spanning Tree

With this dialog you can:
- switch the Rapid Spanning Tree Protocol on/off
- display bridge-related information on the Spanning Tree Protocol
- configure device-related parameters of the Rapid Spanning Tree Protocol
- set port-related parameters of the Rapid Spanning Tree Protocol.

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

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

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

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

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

Note: RSTP reduces a layer 2 network topology with redundant paths into a tree structure (Spanning Tree) that does not contain any more redundant paths. One of the 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: 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.

6.2.1 Global

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.

Parameter	Meaning	Possible Values	Default Setting
Function	Switch the RSTP function for this device “On” or “Off”. If you switch off the RSTP for a device globally, the device floods the RSTP packets received like normal Multicast packets to the ports. Thus the device behaves transparently with regard to RSTP packets.	on, off	
MRP compatibility	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. 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 avoid a connection interruption for devices outside the Ring.	`On`, `Off`	Off
Root Information	In every RSTP environment, there is a root Switch that is responsible for controlling the RSTP function. The parameters of the current root Switch are displayed here. – **Root ID:** Displays the bridge identifier of the root Switch. This is made up of the priority value and the MAC address of the device. “This device is root”: A checkmark shows that the device is currently the root Switch. – **Root Port:** Displays the port that leads to the root Switch. If you have configured the device itself as the root Switch, 0.0 is displayed. – `Root Cost:` Displays the root costs to the root Switch. If you have configured the device itself as the root Switch, 0 is displayed for the costs.		

Table 25: Global Spanning Tree settings, basic function

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 ≤ n*4096 ≤ 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 25: Global Spanning Tree settings, basic function

Parameter	Meaning	Possible Values	Default Setting
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).		
Topology Changes	This field displays the number of changes since RSTP started.		
Time since last change	This field displays the time that has elapsed since the last network reconfiguration.		
Information	This frame shows whether there is a configuration conflict. In this case, the device with the MAC address displayed is located outside the MRP-Ring. The priority displayed for this device is better (numerically smaller) than the priority of the root bridge in the MRP-Ring. To resolve this conflict, set the device displayed to a worse priority (numerically greater) than the priority of the root bridge in the MRP-Ring.		

Table 25: Global Spanning Tree settings, basic function

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

`Forward Delay` ≥ (`Max Age`/2) + 1

If you enter values that violate this rule, the device will replace these values by the last valid values or the default values.

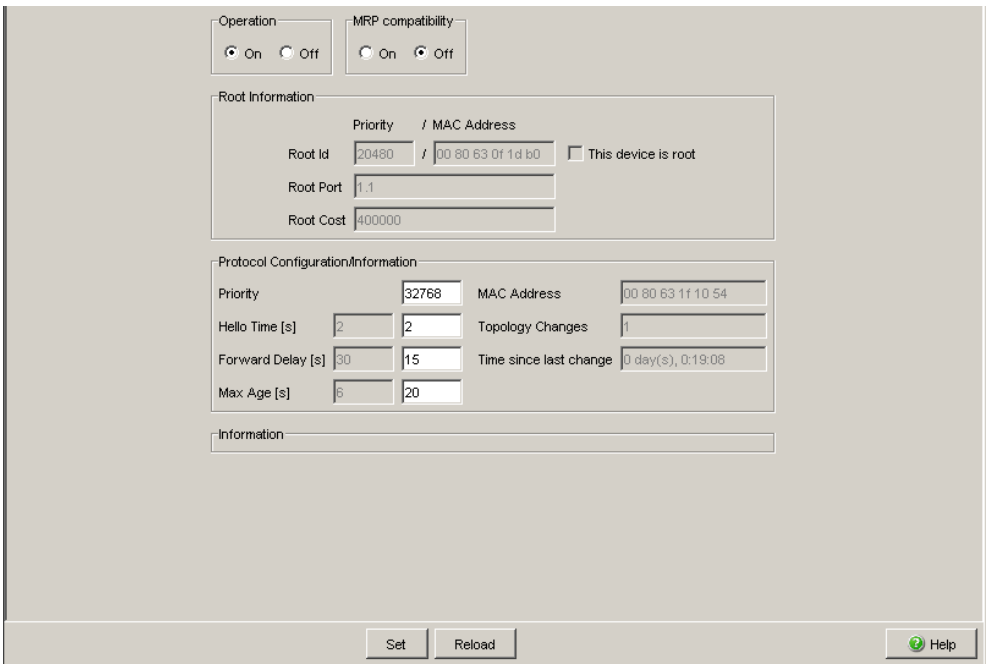


Figure 30: RSTP global dialog

6.2.2 Rapid Spanning Tree Port

Parameter	Meaning	Possible Values	Default Setting
STP State	Here you can turn RSTP on or off for this port. If you turn RSTP off for this port while RSTP is globally enabled for the device, the device will discard RSTP frames received on this port.	on, off	on
Port state	Displays the port state.	disabled, forwarding, discarding, blocking, learning	-
Port Priority	Here you enter the first byte of the port identificatio.	16 ≤ n·16 ≤ 240	128
Port Path Cost	Enter the path costs to indicate preference for redundant paths. If the value is 0, the Switch automatically calculates the path costs according to the transmission rate.	0 - 200.000.000	0
Admin EdgePort	If the parameter is set to "true“, the port will transition to the forwarding state. If the port nevertheless receives an RSTP frame, it will transition to the blocking state and the bridge will then determine the new port role. .If the parameter’s value is "false“, the port remains in the blocked state until the bridge has determined the port role. Only after that will the port transition to its final state.	true, false	false
Oper-Edge-Port	Is "true“ if no RSTP frames have been received, i. e., a terminal device that does notsend RSTP frames is connected to this port. Is "false“ if RSTP frames have been received, i. e., no terminal device but a bridge is connected.	true, false	-

Table 26: Port-related RSTP settings and displays

Parameter	Meaning	Possible Values	Default Setting
Auto Edge Port	The setting for Auto Edge Port only takes effect if the parameter "Oper Edge Port“ has been set to "false“. if "Auto Edge Port“ is set to "true“, the port will transition to the forwarding state within 1.5 * Hello Time (3 seconds). If is is set to "false“, it will take 30 seconds until the edge port forwards data frames.	true, false	true
Oper PointToPoint	If there is a full-duplex connection between two RSTP devices at this port, Oper PointToPoint is “true”; otherwise “false” is displayed (e.g. if a hub is connected). The point-to-point connection makes a direct connection between two RSTP devices. The direct, decentralized communication between the two Switches results in a fast reconfiguration time.	true, false	auto (determined from duplex mode: FDX: true HDX: false)
Designated Root	Displays the bridge identification of the designated root bridge for this port.	Bridge identification (hexadecimal)	-
Designated Cost	Display of the costs for the path from this port to the root Switch.	Cost	-
Designated Port	Display of the port identifier (on the designated Switch) of the port that connects to the root bridge - for the local port.	Port identification (hexadecimal) and port number	-

Table 26: Port-related RSTP settings and displays

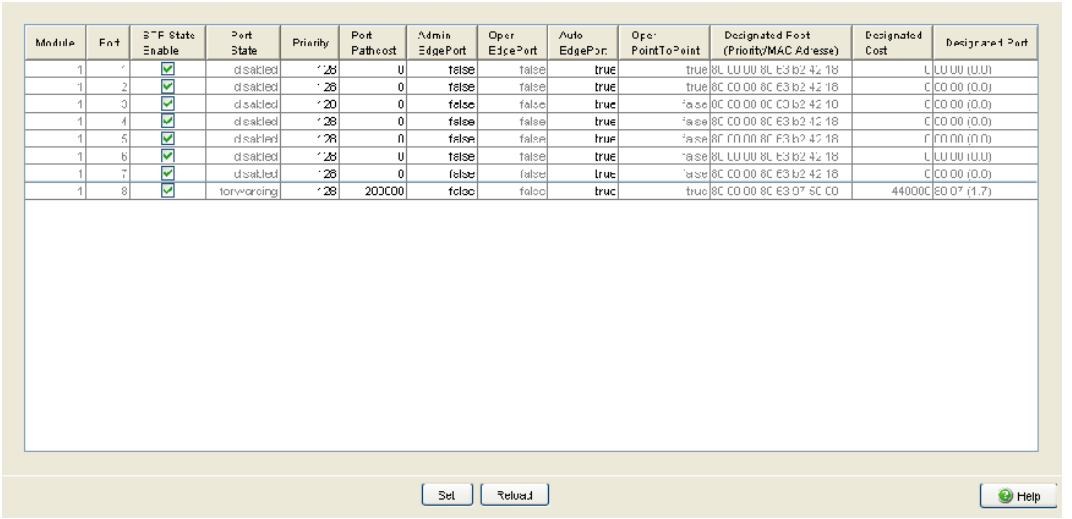


Figure 31: RSTP Port dialog

7 Diagnostics

The diagnosis menu contains the following tables and dialogs:

- Event Log
- Ports (statistics, utilization)
- Topology Discovery
- Port Mirroring
- Device Status
- Signal Contact
- Alarms (Traps)
- Report (log file, system information)
- Self Test

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

7.1 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.

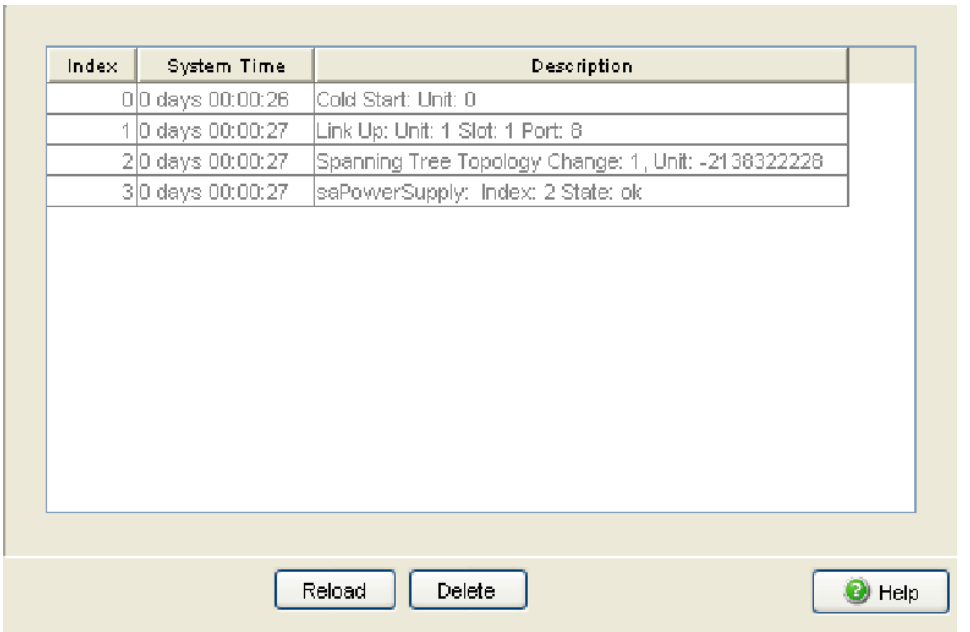


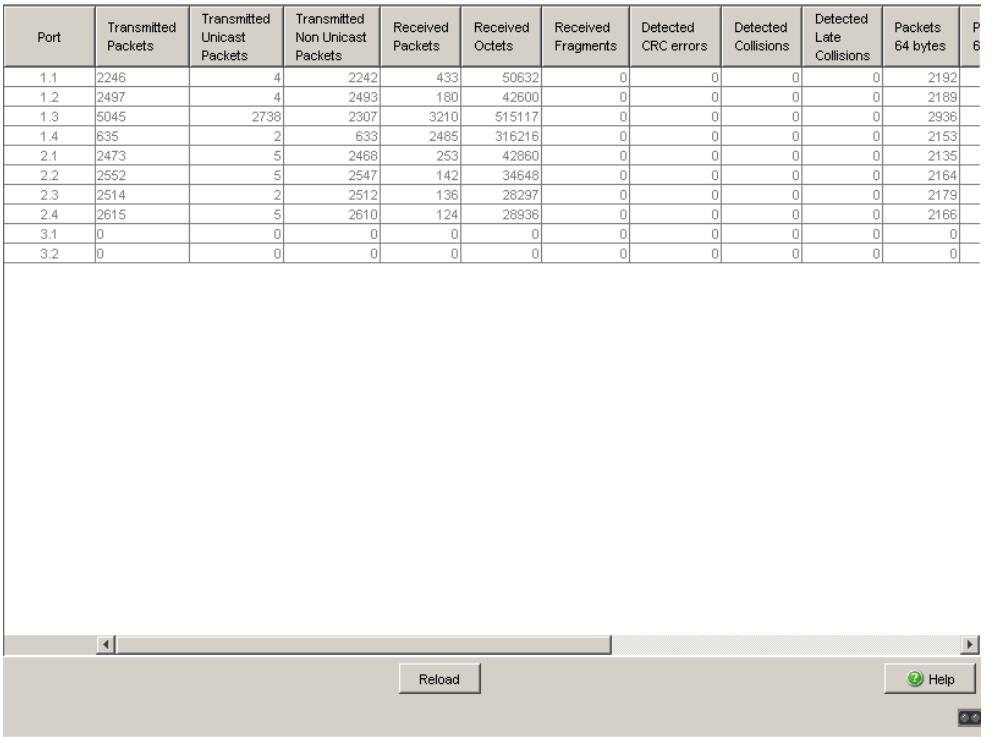
Figure 32: Event log table

7.2 Ports

The port menu contains displays and tables for the individual ports:
- Statistics table
- Utilization

7.2.1 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.



Port	Transmitted Packets	Transmitted Unicast Packets	Transmitted Non Unicast Packets	Received Packets	Received Octets	Received Fragments	Detected CRC errors	Detected Collisions	Detected Late Collisions	Packets 64 bytes
1.1	2246	4	2242	433	50632	0	0	0	0	2192
1.2	2497	4	2493	180	42600	0	0	0	0	2189
1.3	5045	2738	2307	3210	515117	0	0	0	0	2936
1.4	635	2	633	2485	316216	0	0	0	0	2153
2.1	2473	5	2468	253	42860	0	0	0	0	2135
2.2	2552	5	2547	142	34648	0	0	0	0	2164
2.3	2514	2	2512	136	28297	0	0	0	0	2179
2.4	2615	5	2610	124	28936	0	0	0	0	2166
3.1	0	0	0	0	0	0	0	0	0	0
3.2	0	0	0	0	0	0	0	0	0	0

Figure 33: Port statistics, table

7.2.2 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.

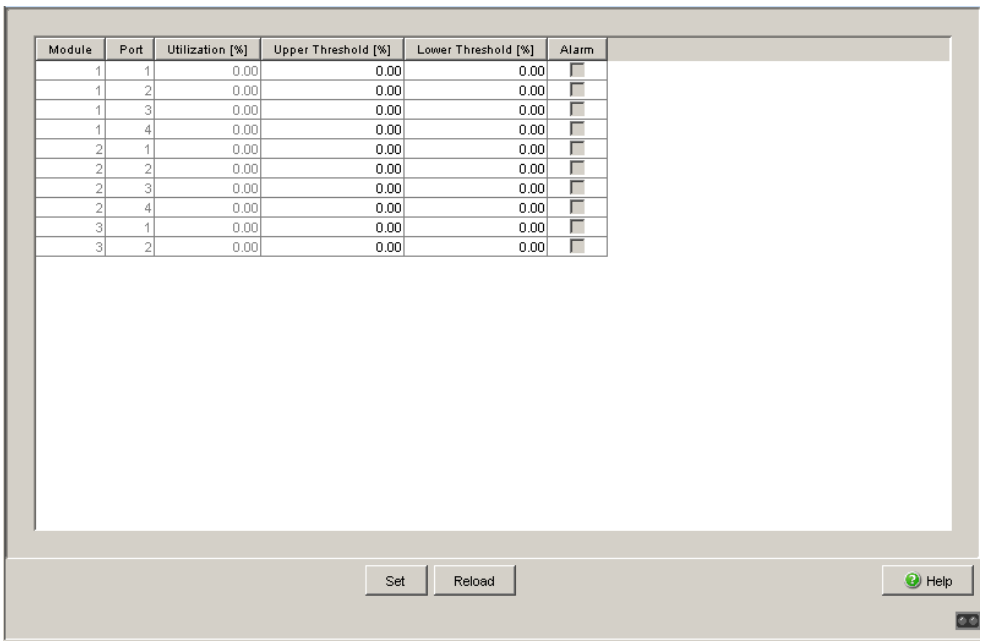


Figure 34: Network load dialog

7.3 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.

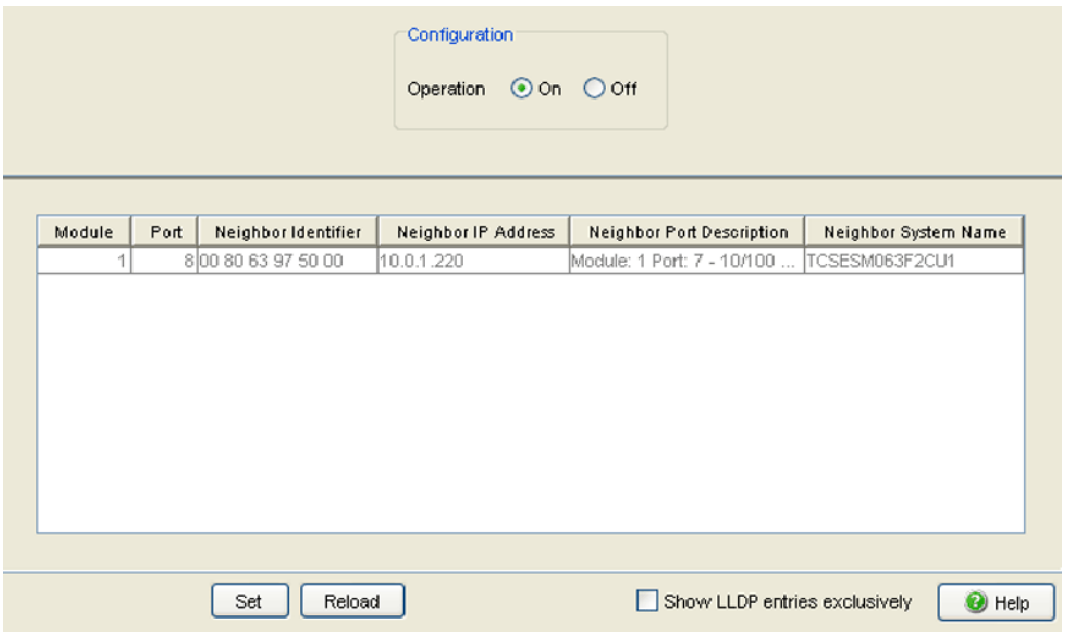


Figure 35: Topology Discovery dialog

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 56 „Switching Global“).

7.4 Port Mirroring

The port mirroring function enables you to review the data traffic at a device port for diagnostic purposes. The device additionally forwards (mirrors) this data to another port. This process is also called port mirroring.
The port to be observed is called the source port. The port to which the data to be observed is copied is called the destination port.

In port mirroring, the device copies valid incoming **and** outgoing data packets of the source port to the destination port. The data traffic at the source port is not influenced by port mirroring.
A management tool connected at the destination port, e.g. an RMON probe, can thus monitor the data traffic of the source port. Set the destination port as a member in all VLANs.
The destination port forwards both data to be sent and received data.

☐ Select the source port whose data traffic you want to observe.

☐ Select the destination port to which you have connected your management tool.

☐ Select "enabled" to switch on the function.

The "Delete" button in the dialog allows you to reset all the port mirroring settings of the device to the state on delivery.

Note: In active port mirroring, the specified port is used solely for observation purposes.

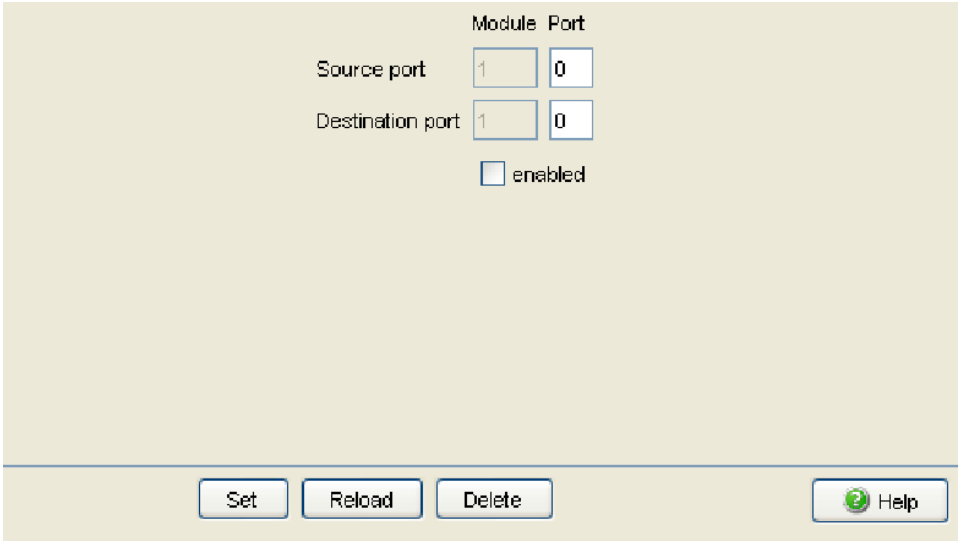


Figure 36: Portmirroring dialog

7.5 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.

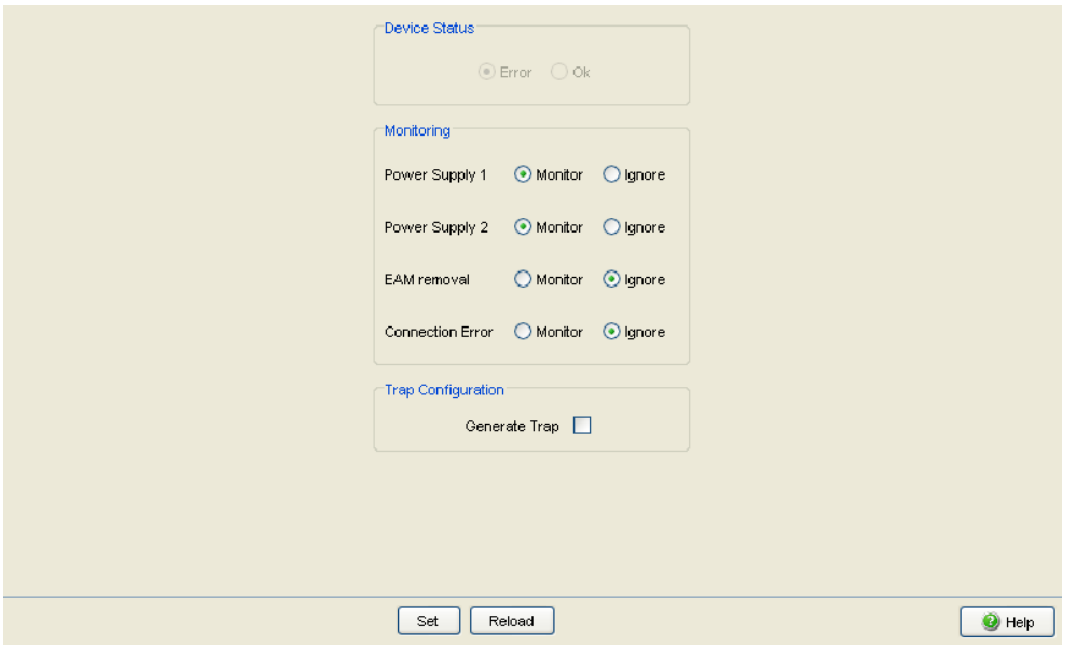


Figure 37: Device Status Dialog

☐ In the "Monitoring" field, you select the events you want to monitor.

The events which can be selected are:

Name	Meaning
Power supply ...	Monitor/ignore supply voltage(s).
EAM removal	Monitor/ignore the removal of the EAM.
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 (see on page 29 „Port Configuration“). 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.

Table 27: Device Status

☐ 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 page 108 „Function monitoring“).

7.6 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.

7.6.1 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.

7.6.2 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.
- 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).
- 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 78 „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 MRP it only reports detected errors in the local configuration.

7.6.3 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 106 „Device Status“) and thereby offers remote diagnosis.
The device status “Error detected” (see on page 106 „Device Status“) is reported by means of a break in the contact via the potential-free signal contact (relay contact, closed circuit).

7.6.4 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.

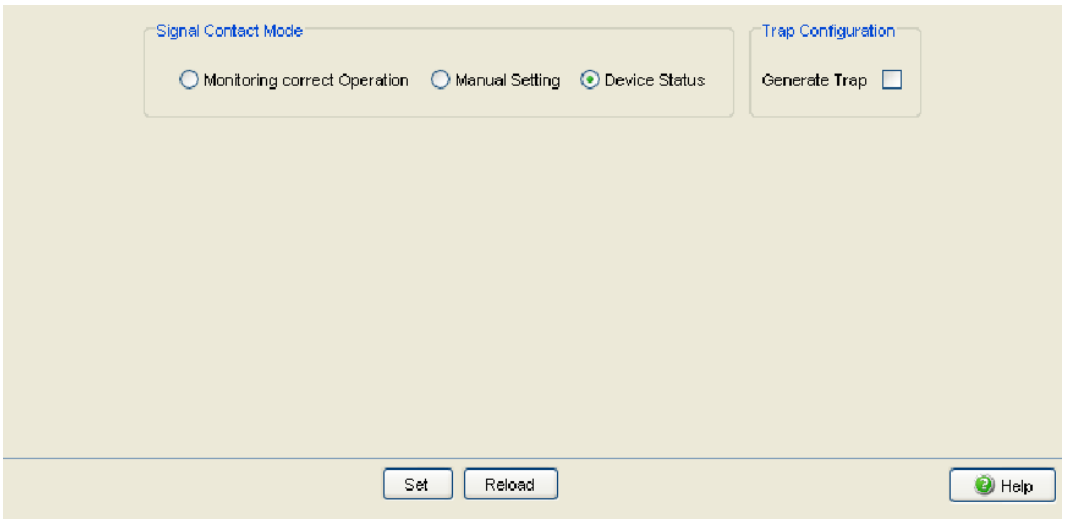


Figure 38: Signal Contact Dialog

7.7 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 "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 (see on page 42 „SNMPv1/v2 Access Settings“).
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: – The status of a supply voltage has changed (see the `System` dialog). – The status of the signal contact has changed. To take this event into account, you activate “Create trap when status changes” in the `Diagnostics:Signal Contact 1/2` dialog. – A media module has been added or removed (only for modular devices). – The Memory Backup Adapter (EAM) has been added or removed.
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.

Table 28: Trap categories

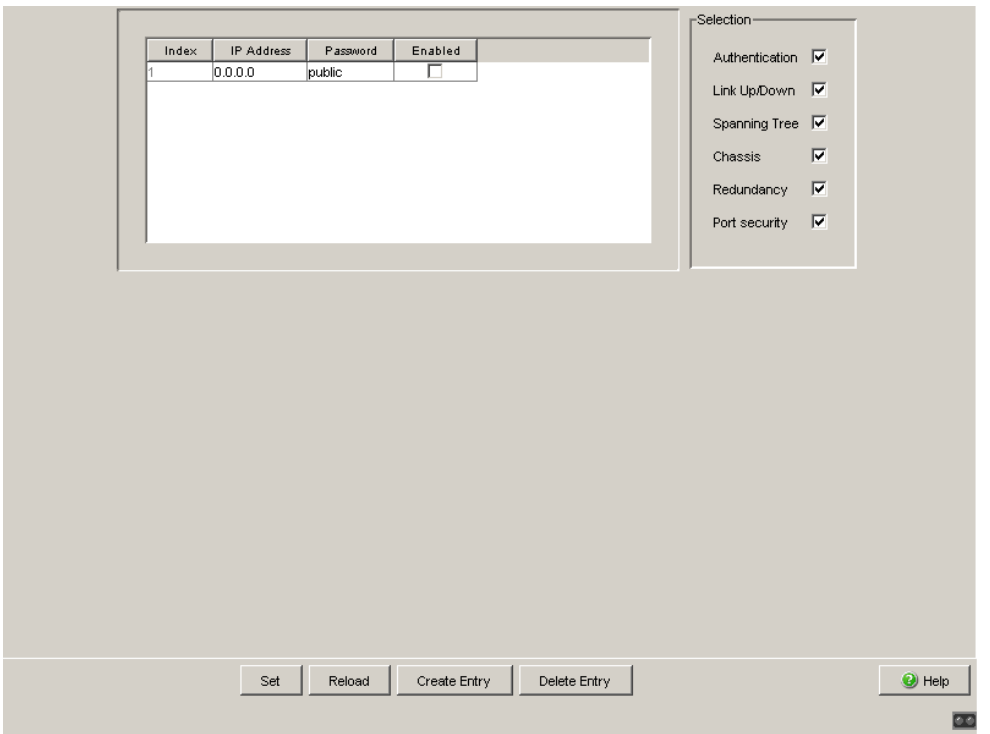


Figure 39: Alarms Dialog

7.8 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.

7.9 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.

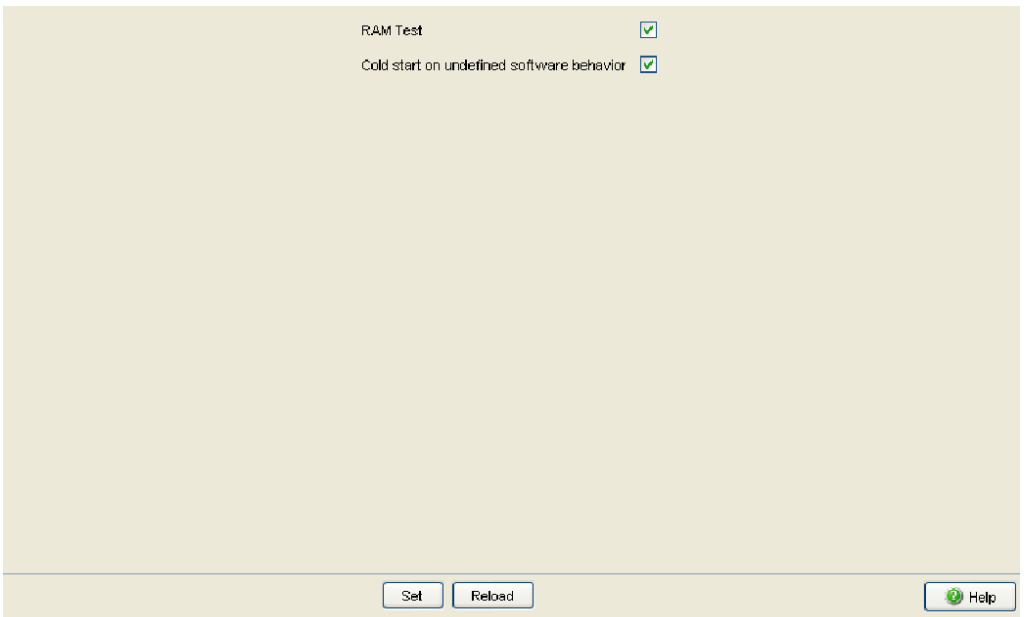


Figure 40: Self-test dialog

8 Advanced

The menu contains the dialogs, displays and tables for:

- DHCP Relay Agent

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.

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:
`B30600000100010100060080630006 1E`

☐ 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.

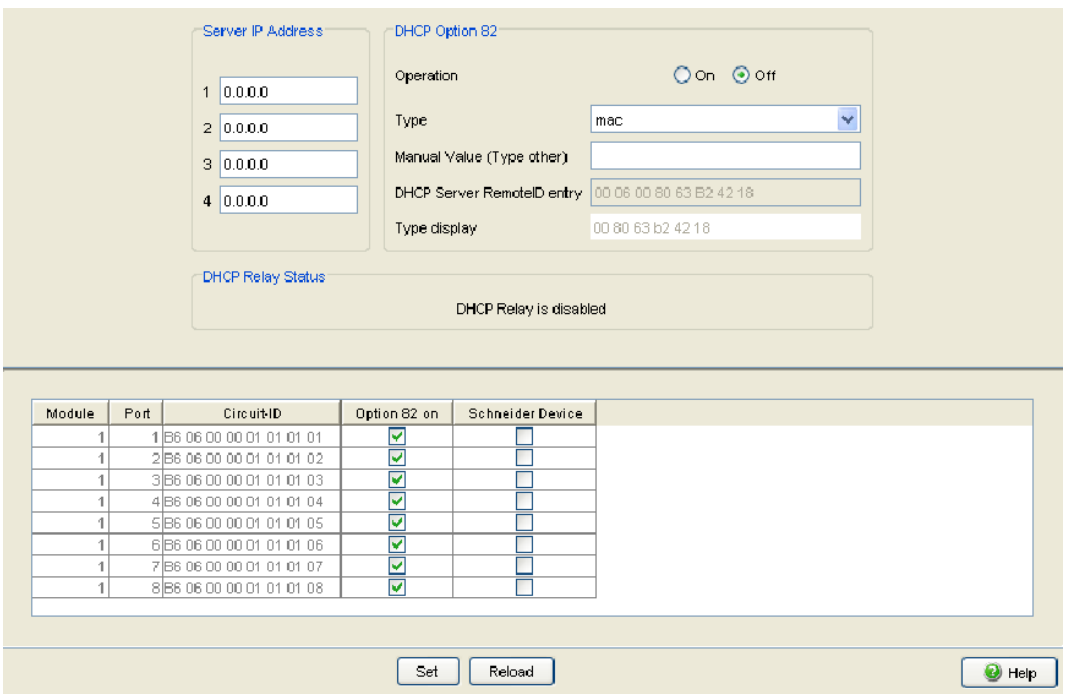


Figure 41: DHCP Relay Agent dialog

A Appendix

A.1 Technical Data

Switching	
Size of MAC address table (incl. static filters)	2,048
Max. number of statically configured multicast MAC address filters	64
Max. number of statically configured unicast MAC address filters	100
Max. length of over-long packets (from rel. 03.0.00)	1,552 bytes

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)

A.5.2 Broadcom Corporation

B Index