HIRSCHMANN

A BELDEN BRAND

Reference Manual

Web-based Interface
Industrial ETHERNET Switch
RSB20, OCTOPUS OS20/OS24 Managed

RM Web L2B
Release 5.3 05/2012

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

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

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

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

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

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

Contents

About this Manual

The “Web-based Interface” reference manual contains detailed information on using the Web interface to operate the individual functions of the device.

The “Command Line Interface” Reference Manual contains detailed information on using the Command Line Interface to operate the individual functions of the device.

The “Installation” user manual contains a device description, safety instructions, a description of the display, and the other information that you need to install the device.

The “Basic Configuration” user manual contains the information you need to start operating the device. It takes you step by step from the first startup operation through to the basic settings for operation in your environment.

The Industrial HiVision Network Management Software provides you with additional options for smooth configuration and monitoring:

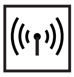
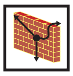
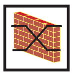
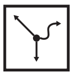
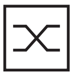
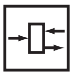
- Simultaneous configuration of multiple devices
- Graphic interface with network layout
- Auto-topology discovery
- Event log
- Event handling
- Client/server structure
- Browser interface
- ActiveX control for SCADA integration
- SNMP/OPC gateway.

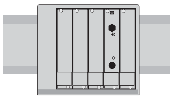
Key

The designations used in this manual have the following meanings:

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

Symbols used:

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

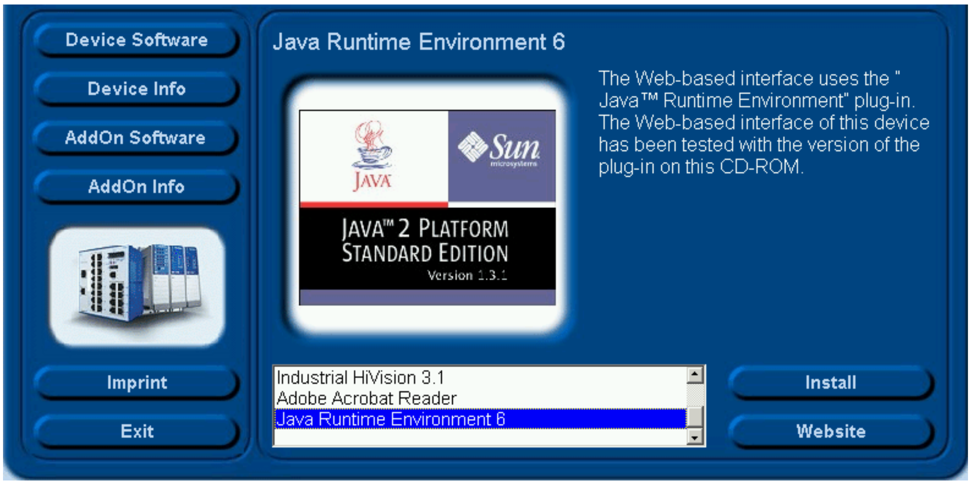
✳	Hub
🖥	A random computer
🟦	Configuration Computer
🗄	Server
	PLC - Programmable logic controller
	I/O - Robot

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 “Additional Software”, select `Java Runtime Environment` and click on “Installation”.



Java Runtime Environment 6

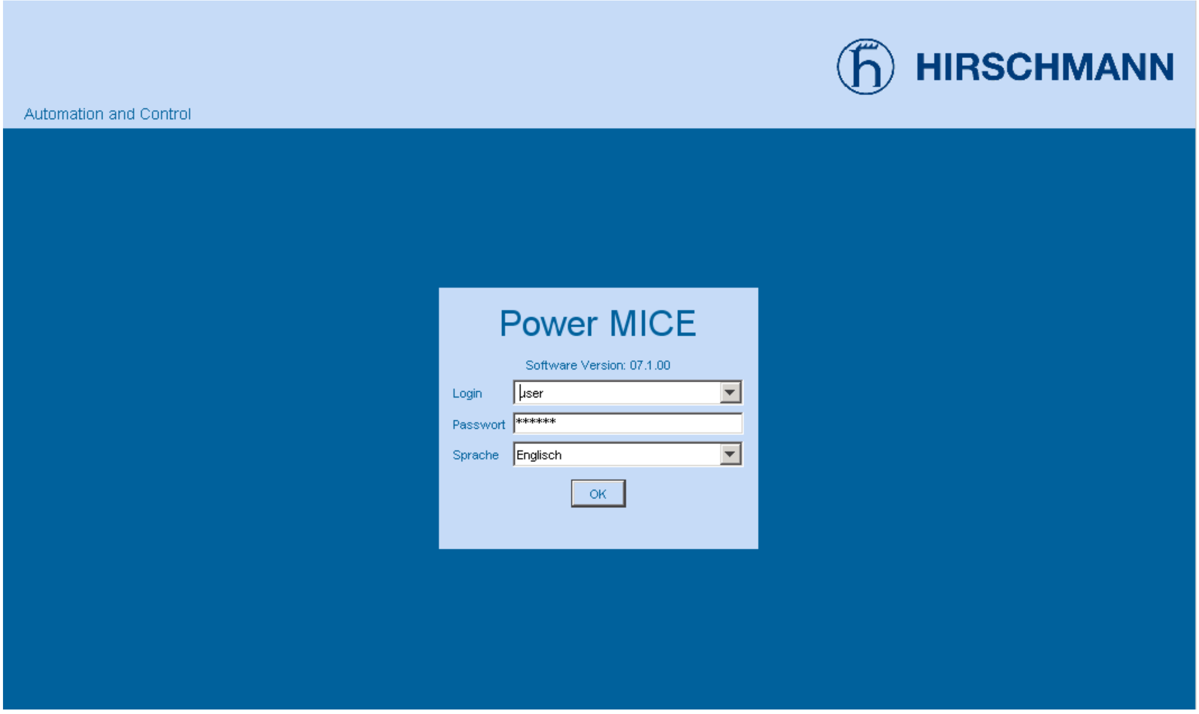
The Web-based interface uses the " Java™ Runtime Environment" plug-in. The Web-based interface of this device has been tested with the version of the plug-in on this CD-ROM.

Industrial HiVision 3.1
Adobe Acrobat Reader
Java Runtime Environment 6

Figure 1: Installing Java

□ Start your Web browser.
□ Verify that you have activated Java in the security settings of your Web 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.



Power MICE

Software Version: 07.1.00

Login: user

Passwort: ******

Sprache: Englisch

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.

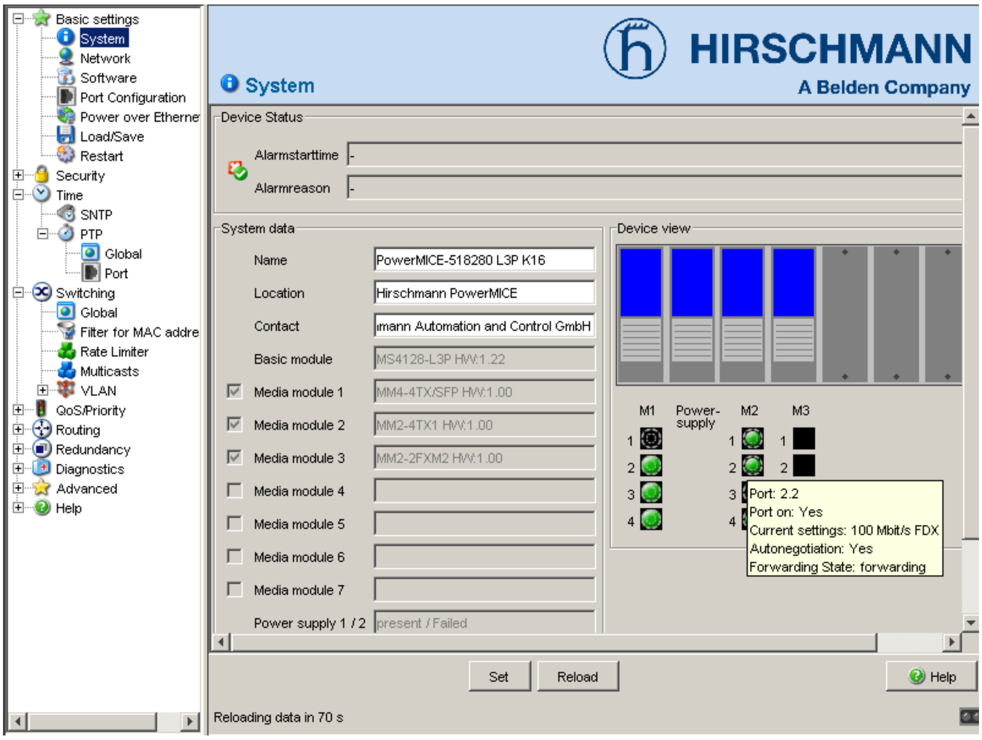
The user interface (Web-based Interface) of the device appears on the screen.

Note: The changes you make in the dialogs will be copied to the volatile memory of the device (RAM) 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 34 “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.

The user interface (Web-based Interface) of the device appears on the screen.



Alarmstarttime -
Alarmreason -

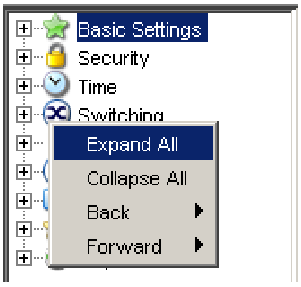
Name PowerMICE-518280 L3P K16
Location Hirschmann PowerMICE
Contact ımann Automation and Control GmbH
Basic module MS4128-L3P HW:1.22
☑ Media module 1 MM4-4TX/SFP HW:1.00
☑ Media module 2 MM2-4TX1 HW:1.00
☑ Media module 3 MM2-2FXM2 HW:1.00
☐ Media module 4
☐ Media module 5
☐ Media module 6
☐ Media module 7
Power supply 1 / 2 present / Failed

Port: 2.2
Port on: Yes
Current settings: 100 Mbit/s FDX
Autonegotiation: Yes
Forwarding State: forwarding

Reloading data in 70 s

Figure 3: User interface (Web-based Interface) 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

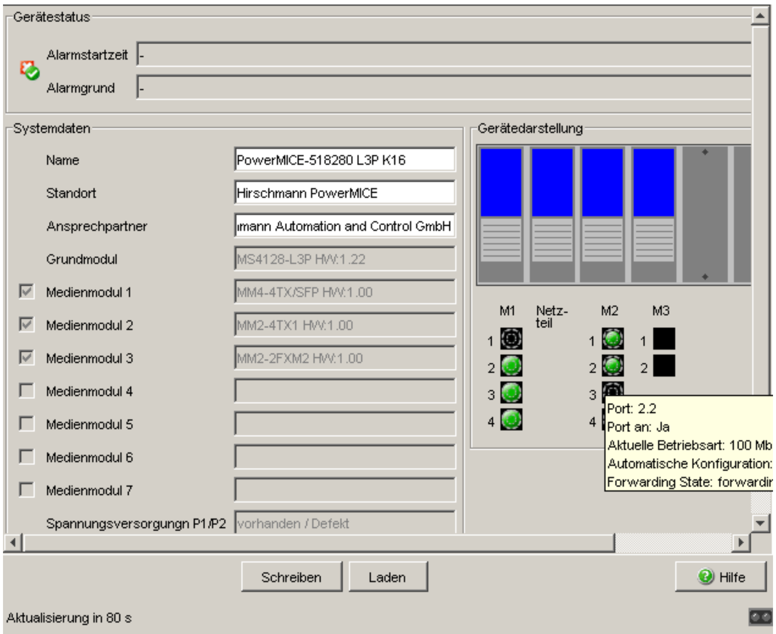
The Basic Settings menu contains the dialogs, displays and tables for the basic configuration:

- System
- Network
- Software
- Port configuration
- Power over Ethernet (PoE)
- 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



Gerätestatus

Alarmstartzeit -

Alarmgrund -

Systemdaten

	Name	PowerMICE-518280 L3P K16
	Standort	Hirschmann PowerMICE
	Ansprechpartner	ımann Automation and Control GmbH
	Grundmodul	MS4128-L3P HW:1.22
☑	Medienmodul 1	MM4-4TX/SFP HW:1.00
☑	Medienmodul 2	MM2-4TX1 HW:1.00
☑	Medienmodul 3	MM2-2FXM2 HW:1.00
☐	Medienmodul 4	
☐	Medienmodul 5	
☐	Medienmodul 6	
☐	Medienmodul 7	
	Spannungsversorgungn P1/P2	vorhanden / Defekt

Gerätedarstellung

Port: 2.2
Port an: Ja
Aktuelle Betriebsart: 100 Mb
Automatische Konfiguration:
Forwarding State: forwardir

Aktualisierung in 80 s

Figure 4: "System" Submenu

Device state

This section of the user interface (Web-based Interface) provides information on the device status and the alarm states the device has detected.

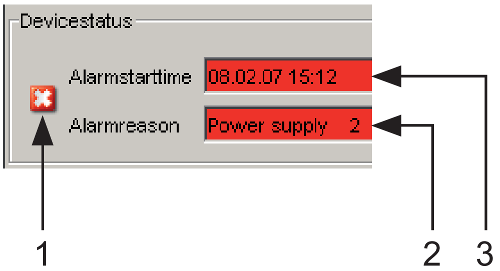


Figure 5: Device status and display of detected alarms
1 - Symbol indicates the Device Status
2 - Cause of the oldest existing alarm detected
3 - Time of the oldest existing alarm detected

System Data

This area of the graphical user interface displays the system parameters of the device. In the fields with a white background, you have the option of changing the settings.

- 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	Shows the 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 status of the individual ports is indicated by one of the symbols listed below. You will get a full description of the port's status by positioning the mouse pointer over the port's symbol.

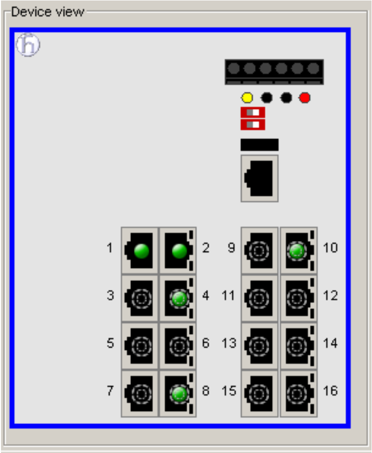


Figure 6: Device View

What the symbols mean:

●●●● The port (10, 100 Mbit/s, 1, 10 Gbit/s) is enabled and connection is OK.

⊖ The port is blocked by network management and has no connection.

⊖ The port is blocked by network management and has no connection.

▣ The port is in auto-negotiation mode.

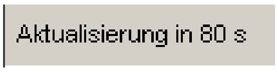
⦶ The port is in HDX mode.

⊕ The port (100 Mbit/s) is in the discard mode of a redundancyprotocol, for example Spanning Tree or HIPER-Ring.

⊕ The port is in routing mode (100 Mbit/s).

Reloading

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

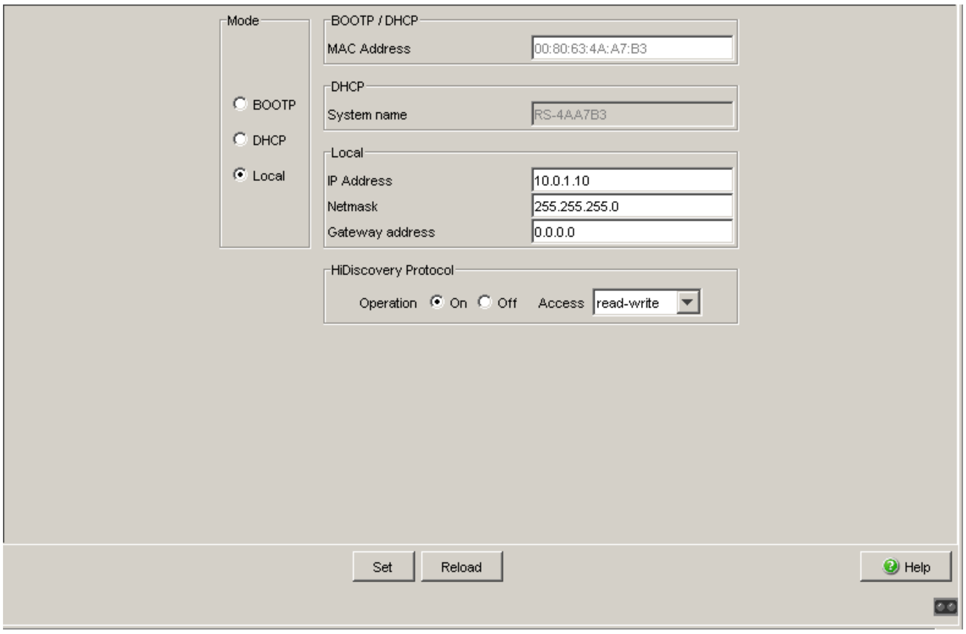


Aktualisierung in 80 s

Figure 7: Time to next Reload

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 HiDiscovery access.



Mode

○ BOOTP

○ DHCP

● Local

BOOTP / DHCP

MAC Address	00:80:63:4A:A7:B3

DHCP

System name	RS-4AA7B3

Local

IP Address	10.0.1.10
Netmask	255.255.255.0
Gateway address	0.0.0.0

HiDiscovery Protocol

Operation ● On ○ Off Access read-write

Figure 8: Network parameters dialog

□ Under “Mode”, you enter where the device gets its IP parameters:
- ▶ In the BOOTP mode, the configuration is via a BOOTP or DHCP server on the basis of the MAC address of the device (see on page 33 “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 33 “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.

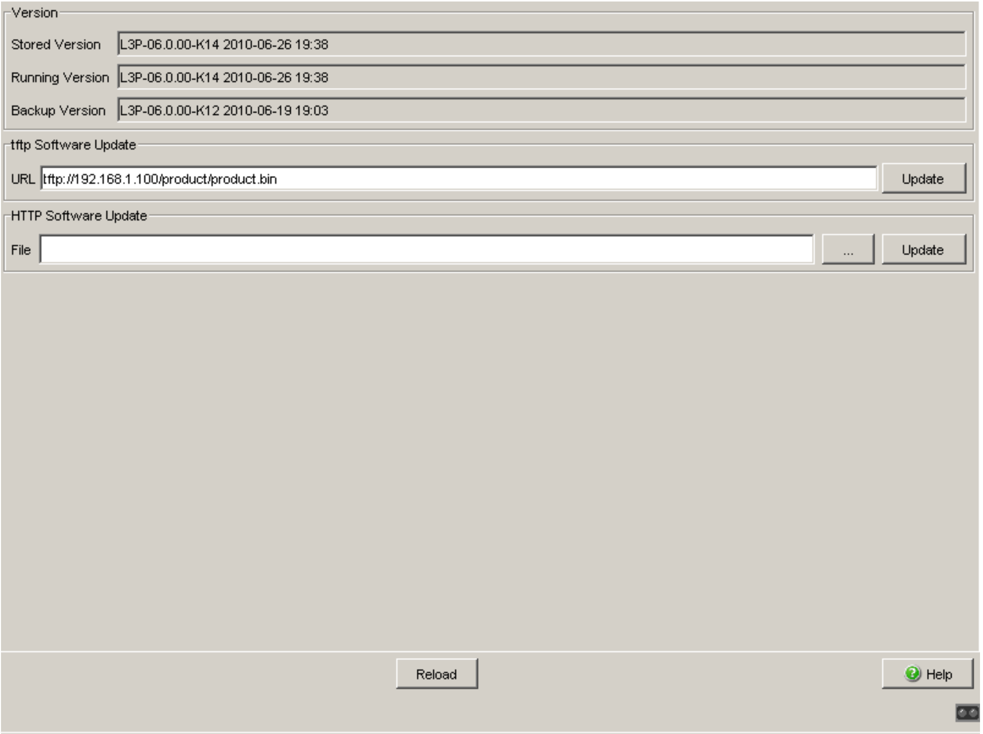
□ You enter the name applicable to the DHCP protocol in the “Name” line in the system dialog of the Web-based interface.

□ The HiDiscovery protocol allows you to allocate an IP address to the device on the basis of its MAC address. Activate the HiDiscovery protocol if you want to allocate an IP address to the device from your PC with the enclosed HiDiscovery software (state 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.



Version

Stored Version L3P-06.0.00-K14 2010-06-26 19:38

Running Version L3P-06.0.00-K14 2010-06-26 19:38

Backup Version L3P-06.0.00-K12 2010-06-19 19:03

tftp Software Update

URL tftp://192.168.1.100/product/product.bin

HTTP Software Update

File

Figure 9: Software dialog

1.3.1 View the software versions present on the device

The dialog shows the existing software versions:

- Stored Version:
  The version of the software stored in the flash memory.
- Running Version:
  The version of the software currently running.
- Backup Version:
  The version of the previous software 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 38 “Restart”).

1.3.3 HTTP Software Update

For an HTTP software update (via a file selection window), copy the device software to 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 finished.

▶ Update aborted. Reason: incorrect file.

▶ Update aborted. Reason: saving unsuccessful.

▶ File not found (reason: file name not found or does not exist).

▶ Unsuccessful Connection (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 can set the operating mode for this port. The choice of operating modes depends on the media module. The possible operating modes are:
  - 10 Mbit/s half duplex (HDX)
  - 10 Mbit/s full duplex (FDX)
  - 100 Mbit/s half duplex (HDX)
  - 100 Mbit/s full duplex (FDX)
  - 1000 Mbit/s half duplex (HDX)
  - 1000 Mbit/s full duplex (FDX)
  - 10 Gbit/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).

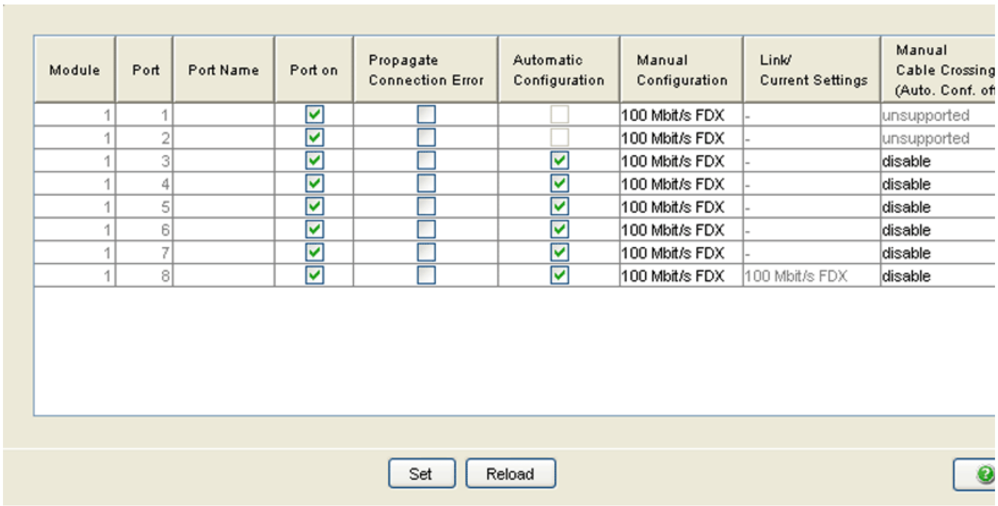
Note: The active automatic configuration has priority over the manual configuration.

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

Port type	Bit rate	Autonegotiation (automatic configuration)	Port setting	Duplex
TX	100 Mbit/s	off	on	100 Mbit/s full duplex (FDX)
Optical	100 Mbit/s	off	on	100 Mbit/s full duplex (FDX)

Table 2: Port settings for ring ports

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



Module	Port	Port Name	Port on	Propagate Connection Error	Automatic Configuration	Manual Configuration	Link/ Current Settings	Manual Cable Crossing (Auto. Conf. of
1	1		☑	□	□	100 Mbit/s FDX	-	unsupported
1	2		☑	□	□	100 Mbit/s FDX	-	unsupported
1	3		☑	□	☑	100 Mbit/s FDX	-	disable
1	4		☑	□	☑	100 Mbit/s FDX	-	disable
1	5		☑	□	☑	100 Mbit/s FDX	-	disable
1	6		☑	□	☑	100 Mbit/s FDX	-	disable
1	7		☑	□	☑	100 Mbit/s FDX	-	disable
1	8		☑	□	☑	100 Mbit/s FDX	100 Mbit/s FDX	disable

Figure 10: Port Configuration Table Dialog

1.5 Power over ETHERNET

For the devices

- ▶ OS24-080900T5T5TFFBHH
- ▶ OS24-080900T5T5TNEBHH

The device supports Power over ETHERNET according to IEEE 802.3at (PoE+) and allows you to supply current to devices such as IP phones via the twisted-pair cable.
On delivery, the Power over ETHERNET function is activated globally and on all PoE-capable ports.

The device provides a nominal power of 61.1 W for the sum of all PoE ports. Should the connected devices require more PoE power than is provided, the device then switches PoE off at the ports. The device first switches PoE off at the ports with the higher port number.

- ☐ With “Function on/off” you turn the PoE on or off.
- ☐ With “Send Trap” you can get the device to send a trap in the following cases:
  - – If a value exceeds/falls below the performance threshold.
  - – If the PoE supply voltage is switched on/off at at least one port.
- ☐ Enter the power threshold in “Threshold”. When this value is exceeded/ not achieved, the device will send a trap, provided that “Send trap” is enabled. For the power threshold you enter the power yielded as a percentage of the nominal power.
- ☐ “Nominal Power” displays the power that the device nominally provides for all PoE ports together.
- ☐ “Reserved Power” displays the maximum power that the device provides to all the connected PoE devices together on the basis of their classification.
- ☐ “Delivered Power” shows how large the current power requirement is at all PoE ports.

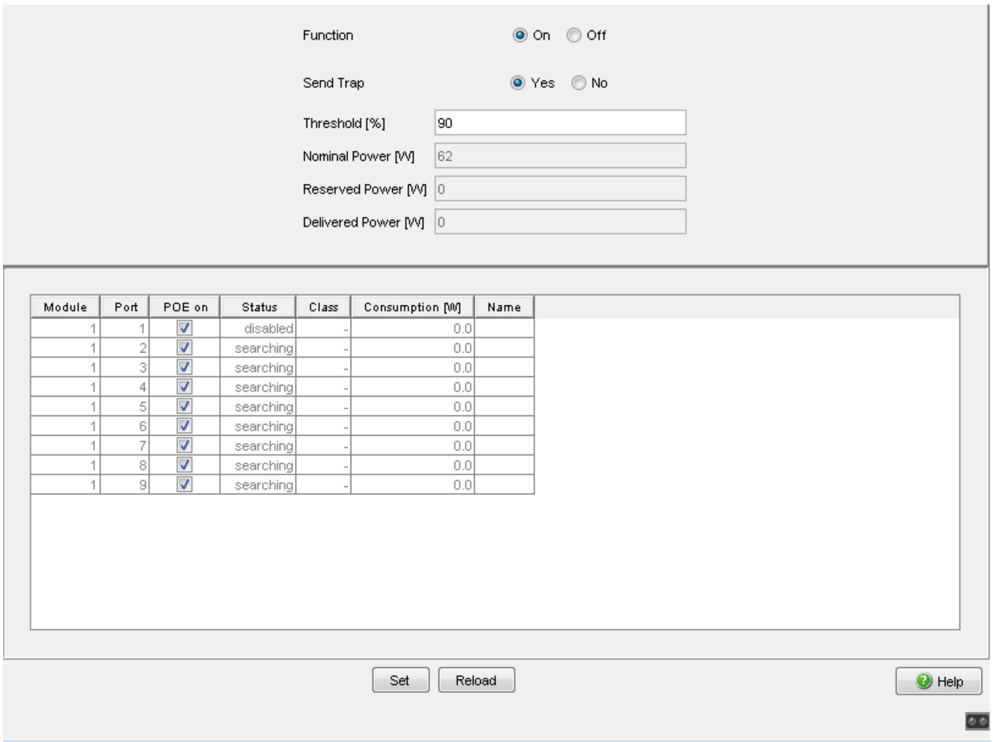
The difference between the "nominal" and "reserved" power indicates how much power is still available to the free PoE+ ports.

- ☐ In the “POE on” column, you can enable/disable PoE at this port.
- ☐ The “Status” column indicates the PoE status of the port.

□ The "Class" column indicates the class of the connected device:
Class: Maximum delivered power
0: 15.4 W
1: 4.0 W
2: 7.0 W
3: 15.4 W
4: 30.0 W

□ The column „Consumption [W]“ displays the current power delivered at the respective port.

□ The “Name” column indicates the name of the port, see `Basic settings:Port configuration`.



Function ● On ○ Off

Send Trap ● Yes ○ No

Threshold [%]	90
Nominal Power [W]	62
Reserved Power [W]	0
Delivered Power [W]	0

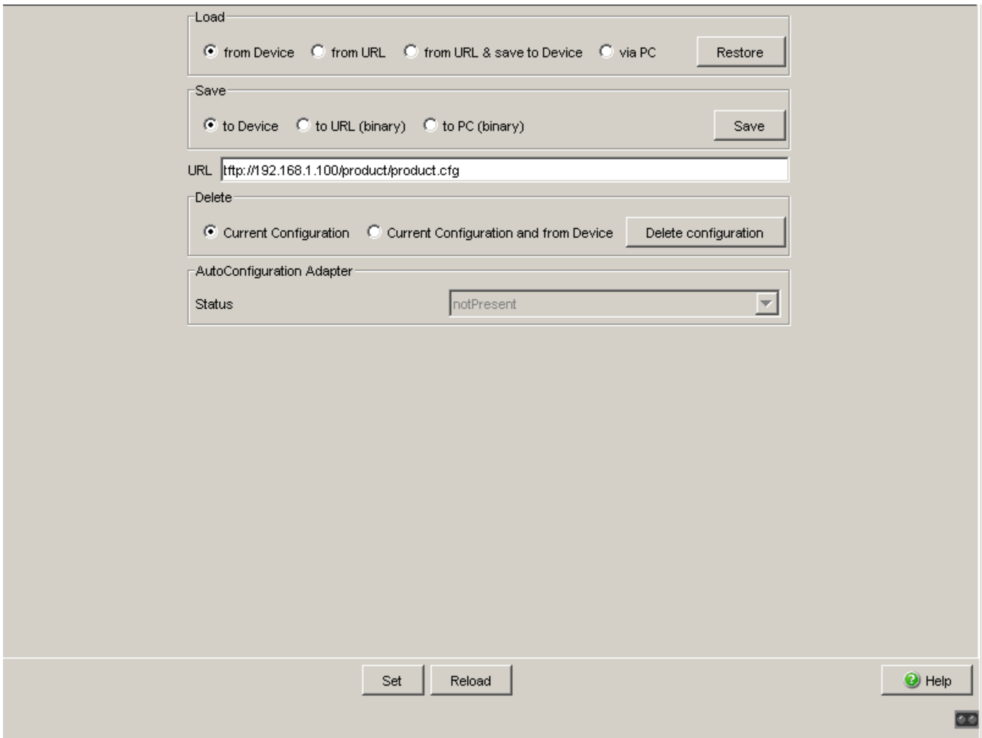
Module	Port	POE on	Status	Class	Consumption [W]	Name
1	1	☑	disabled	-	0.0	
1	2	☑	searching	-	0.0	
1	3	☑	searching	-	0.0	
1	4	☑	searching	-	0.0	
1	5	☑	searching	-	0.0	
1	6	☑	searching	-	0.0	
1	7	☑	searching	-	0.0	
1	8	☑	searching	-	0.0	
1	9	☑	searching	-	0.0	

Figure 11: Power over Ethernet dialog

1.6 Loading/Saving the Configuration

With this dialog you can:

- load a configuration,
- save a configuration,
- enter a URL,
- restore the delivery configuration,
- cancel a configuration change.



Load
● from Device ○ from URL ○ from URL & save to Device ○ via PC

Save
● to Device ○ to URL (binary) ○ to PC (binary)

URL: tftp://192.168.1.100/product/product.cfg

Delete
● Current Configuration ○ Current Configuration and from Device

AutoConfiguration Adapter
Status: notPresent

Figure 12: Load/Save dialog

1.6.1 Loading a 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.

1.6.2 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 22) 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.

1.6.3 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`).

Note: 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.

1.6.4 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. In this case, the device deletes its configuration in the volatile memory as well as in the non-volatile memory. This includes the IP address. The device will be reachable again over the network after it has obtained a new IP address, e.g., via DHCP or the V.24 interface.

1.6.5 Using the AutoConfiguration Adapter (ACA)

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

Note: The described devices use the following AutoConfiguration Adapter: ACA 11.

- **Storing the current configuration data in the ACA:**
  You have the option of transferring the current device configuration, including the SNMP password, to the ACA and the flash memory by using the “to device” option in the “Save” frame .

You have the option of transferring the current device configuration, including the SNMP password, to the ACA and the flash memory by using the “to device” option in the “Save” frame .

- **Transferring the configuration data from the ACA:**
  When you restart with the ACA connected, the device adopts the configuration data of the ACA and saves it permanently in the flash memory. If the connected ACA 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 ACA, the device compares the password in the device with the password in the ACA 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 ACA present
ok	The configuration data from the ACA and the device match.
removed	The ACA was removed after booting.
notInSync	- The configuration data of the ACA and the device do not match, or only one file exists[a], or - no configuration file is present on the ACA or on the device[b].
outOfMemory	The local configuration data is too extensive to be stored on the ACA.
wrongMachine	The configuration data in the ACA originates from a different device type and cannot be read or converted.
checksumErr	The configuration data is damaged.

Table 3: ACA status

[a] In these cases, the ACA status is identical to the status “ACA not in sync”, which sends “Not OK” to the signal contacts and the device status.,
[b] In this case, the ACA status (“notInSync”) deviates from the status “ACA not in sync”, which sends “OK” to the signal contacts, and the device status.

1.7 Restart

This dialog provides you with the following functions:

- initiate a cold start of the device. The device reloads the software from the non-volatile memory, restarts, and performs a self-test.
  Reload the website in your browser to reaccess the device after restarting.
- 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 such as Industrial HiVision.

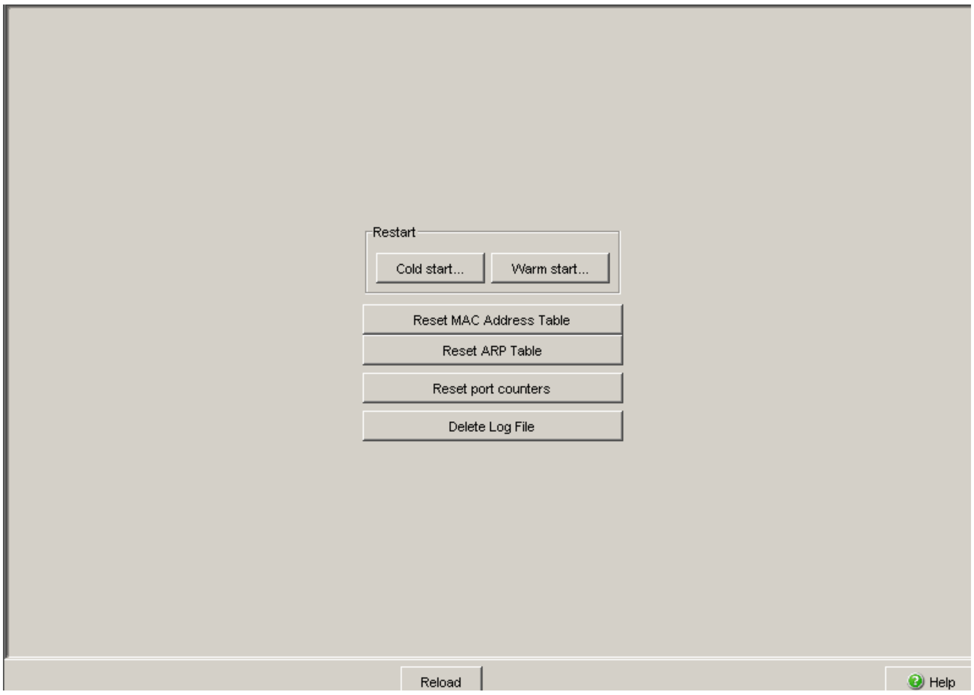


Figure 13: Restart Dialog

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

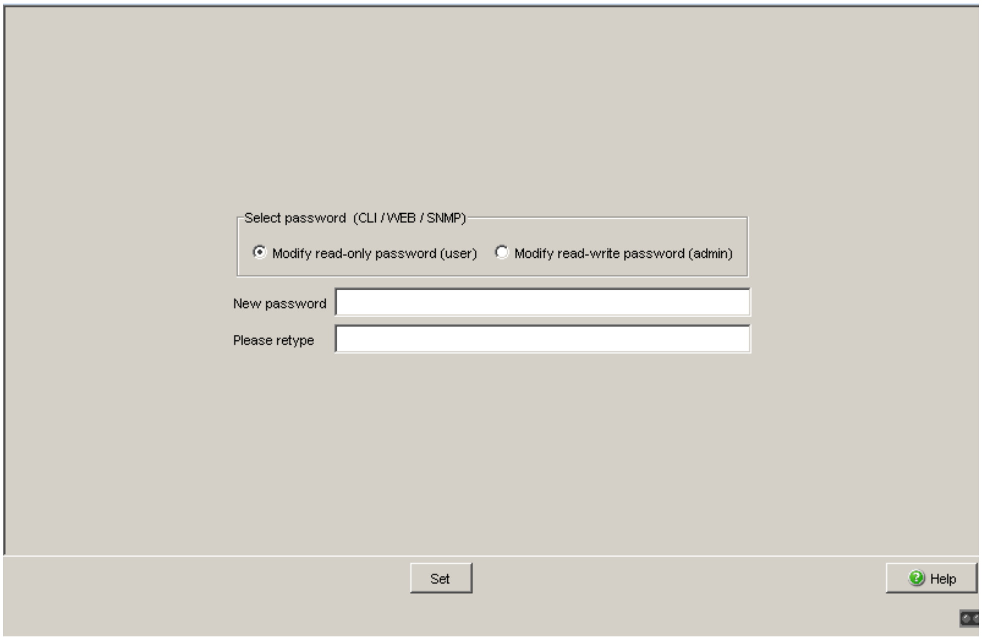
This dialog gives you the option of changing the read and read/write passwords for access to the device via the Web-based interface, via the CLI, and via SNMPv3 (SNMP version 3).
Set different passwords for the read password and the read/write password so that a user that only has read access (user name “user”) does not know, or cannot guess, the password for read/write access (user name “admin”).
If you set identical passwords, when you attempt to write this data the device reports a general error.

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

Note: Passwords are case-sensitive.

☐ Select “Modify read-only password (user)” to enter the read password.
☐ Enter the new read password in the “New password” line and repeat your entry in the “Please retype” line.

☐ Select “Modify read-write password (admin)” to enter the read/write password.
☐ Enter the read/write password and repeat your entry.



Select password (CLI / WEB / SNMP)

● Modify read-only password (user) ○ Modify read-write password (admin)

New password

Please retype

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.

You can block access via a Web browser in a separate dialog (see on page 48 “Web Access”).

Access at IP address level is restricted in a separate dialog (see on page 45 “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 manage the device with HiVision and communicate with earlier versions of SNMP.

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

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

  Note: Passwords are case-sensitive.
- In the “IP Address” column, you enter the IP address which may access the device. No entry in this field, or the entry “0.0.0.0”, allows access to this device from computers with any IP address. In this case, the only access protection is the password.
- In the “IP Mask” column, much the same as with netmasks, you have the option of selecting a group of IP addresses.
  Example:
  255.255.255.255: a single IP address
  255.255.255.240 with IP address = 172.168.23.20:
  the IP addresses 172.168.23.16 to 172.168.23.31.

Binary notation of the mask 255.255.255.240:
1111 1111 1111 1111 1111 1111 1111 0000
mask bits
Binary notation of the IP address 172.168.23.20:
1010 1100 1010 1000 0001 0111 0001 0100

The binary representation of the mask with the IP address yields
an address range of:
1010 1100 1010 1000 0001 0111 0001 0000 bis
1010 1100 1010 1000 0001 0111 0001 1111
i.e.: 172.168.23.16 to 172.168.23.31

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

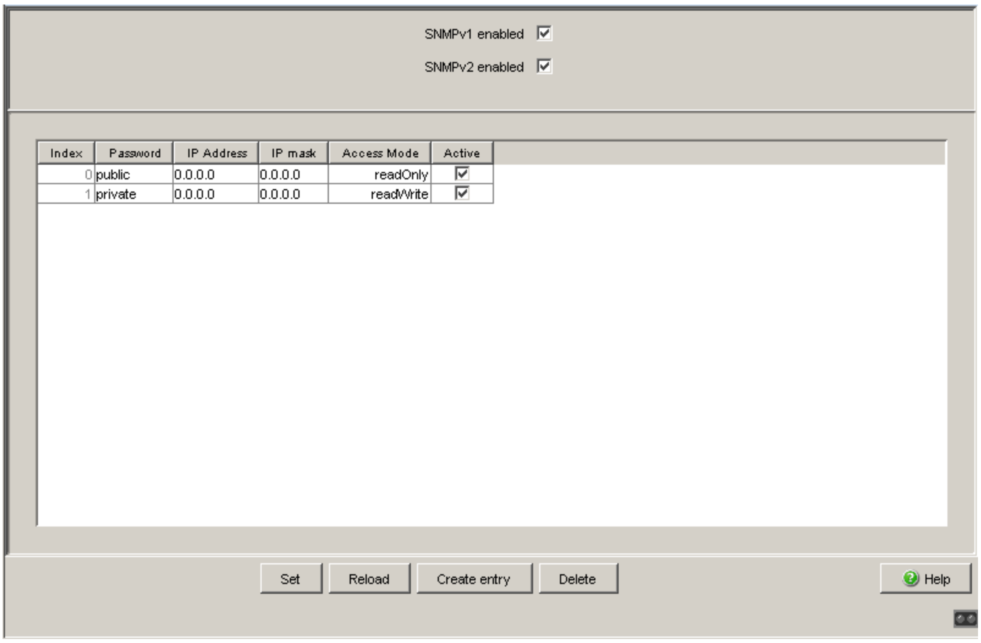
  Note: The password for the “readOnly” access mode is the same as the SNMPv3 password for read access.
  The password for the “readWrite” access mode is the same as the SNMPv3 password for read/write access.
  If you are changing one of the passwords, manually set the corresponding password for SNMPv3 to the same value (see on page 42 “Password / SNMPv3 access”). This way you ensure that you can also access with the same password via SNMPv3.

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

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

- With “Create entry” you create a new row in the table.
- With “Delete entry” you delete selected rows in the table.

Note: The device prevents deleting or changing the row with the password currently in use.



SNMPv1 enabled ☑

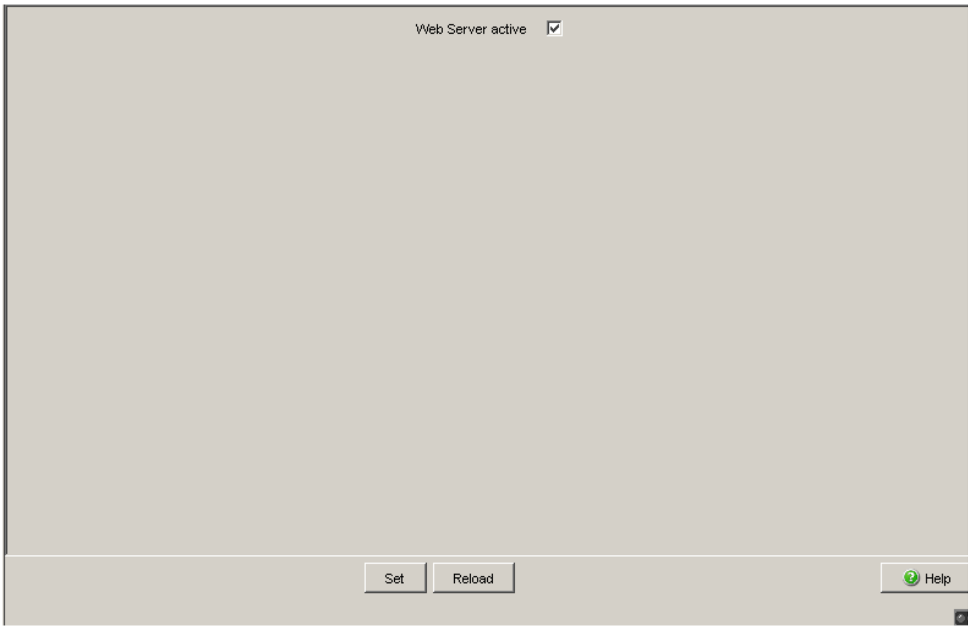
SNMPv2 enabled ☑

Index	Password	IP Address	IP mask	Access Mode	Active
0	public	0.0.0.0	0.0.0.0	readOnly	☑
1	private	0.0.0.0	0.0.0.0	readWrite	☑

Figure 15: SNMPv1/v2 Access Dialog

2.3 Web Access

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



Web Server active ☑

Figure 16: Web Access dialog

2.3.1 Description of Web Access (http)

The device's Web server allows you to configure the device by using the Web-based interface. You can deactivate the Web server to prevent Web access to the device.
The server is activated in its state on delivery.

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 “System Time (UTC)” displays the time with reference to Universal Time Coordinated.
The time displayed is the same worldwide. Local time differences are not taken into account.

▶ The ”system time” uses "System Time (UTC)", allowing for the local time difference from "System Time (UTC)".
“System time” = “System Time (UTC)” + “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`, `ptp` and `sntp`. The source is initially `local`.
If PTP is activated and the device receives a valid PTP frame, it sets its time source to `ptp`. If SNTP is activated and if the device receives a valid SNTP packet, the device sets its time source to `sntp`. The device gives the PTP time source priority over SNTP

□ With “Set time from PC”, the device takes the PC time as the system time and calculates the system time (UTC) using the local time difference.
“System Time (UTC)” = “system time” - “local offset”

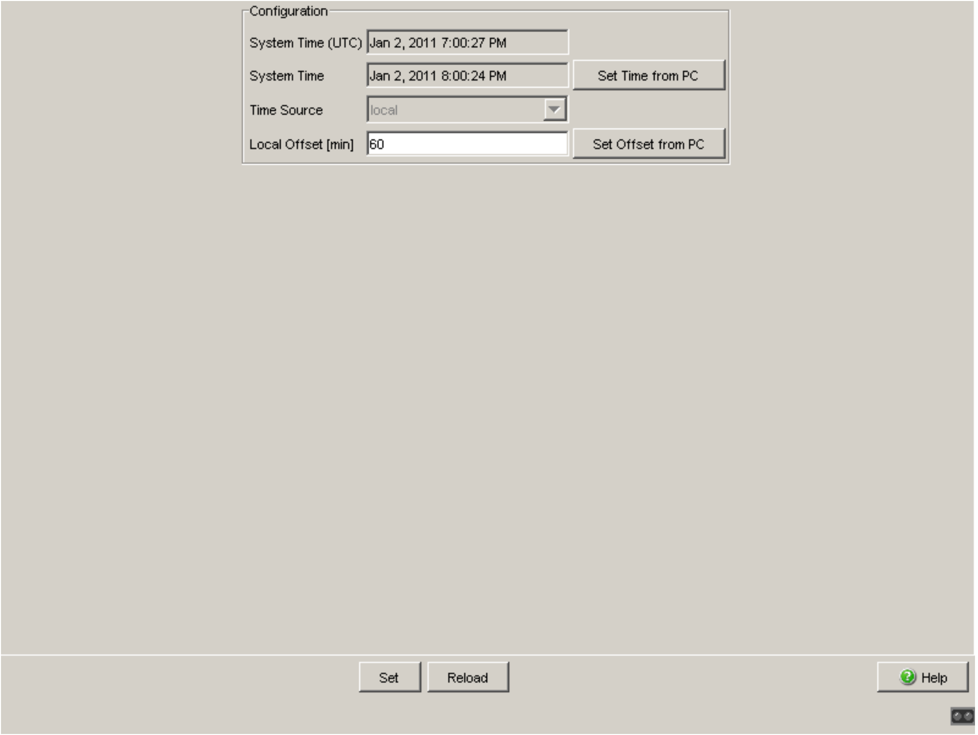
▶ The “local offset” is for displaying/entering the time difference between the local time and the “System Time (UTC)”.

□ 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.



Configuration

System Time (UTC): Jan 2, 2011 7:00:27 PM

System Time: Jan 2, 2011 8:00:24 PM

Time Source: local

Local Offset [min]: 60

Figure 17: Time Dialog:Basic Settings

3.1 SNTP configuration

The Simple Network Time Protocol (SNTP) enables you to synchronize the system time in your network.
The device supports the SNTP client and the SNTP server function.

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

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

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

Parameter	Meaning
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/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: SNTP Server Configuration

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

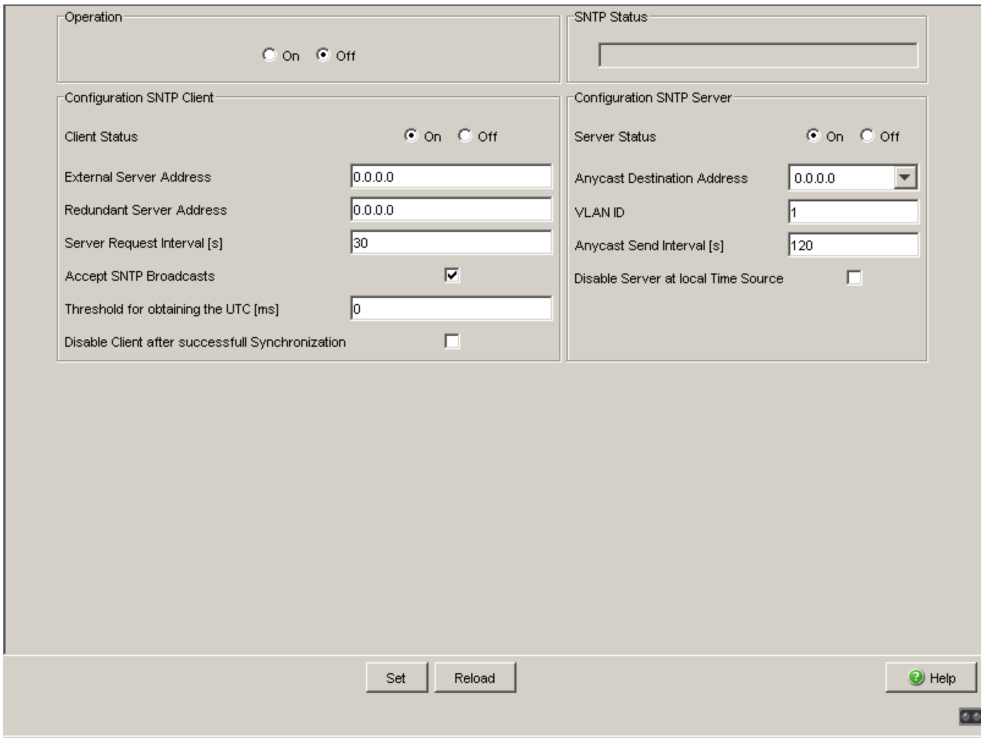
Table 7: Periodic sending of SNTP packets

Parameter	Meaning	Possible Values	Default Setting
Client Status	Switches the SNTP client On/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: SNTP Client Configuration

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, switch off the reception of SNTP Broadcasts (see “Accept SNTP Broadcasts”). You thus ensure that the device only takes the time from a defined SNTP server.



Operation

○ On ● Off

SNTP Status

Configuration SNTP Client

Client Status ● On ○ Off

External Server Address 0.0.0.0

Redundant Server Address 0.0.0.0

Server Request Interval [s] 30

Accept SNTP Broadcasts ☑

Threshold for obtaining the UTC [ms] 0

Disable Client after successfull Synchronization □

Configuration SNTP Server

Server Status ● On ○ Off

Anycast Destination Address 0.0.0.0

VLAN ID 1

Anycast Send Interval [s] 120

Disable Server at local Time Source □

Figure 18: SNTP Dialog

3.2 PTP (IEEE 1588)

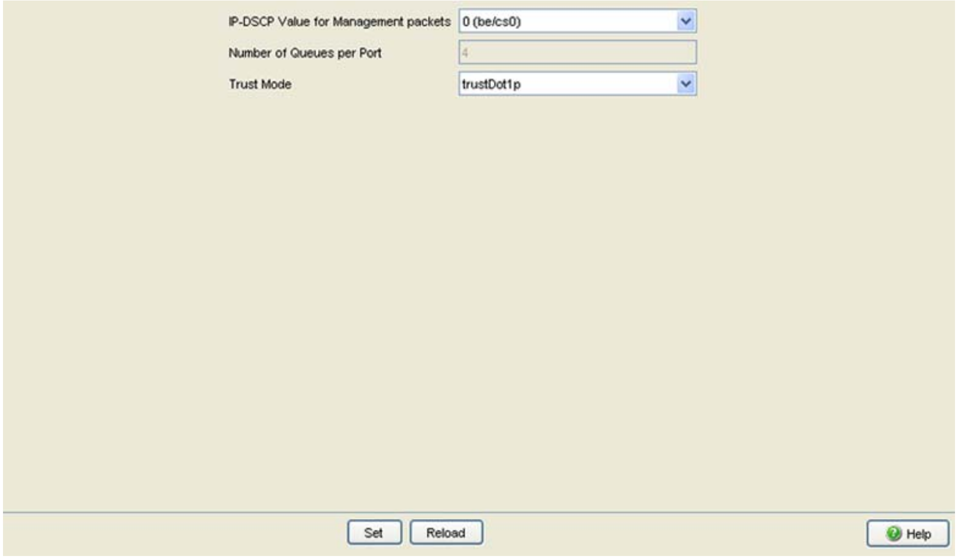
Precise time management is required for running time-critical applications via a LAN.
The IEEE 1588 standard with the Precision Time Protocol (PTP) describes a procedure that determines the best master clock in a LAN and thus enables precise synchronization of the clocks in this LAN.

Devices without PTP hardware support, which only have ports absent a time stamp unit, support the PTP simple mode. This mode gives a less accurate division of time.

With these devices

- 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.

Note: In the simple mode a device synchronizes itself with PTP messages received. This mode provides a precision comparable to SNTP absent other functions, such as PTP management or runtime measuring.
If you want to transport PTP time accurately through your network, only use devices with PTP hardware support on the transport paths.



IP-DSCP Value for Management packets: 0 (be/cs0)

Number of Queues per Port: 4

Trust Mode: trustDot1p

Figure 19: Dialog PTP

4 Switching

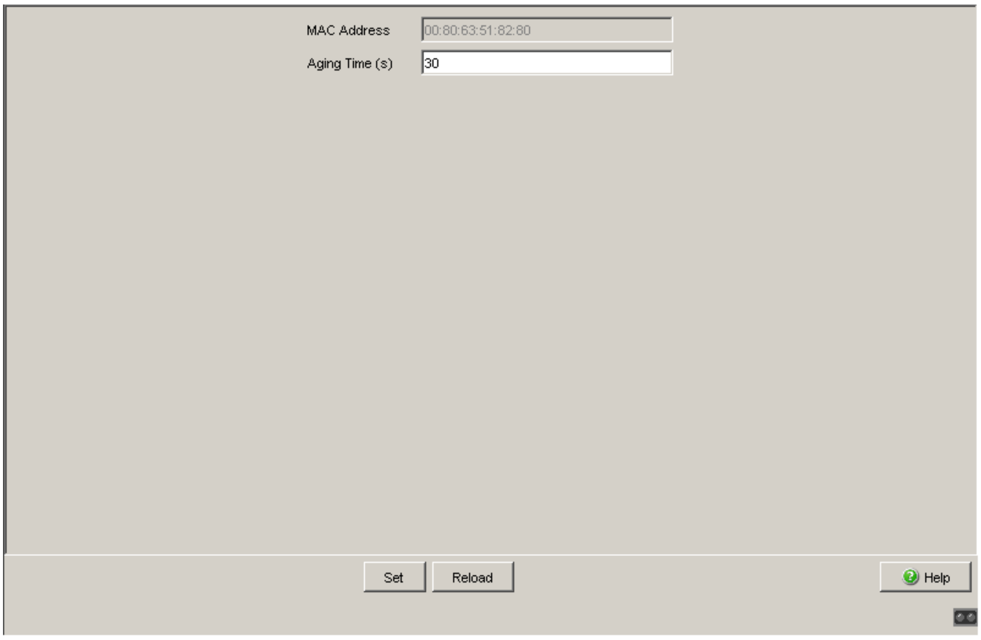
The switching menu contains the dialogs, displays and tables for configuring the switching settings:

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

4.1 Switching Global

Variable	Meaning	Possible Values	Default Setting
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



MAC Address: 00:80:63:51:82:80

Aging Time (s): 30

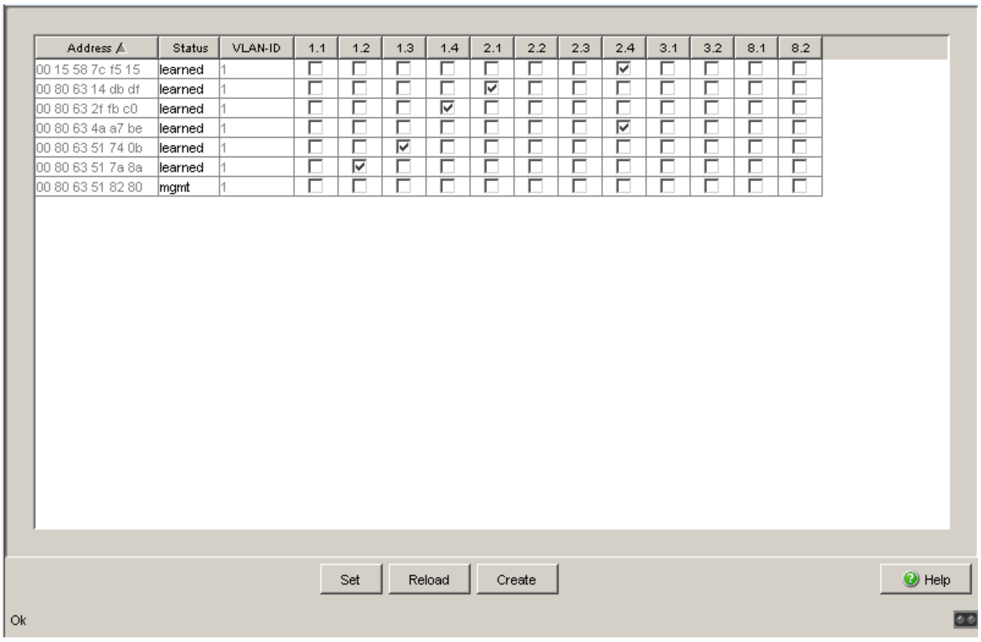
Figure 20: Dialog Switching Global

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 on page 33 “Loading/Saving the Configuration”).
- `igmp`: The filter was created by IGMP Snooping.

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



Address	Status	VLAN-ID	1.1	1.2	1.3	1.4	2.1	2.2	2.3	2.4	3.1	3.2	8.1	8.2
00 15 58 7c f5 15	learned	1	□	□	□	□	□	□	□	☑	□	□	□	□
00 80 63 14 db df	learned	1	□	□	□	□	☑	□	□	□	□	□	□	□
00 80 63 2f fb c0	learned	1	□	□	□	☑	□	□	□	□	□	□	□	□
00 80 63 4a a7 be	learned	1	□	□	□	□	□	□	□	☑	□	□	□	□
00 80 63 51 74 0b	learned	1	□	□	☑	□	□	□	□	□	□	□	□	□
00 80 63 51 7a 8a	learned	1	□	☑	□	□	□	□	□	□	□	□	□	□
00 80 63 51 82 80	mgmt	1	□	□	□	□	□	□	□	□	□	□	□	□

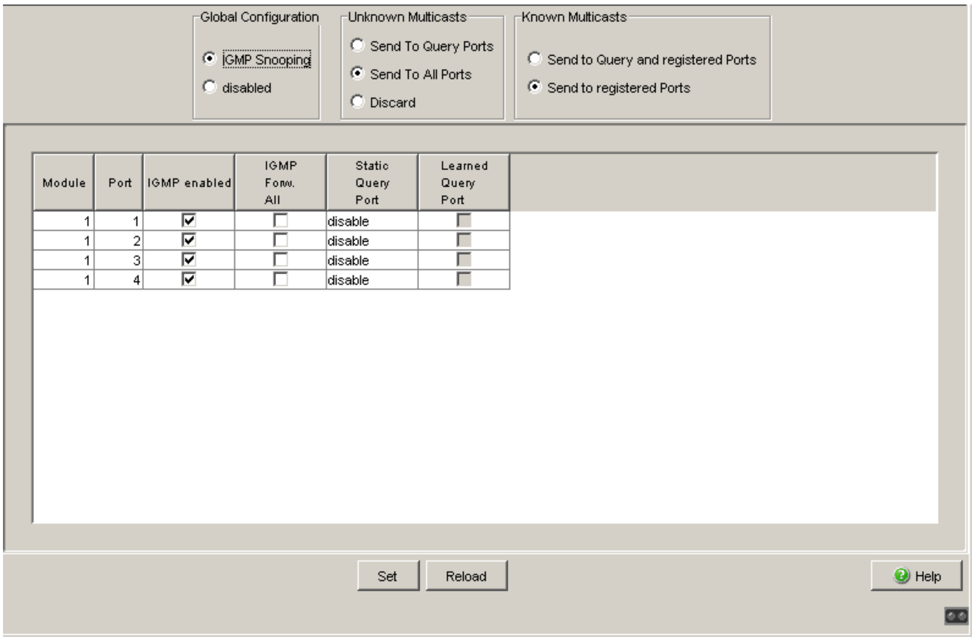
Figure 21: Filter Table dialog

Note: The 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 function globally,
- configure the IGMP protocol globally and per port.



Global Configuration

● IGMP Snooping
○ disabled

Unknown Multicasts

○ Send To Query Ports
● Send To All Ports
○ Discard

Known Multicasts

○ Send to Query and registered Ports
● Send to registered Ports

Module	Port	IGMP enabled	IGMP Forw. All	Static Query Port	Learned Query Port
1	1	☑	□	disable	□
1	2	☑	□	disable	□
1	3	☑	□	disable	□
1	4	☑	□	disable	□

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	Bedeutung	Wertebereich	Voreinstellung
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.	2-3,599 s[a]	125 s
IGMP settings			
Current querier IP address	Display the IP address of the router/ switch that has the query function.		
Max. Response Time	Zeit eingeben, innerhalb derer die Multicast-Gruppen-Mitglieder auf ein Query antworten sollen. Die Multicast-Gruppen-Mitglieder wählen einen zufälligen Wert innerhalb der Response Time für ihre Antwort aus, um zu verhindern, dass alle Multicast-Gruppen-Mitglieder gleichzeitig auf den Query antworten.	Protokoll Version - 1, 2: 1-25 s - 3: 1-3.598 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.	3-3,600 s[a]	260 s

Table 11: IGMP Querier and IGMP settings

a. Beachten Sie den Parameter-Zusammenhang zwischen Max.-Response-Time, Sende-Intervall und Group-Membership-Intervall (see table 12.)

The parameters
– Max. Response Time,
– Send Interval and
– Group Membership Interval
have a relationship to one another:

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 addresses not learned with IGMP Snooping
▶ known MAC/IP multicast addresses 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

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 on	Switch IGMP on/off for each port. Switching IGMP off at a port prevents registration for this port. Prerequisite: The IGMP Snooping function is activated globally.	`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: The IGMP Snooping function is activated globally. **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 Hirschmann 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: The IGMP Snooping function is activated globally.	`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:

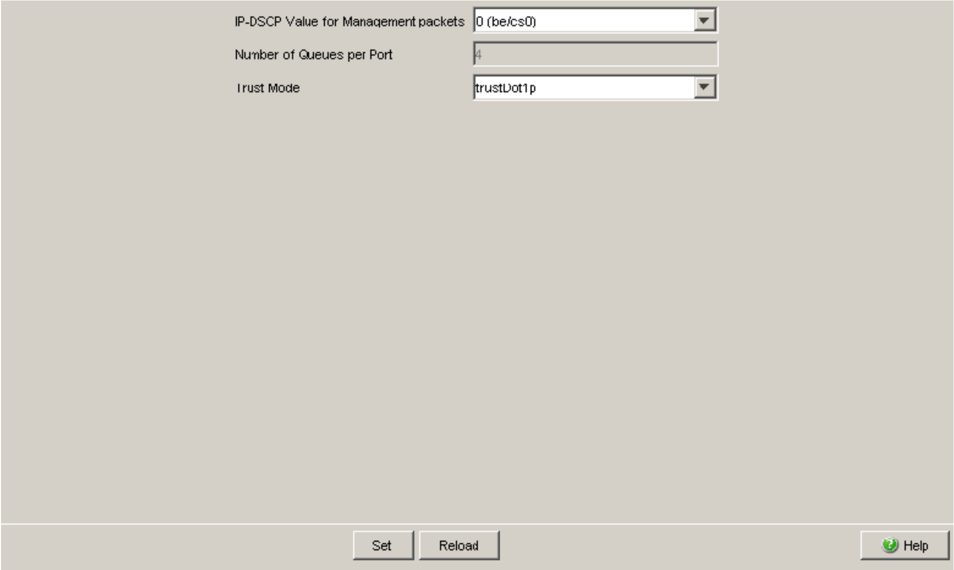
- enter the IP-DSCP value for management packets in the range 0 to 63 (default setting: 0 (be/cs0)).
  In order for you to have full access to the management of the device, even when there is a high network load, the device enables you to prioritize management packets.
  In prioritizing management packets (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 (8 for MACH 4000, MACH 104, MACH 1040 and PowerMICE) 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



IP-DSCP Value for Management packets: 0 (be/cs0)

Number of Queues per Port: 4

Trust Mode: trustDot1p

Figure 23: Global dialog

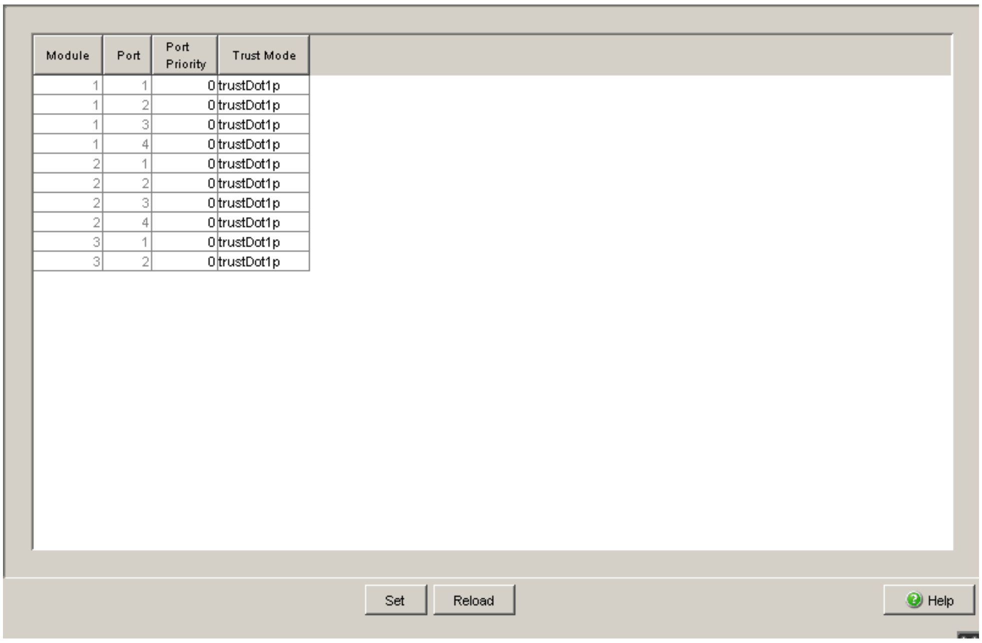
5.2 Port Configuration

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



Module	Port	Port Priority	Trust Mode
1	1	0	trustDot1p
1	2	0	trustDot1p
1	3	0	trustDot1p
1	4	0	trustDot1p
2	1	0	trustDot1p
2	2	0	trustDot1p
2	3	0	trustDot1p
2	4	0	trustDot1p
3	1	0	trustDot1p
3	2	0	trustDot1p

Figure 24: Port configuration dialog

5.2.1 Entering the port priority

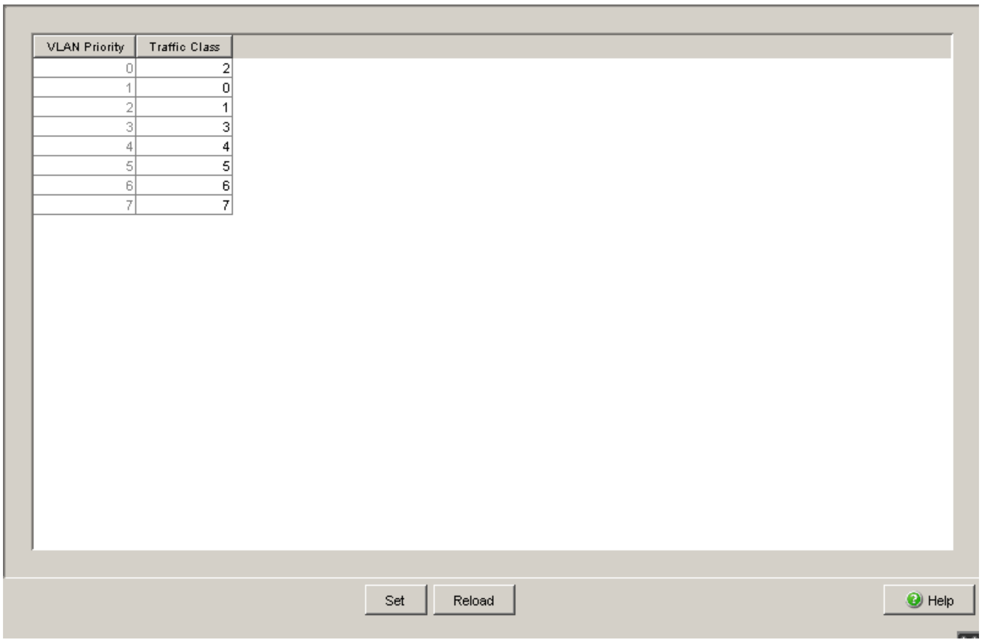
□ Double-click a cell in the “Port priority” column and enter the priority (0-7). According to the priority entered, the device assigns the data packets that it receives at this port to a traffic class (see table 17).
Prerequisite:
Setting in the dialog `Global: Trust Mode: untrusted`(see on page 72 “Global”) or
Setting in the dialog `Global: Trust Mode: trustDot1p`(see on page 72 “Global”) and the data packets do not contain a VLAN tag or
Setting in the dialog `Global: Trust Mode: trustIpDscp`(see on page 72 “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.



VLAN Priority	Traffic Class
0	2
1	0
2	1
3	3
4	4
5	5
6	6
7	7

Figure 25: 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

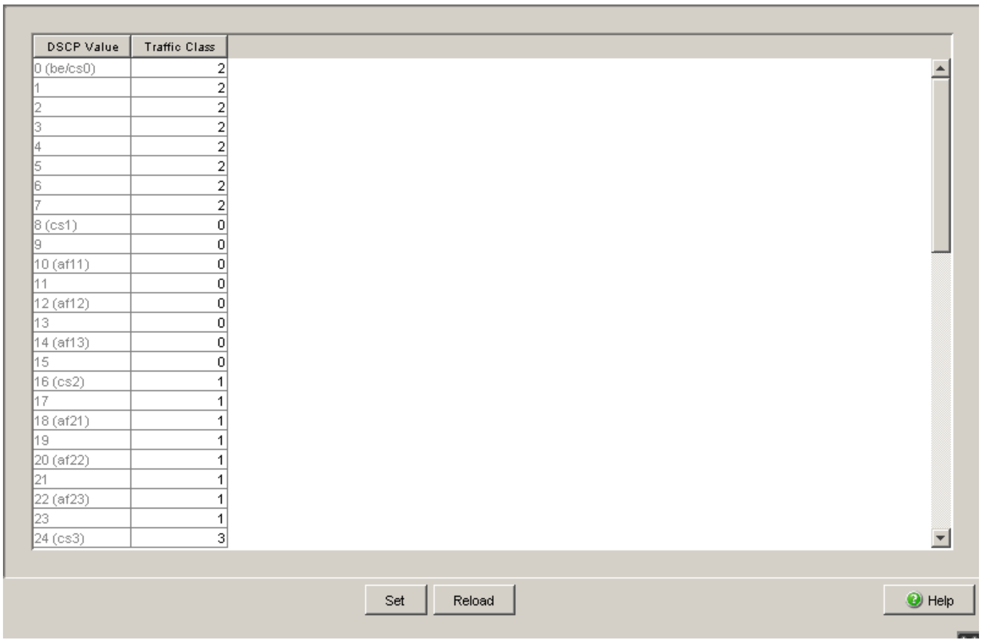
Table 18: Assigning the VLAN priority to the 4 traffic classes

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).



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

Figure 26: 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
- Sub-Ring
- Redundant coupling of Rings and network segments
- 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 aid of a device's **R**ing **M**anager (RM) function you can close both ends of a backbone in a line-type configuration to form a redundant ring.

- Within a HIPER-Ring, you can use any combination of the following devices:
  - RS2-./.
  - RS2-16M
  - RS2-4R
  - RS20, RS30, RS40
  - RSB20
  - RSR20, RSR30
  - OCTOPUS
  - MICE
  - MS20, MS30
  - PowerMICE
  - MACH 100
  - MACH 1000
  - MACH 3000
  - MACH 4000
- Within an MRP-Ring, you can use devices that support the MRP protocol based on IEC62439.

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: Only one Ring Redundancy method can be enabled on one device 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
TX	100 Mbit/s	off	on	100 Mbit/s full duplex (FDX)
Optical	100 Mbit/s	off	on	100 Mbit/s full duplex (FDX)

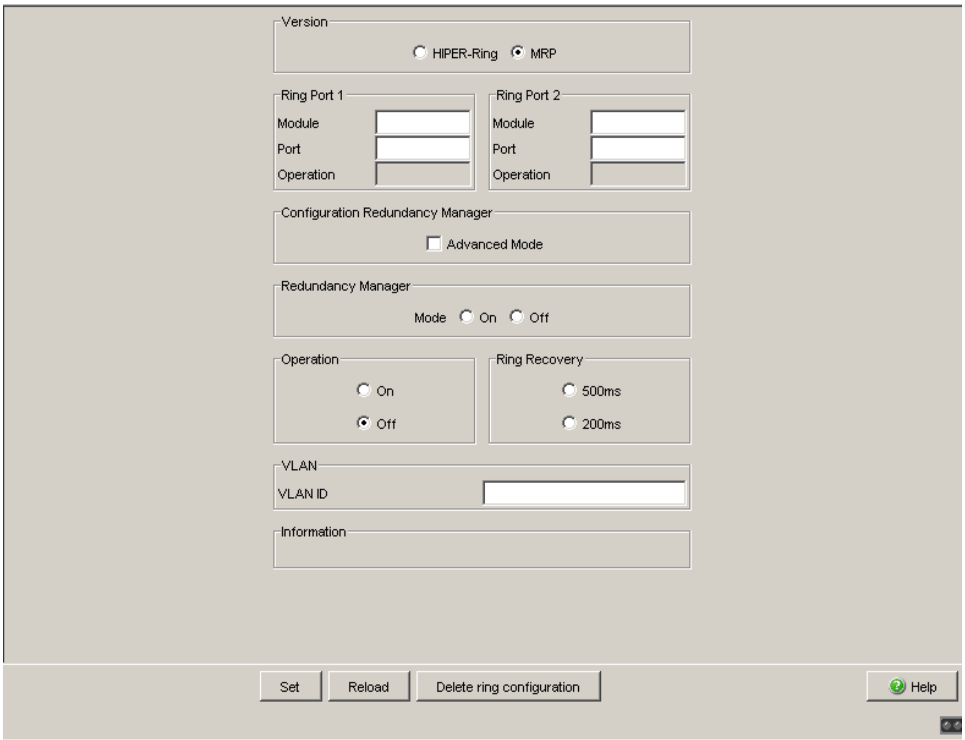
Table 21: Port settings for ring ports

Note: Configure all the devices of the HIPER-Ring individually. Before you connect the redundant line, you must complete the configuration of all the devices of the HIPER-Ring. You thus avoid loops during the configuration phase.

Note: As an alternative to using software to configure the HIPER-Ring, with devices RS20/30/40 and MS20/30 you can also use DIP switches to enter a number of settings on the devices. You can also use a DIP switch to enter a setting for whether the configuration via DIP switch or the configuration via software has priority. The state on delivery is “Software Configuration”. You will find details on the DIP switches in the “Installation” user manual.

Parameter	Meaning
Ring port X.X operation	Display in “Operation” field: `active:` This port is switched on and has a link. `inactive:` This port is switched off or it has no link.
Ring Manager Status	Status information, no input possible: `Active (redundant line)`: The redundant line was closed because a data line or a network component within the ring failed. `Inactive:` The redundant ring is open, and all data lines and network components are working.
Ring Manager Mode	If there is exactly one device, you switch the Ring Manager function on at the ends of the line.
Ring Recovery	The settings in the ”Ring Recovery“ frame are only effective for devices that are ring managers. In the ring manager, select the desired value for the test packet timeout for which the ring manager waits after sending a test packet before it evaluates the test packet as lost. ▶ `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



Version

○ HIPER-Ring ● MRP

Ring Port 1

Module

Port

Operation

Ring Port 2

Module

Port

Operation

Configuration Redundancy Manager

□ Advanced Mode

Redundancy Manager

Mode ○ On ○ Off

Operation

○ On

● Off

Ring Recovery

○ 500ms

○ 200ms

VLAN

VLAN ID

Information

Figure 27: 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 via software or DIP switches, the device sets the corresponding settings for the pre-defined ring ports in the configuration table (transmission rate and mode). If you switch off the HIPER-Ring function, the ports, which are changed back into normal ports, keep the ring port settings. Independently of the DIP switch setting, you can still change the port settings via the software.

6.1.2 Configuring the MRP-Ring

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

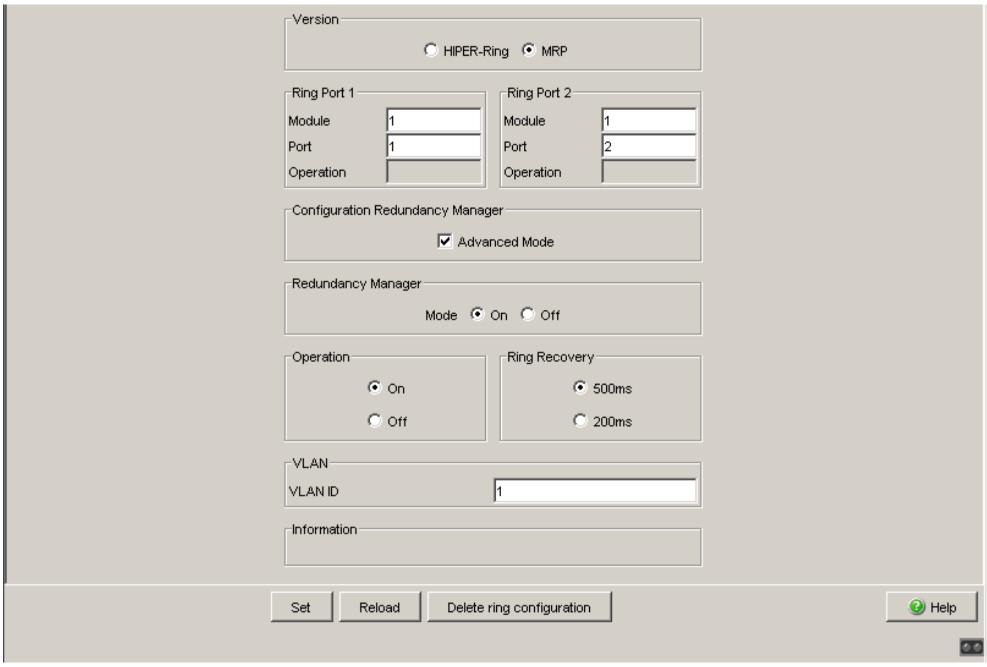
Port type	Bit rate	Autonegotiation (automatic configuration)	Port setting	Duplex
TX	100 Mbit/s	off	on	100 Mbit/s full duplex (FDX)
Optical	100 Mbit/s	off	on	100 Mbit/s full duplex (FDX)

Table 23: Port settings for ring ports

Note: Configure all the devices of the MRP-Ring individually. Before you connect the redundant line, you must have completed the configuration of all the devices of the MRP-Ring. You thus avoid loops during the configuration phase.

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.
Ring Manager Configuration	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 Hirschmann devices that support the MRP-Ring also support the advanced mode.
Ring Manager Mode	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



Version

○ HIPER-Ring ● MRP

Ring Port 1

Module 1

Port 1

Operation

Ring Port 2

Module 1

Port 2

Operation

Configuration Redundancy Manager

☑ Advanced Mode

Redundancy Manager

Mode ● On ○ Off

Operation

● On

○ Off

Ring Recovery

● 500ms

○ 200ms

VLAN

VLAN ID 1

Information

Figure 28: 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 help 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: You have the option of coupling RSTP network segments to an MRP-Ring. For this, you activate the MRP compatibility. This enables you to operate RSTP via an MRP-Ring.
If the root bridge is within the MRP-Ring, the devices in the MRP-Ring count as a single device when calculating the length of the branch. A device that is connected to a random Ring bridge receives such RSTP information as if it were directly connected to the root bridge.

Note: The RSTP standard dictates that all the devices within a network work with the (Rapid) Spanning Tree Algorithm. If STP and RSTP are used at the same time, the advantages of faster reconfiguration with RSTP are lost in the network segments that are operated in combination.
A device that only supports RSTP works together with MSTP devices by not assigning an MST region to itself, but rather the CST (Common Spanning Tree).

Note: By changing the IEEE 802.1D-2004 standard for RSTP, the Standards Commission reduced the maximum value for the “Hello Time” from 10 s to 2 s. When you update the Switch software from a release before 5.0 to release 5.0 or higher, the new software release automatically reduces the locally entered “Hello Time” values that are greater than 2 s to 2 s.
If the device is not the RSTP root, “Hello Time” values greater than 2 s can remain valid, depending on the software release of the root device.

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.

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 help 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

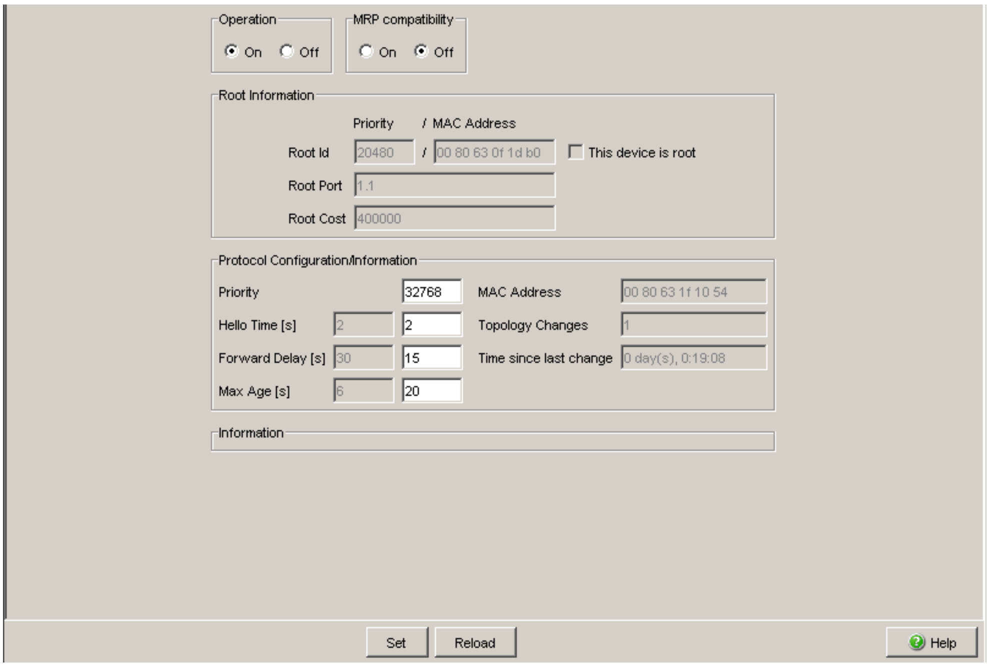
Parameter	Meaning	Possible Values	Default Setting
Bridge ID (read only)	The local Bridge ID, made up of the local priority and its own MAC address. The format is ppppp / mm mm mm mm mm mm, with: ppppp: priority (decimal) and mm: the respective byte of the MAC address (hexadecimal).		
Topology Changes	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.



Operation: ● On ○ Off

MRP compatibility: ○ On ● Off

Root Information

	Priority	/ MAC Address	
Root Id	20480	00 80 63 0f 1d b0	□ This device is root
Root Port	1.1		
Root Cost	400000		

Protocol Configuration/Information

Priority		32768	MAC Address	00 80 63 1f 10 54
Hello Time [s]	2	2	Topology Changes	1
Forward Delay [s]	30	15	Time since last change	0 day(s), 0:19:08
Max Age [s]	6	20		

Information

Figure 29: RSTP global dialog

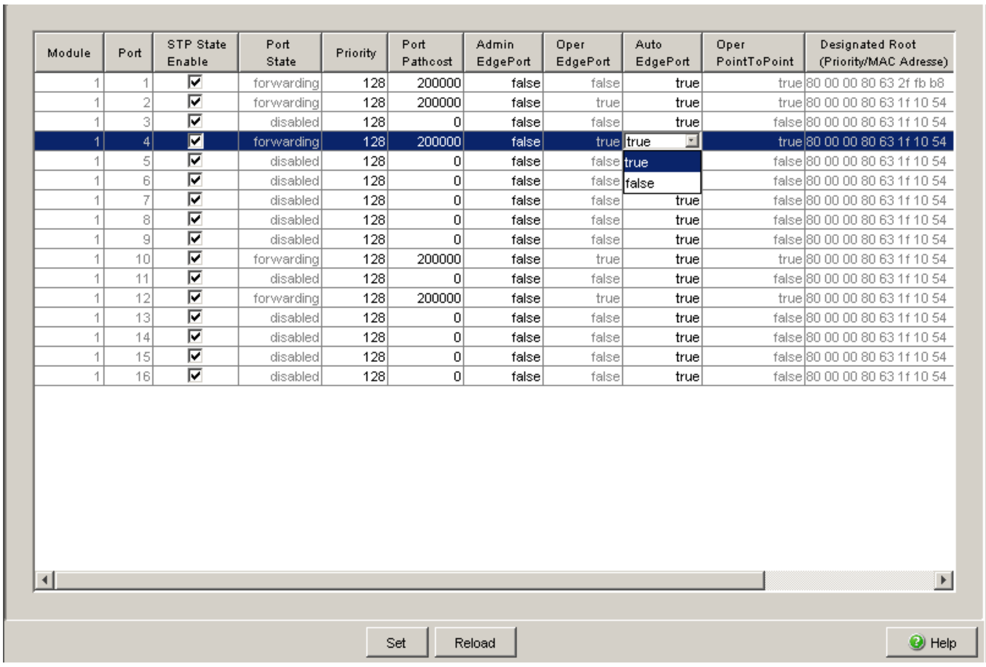
6.2.2 Rapid Spanning Tree Port

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



Module	Port	STP State Enable	Port State	Priority	Port Pathcost	Admin EdgePort	Oper EdgePort	Auto EdgePort	Oper PointToPoint	Designated Root (Priority/MAC Adresse)
1	1	☑	forwarding	128	200000	false	false	true	true	80 00 00 80 63 2f fb b8
1	2	☑	forwarding	128	200000	false	true	true	true	80 00 00 80 63 1f 10 54
1	3	☑	disabled	128	0	false	false	true	false	80 00 00 80 63 1f 10 54
1	4	☑	forwarding	128	200000	false	true	true	true	80 00 00 80 63 1f 10 54
1	5	☑	disabled	128	0	false	false	true	false	80 00 00 80 63 1f 10 54
1	6	☑	disabled	128	0	false	false	false	false	80 00 00 80 63 1f 10 54
1	7	☑	disabled	128	0	false	false	true	false	80 00 00 80 63 1f 10 54
1	8	☑	disabled	128	0	false	false	true	false	80 00 00 80 63 1f 10 54
1	9	☑	disabled	128	0	false	false	true	false	80 00 00 80 63 1f 10 54
1	10	☑	forwarding	128	200000	false	true	true	true	80 00 00 80 63 1f 10 54
1	11	☑	disabled	128	0	false	false	true	false	80 00 00 80 63 1f 10 54
1	12	☑	forwarding	128	200000	false	true	true	true	80 00 00 80 63 1f 10 54
1	13	☑	disabled	128	0	false	false	true	false	80 00 00 80 63 1f 10 54
1	14	☑	disabled	128	0	false	false	true	false	80 00 00 80 63 1f 10 54
1	15	☑	disabled	128	0	false	false	true	false	80 00 00 80 63 1f 10 54
1	16	☑	disabled	128	0	false	false	true	false	80 00 00 80 63 1f 10 54

Figure 30: RSTP Port dialog

7 Diagnostics

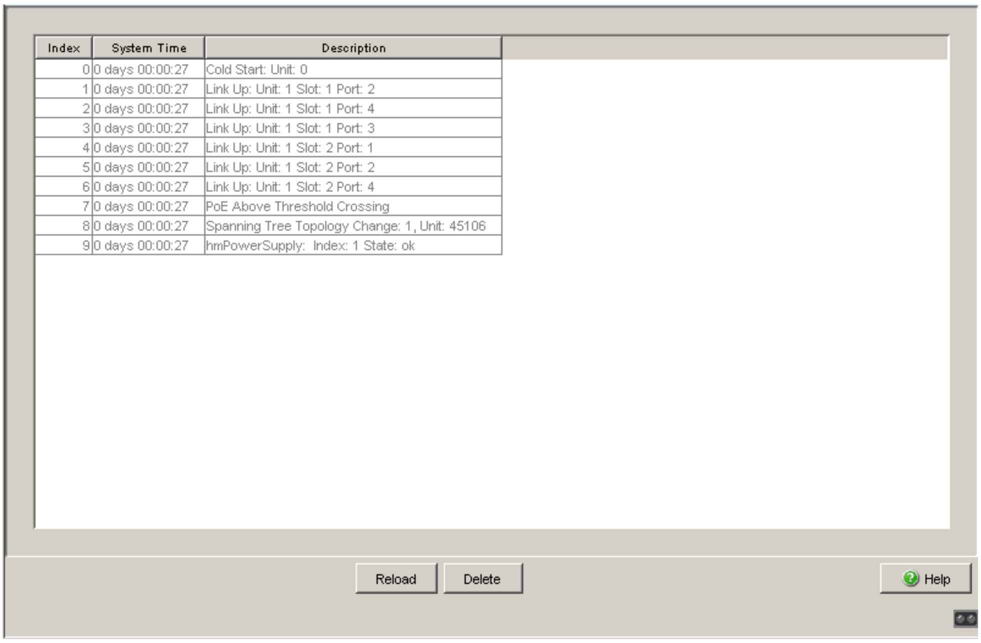
The diagnosis menu contains the following tables and dialogs:

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

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

7.1 Event Log

The table lists the logged events with a time stamp.
The “Reload” button allows you to update the content of the event log, and with the “Delete” button you delete the content of the event log.



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

Figure 31: Event log table

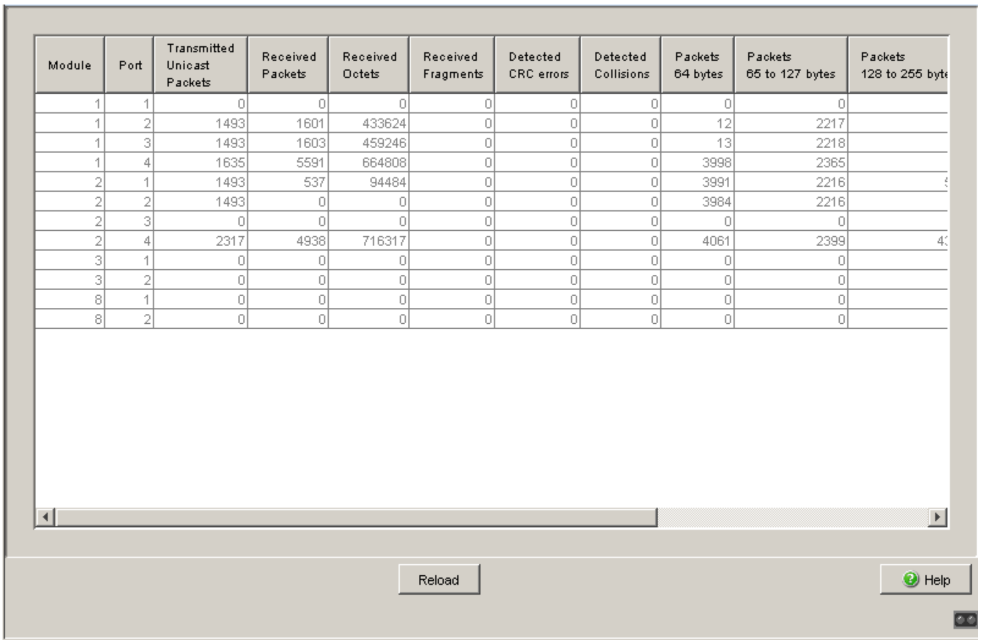
7.2 Ports

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

- Statistics table
- Utilization
- SFP Modules

7.2.1 Statistics table

This table shows you the contents of various event counters. In the Restart menu item, you can reset the event counters to zero using "Warm start", "Cold start" or "Reset port counter".
The packet counters add up the events sent and the events received.



Module	Port	Transmitted Unicast Packets	Received Packets	Received Octets	Received Fragments	Detected CRC errors	Detected Collisions	Packets 64 bytes	Packets 65 to 127 bytes	Packets 128 to 255 byt
1	1	0	0	0	0	0	0	0	0	
1	2	1493	1601	433624	0	0	0	12	2217	
1	3	1493	1603	459246	0	0	0	13	2218	
1	4	1635	5591	664808	0	0	0	3998	2365	
2	1	1493	537	94484	0	0	0	3991	2216	5
2	2	1493	0	0	0	0	0	3984	2216	
2	3	0	0	0	0	0	0	0	0	
2	4	2317	4938	716317	0	0	0	4061	2399	43
3	1	0	0	0	0	0	0	0	0	
3	2	0	0	0	0	0	0	0	0	
8	1	0	0	0	0	0	0	0	0	
8	2	0	0	0	0	0	0	0	0	

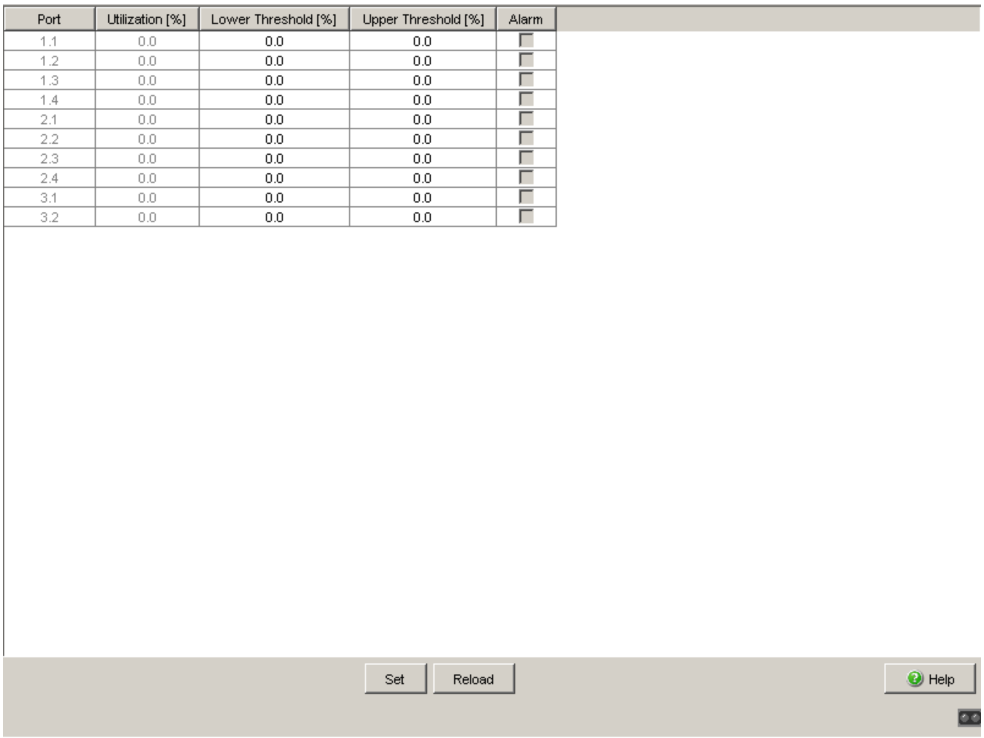
Figure 32: Port statistics table

7.2.2 Network load

This table displays the network load of the individual ports. The network load is the data quantity that the port received in the previous 30 s, compared to the maximum possible data quantity at its currently configured data rate.

In the “Upper Threshold[%]” column you enter the top threshold value for the 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 this threshold value is not met, the device removes the check mark previously set.



Port	Utilization [%]	Lower Threshold [%]	Upper Threshold [%]	Alarm
1.1	0.0	0.0	0.0	□
1.2	0.0	0.0	0.0	□
1.3	0.0	0.0	0.0	□
1.4	0.0	0.0	0.0	□
2.1	0.0	0.0	0.0	□
2.2	0.0	0.0	0.0	□
2.3	0.0	0.0	0.0	□
2.4	0.0	0.0	0.0	□
3.1	0.0	0.0	0.0	□
3.2	0.0	0.0	0.0	□

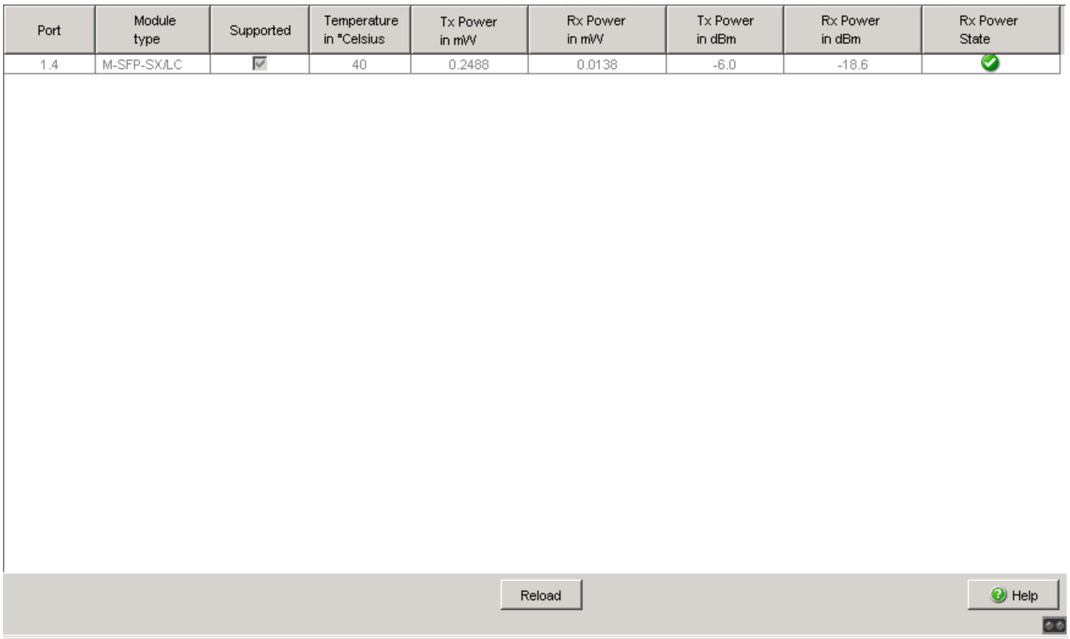
Figure 33: Network load dialog

7.2.3 SFP modules

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

Parameter	Meaning
Module.Port	Port identification using module and port numbers of the device, e.g. 2.1 for port one of module two.
Module type	Type of SFP module, e.g. M-SFP-SX/LC.
Supported	Shows whether the media module supports the SFP module.
Temperature in °C	Shows the SFP's operating temperature.
Tx Power in mW	Shows the transmission power in mW.
Rx Power in mW	Shows the receive power in mW.
Tx power in dBm	Shows the transmission power in dBm.
Rx power in dBm	Shows the receive power in dBm.
Receive Power Status	Shows the power level of the signal received. – `good receiver power` – `limited receiver power` – `insufficient receiver power`

Table 27: SFP Modules dialog



Port	Module type	Supported	Temperature in °Celsius	Tx Power in mW	Rx Power in mW	Tx Power in dBm	Rx Power in dBm	Rx Power State
1.4	M-SFP-SX/LC	☑	40	0.2488	0.0138	-6.0	-18.6	✓

Figure 34: SFP Modules dialog

7.3 Topology Discovery

The table on the “LLDP” tab page shows you the collected LLDP information for neighboring devices. This information enables the network management station to map the structure of your network.

Activating “Display FDB entries” below the table allows you to add entries for devices without active LLDP support to the table. In this case, the device also includes information from its FDB (forwarding database).
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.

When only devices without active topology recognition 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.
You can find the MAC addresses of devices, which the topology table hides for clarity's sake, in the address table (FDB), (see on page 61 “Filters for MAC addresses”).

7.4 Port Mirroring

The port mirroring function enables you to review the data traffic at up to 8 ports of the device for diagnostic purposes. The device additionally forwards (mirrors) the data for these ports to another port. This process is also called port mirroring.
The ports to be reviewed are known as source ports. The port to which the data to be reviewed is copied is called the destination port. You can only use physical ports as source or destination ports.

In port mirroring, the device copies valid incoming **and** outgoing data packets of the source port to the destination port. The device does not affect the data traffic at the source ports during port mirroring.
A management tool connected at the destination port, e.g. an RMON probe, can thus monitor the data traffic of the source ports in the sending and receiving directions.

The destination port forwards all data to be sent.
On the devices PowerMICE, MACH 104, MACH 1040 and MACH 4000, the destination port blocks received data, on all other devices, the destinations port also forwards received data.

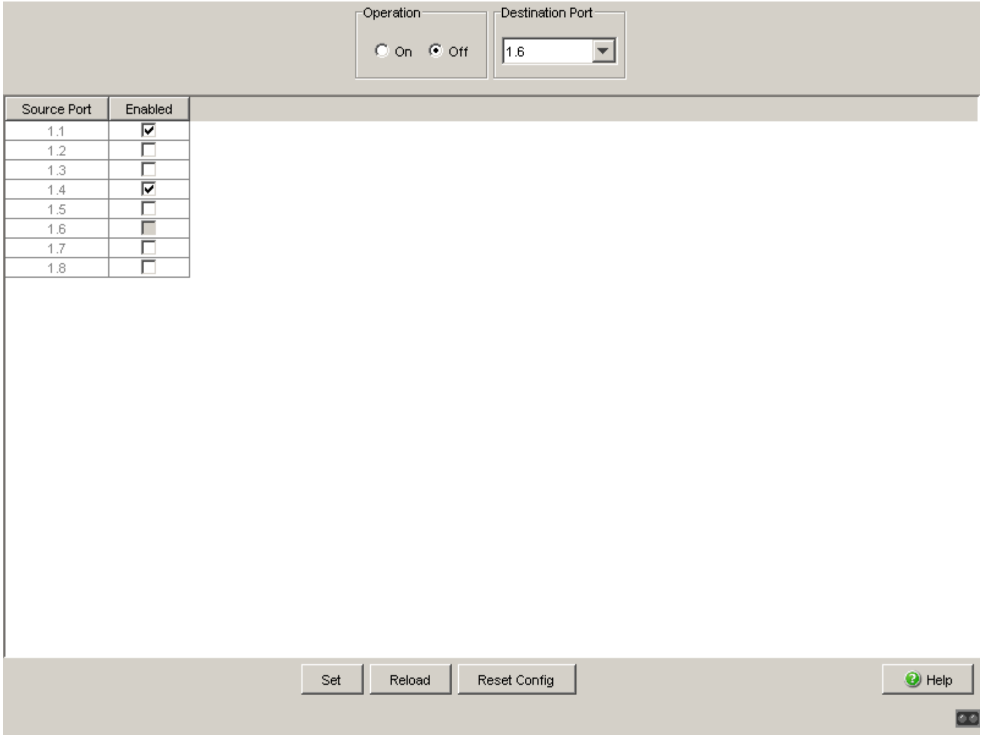
□ Select the source ports whose data traffic you want to review from the list of physical ports by checkmarking the relevant boxes.
You can select a maximum of 8 source ports. Ports that cannot be selected are displayed as inactive by the device, e.g. the port currently being used as the destination port, or if you have already selected 8 ports.
Default setting: no source ports.

□ Select the destination port to which you have connected your management tool from the list element in the “Destination Port” frame.
The device does not display ports that cannot be selected in the list, e.g. the ports currently being used as source ports. Default setting: port 0.0 (no destination port).

□ Select “On” in the “Function” frame to switch on the function. Default setting: “Off”.

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

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



Operation: ○ On ● Off

Destination Port: 1.6

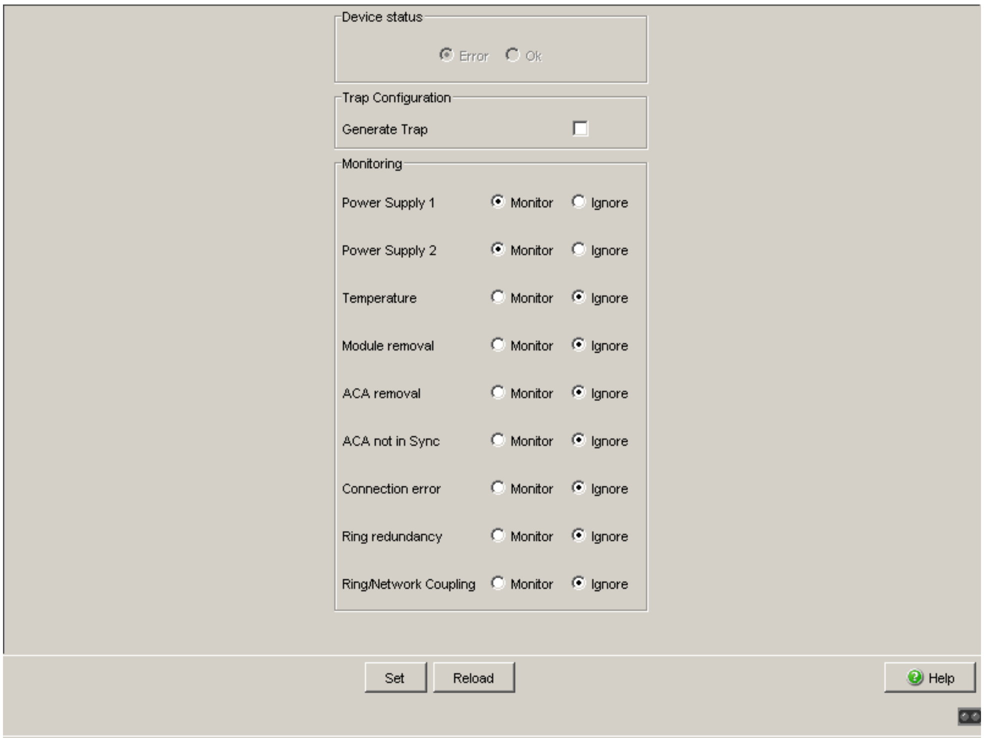
Source Port	Enabled
1.1	☑
1.2	□
1.3	□
1.4	☑
1.5	□
1.6	□
1.7	□
1.8	□

Figure 35: Port Mirroring 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.

The device displays its current status as “Error” or “OK” in the “Device Status” frame. The device determines this status from the individual monitoring results.



Device status

● Error ○ Ok

Trap Configuration

Generate Trap □

Monitoring

Power Supply 1	● Monitor	○ Ignore
Power Supply 2	● Monitor	○ Ignore
Temperature	○ Monitor	● Ignore
Module removal	○ Monitor	● Ignore
ACA removal	○ Monitor	● Ignore
ACA not in Sync	○ Monitor	● Ignore
Connection error	○ Monitor	● Ignore
Ring redundancy	○ Monitor	● Ignore
Ring/Network Coupling	○ Monitor	● Ignore

Figure 36: Device State dialog (for PowerMICE)

□ 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).
ACA removal	Monitor/ignore the removal of the ACA.
ACA not in sync	Monitor/ignore non-matching of the configuration on the device and on the ACA[a] .
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 28 “Port Configuration”). Link status is not monitored in the state on delivery.

Table 28: Device Status

Name	Meaning
Ring Redundancy	Monitor/ignore ring redundancy (for HIPER-Ring only in Ring Manager mode). On delivery, ring redundancy is not monitored. If the device is a normal ring subscriber and not the ring manager, it reports the following: ▶ nothing (for the HIPER-Ring) ▶ detected errors in the local configuration (for Fast HIPER-Ring and for MRP)
Ring/Network coupling	Monitor/ignore the redundant coupling operation. On delivery, no monitoring of the redundant coupling is set. For two-Switch coupling with control line, the slave additionally reports the following conditions: – Incorrect link status of the control line – Partner device is also a slave (in standby mode). **Note:** In two-Switch coupling, both Switches must have found their respective partners.

Table 28: Device Status

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

☐ Select "Generate Trap" in the "Trap Configuration" field to activate the sending of a trap if the device state changes.

Note: With a non-redundant voltage supply, the device reports the absence of a supply voltage. If you do not want this message to be displayed, feed the supply voltage over both inputs or switch off the monitoring (see on page 114 “Signal contact”).

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 "Signal Contact 1" or "Signal Contact 2" card index (for devices with two signal contacts).
☐ Select the “Manual Setting” mode in the “Signal Contact Mode” field. This mode enables you to control this signal contact remotely.
☐ Select “Open” in the “Manual Setting” field to open the contact.
☐ Select “Closed” in the “Manual Setting” field to close the contact.

Application options:

- ▶ Simulation of an error during SPS error 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).[1] 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.

▶ Removing a module. Select “Monitor” for removing modules if the signal contact is to report the removal of a module (for modular devices).

▶ The removal of the ACA. Select “Monitor” for ACA removal if the signal contact is to report the removal of an ACA (for devices which support the ACA).

▶ Non-matching of the configuration in the device and on the ACA[2]. Select “Monitor” ACA not in sync if the signal contact is to report the non-matching of the configuration (for devices which support ACA).

▶ The link error (non-functioning 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. On delivery, the link monitoring is inactive. You select “Monitor” for link errors if device is to use the signal contact to report a defective 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 84 “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.

[1] You can install additional power supplies in a MACH4000 device, which the device reports as P3-1, P3-2, P4-1 and P4-2 in its user interfaces. You will find details on the power supplies in the document Installation Guide.

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

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.

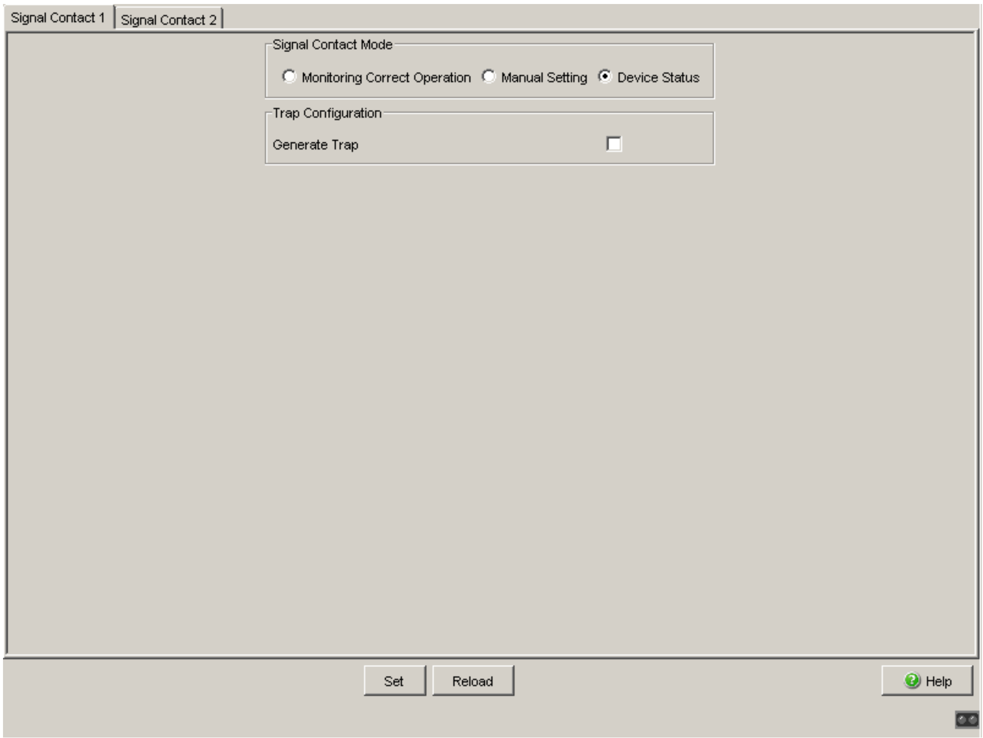
7.6.3 Device status

□ 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 111 “Device Status”) and thereby offers remote diagnosis.
The device status “Error detected” (see on page 111 “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.



Signal Contact 1 | Signal Contact 2

Signal Contact Mode

○ Monitoring Correct Operation ○ Manual Setting ● Device Status

Trap Configuration

Generate Trap □

Figure 37: Signal Contact Dialog

7.7 Alarms (Traps)

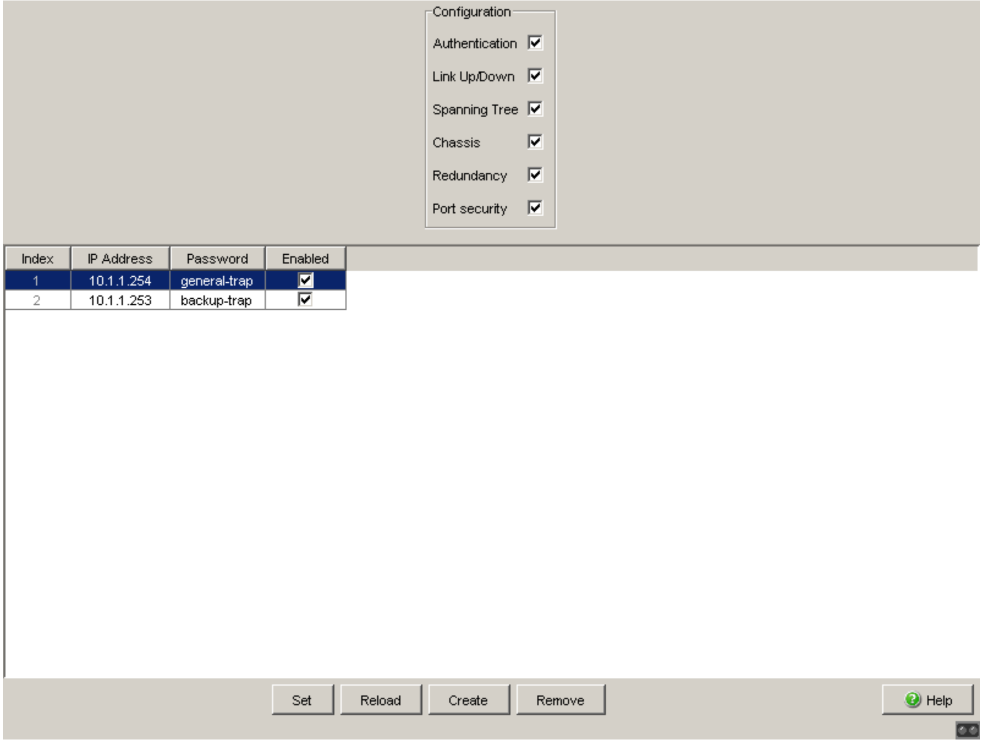
This dialog allows you to determine which events trigger an alarm (trap) and where these alarms should be sent.

□ Select “Create”.
□ In the "IP 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 that the device should take into account when it sends traps. Default setting: inactive.
□ In the “Configuration” frame, select the trap categories from which you want to send traps. Default setting: all trap categories are active.

The events which can be selected are:

Name	Meaning
Authentication	The device has rejected an unauthorized access attempt (see on page 45 “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 AutoConfiguration Adapter (ACA), has been added or removed. - The configuration on the AutoConfiguration Adapter(ACA) does not match that in the device. – The temperature thresholds have been exceeded/not reached. – The receiver power status of a port with an SFP module has changed (see dialog `Diagnostics:Ports:SFP Modules`).
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 29: Trap categories



Configuration

- Authentication ☑
- Link Up/Down ☑
- Spanning Tree ☑
- Chassis ☑
- Redundancy ☑
- Port security ☑

Index	IP Address	Password	Enabled
1	10.1.1.254	general-trap	☑
2	10.1.1.253	backup-trap	☑

Figure 38: Alarms Dialog

7.8 Report

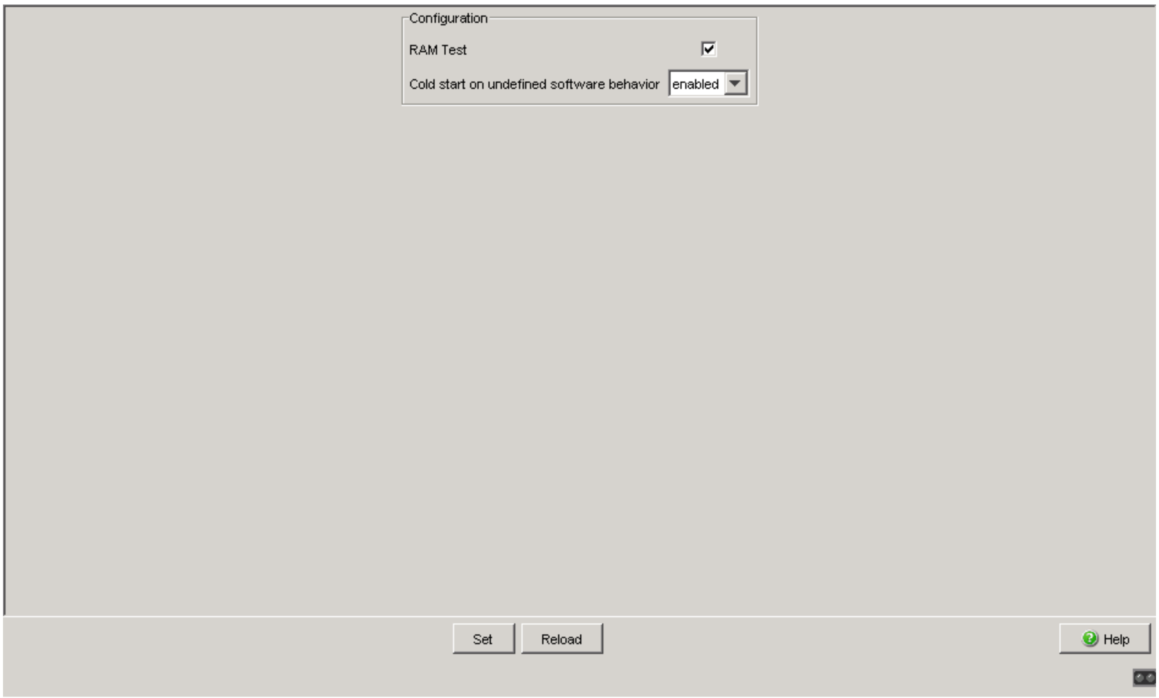
The following reports are available for the diagnostics:

- 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 shortens the booting time for a cold start of the device.
  Default setting: activated.
- allow or prevent a restart due to an undefined software or hardware state.
  Default setting: activated.



Configuration

RAM Test ☑

Cold start on undefined software behavior: enabled

Figure 39: Self-test dialog

8 Advanced

The menu contains the dialogs, displays and tables for:

- DHCP Relay Agent

8.1 DHCP Relay Agent

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 in the table shows you the value that you enter when configuring your DHCP server. In addition to the port number, the “Circuit ID” also includes the ID of the VLAN that the DHCP relay received the DHCP query from.

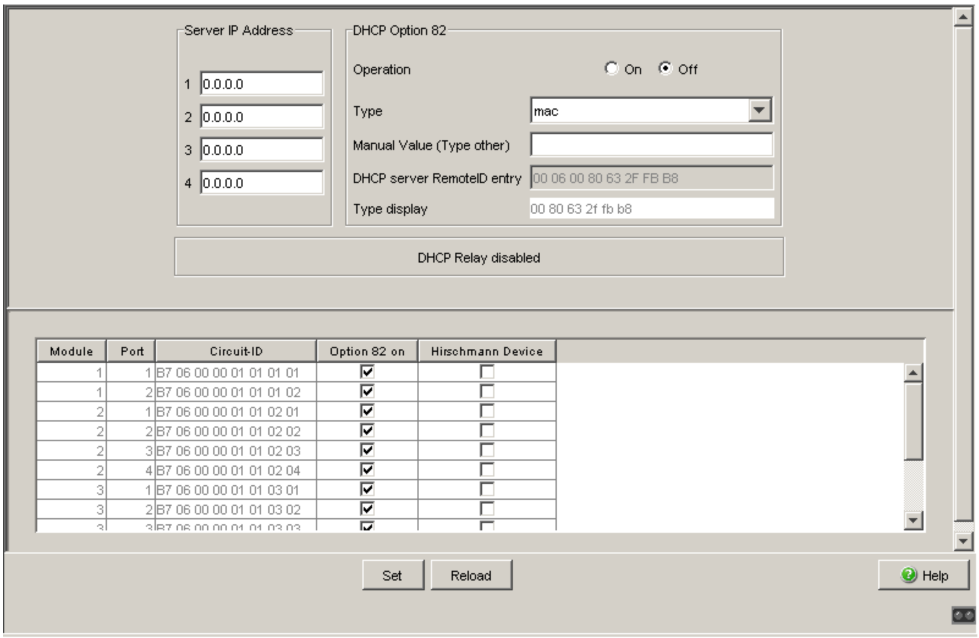
Note: The VLAN ID is located in the circuit ID's 4th and 5th octet. The circuit ID displayed applies to untagged frames. If the DHCP relay receives a VLAN-tagged frame, then the circuit ID that it sends to the DHCP server can deviate from the one displayed.

Example of a configuration of your DHCP server:
Type: `mac`
Remote ID entry for DHCP server: `00 06 00 80 63 00 06 1E`
Circuit ID: `B3 06 00 00 01 00 01 01`

This results in the entry for the “Hardware address” in the DHCP server:
`B306000001000101000600806300061E`

□ In the “Option 82 on” column in the table, you can switch this function on/off for each port.

□ In the "Hirschmann Device" column, you check the ports to which a Hirschmann device is connected.



Server IP Address
1 0.0.0.0
2 0.0.0.0
3 0.0.0.0
4 0.0.0.0

DHCP Option 82
Operation ○ On ● Off
Type: mac
Manual Value (Type other):
DHCP server RemoteID entry: 00 06 00 80 63 2F FB B8
Type display: 00 80 63 2f fb b8

DHCP Relay disabled

Module	Port	Circuit-ID	Option 82 on	Hirschmann Device
1	1	B7 06 00 00 01 01 01 01	☑	□
1	2	B7 06 00 00 01 01 01 02	☑	□
2	1	B7 06 00 00 01 01 02 01	☑	□
2	2	B7 06 00 00 01 01 02 02	☑	□
2	3	B7 06 00 00 01 01 02 03	☑	□
2	4	B7 06 00 00 01 01 02 04	☑	□
3	1	B7 06 00 00 01 01 03 01	☑	□
3	2	B7 06 00 00 01 01 03 02	☑	□
3	3	B7 06 00 00 01 01 03 03	☑	□

Figure 40: DHCP Relay Agent dialog

8.2 Command Line

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

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

A Appendix

A.1 Technical Data

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 IEEE 802.1Q-2005 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)
IEEE 802.1Q-2005	Spanning Tree (STP), Rapid Spanning Tree (RSTP), Multiple Spanning Tree (MSTP)
IEEE 802.1X	Port Authentication
IEEE 802.3-2002	Ethernet
IEEE 802.3ac	VLAN Tagging
IEEE 802.3at-2009	Power over Ethernet (PoE+)
IEEE 802.3x	Flow Control

A.4 Underlying IEC Norms

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

A.5 Copyright of Integrated Software

A.5.1 Bouncy Castle Crypto APIs (Java)

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

A.5.2 Broadcom Corporation

(c) Copyright 1999-2012 Broadcom Corporation. All Rights Reserved.

B Readers’ Comments

What is your opinion of this manual? We are always striving to provide as comprehensive a description of our product as possible, as well as important information that will ensure trouble-free operation. Your comments and suggestions help us to further improve the quality of our documentation.

Your assessment of this manual:

	Very good	Good	Satisfactory	Mediocre	Poor
Precise description	O	O	O	O	O
Readability	O	O	O	O	O
Understandability	O	O	O	O	O
Examples	O	O	O	O	O
Structure	O	O	O	O	O
Completeness	O	O	O	O	O
Graphics	O	O	O	O	O
Drawings	O	O	O	O	O
Tables	O	O	O	O	O

Did you discover any errors in this manual?
If so, on what page?

Suggestions for improvement and additional information:

General comments:

Sender:

Company / Department:

Name / Telephone no.:

Street:

Zip code / City:

e-mail:

Date / Signature:

Dear User,

Please fill out and return this page

- as a fax to the number +49 (0)7127 14-1600 or
- by post to

  Hirschmann Automation and Control GmbH
  Department 01RD-NT
  Stuttgarter Str. 45-51
  72654 Neckartenzlingen

C Index

D Further Support

Technical Questions

For technical questions, please contact any Hirschmann dealer in your area or Hirschmann directly.

You will find the addresses of our partners on the Internet at http://www.hirschmann.com

Contact our support at https://hirschmann-support.belden.eu.com

You can contact us

in the EMEA region at

- Tel.: +49 (0)1805 14-1538
- E-mail: hac.support@belden.com

in the America region at

- Tel.: +1 (717) 217-2270
- E-mail: inet-support.us@belden.com

in the Asia-Pacific region at

- Tel.: +65 6854 9860
- E-mail: inet-ap@belden.com

Hirschmann Competence Center

The Hirschmann Competence Center is ahead of its competitors:

- Consulting incorporates comprehensive technical advice, from system evaluation through network planning to project planning.
- Training offers you an introduction to the basics, product briefing and user training with certification.
  The current technology and product training courses can be found at http://www.hicomcenter.com
- Support ranges from the first installation through the standby service to maintenance concepts.

With the Hirschmann Competence Center, you have decided against making any compromises. Our client-customized package leaves you free to choose the service components you want to use.
Internet:
http://www.hicomcenter.com

HIRSCHMANN

A BELDEN BRAND