HIRSCHMANN
A Belden Company

Reference Manual

Web-based Interface
Industrial ETHERNET (Gigabit) Switch
RS20/RS30/RS40, MS20/MS30, OCTOPUS

Technical Support
HAC-Support@hirschmann.de

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 guaranteed in the contract. This publication has been created by Hirschmann Automation and Control GmbH according to the best of our knowledge. Hirschmann reserves the right to change the contents of this manual without prior notice. Hirschmann can give no guarantee in respect of the correctness or accuracy of the details in this publication.

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.

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

Content

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 all the other information that you need to install the device before you begin with the configuration of the device.

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

The “Redundancy Configuration” user manual contains all the information you need to select a suitable redundancy procedure and configure it.

The “Industry Protocols” user manual describes how the device is connected by means of a communication protocol commonly used in the industry, such as EtherNet/IP and PROFINET.

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

- Event logbook.
- Configuration of „System Location“ and „System Name“.
- Configuration of the network address range and SNMP parameters.
- Saving the configuration on the device.
- Simultaneous configuration of multiple devices.
- Configuration of the port display color red for a connection error.

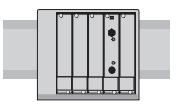
Key

The designations used in this manual have the following meanings:

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

Symbols used:

	Router with firewall
	Switch with firewall
	Router
	Switch
	Bridge
	Hub

	A random computer
	Configuration Computer
	Server
	PLC - Programmable logic controller
	I/O - Robot

1 Opening the Web-based Interface

To open the Web-based interface, you will 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 the “Java™ Runtime Environment Version 1.4.2.x, 1.5.x or 6.x” plug-in. If it is not installed on your computer yet, it will be installed automatically via the Internet when you start the Web-based interface for the first time. This installation is very time-consuming.

For Windows users: cancel the installation. Install the plug-in from the enclosed CD-ROM. To do this, you go to “Additional Software”, select `Java Runtime Environment` and click on “Installation”.

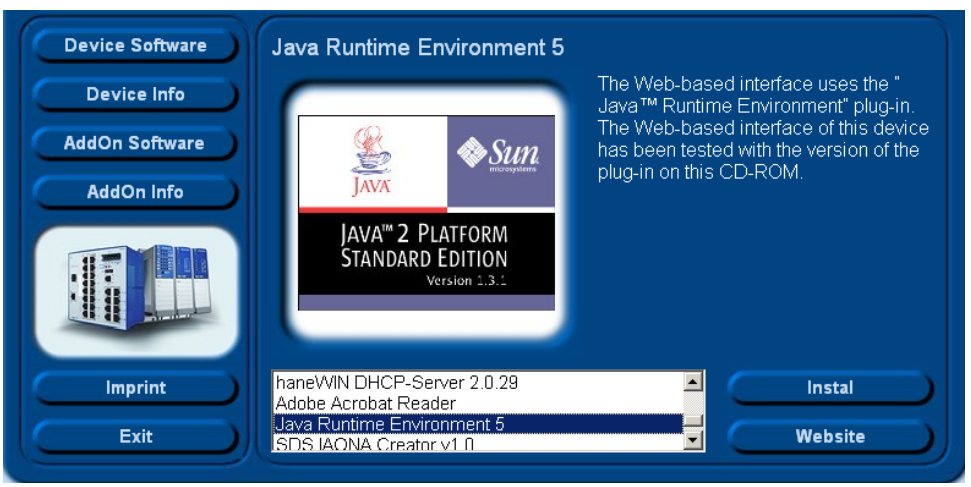


Figure 1: Installing Java

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

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

The login window appears on the screen.

Figure 2: Login window

☐ Select the desired language.
☐ In the drop-down menu, 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, appears in the password field. If you wish to have write access to the device, then highlight the contents of the password field and overwrite it with the password “private” (default setting).
☐ Click on OK.

The Web site of the device appears on the screen.

Note: The changes you make in the dialogs are copied to the device when you click on “Write”. Click on “Load” to update the display.

Note: You can block your access to the device by entering an incorrect configuration.
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.

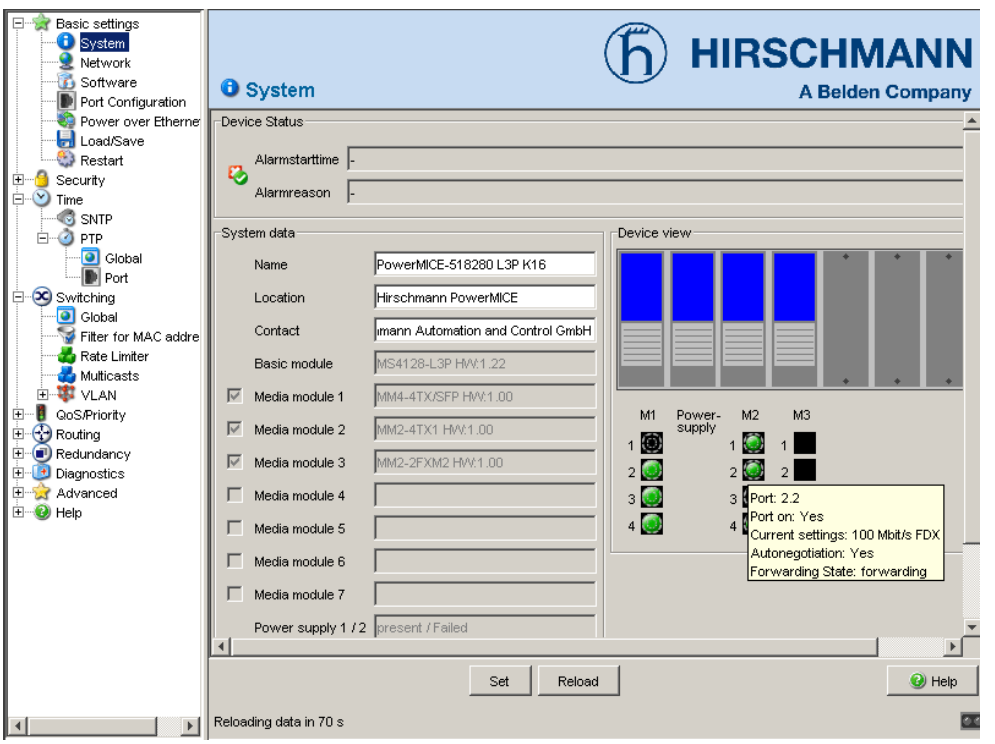
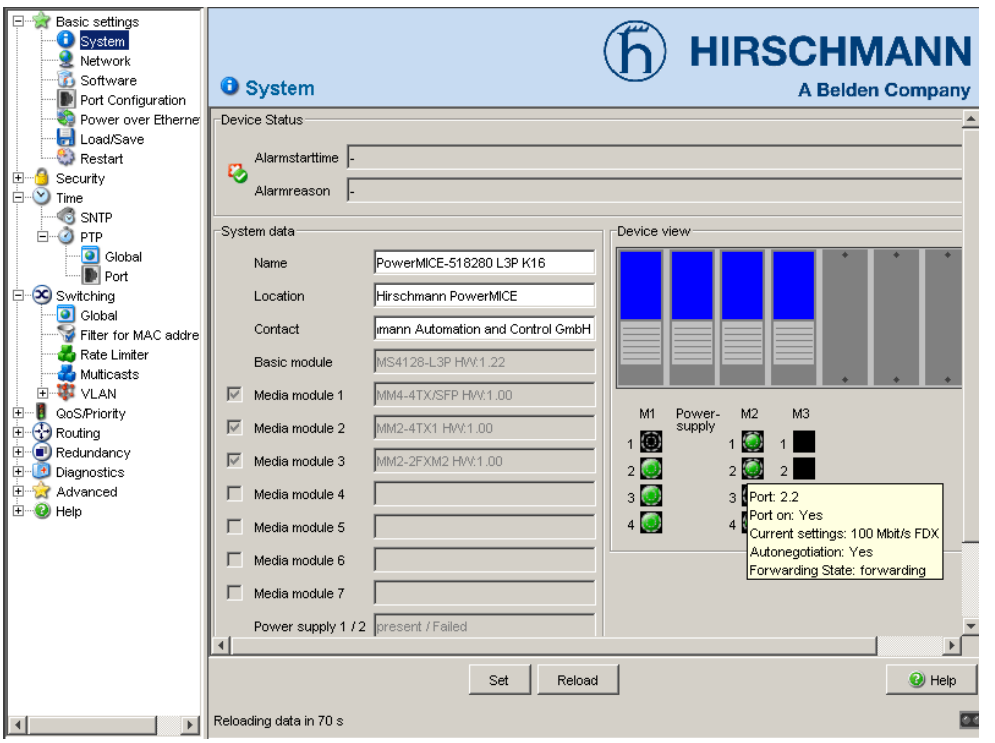


Figure 3: Website of the device with speech-bubble help

The menu section displays the menu items. By placing the mouse pointer in the menu section and clicking the right 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.



2 Basic Settings

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

- System
- Network
- Software
- Port configuration
- Power over Ethernet
- Load/Save
- Restart

2.1 System

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

- Device status
- System data
- Device view
- Reloading data

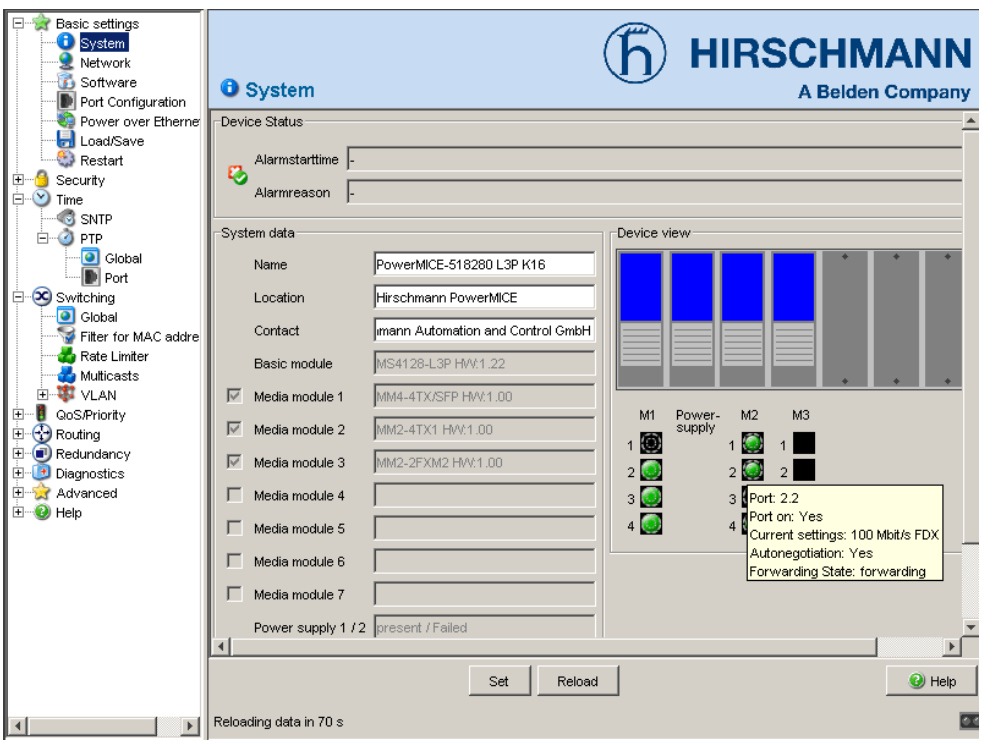


Figure 4: "System" submenu

Device status

This section of the website provides information on the device status and the alarm state of the device.

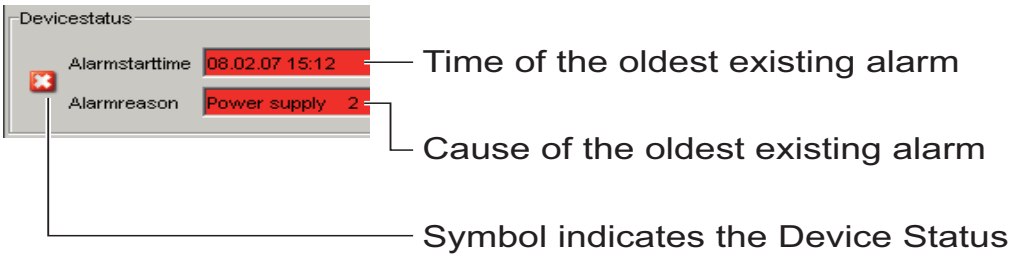


Figure 5: Device status and alarm display

System data

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

- the system name,
- the location description,
- the name of the contact person for this device,
- the availability of the media modules (see fig. 6) and
- the temperature threshold values.

Name	Meaning
Name	System name of this device
Location	Location of this device
Contact person	Contact person for this device
Basic module	Hardware version of the basic module
Media module 1	Hardware version of media module 1
Media module 2	Hardware version of media module 2
Media module 3	Hardware version of media module 3
Media module 4	Hardware version of media module 4
Media module 5	Hardware version of media module5
Media module 6	Hardware version of media module 6
Media module 7	Hardware version of media module 7
Power supply (P1/P2)	Status of the power supply units
Operating time	Time that has elapsed since the device was last restarted.
Temperature	Temperature in the device. Lower/upper temperature threshold values. If the temperature goes outside this range, the device generates an alarm message.

Table 1: System data

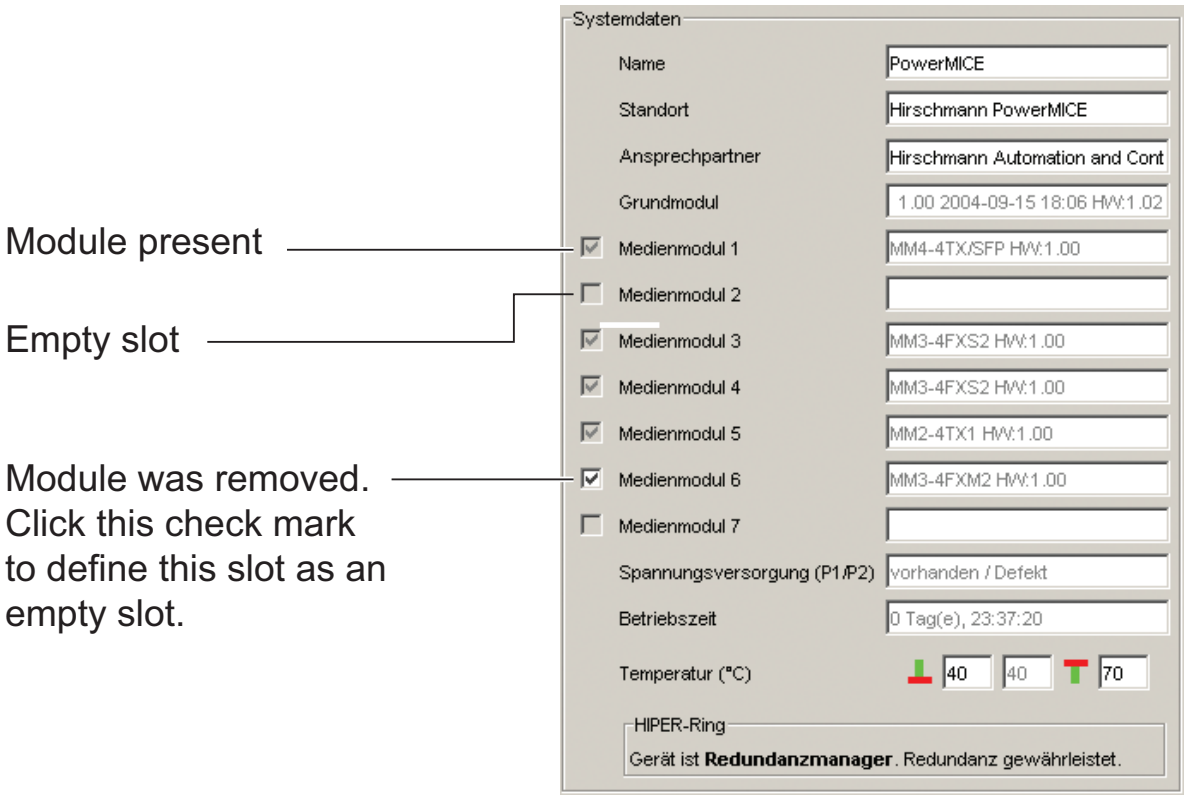


Figure 6: Availability of the media modules

Device view

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

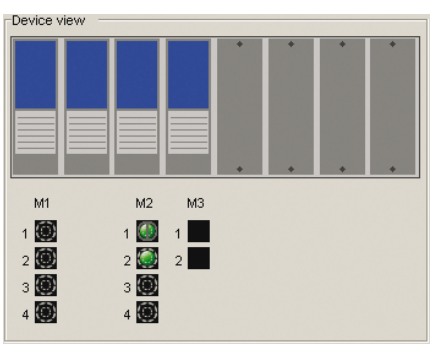


Figure 7: Device view

Meaning of the symbols:

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

The port is disabled by the management and it has a connection.

The port is disabled by the management and it has no connection.

The port is in autonegotiation mode.

The port is in HDX mode.

The port is in RSTP discarding mode (100 Mbit/s).

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

Updating

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

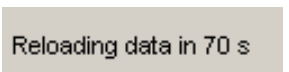


Figure 8: Time until update

2.2 Network

With the `Basics:Network` dialog you define the source from which the device gets its IP parameters after starting, and you assign the IP parameters and VLAN ID and configure the HiDiscovery access.

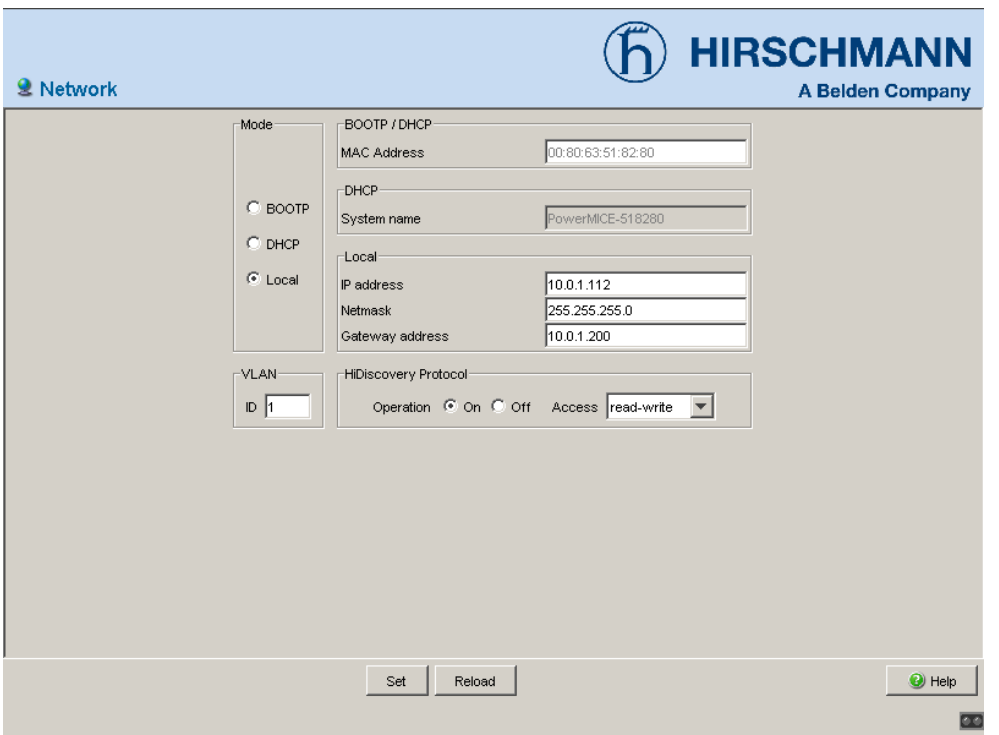


Figure 9: Network parameters dialog

☐ Under "Mode", enter where the device is to obtain 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 page 30 „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 page 30 „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 "VLAN ID" frame enables you to assign a VLAN to the agent. If you enter the illegal VLAN ID "0" here, the agent can be accessed by all VLANs.

- The HiDiscovery protocol allows you to assign an IP address to the device on the basis of its MAC address. Activate the HiDiscovery protocol if you want to assign an IP address to the device from your PC with the enclosed HiDiscovery software (setting on delivery: active).

2.3 Software

The software dialog enables you to carry out a software update of the device via tftp or file selection.

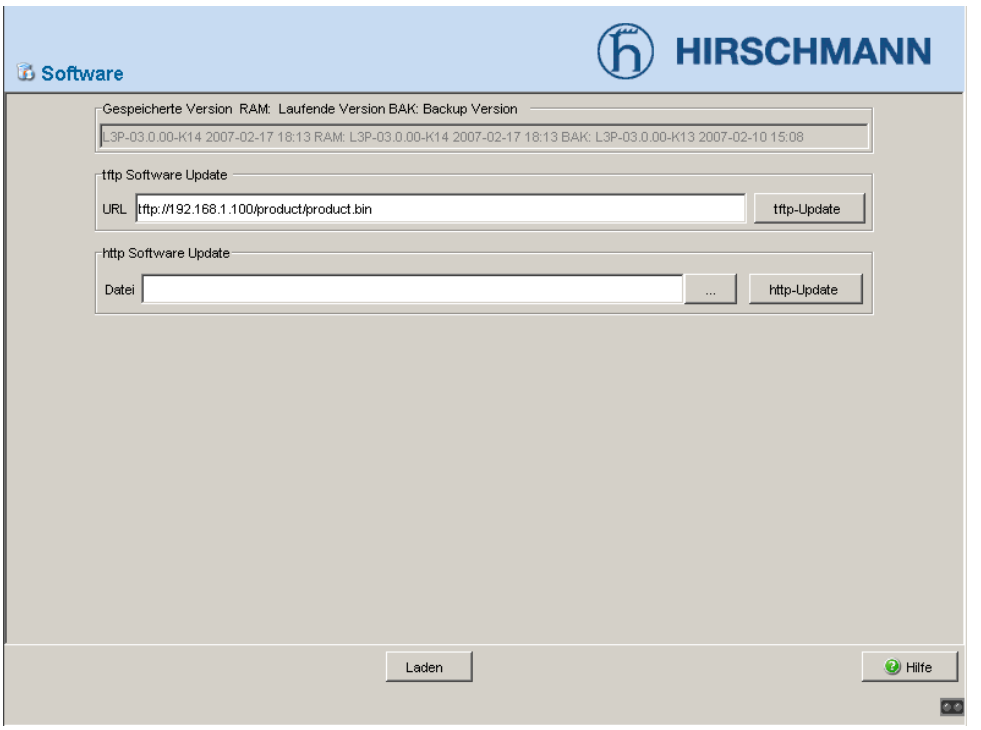


Figure 10: Software dialog

2.3.1 Update via file selection

For an update via a file selection window, the device software must be on a drive that you can access via your PC.

☐ In the file selection frame, click on "...".

☐ In the file selection window, select the device software (device.bin) and click on "Open".

☐ Click on "Update" to transfer the software to the device.

The end of the update is indicated by one of the following messages:
- Update completed successfully.
- Update failed. Reason: incorrect file.
- Update failed. Reason: error when saving.

☐ After loading successfully, activate the new software:
Select the dialog `Basic Settings: Restart` 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.

2.3.2 tftp 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://149.218.112.5/mice/mice.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 „Restart“ dialog on page 35“).

2.4 Port Configuration

This configuration table allows you to configure every port of the device.

- In the “Port Name” column, you can enter a name for every port.
- In the “Ports on” column, you can switch on the port by marking it here.
- In the “Propagate connection error ” column, you can specify that the signal contact is to be opened when a link alarm occurs.
- In the “Automatic Configuration” column, you can activate the automatic selection the operating mode (Autonegotiation) and the automatic assigning of the connections (Auto cable crossing) of a TP port by marking the appropriate field. After the automatic configuration has been switched on, it takes a few seconds for the operating mode to be set.
- In the “Manual Configuration” column, you set the operating mode for this port. The choice of operating modes depends on the media module. The possible operating modes are:
  - 10 Mbit/s half duplex (HDX),
  - 10 Mbit/s full duplex (FDX),
  - 100 Mbit/s half duplex (HDX),
  - 100 Mbit/s full duplex (FDX),
  - 1000 Mbit/s half duplex (HDX) and
  - 1000 Mbit/s full duplex (FDX).
- The “Link/Current settings” column displays the current operating mode and thereby also an existing connection.
- In the “Cable-Crossing” 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 port output and port input of the TP port.
  - disable: the device does not swap the port output and port input of the TP port.
  - unsupported: the port does not support this function (optical port, TP SFP port).
- In the “Flow Control” column, you checkmark this port to specify that flow control is active here. You also activate the global “Flow Control” switch in the „Switching Global“ dialog on page 60.

Note: If you have set up VLANs, pay attention to the “Transparent mode” under „Setting up the VLAN“ on page 73“.

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:

Bit rate	100 Mbit/s	1000 Mbit/s
Autonegotiation (automatic configuration)	Off	On
Port	On	On
Duplex	Full	–

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.

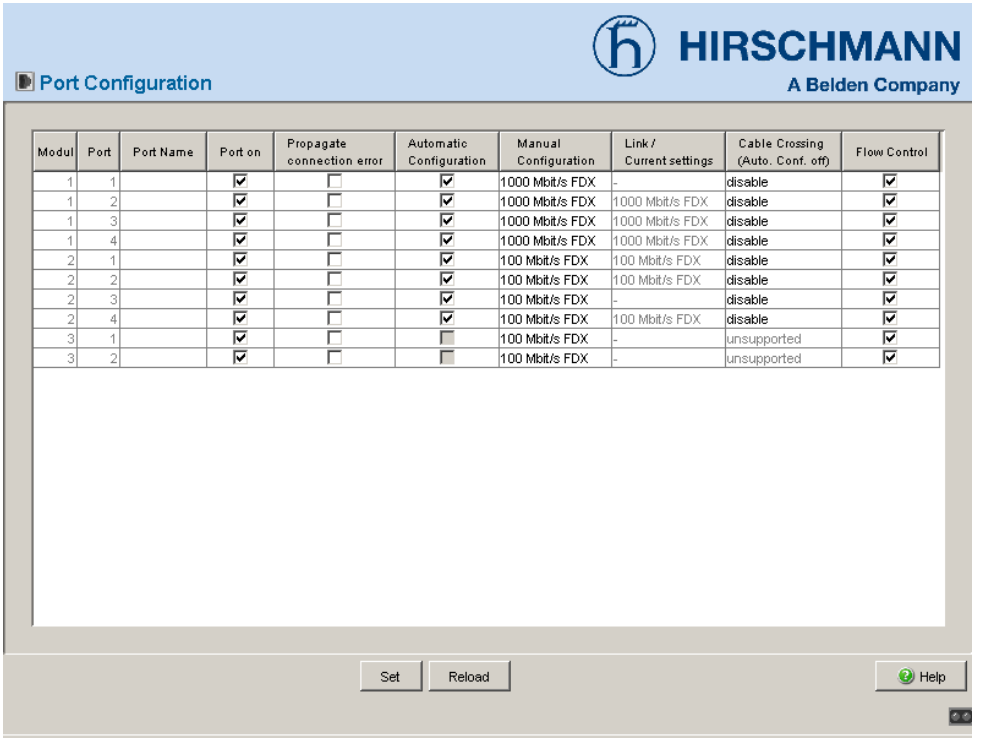


Figure 11: Port configuration table dialog

2.5 Power over ETHERNET

If the device is equipped with PoE media modules (MS20/30, Power MICE, MACH 4000) or PoE ports (OCTOPUS ... PoE), you will then have the option of supplying current to devices such as IP phones via the twisted-pair cable. PoE media modules support Power over ETHERNET according to IEEE 802.3af.
On delivery, the Power over ETHERNET function is activated globally and on all ports.
If the device is equipped with PoE media modules, you will then have the option of supplying current to devices such as IP phones via the twisted-pair cable. PoE media modules support Power over ETHERNET according to IEEE 802.3af.
On delivery, the Power over ETHERNET function is activated globally and on all ports.

System power for MS20/30 and Power MICE:
The device provides the nominal system power for the sum of all PoE ports plus a surplus. Because the PoE media module gets its operating voltage externally, the device does not know the possible system power. The device therefore assumes for now a "nominal system power" of 60 Watt per PoE media module.

Nominal power for OCTOPUS 8M-.PoE:
The device provides the nominal power for the sum of all PoE ports plus a surplus. Because the device gets its PoE voltage externally, the device does not know the possible nominal power.
The device therefore assumes a “nominal power” of 15 Watt per PoE port for now.

- ☐ 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 “Port on” column, you can enable/disable PoE at this port.
- ☐ The “Status” column indicates the PoE status of the port.
- ☐ In the “Priority” column (MACH 4000), set the PoE priority of the port to “low”, “high” or “critical”.
- ☐ The “Class” column shows the class of the connected device:

Class	Maximum power delivered
0	15.4 W = state on delivery
1	4.0 W
2	7.0 W
3	15.4 W
4	Reserved, treat as class 0

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

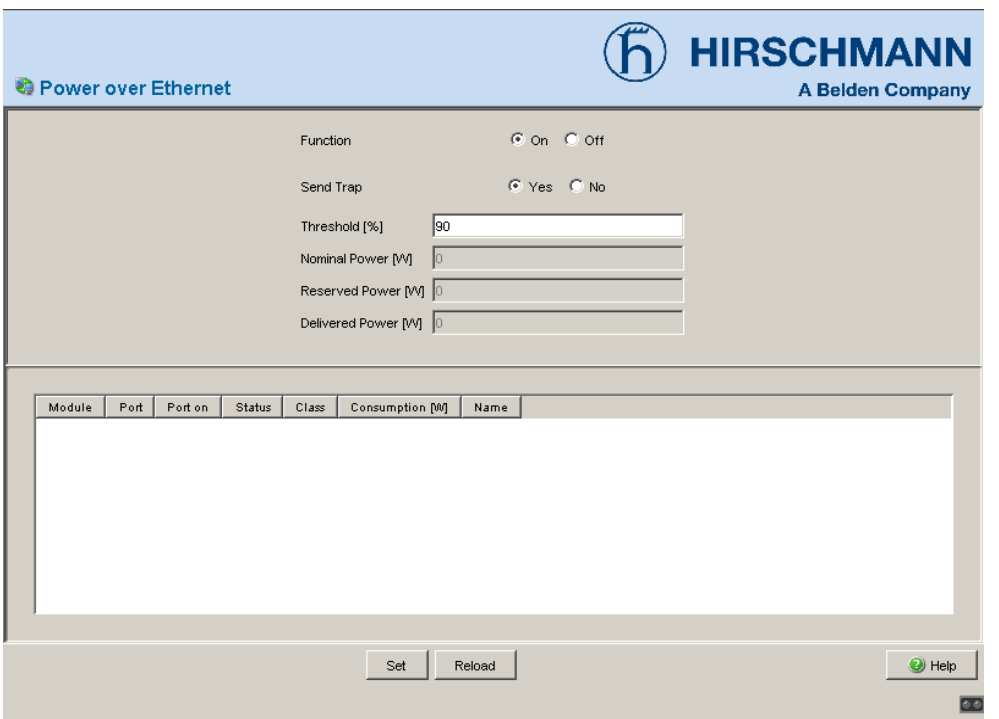


Figure 12: Power over Ethernet dialog

2.6 Load/Save

With this dialog you can:

- load a configuration,
- save a configuration,
- enter a URL,
- restore the delivery configuration,
- use the ACA for configuring,
- cancel a configuration change.

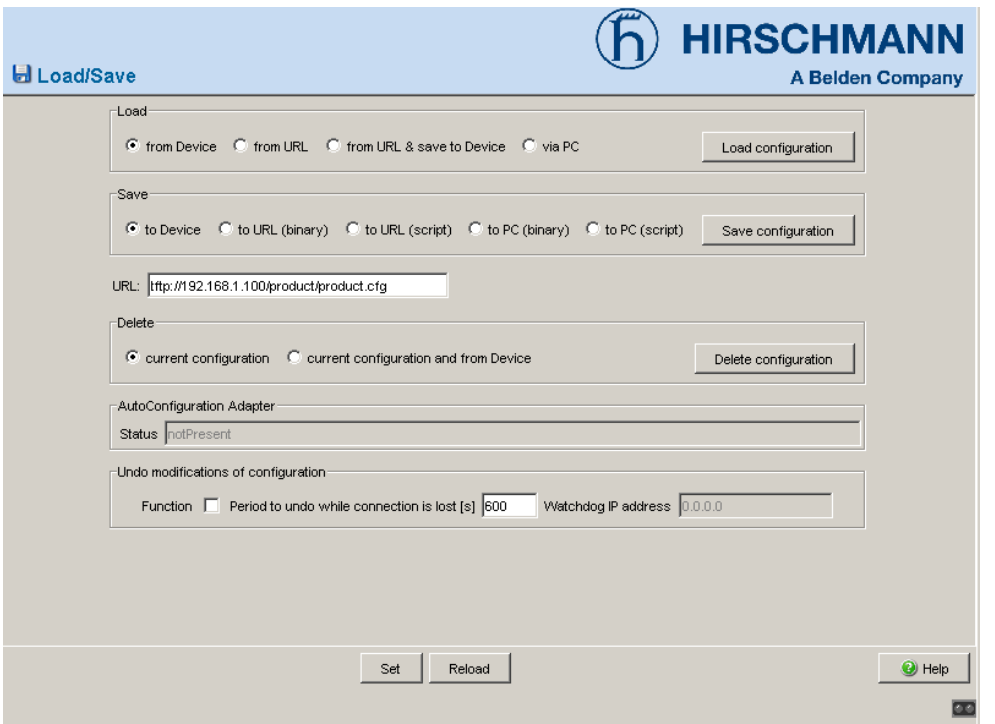


Figure 13: Load/store dialog

2.6.1 Loading the configuration

In the "Load" frame, you have the option to

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

If you change the current configuration (for example, by switching a port off), the load/save symbol in the menu area changes from a disk symbol into a yellow triangle. After saving the configuration, the load/save symbol changes back into the disk symbol.

2.6.2 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 on page 20 „Network“) 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, then finish the loading process by loading the local configuration in the "Load" frame.

If you change the current configuration (for example, by switching a port off), the load/save symbol in the menu area changes from a disk symbol into a yellow triangle. After saving the configuration, the load/save symbol changes back into the disk symbol.

2.6.3 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://149.218.112.5/mice/config.dat`).
The configuration file includes all configuration data, including the password. Therefore pay attention to the access rights on the tftp server.

2.6.4 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 to the state on delivery. After the next restart, the IP address is also in the state on delivery.

2.6.5 Using the AutoConfiguration Adapter (ACA)

The ACAs are devices for saving the configuration data of a device. In the case of a device failure, an ACA enables the configuration data to be transferred easily by means of a substitute device of the same type.

Note: If you replace a device with DIP switches, please ensure that the DIP switch settings are identical.

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

- **Transferring the configuration data from the ACA:**
  When you restart 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 it is completely new, the device loads the data from the flash memory.

  Note: Before loading the configuration data from the ACA, the device compares the password stored 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 stored locally or
  - The local password is the initial state of delivery password or
  - No configuration is saved locally.

Status	Meaning
notPresent	No ACA present.
ok	The configuration data from the ACA and the device are consistent.
removed	The ACA has been removed after booting.
notInSync	The configuration data from the ACA and the device are not consistent.
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

2.6.6 Canceling a configuration change

Operation

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

☐ Activate the function before you configure the device so that after an incorrect configuration has interrupted your connection to the device, you will be connected to the device again.

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

Note: Deactivate the function after you have successfully saved the configuration. You thus prevent the device from reloading the configuration after the time period entered has elapsed, when you close the web interface.

Watchdog IP address

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

2.7 Restart

With this dialog you can:

- Cold start the device. In a cold start, the device reloads the software from the non-volatile memory, restarts, and performs a self-test.
- Warm start the device. In this case the device checks the software in the volatile memory and restarts.
- 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 have problems with the connection, 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 HiVision.

Figure 14: Restart dialog

3 Security

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

- Password
- SNMPv1/v2 access
- Telnet/Web access
- Port security

3.1 Password / SNMP

This dialog gives you the option of changing the read and read/write passwords for access to the device via the Web-based interface/CLI/SNMP. Please note that passwords are case-sensitive. For security reasons, the read password and the read/write password must not be identical.

The Web-based interface and the user interface communicate via SNMP version 3.

☐ Select "Modify read-only password" 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" to enter the read/write password.
☐ Enter the read/write password and repeat your entry.

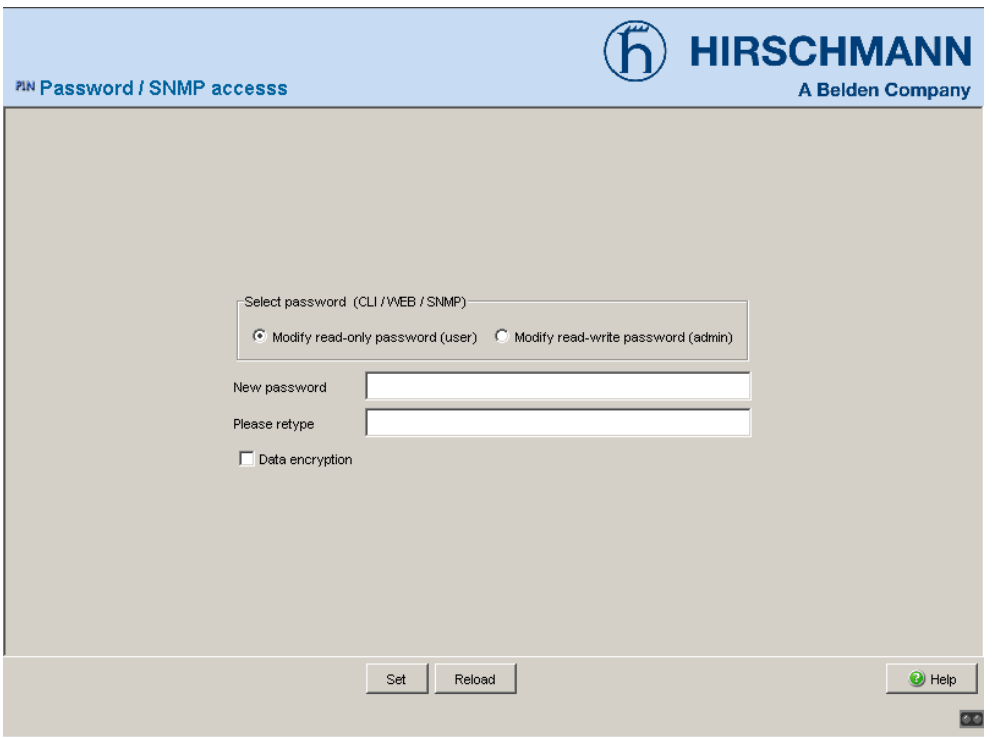


Figure 15: Password dialog

Important: If you do not know a password with read/write access, you will not have write access to the device!

Note: After changing the password for write access, restart the Web interface in order to access the device.

Note: For security reasons, the passwords are not displayed. Make a note of every change! You cannot access the device without a valid password!

Note: For security reasons, SNMP version 3 encrypts the password. With the "SNMPv1" or "SNMPv2" setting in the Security:SNMPv1/v2 access dialog, the password becomes readable again.

Note: In SNMP version 3, use between 5 and 32 characters for the password, because many applications do not accept shorter passwords.

Access via a Web browser can be blocked in the dialog „Telnet/Web Access“ on page 43.

Access at IP address level is restricted in the dialog „SNMPv1/v2 Access Setting“ on page 40.

3.2 SNMPv1/v2 Access Setting

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: For displaying the entries of the dialog you need read-write access.

- In the "Index" column, you enter the current number to which the access restriction applies.
- Enter the password with which this computer may access the device in the "Password" column. Please note that passwords are case-sensitive. This password is independent of the SNMPv3 password.
- 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", enables access to the 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 network masks, you can select 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 or with the read/write password.
- You can activate/deactivate this table entry in the "Active" column.

Important: If no line is marked, then there are no access restrictions as regards the IP addresses!

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

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

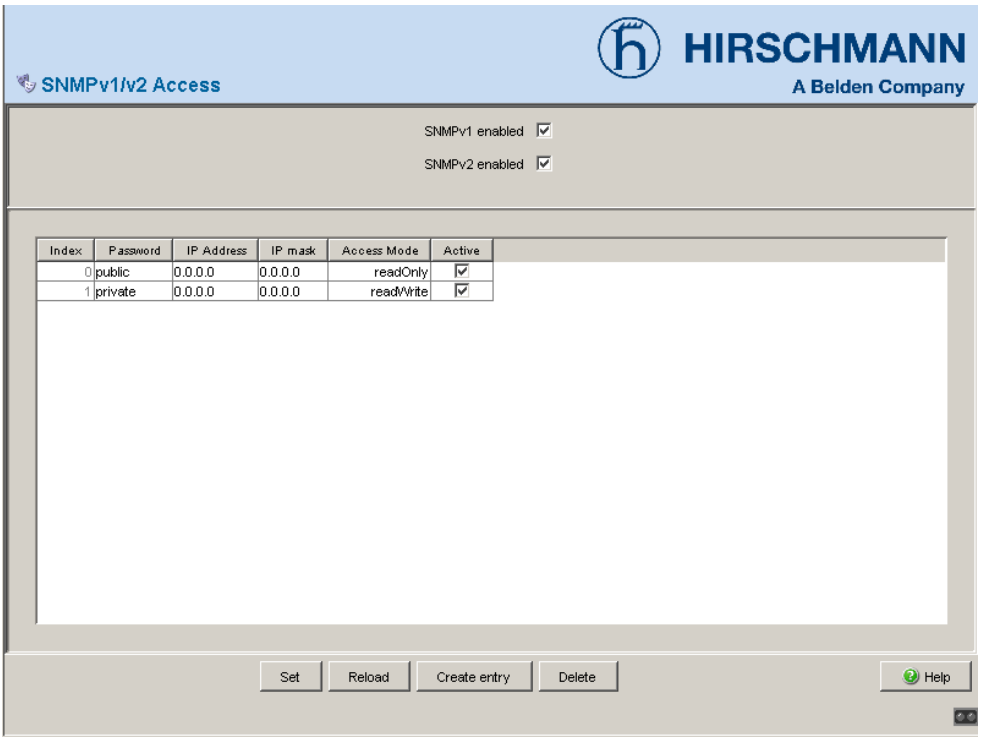


Figure 16: SNMPv1/v2 access dialog

3.3 Telnet/Web Access

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

Figure 17: Telnet/Web access dialog

3.3.1 Description of Telnet access

The Telnet server of the device allows you to configure the device by using the Command Line Interface (in-band). You can deactivate the Telnet server to prevent Telnet access to the device.
On delivery, the server is activated.
After the Telnet server has been deactivated, you will no longer be able to access the device via a new Telnet connection. If a Telnet connection already exists, it is kept.

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

3.3.2 Description of Web access

The Web server of the device 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.
On delivery, the server is activated.

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

Note: The Command Line Interface and this dialog allow you to reactivate the Telnet server.

3.4 Port Security

In this dialog you can specify for each port from which terminal devices data can be received and sent to other ports. This function protects the network from unauthorized access.

☐ First select whether you want MAC-based or IP-based port security.

☐ If you have selected MAC-based security, you enter the MAC addresses of the devices with which a data exchange at this port is permitted in the "Allowed Mac Address" column. You can enter up to 10 MAC addresses, separated by a space character. If no entry is made, all devices can receive data.

▶ The "Current MAC Address" column shows the MAC address of the device from which data was last received. By pressing the left mouse button, you can copy an entry from the "Current MAC Address" column into the "Allowed MAC Address" column.

☐ If you have selected IP-based security, you enter the IP addresses of the devices with which a data exchange at this port is permitted in the "Allowed IP Address" column. You can enter up to 10 IP addresses, separated by a space character. If no entry is made, all devices can receive data.

☐ In the "Action" column you select whether an unauthorized access bid should be followed by
- ▶ no action (none) or
- ▶ the sending of an alarm (trap) (trapOnly) or
- ▶ the disabling of the port by the corresponding entry in the port configuration table (see on page 29 „Load/Save“) and the sending of an alarm (trap) (portDisable).

▶ The "Port Status" column indicates the status of the port.
Display "enabled": this port is switched on and transmitting.
Display "disabled": this port is switched off and not transmitting.
The port is switched on if
an authorized address accesses the port
or
"trapOnly" or "none" are selected under "Action" and an unauthorized address attempts to access the port.

The port is switched off if
"portDisable" is selected under "Action" and an unauthorized address attempts to access the port.

☐ In the "Action" column you select whether an unauthorized access attempt should be followed by
- no action (none) or
- the sending of an alarm (trap) (trapOnly) or
- the disabling of the port by the corresponding entry in the port configuration table (see on page 24 „Port Configuration“) and the sending of an alarm (trap) (portDisable).

Note: This entry in the port configuration table is part of the configuration (see on page 29 „Load/Save“) and is saved together with the configuration.

Note: Prerequisites for the device to be able to send an alarm (trap) (see on page 144 „Alarms (Traps)“):
– at least one recipient is entered
– the corresponding status (“active”) is selected
– “port security” is selected.

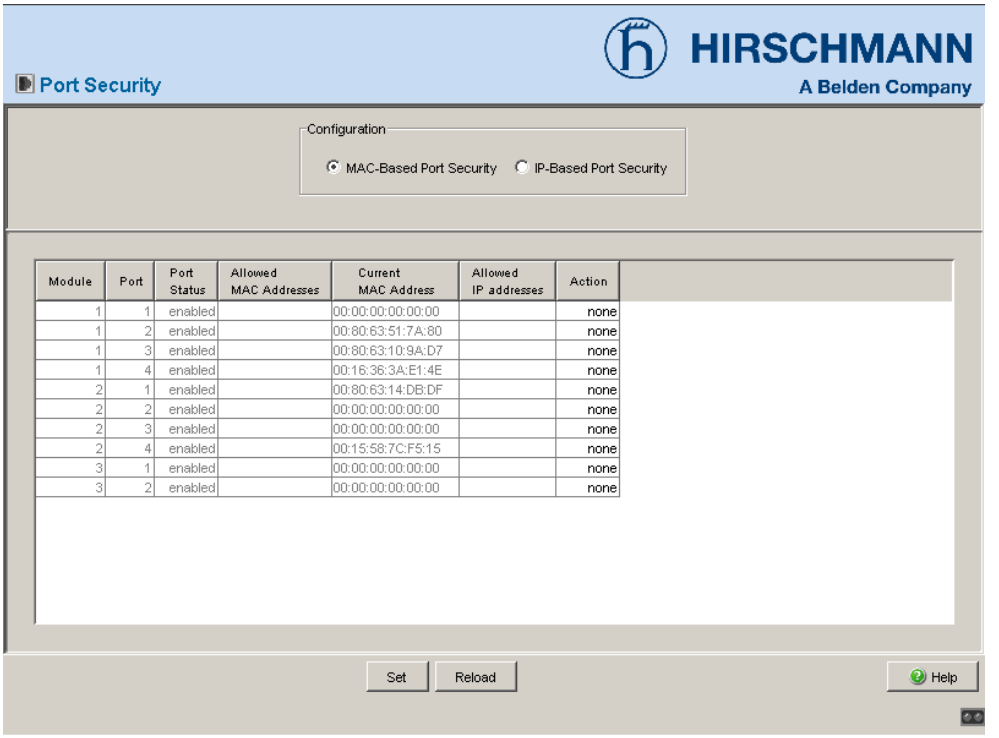


Figure 18: Port Security dialog

Note: Since the device is a layer 2 device, it translates the IP addresses entered into MAC addresses. For this, exactly one IP address must be assigned to a MAC address.
Please keep in mind that when using a router, for example, several IP addresses can be assigned to one MAC address, namely that of the router. This means that all packets of the router will pass the port unchecked if the permitted IP address is that of the router.
If a connected device sends packets with other MAC addresses and a permitted IP address, the device will disable the port.

4 Time

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

- The "IEEE 1588 time" displays the time determined using PTP.
  The "SNTP time" displays the time with reference to Universal Time Coordinated (UTC).
  The time displayed is the same worldwide. Local time differences are not taken into account.

- The "System time" uses the "IEEE 1588 / SNTP time", allowing for the local time difference from "IEEE 1588 / SNTP time".
  "System time" = "IEEE 1588 / SNTP time" + "Local offset"

- "Time source" displays the source of the following time data. The device automatically selects the source with the greatest accuracy.

☐ With "Set time from PC" the device takes the PC time as the system time and calculates the IEEE 1588 / SNTP time using the local time difference.
"IEEE 1588 / SNTP time" = "System time" - "Local offset"

☐ The "Local Offset" is for displaying/entering the time difference between the local time and the "IEEE 1588 / SNTP time".
With "Set offset from PC", the agent 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. 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 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.

Note: There may be a maximum of one device with an enabled PTP function and enabled SNTP function in an SNTP cascade.

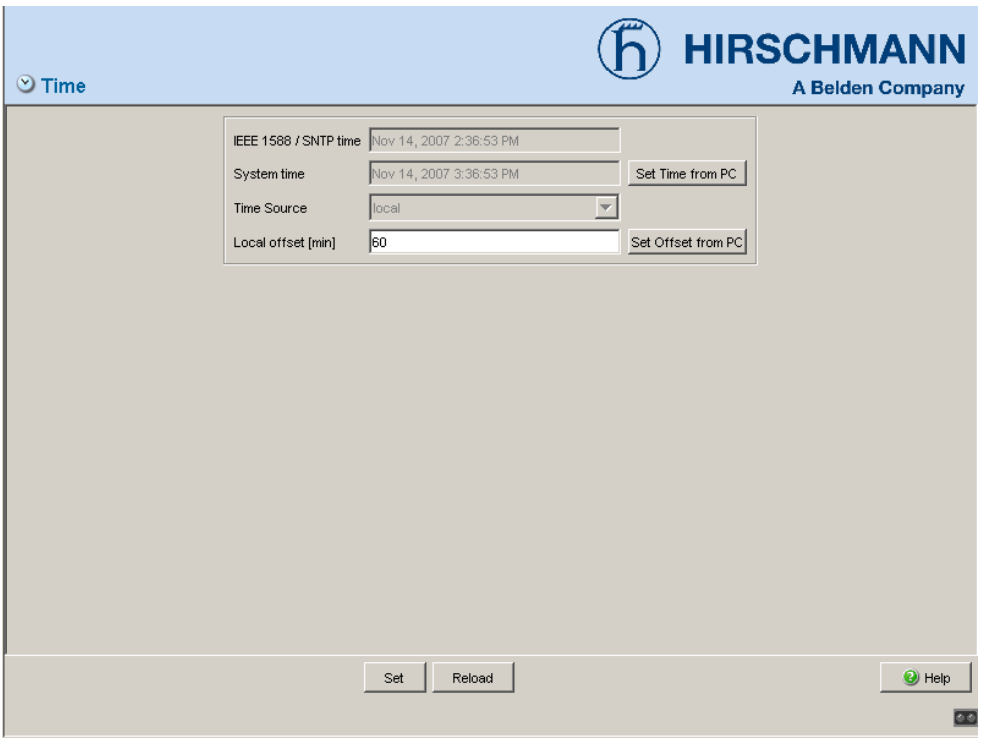


Figure 19: Time dialog

4.1 SNTP configuration

The Simple Network Time Protocol (SNTP) enables you to synchronize the system time in your network.
The device supports the SNTP Server and SNTP Client functions.
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. The SNTP client obtains the UTC from the SNTP server.

Note: For the most accurate system time distribution possible, avoid having network components (routers,switches, hubs) which do not support SNTP in the signal path between the SNTP server and the SNTP client.

- Configuration SNTP Client and Server
  - ☐ 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.

- SNTP Status
  - ☐ The "Status message" displays conditions such as "Server cannot be reached".

- Configuration SNTP Server
  - ☐ In "Anycast destination address" you enter the IP address to which the SNTP server on the device sends the SNTP packets.

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 4: Periodic sending of SNTP packets

- ☐ In "VLAN ID" you specify the VLAN to which the device may periodically send SNTP packages.
- ☐ In "Anycast send interval" you specify the interval at which the device sends SNTP packets (valid entries: 1 second to 3600 seconds, on delivery: 120 seconds).
- ☐ With "Disable Server at local time source" the device disables the SNTP server function if the status of the time source is "local" (see Time dialog).

▶ Configuration SNTP Client

- ☐ In "External server address" you enter the IP address of the SNTP server from which the device periodically requests the system time.
- ☐ In "Redundant server address" you enter the 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.

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

- ☐ In "Server request interval" you specify the interval at which the device requests SNTP packets (valid entries: 1 second to 3600 seconds, on delivery: 30 seconds).
- ☐ With "Accept SNTP Broadcasts" the device takes the system time from SNTP broadcast/Multicast packets that it receives.
- ☐ With "Threshold for obtaining the UTC" you can reduce the frequency of time alterations. Enter the threshold in milliseconds. The device changes the time as soon as the deviation from the server time is above this threshold.

☐ With "Disable client after successful synchronization" you disable further time synchronizations once the device has synchronized its time with the server.

Note: For the most accurate system time distribution possible, avoid having network components (routers,switches, hubs) which do not support SNTP in the signal path between the SNTP server and the SNTP client.

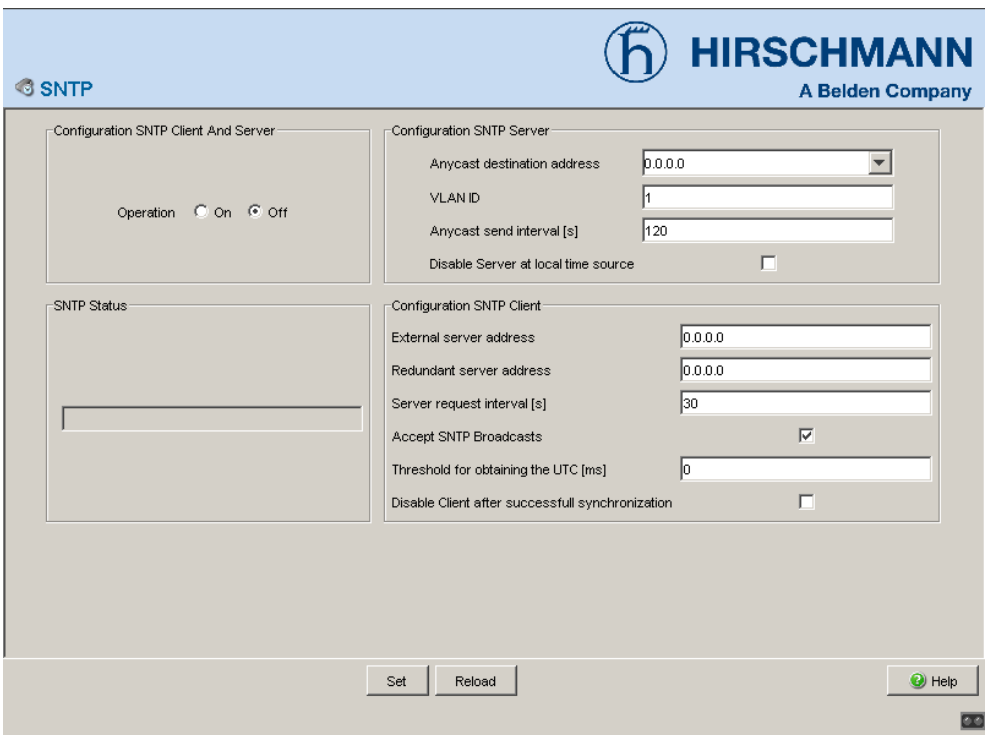


Figure 20: SNTP dialog

4.2 PTP configuration

MS20/MS30:
PTP offers you the dialogs

- „PTP Global (MS20/MS30, Power MICE)“
- „PTP Port (MS20/MS30, Power MICE)“

Precise time management is required for running time-critical applications via a LAN.
The IEEE 1588 standard with the Precision Time Protocol (PTP) describes a procedure that assumes one clock is the most accurate and thus enables precise synchronization of all clocks in an LAN.
RS20/RS30/RS40, OCTOPUS:

- IEEE 1588/PTP function
  In this frame you switch the PTP on/off.

4.2.1 PTP Global (MS20/MS30, Power MICE)

This dialog offers you the option of making basic settings for the Precision Time Protocol.

- IEEE 1588/PTP function
  In this frame you switch the PTP on/off.

- Configuration IEEE 1588/PTP
  `Clock Mode`: Mode of the local clock.
  The options are:
  – `ptp-mode-boundary-clock`,
  – `ptp-mode-simple-ptp` (without delay correction or specification of best clock). Select this mode if the device does not have a timestamp unit (RT module).

  `Sync Interval`: period for transmitting synchronization messages, specified in seconds. You apply the changes with "Reinitialize".

`SyncLowerBound`: Bottom PTP synchronization threshold value, specified in nanoseconds. If the sum of (reference time - local time) is lower than the value of the bottom PTP synchronization threshold, then the local clock is deemed as synchronous with the reference clock.

`SyncUpperBound`: Top PTP synchronization threshold value, specified in nanoseconds. If the sum of (reference time - local time) is greater than the value of the top PTP synchronization threshold, then the local clock is deemed as not being synchronous with the reference clock.

`Subdomain Name`: Name of the PTP subdomain to which the local clock belongs. You apply the changes with "Reinitialize".

`Preferred Master`: Defines the local clock as the preferred master. If PTP does not find another preferred master, then the local clock is used as the grandmaster clock. If PTP finds other preferred masters, then PTP determines which of the preferred masters is used as the grandmaster clock.

- Status IEEE 1588/PTP (with MS 20/30 and PowerMICE)
  `Is Synchronized`: The local clock runs synchronously with the reference clock, compare `SyncLowerBound` and `SyncUpperBound`.

  `Offset to Master`: Total deviation of the local clock from the reference clock in nanoseconds.

  `Max. Offset Absolute`: Total deviation of the local clock from the reference clock in nanoseconds since the local clock was last reset. The local clock is reset with "Reinitialize" in this dialog or by resetting the device.

  `Delay to Master`: Single signal runtime between the local device and reference clock in nanoseconds.

  `GrandmasterUUID`: MAC address of the grandmaster clock (Unique Universal Identifier).

  `ParentUUID`: MAC address of the master clock with which the local time is directly synchronized.

  `Clock Stratum`: Qualification of the local clock.

  `Clock Identifier`: Clock properties (e.g accuracy, epoch, etc.).

With "Reinitialize" you trigger the synchronization of the local clock.

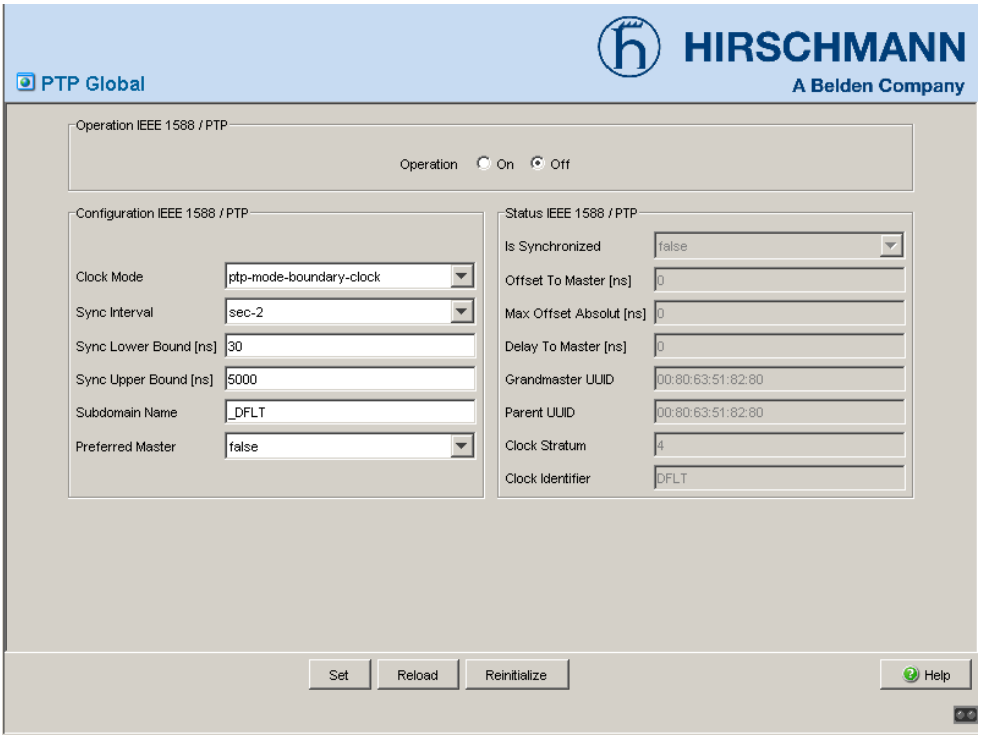


Figure 21: PTP-Global (with MS 20/30 and PowerMICE)

4.2.2 PTP Port (MS20/MS30, Power MICE)

This dialog
– Allows you to make port-related PTP settings and
– Displays port-related PTP statuses.

▶ PTP enable
`enable`: Port sends/receives PTP synchronization messages,
`disable`: Port blocks PTP synchronization messages.

- PTP Port Burst enable
  `enable`: 2 to 8 synchronization runs take place during the synchronization interval. This enables faster synchronization with a correspondingly higher network load.
  `disable`: One synchronization run is performed in a synchronization interval.
- PTP Status
  `initializing`: Port is in the initialization phase.
  `faulty`: Port fault. Error in the PTP protocol.
  `disabled`: PTP function is switched off at this port.
  `listening`: Port has not received any information and is waiting for synchronization messages.
  `pre-master`: Port is in PTP pre-master mode.
  `master`: Port is in PTP master mode.
  `passiv`: Port is in PTP passive mode.
  `uncalibrated`: Port is in PTP passive mode.
  `slave`: Port is in PTP slave mode.

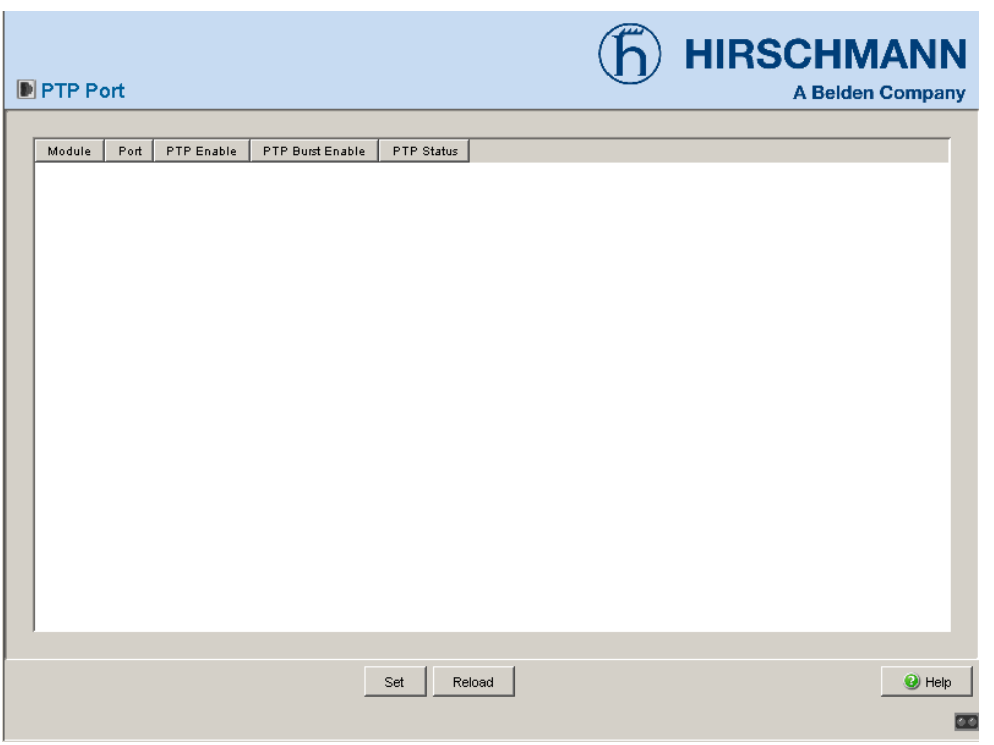


Figure 22: PTP port

5 Switching

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

- Switching Global
- Filters for MAC addresses
- Rate Limiter
- Multicasts
- VLAN

5.1 Switching Global

This dialog is used to

- display the MAC address of the device
- enter the aging time for all dynamic entries in the range from 15 to 3825 s (unit: 1 s; default setting: 30 s).
  In connection with the router redundancy (see MACH 3000), select a time greater than/equal to 30 seconds.
- enable/disable the flow control
- enable/disable the address learning
- set the maximum packet size (frame size).
  Select "1632" if you want the device to transmit packets with double tagging. You can thus operate the device in networks with MPLS Switches/ routers, for example.

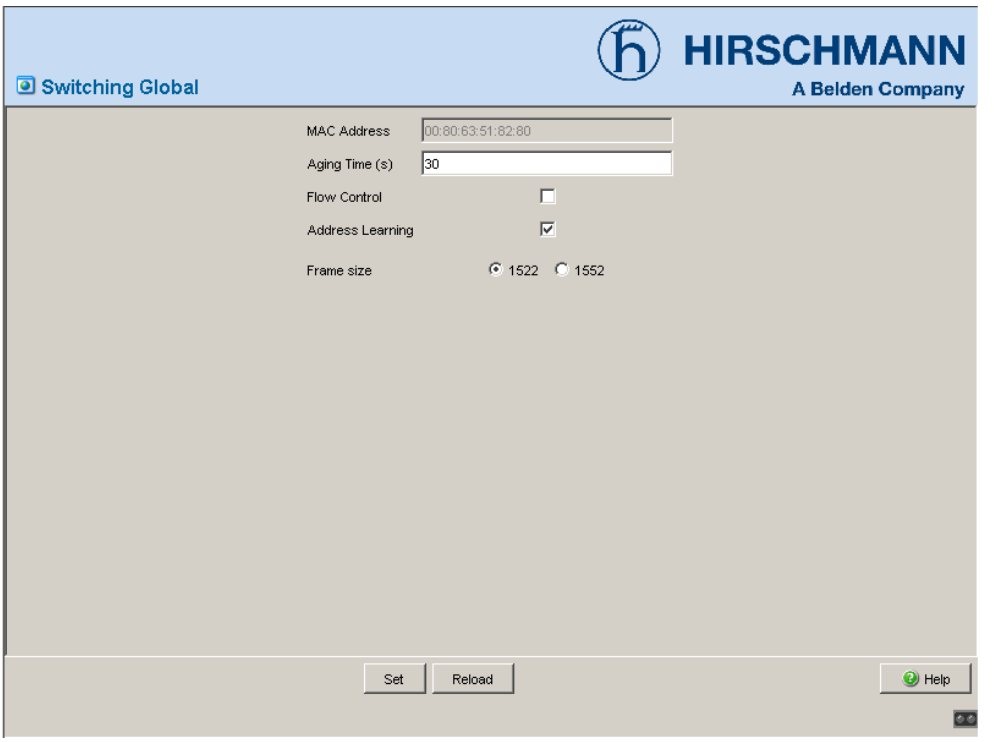


Figure 23: Switching Global

5.2 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 status settings 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 29 „Load/Save“).
- `gmrp`: the filter was created by GMRP.
- `gmrp/permanent`: GMRP added further port markings to the filter after it was created by the administrator. The port markings added by the GMRP are deleted by a restart .
- `igmp`: the filter was created by IGMP.

In the "Create" dialog (see buttons below), you can set up new filters.

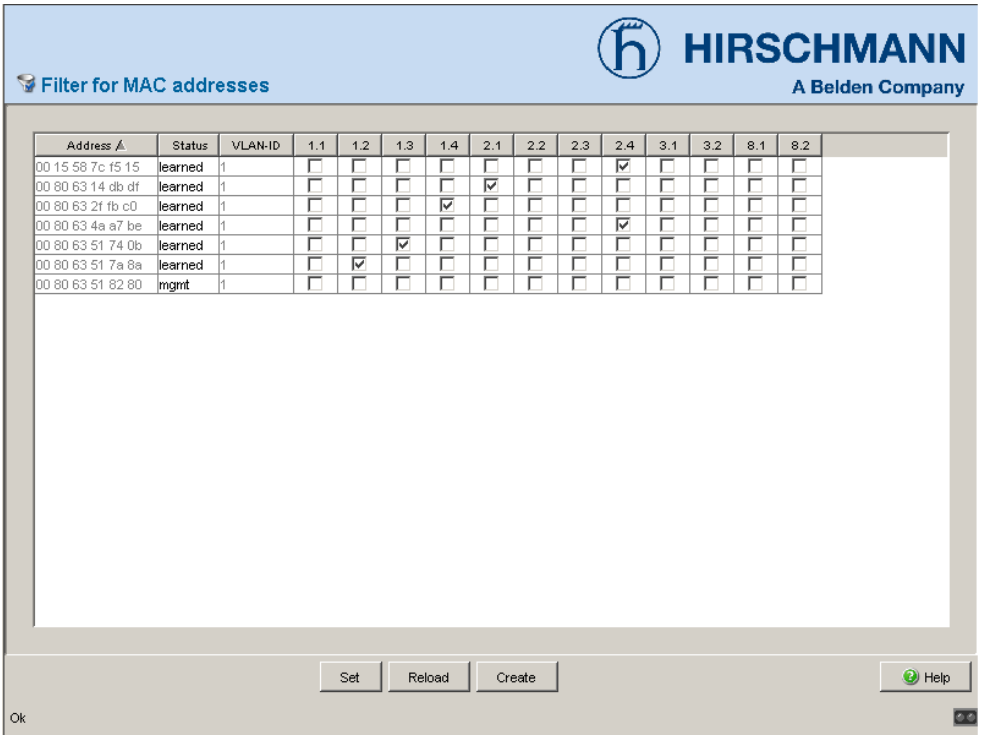


Figure 24: Filter table dialog

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

5.3 Rate Limiter

To ensure reliable data exchange during heavy traffic, the device can limit the traffic.

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

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

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

5.3.1 Rate Limiter settings

- "Ingress Limiter (kbit/s)" allows you to enable or disable the input limiting function for all ports.
- "Egress Limiter (Pkt/s)" allows you to enable or disable the broadcast output limiter function at all ports.
- "Egress Limiter (kbit/s)" allows you to enable or disable the output limiter function for all packet types at all ports.

Setting options per port:

- "Ingress Packet Types" allows you to select the packet type for which the limit is to apply:
  - `All`, limits the total inbound data volume at this port.
  - `BC`, limits the broadcast packets received at this port.
  - `BC + MC`, limits broadcast packets and Multicast packets received at this port.
  - `BC + MC + uUC`, limits broadcast packets, Multicast packets, and unknown Unicast packets received at this port.
- Ingress Limiter Rate for the inbound packet type selected:
  - = 0, no ingress limit at this port.

- > 0, maximum inbound traffic rate in kbit/s that can be received at this port.

- Egress Limiter Rate for broadcast packets:
  - = 0, no rate limit for outbound broadcast packets at this port.
  - > 0, maximum number of outbound broadcasts per second that can be sent at this port.
- Egress Limiter Rate for the entire data stream:
  - = 0, no rate limit for outbound data stream at this port.
  - > 0, maximum outbound transmission rate in kbit/s sent at this port.

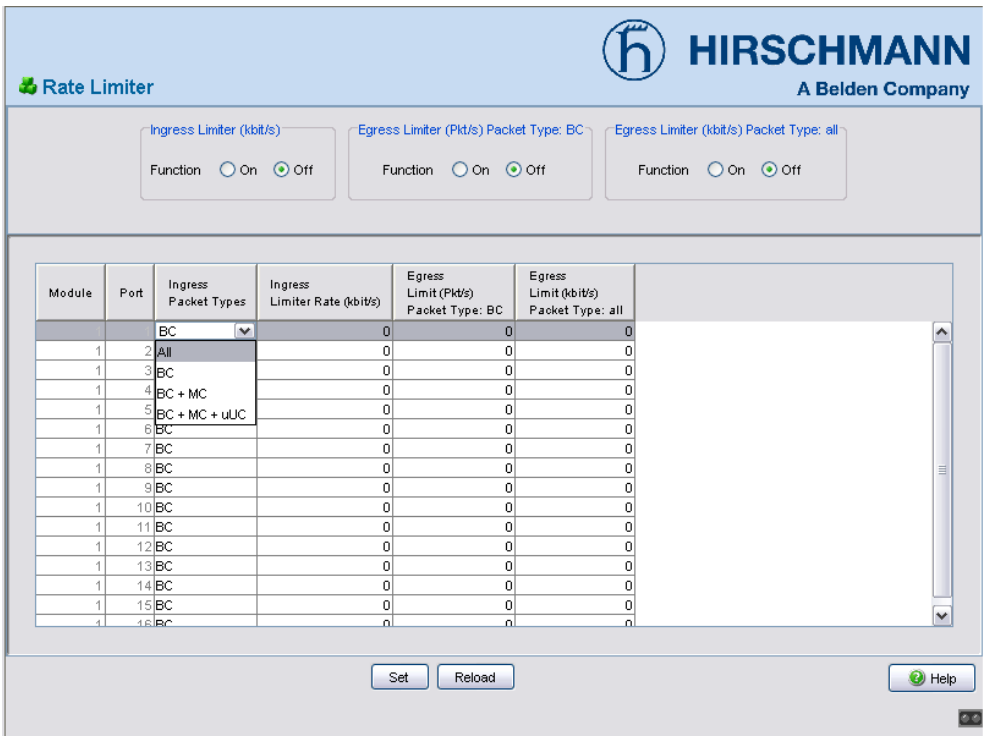


Figure 25: Rate Limiter dialog

5.4 Multicasts

The **I**nternet **G**roup **M**anagement **P**rotocol (IGMP) describes the distribution of Multicast information between routers and terminal devices on Layer 3. Routers with an active IGMP function periodically send queries () to find out which IP Multicast group members are connected to the LAN. Multicast group members reply with a Report message. This Report message contains all the parameters required by the IGMP. The router records the IP Multicast group address from the Report message in its routing table. The result of this is that it transfers frames with this IP Multicast group address in the destination address field only in accordance with the routing table.
Devices which no longer want to be members of a Multicast group can cancel their membership by means of a Leave message (from IGMP version 2), and they do not transmit any more Report messages. In IGMP versions 1 and 2, the router removes the routing table entry if it does not receive any Report messages within a specified period of time (aging time).
If there are multiple routers with an active IGMP function in the network, then they work out among themselves which router performs the Query function. If there is no router in the network, then a suitably equipped Switch can perform the Query function.

A Switch that connects a Multicast receiver with a router can evaluate the IGMP information with the aid of the IGMP Snooping procedure.
IGMP Snooping translates IP Multicast group addresses into MAC Multicast addresses, so that the IGMP functions can also be used by Layer 2 Switches. The Switch enters the MAC addresses of the Multicast receivers, with are obtained via IGMP Snooping from the IP addresses, in the static address table. Thus the Switch blocks Multicast packets at the ports at which no Multicast receivers are connected.

Basic setting "Global setting": disabled

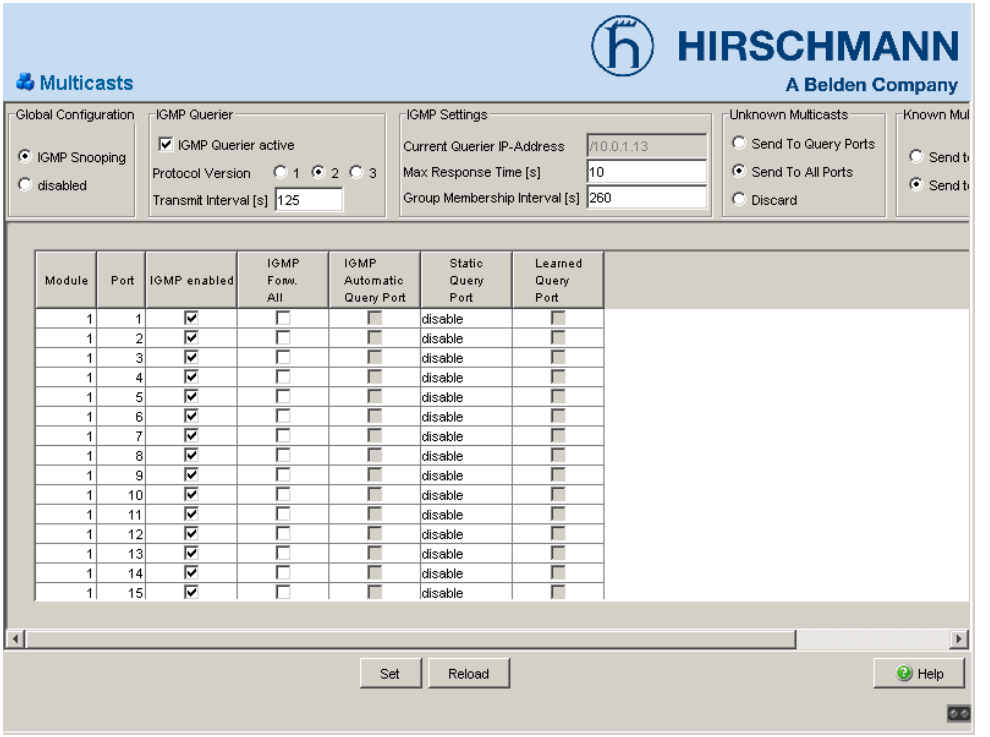


Figure 26: IGMP/Unknown Multicasts dialog

5.4.1 Global settings

"IGMP Snooping" allows you to enable IGMP Snooping globally for the entire device.
If IGMP Snooping is disabled, then

- 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.

"inactive" disables IGMP Snooping.

5.4.2 IGMP Querier

“IGMP Querier active” allows you to enable/disable the Query function.

The Protocol selection fields allow you to select IGMP version 1, 2 or 3.

In “Sending interval” you specify the interval at which the device sends query packets (valid entries: 2-3599 s, default setting: 125 s). All IGMP-capable terminal devices respond to a query with a report message, thus generating a network load.
Select large sending intervals if you want to reduce the load on your network and can accept the resulting longer switching times.
Select small sending intervals if you require short switching times and can accept the resulting network load.

5.4.3 IGMP settings

“Current querier IP address” shows you the IP address of the router that has the query function.

In “Response Time” you specify the period within which the Multicast group members respond to a query (valid values: 1-3598 s, default setting: 10 s). The Multicast group members select a random value within the response time for their response, to prevent all the Multicast group members responding to the query at the same 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.

In “Group Membership Interval” you specify the period for which a dynamic Multicast group remains entered in the device if it does not receive any report messages (valid values: 3-3600 s, default setting: 260 s).

5.4.4 Unknown Multicasts

In this frame you can determine how the device in IGMP mode sends packets with an unknown MAC/IP Multicast address that was not learned through IGMP Snooping.

- "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.

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.

5.4.5 Known Multicasts

In this frame you can determine how the device in IGMP mode sends packets with known MAC/IP Multicast addresses that were learned through IGMP Snooping.

- "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.
  This standard setting sends all Multicasts to all query ports and to registered ports. The advantage of this is that it works in most 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, which deviates from the standard, is that it uses the available bandwidth optimally through direct distribution. It requires additional port settings.
  Application: Routing protocol PIM-SM.

5.4.6 Settings per port (table)

- IMGP on per port
  This table column enables you to enable/disable the IGMP for each port when the global IGMP Snooping is enabled. Disabling the IGMP at a port prevents registration for this port.
- IGMP Forward All per port
  This table column enables you to enable/disable the "Forward All" IGMP Snooping function for each port when the global IGMP Snooping is enabled. With the "Forward All" function, the device sends to this port all data packets with a Multicast address in the destination address field.

  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 are using IGMP version 1 in a subnetwork, you must also use IGMP version 1 in the entire network.

- IGMP Automatic Query Port
  This table column shows you which ports the device has learned as query ports, if "automatic" is selected in "Static Query Port".
- Static Query Port
  The device sends IGMP report messages to the ports at which it receives IGMP queries (disable = default setting).
  This column allows you to also send IGMP report messages to
  other selected ports (enable) or
  to connected Hirschmann devices (automatic).
- Learned Query Port

This table column shows you at which ports the device has received IGMP queries, if "disable" is selected in "Static Query Port".

Note: If the device is connected to a HIPER-Ring, in the case of a ring interruption you can ensure quick reconfiguration of the network for data packets with registered Multicast destination addresses by:

- enabling IGMP on the ring ports and globally, and
- enabling "IGMP Forward All" per port on the ring ports.

5.5 VLAN

Under VLAN you will find all the tables and attributes for configuring and monitoring the VLAN function in accordance with the IEEE 802.1Q standard.

Note: When configuring the VLAN, ensure that the port to which your management station is connected can still send the data of the management station after the VLAN configuration is saved. Assigning this port to the VLAN with ID 1 ensures that the management station data is always sent.

Note: Save the VLAN configuration to non-volatile memory (see fig. 27).

Note: The 255 available VLANs can use any VLAN ID between 1 and 4042.

Note: In a HIPER-Ring with VLANs, you should only operate devices with the software that supports this function:

- RS2 xx/xx (from vers. 7.00),
- RS2-16M,
- RS 20, RS 30, RS 40 (L2E, L2P)
- MICE (from rel. 3.0) or
- Power MICE
- MS 20, MS 30
- RSR20, RSR30
- MACH 1000
- MACH 4000
- MACH 3000 (from rel. 3.3)
- OCTOPUS

Note: In the HIPER-Ring configuration, select for the ring ports

- VLAN ID 1 and "Ingress Filtering" in the port table and

- VLAN membership `U` in the static VLAN table.

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

- VLAN ID 1 and "Ingress Filtering" in the port table and
- VLAN membership `U` in the static VLAN table.

5.5.1 Setting up the VLAN

You will find an example configuration in the Basic Configuration user manual.

To set up VLANs, you first create the desired VLANs in the VLAN static table:

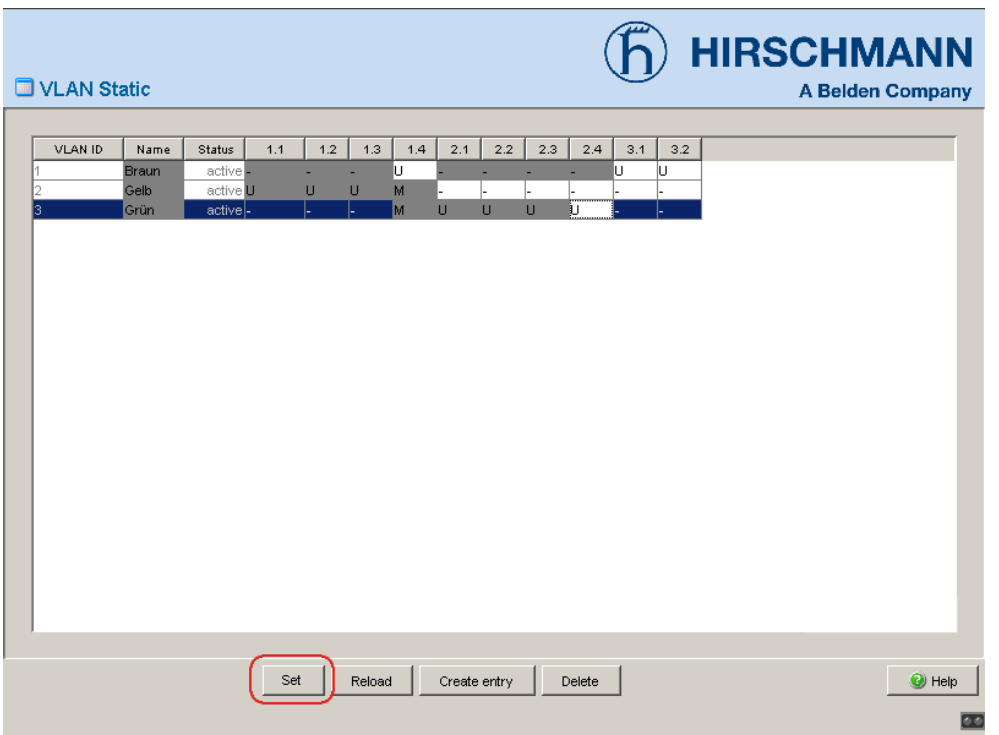


Figure 27: VLAN Static table

☐ After clicking "Create entry", you enter the corresponding VLAN ID. A new row appears in the table.

☐ Enter the name of your choice for this VLAN.

☐ Define the membership of the ports you require.
- Not a member of the VLAN.
M Member of the VLAN; send data packets with tag.
U Member of the VLAN; send data packets without tag.

☐ After creating the VLANs, you specify the rules for received data in the port table (Port):

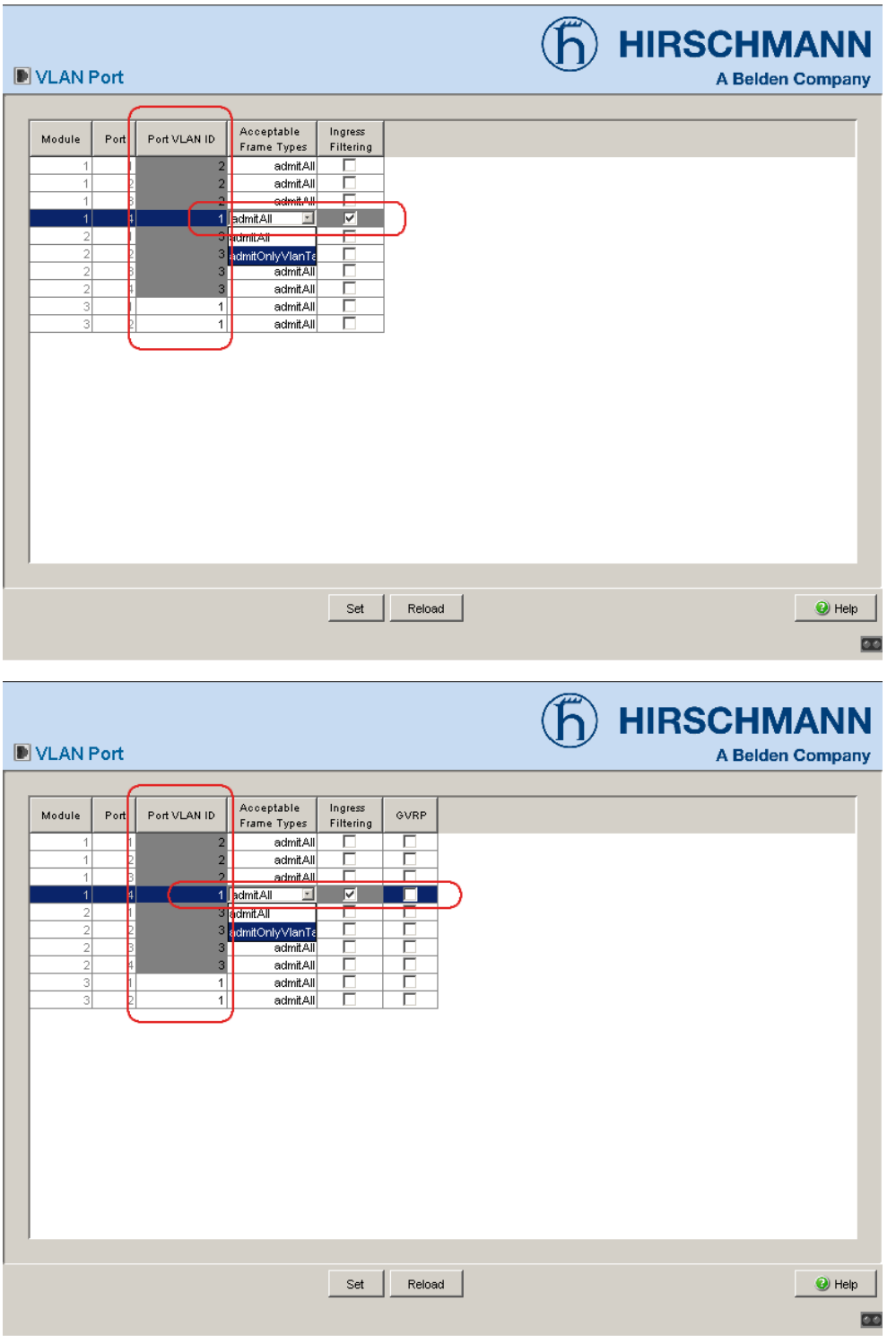


Figure 28: VLAN Port table

▶ Port VLAN ID specifies to which VLAN a received untagged data packet is assigned.

- Acceptable Frame Types specifies whether data packets without a tag may also be received.
- Ingress Filtering specifies whether the received tags are evaluated.

Note: If you selected `admitOnlyVlan` under "Acceptable Frame Types" and GVRP is active, you assign the value 0 to the VLAN ID in `Basic Settings:Network` (see page 20).

Note: Ports not displayed are participants in the link aggregation. Ports with module number 8 are participants in the link aggregation.

You now select the other settings in the VLAN Global dialog:

☐ Activate the "Transparent mode" in order to be able to send priority-tagged packets without VLAN membership, i.e. with VLAN ID "0". In this mode, the VLAN ID "0" remains in the packet, regardless of setting of the port VLAN ID in the "VLAN Port" dialog.

Note: If you are using the GOOSE protocol in accordance with IEC61850-8-1, you activate the "VLAN 0 transparent mode". Thus the prioritizing information remains in the data packet in accordance with IEEE802.1D/p when the device forwards the data packet.The same applies to other protocols that use this prioritizing in accordance with IEEE802.1D/p but that do not require any VLANs in accordance with IEEE802.1Q.

Note: For RS20/RS30/RS40, MS20/MS30, RSR20/RSR30, MACH 1000 and OCTOPUS
in "transparent mode" the devices ignore the set port VLAN ID. Set the VLAN membership of the ports of VLAN 1 to "member" or "untagged".

☐ Select the VLAN mode in the "Learning" frame.
"Independent VLAN" (default setting) divides the forwarding database virtually (see „Filters for MAC addresses“) into one independent forwarding database for each VLAN. The device cannot assign data packets with a destination address in another VLAN, and so floods it to all ports of the VLAN.
Application area: Setting up identical networks that use the same MAC addresses.
"Shared VLAN" uses the same forwarding database for all VLANs (see „Filters for MAC addresses“). The device cannot assign data packets with a destination address in another VLAN, and so only forwards them to the

destination port if the receiving port is also a member of the VLAN group of the destination port.
Application area: In the case of overlapping VLANs, the device can distribute directly across VLANs, as long as the ports involved belong to one group of VLANs.

☐ Perform a warm start (see on page 35 „Restart“) of the device if you have changed the mode. Thus the device takes over the setting under "Mode".

Note: The device displays the current status under "Status" in the "Learning" frame.

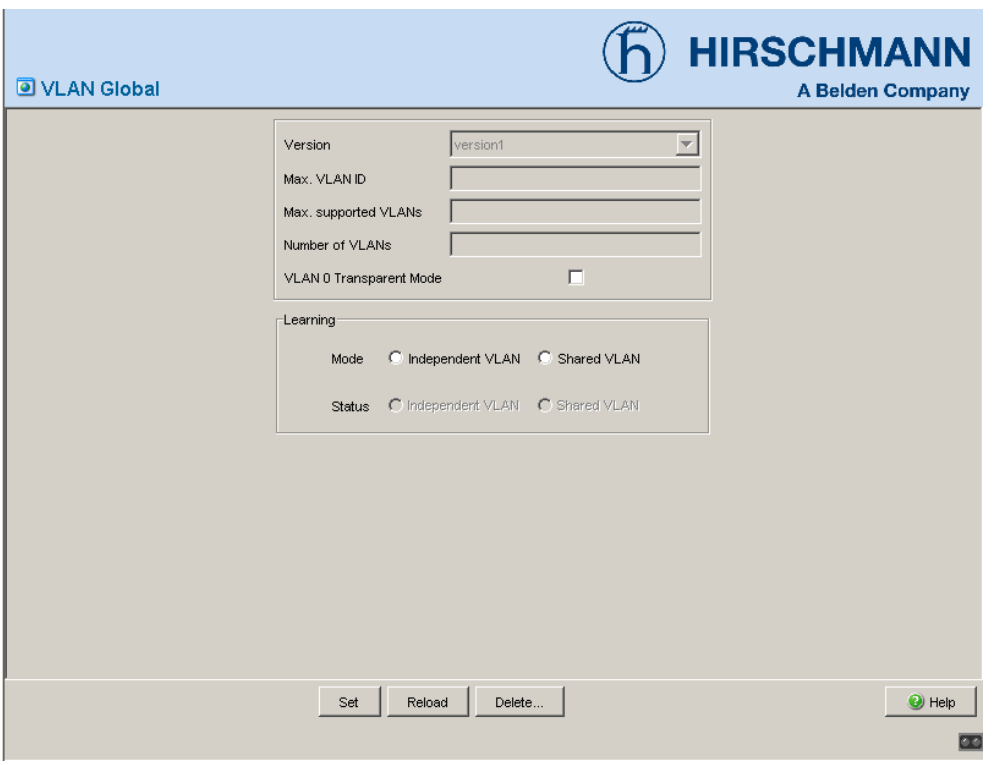


Figure 29: VLAN Global dialog

5.5.2 Displaying the VLAN configuration

The `Current` table shows the configured VLANs.

Status:
Other: This entry only appears for VLAN 1. VLAN 1 is specified by the system and always exists.
Permanent: This entry is permanent and is kept after the next reset of the device.

Ports x.x: Membership of the respective port.
- Not a member of the VLAN.
`M` Member of the VLAN; send data packets with tag.
`F`Not a member of the VLAN.
`U` Member of the VLAN; send data packets without tag.

Figure 30: VLAN Current table

5.5.3 Deleting VLAN settings

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

The "Delete" button in the VLAN Static dialog allows you to delete a row selected in the table.

5.5.4 Example of a VLAN configuration

You will find an example configuration in the Basic Configuration user manual.

6 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
- 802.1D/p Mapping
- IP DSCP mapping

6.1 Global

With this dialog you can:

- enter the VLAN priority for management packets in the range 0 to 7 (default setting: 0).
  In order for you to have full access to the management of the device, even when there is a high network load, the device enables you to prioritize management packets.
  In prioritizing management packets (SNMP, Telnet, etc.), the device sends the management packets with priority information.
  Note the assignment of the VLAN priority to the traffic class (see table 8).
- 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 9).

  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 four (eight for MACH 4000 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 (assigning them to a traffic class - see „802.1D/p Mapping“) in accordance with this information.
  The device prioritizes received packets that contain no tag information (assigning them to a traffic class - see „Entering the port priority“) in accordance with the port priority of the receiving port.
- "trustIpDscp"
  The device prioritizes received IP packets (assigning them to a traffic class - see „IP DSCP mapping“) in accordance with their DSCP value.
  The device prioritizes received packets that are not IP packets (assigning them to a traffic class - see „Entering the port priority“) in accordance with the port priority of the receiving port.
  For received IP packets:
  The device also performs VLAN priority remarking.
  In VLAN priority remarking, the device modifies the VLAN priority of the IP packets if the packets are to be sent with a VLAN tag (see on page 73 „Setting up the VLAN“).
  Based on the traffic class to which the IP packet was assigned (see above), the device assigns the new VLAN priority to the IP packet in accordance with table 5.
  Example: Received IP packet with a DSCP value of 32 (cs4) is assigned to traffic class 2 (default setting). The packet was received at a port with port priority 2. Thus, according to table 5, the VLAN priority is set to 4.

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 5: VLAN priority remarking

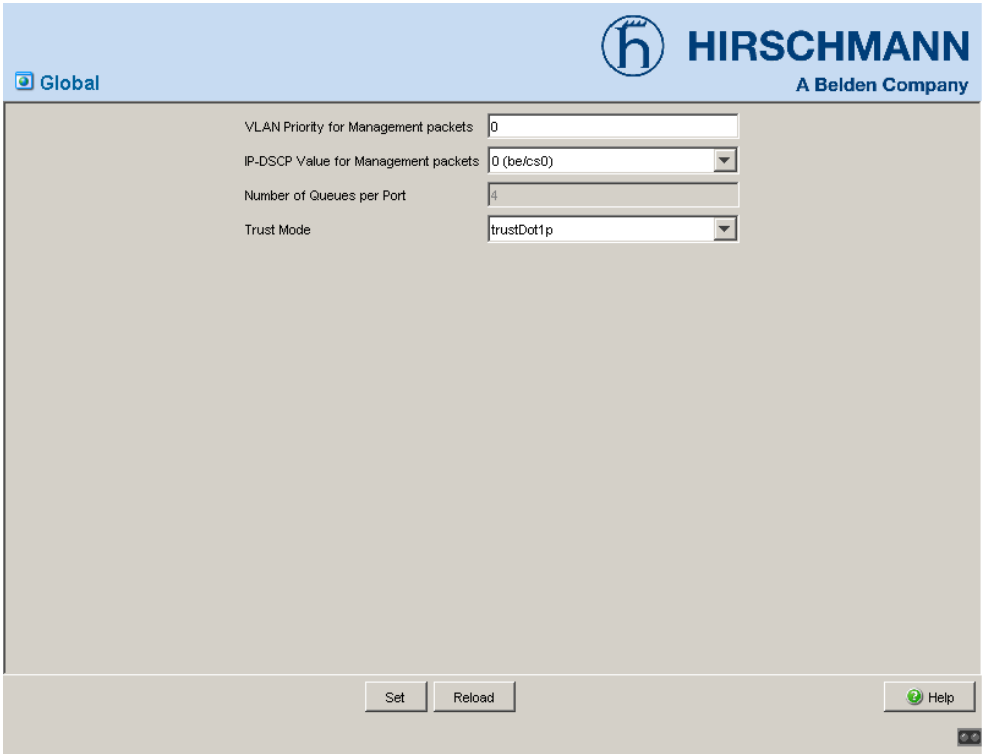


Figure 31: Global dialog

6.2 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 6: Port configuration table

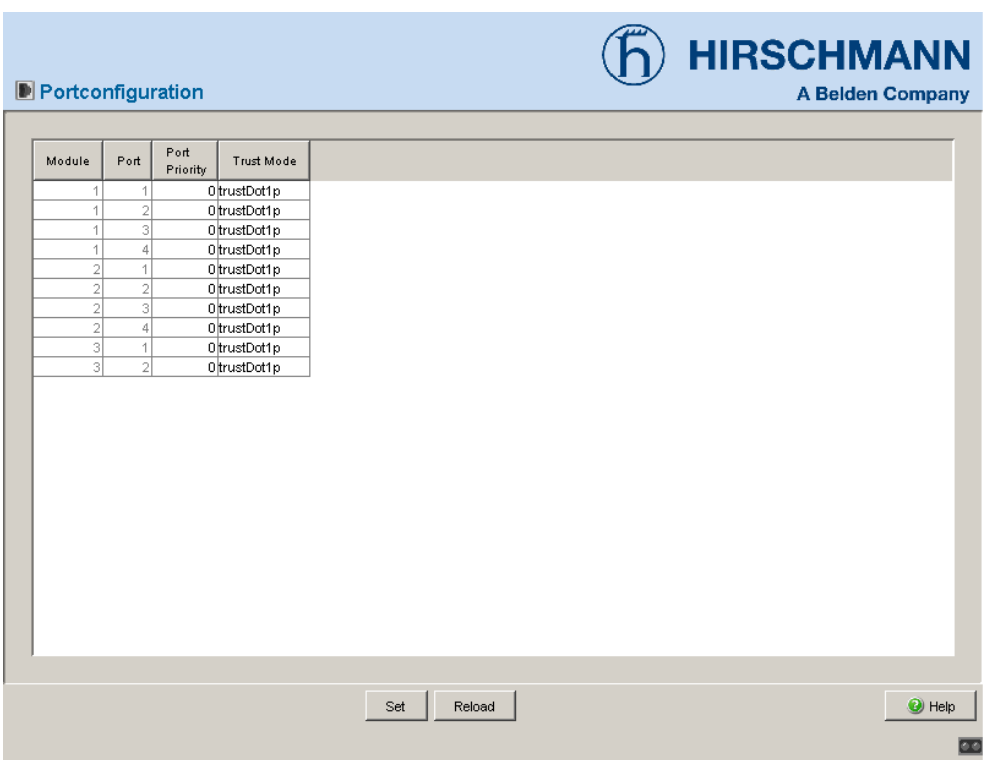


Figure 32: Port configuration dialog

6.2.1 Entering the port priority

☐ Double-click on 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 7).
Requirement:
setting in the `Global:Trust Mode` dialog: untrusted (see page 80) or
setting in the `Global:Trust Mode` dialog: trustDot1p(see page 80) and the data packets do not contain a VLAN tag or
setting in `Global:Trust Mode` dialog: trustIpDscp (see page 80) 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, less than 100 milliseconds of latency and jitter
6	3	Voice, less than 10 milliseconds of latency and jitter
7	3	Network control reserved traffic

Table 7: Assigning the port priority to the four traffic classes

6.3 802.1D/p Mapping

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

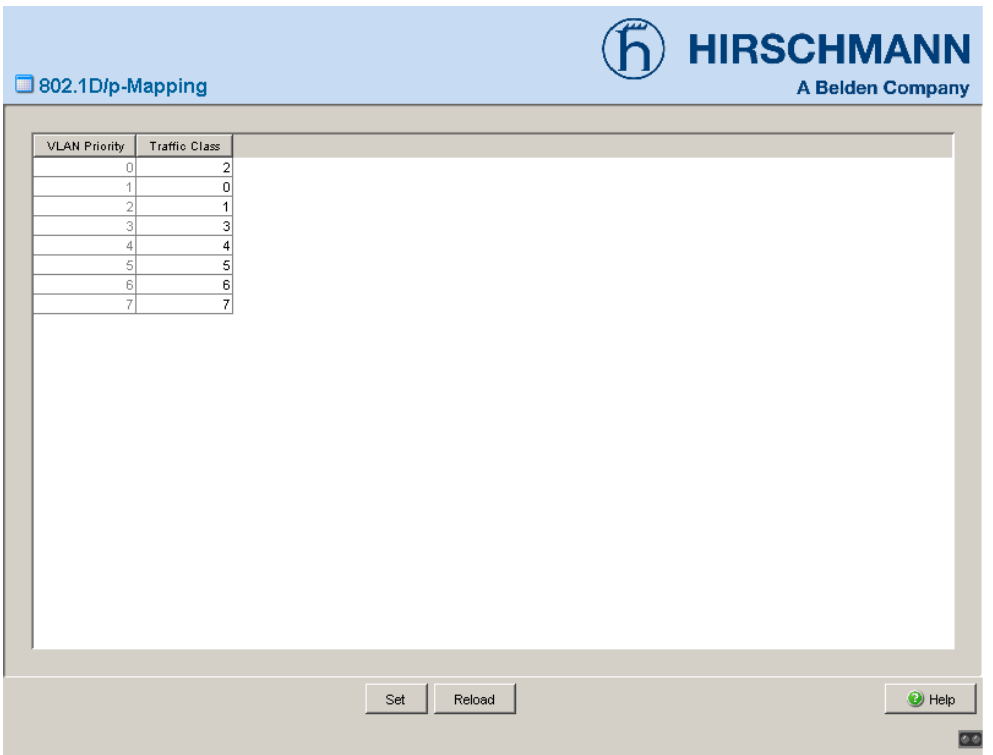


Figure 33: 802.1D/p mapping table

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

VLAN 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, less than 100 milliseconds of latency and jitter
6	3	Voice, less than 10 milliseconds of latency and jitter
7	3	Network control reserved traffic

Table 8: Assigning the VLAN priority to the four traffic classes

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

6.4 IP DSCP mapping

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

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

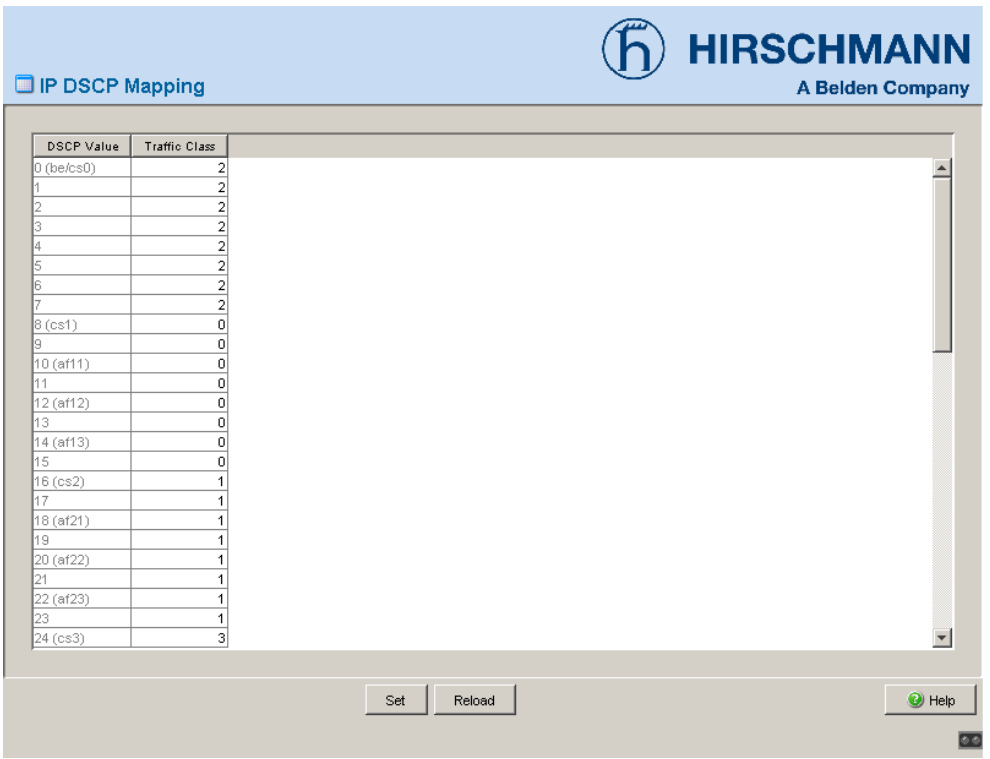


Figure 34: IP DSCP mapping table

The different DSCP values get the device to employ a different forwarding behavior, the 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 9: Mapping the DSCP values onto the traffic classes

7 Redundancy

The device contains a range of redundancy functions:

- HIPER-Ring
- Redundant coupling of HIPER-Rings and network segments
- Rapid Spanning Tree Algorithm (RSTP)

7.1 HIPER-Ring

The concept of the HIPER-Ring enables the construction of high-availability, ring-shaped network structures.
Using the RM function (**R**edundancy **M**anager) of a device with the L2E, L2P, L3E or L3P software, you can close both ends of a backbone in a line structure to a redundant ring, the HIPER-Ring.

Within a HIPER-Ring Version 1, any combination of RS1, RS2-../.., RS2-16M, RS2-4R, RS20, RS30, RS40, MICE, PowerMICE, MS 20, MS 30, RSR20, RSR30, MACH 1000, MACH 3000 and MACH 4000 is possible.
Within a HIPER-Ring Version 2 (MRP Draft), any combination of devices that support this function is possible.
Within a HIPER-Ring Version 3, any combination of RSR20, RSR30 and MACH 1000 is possible.

If a section is down, the ring structure of a

- HIPER-Ring Version 1 of up to 50 devices typically transforms back to a line structure within 150 ms (adjustable to max. 300 ms/500 ms).
- HIPER-Ring Version 2 of up to 50 devices typically transforms back to a line structure within 150 ms (adjustable to max. 200 ms/500 ms).
- HIPER-Ring Version 3 of up to 5 devices typically transforms back to a line structure within 5 ms (maximum 10 ms). If a larger number of devices is being used, the reconfiguration time increases.

7.1.1 Configuring HIPER-Ring Version 1

☐ Set up the network to meet your requirements.

Note: Before you connect the redundant line, you must complete the configuration of HIPER-Ring Version 1.
You thus avoid loops during the configuration phase.

Note: Configure each HIPER-Ring device.

☐ Select the `Redundancy:HIPER-Ring` dialog.

☐ Select `Version 1`.

Note: As an alternative to using software to configure HIPER-Ring Version 1, with devices RS20/30/40 and MS20/30 you can also use a DIP switch to enter a number of settings for HIPER-Ring Version 1. You can also use this 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”.

☐ For each device, you enter the desired ring ports 1 and 2.
The following settings are required for the ring ports (select the `Basic Settings:Port Configuration` dialog):

Bit rate	100 Mbit/s	1000 Mbit/s
Autonegotiation (automatic configuration)	Off	On
Port	On	On
Duplex	Full	–

Table 10: Port settings for ring ports

Note: When using 100 Mbit/s with twisted pair cables, avoid the combination of autonegotiation “off” and cable crossing “automatic”. Use crossover cables with 100 Mbit/s.

Display in “Operation” field:
Active: this port is switched on and has a link.
Inactive: this port is switched off or has no link.

- ☐ At exactly one device, you switch the redundancy manager on at the ends of the line.
- ☐ Select the desired value in the “Ring Recovery” frame for the device for which you have activated the redundancy manager.

Note: Settings in the “Ring Recovery” frame are ineffective for devices that are not the redundancy manager.

Note: If selecting the smaller value for the ring recovery does provide the ring stability necessary to meet the requirements of your network, you select 500 ms.

Figure 35: Selecting HIPER-Ring version, entering ring ports, enabling/disabling redundancy 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.

Note: If you used the DIP switch to activate the function of HIPER-Ring Version 1, RSTP is automatically switched off.

☐ Now you connect the line to the ring. To do this, you connect the two devices to the ends of the line using their ring ports.

The displays in the “Redundancy Manger Status” frame mean:

– “Active (redundant line)”: The ring is open, which means that a data line or a network component within the ring is down.
– “Inactive”: The ring is closed, which means that the data lines and network components are working.

The displays in the “Information” frame mean:
– „“Redundancy guaranteed”: One of the lines affected by the function can fail, whereby the redundant line will then take over the function of the failed line.
– „“Configuration failure”: The function is incorrectly configured or there is an error on ringport link.

Figure 36: Display: Redundancy Manager Status and Information

Note: If VLANS are configured, note the VLAN configuration of the ring ports. In the configuration of HIPER-Ring Version 1, you select for the ring ports
– VLAN ID 1 and
– VLAN membership `U` in the static VLAN table

Note: When you switch from a normal port to a ring port with the DIP switch, the device makes 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 keeps the ring port settings. These settings remain changeable for all ports.

7.1.2 Configuring HIPER-Ring Version 2 (MRP Draft)

☐ Set up the network to meet your requirements.

Note: Before you connect the redundant line, you must complete the configuration of HIPER-Ring Version 2.
You thus avoid loops during the configuration phase.

Note: Configure each HIPER-Ring device.

☐ Select the `Redundancy:HIPER-Ring` dialog.

☐ Select `Version 2 (MRP Draft).`

☐ For each device, you enter the desired ring ports 1 and 2.
The following settings are required for the ring ports (select the `Basic Settings:Port Configuration` dialog):

Bit rate	100 Mbit/s	1000 Mbit/s
Autonegotiation (automatic configuration)	Off	On
Port	On	On
Duplex	Full	–

Table 11: Port settings for ring ports

Note: When using 100 Mbit/s with twisted pair cables, avoid the combination of autonegotiation “off” and cable crossing “automatic”. Use crossover cables with 100 Mbit/s.

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.

☐ At exactly one device, you switch the redundancy manager on at the ends of the line.

Figure 37: Selecting HIPER-Ring version, entering ring ports and enabling/disabling redundancy manager

☐ If a device in the ring does not support the advanced mode for fast switching times, you deactivate the advanced mode in the redundancy manager, in the “Configuration Redundancy Manager” frame.
All Hirschmann devices that support the HIPER-Ring Version 2 (MRP Draft) also support the advanced mode.

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.

The “VLAN” frame enables you to assign HIPER-Ring Version 2 to a VLAN.

☐ If VLANs are configured, then in the “VLAN” frame you select
- VLAN ID 0, if the MRP-Ring configuration is not to be assigned to a VLAN.
Note the VLAN configuration of the ring ports. Then select for the ring ports
- VLAN ID 1 and
- VLAN membership U in the static VLAN table
- a VLAN ID >0, if the MRP-Ring configuration is to be assigned to this VLAN.
Select this VLAN ID in the MRP-Ring configuration for all devices in this MRP-Ring.
Note the VLAN configuration of the ring ports. For all ring ports in this MRP-Ring, select
- this VLAN ID and
- VLAN membership U in the static VLAN table.

☐ Select the desired value in the “Ring Recovery” frame for the device for which you have activated the redundancy manager.

Note: Settings in the “Ring Recovery” frame are ineffective for devices that are not the redundancy manager.

Note: If selecting the smaller value for the ring recovery does provide the ring stability necessary to meet the requirements of your network, you select 500 ms.

☐ Activate the function in the “Operation” frame.

☐ Now you connect the line to the ring. To do this, you connect the two devices to the ends of the line using their ring ports.

The displays in the “Information” frame mean:

– „“Redundancy guaranteed”: One of the lines affected by the function can fail, whereby the redundant line will then take over the function of the failed line.
– „“Configuration failure”: The function is incorrectly configured or there is an error on ringport link.

Figure 38: Configuring the Redundancy Manager, selecting operation, selecting ring recovery and entering VLAN ID. Display: Information.

7.2 Redundant coupling

7.2.1 Configuring the redundant coupling

STAND-BY switch

The Switches have a STAND-BY switch for selecting between the main coupling and the redundant coupling. Depending on the Switch, this switch is a DIP switch or a software switch (`Redundancy:Ring/Network Coupling` dialog), or you can use a switch to select one of the two options.

Switch	STAND-BY switch
RS2-../..	DIP switch
RS2-16M	DIP switch
RS20/RS30/RS40	Can be switched between DIP switch and software switch
MICE/PowerMICE	Can be switched between DIP switch and software switch
MS 20/MS 30	Can be switched between DIP switch and software switch
RSR20/RSR30	Software switch
MACH 1000	Software switch
MACH 3000/MACH 4000	Software switch

Table 12: STAND-BY switches of the Switches

Depending on the Switch used, you choose between the main coupling and the redundant coupling (see table 13).

Switch with	Choice of main coupling or redundant coupling
DIP switch	“STAND-BY” on DIP switch
DIP switch/software switch option	According to the option selected - “Stand-by” on the DIP switch or in the - `Redundancy:Ring/Network Coupling` dialog, by selecting in “Select configuration”. **Note:** These devices have a DIP switch, with which you can choose between the software configuration and the DIP configuration. If the software configuration is set, the other DIP switches have no effect.
Software switch	In the `Redundancy:Ring/Network Coupling` dialog

Table 13: Choice of main coupling or redundant coupling

☐ Select the `Redundancy:Ring/Network Coupling` dialog.
☐ You first select the configuration you want: One-Switch coupling (“1”), two-Switch coupling (“2”) or two-Switch coupling with control line (“3”), (see fig. 39).

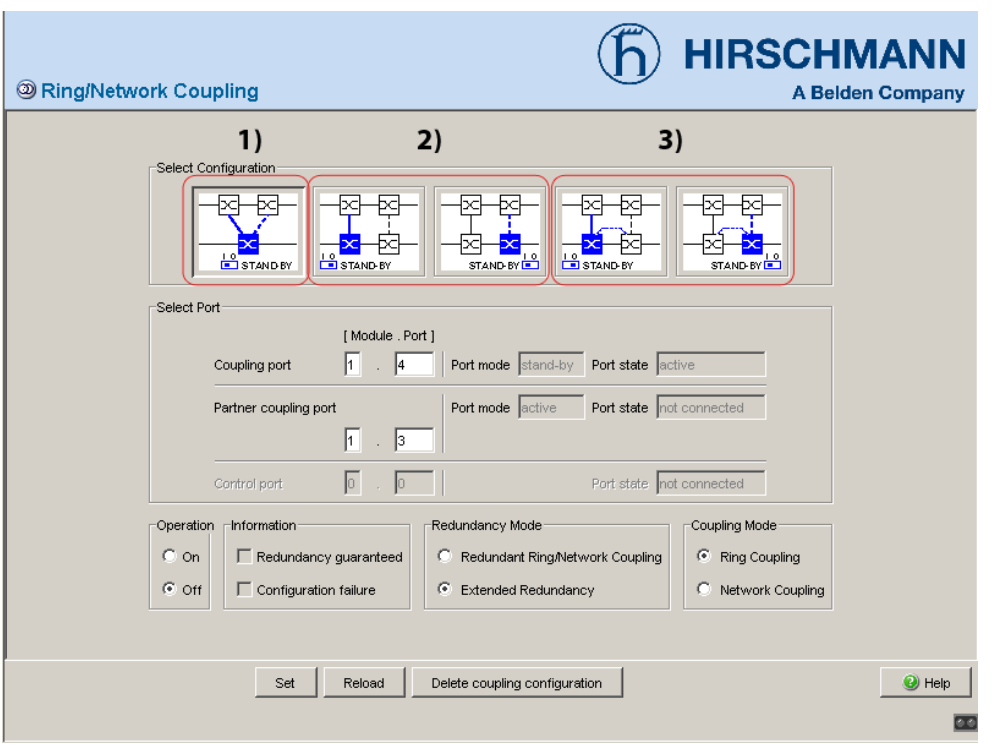


Figure 39: Selecting the configuration

Note: Depending on the STAND-BY DIP switch position, the dialog displays those configurations that are not possible in gray. If you want to select one of these grayed-out configurations, you put the STAND-BY DIP switch on the Switch into the other position.

Note: One-Switch coupling: The redundancy function is assigned to the Switch via the “STAND-BY” setting in the DIP switch, or via the Management.

Note: Two-Switch coupling: The redundancy function is assigned to the Switch in the redundant line via the “STAND-BY” setting in the DIP switch, or via the Management.

Note: Some devices have a DIP switch, with which you can choose between the software configuration and the DIP configuration. If the software configuration is set, the other DIP switches have no effect.

Note: The choice of configuration primarily depends on the topological conditions and the desired level of safety.

Note: For redundancy security reasons, a combination of Rapid Spanning Tree and Ring/Network Coupling is not possible.

One-Switch coupling

☐ Select the `Redundancy:Ring/Network Coupling` dialog.

☐ Select one-Switch coupling (see fig. 40).

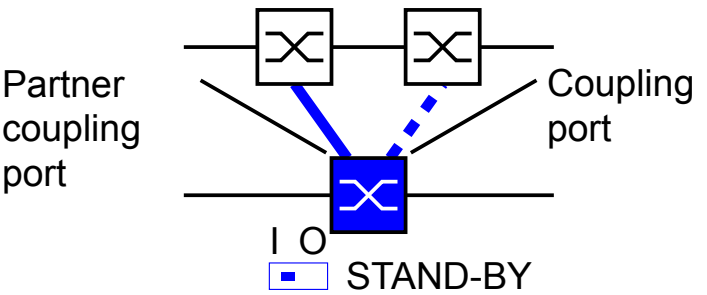


Figure 40: One-Switch coupling

The following settings apply to the Switch displayed in blue in the selected graphic.

☐ Select the partner coupling port (see fig. 41), (see table 14).
With “Partner coupling port” you specify at which port you are connecting the control line.

Switch	Partner coupling port
RS2-../..	Not possible
RS2-16M	Adjustable for all ports (default setting: port 2)
RS20	Adjustable for all ports (default setting: port 1.3)
RS30	Adjustable for all ports (default setting: port 1.3)
RS40	Adjustable for all ports (default setting: port 1.3)
MICE	Adjustable for all ports (default setting: port 1.3)
PowerMICE	Adjustable for all ports (default setting: port 1.3)
MS 20	Adjustable for all ports (default setting: port 1.3)
MS 30	Adjustable for all ports (default setting: port 2.3)
RSR20/30	Adjustable for all ports (default setting: port 1.3)
MACH 1000	Adjustable for all ports (default setting: port 1.3)
MACH 3000	Adjustable for all ports
MACH 4000	Adjustable for all ports (default setting: port 1.3)

Table 14: Port assignment for one-Switch coupling

Note: Configure the partner coupling port and the HIPER-Ring ports on different ports.

☐ Select the coupling port (see fig. 41), (see table 15).
With “Coupling port” you specify at which port you are connecting the redundant line.

Switch	Coupling port
RS2-../..	Not possible
RS2-16M	Adjustable for all ports (default setting: port 1)
RS20	Adjustable for all ports (default setting: port 1.4)
RS30	Adjustable for all ports (default setting: port 1.4)
RS40	Adjustable for all ports (default setting: port 1.4)
MICE	Adjustable for all ports (default setting: port 1.4)
PowerMICE	Adjustable for all ports (default setting: port 1.4)
MS 20	Adjustable for all ports (default setting: port 1.4)
MS 30	Adjustable for all ports (default setting: port 2.4)
RSR20/30	Adjustable for all ports (default setting: port 1.4)
MACH 1000	Adjustable for all ports (default setting: port 1.4)
MACH 3000	Adjustable for all ports
MACH 4000	Adjustable for all ports (default setting: port 1.4)

Table 15: Port assignment for one-Switch coupling

Note: Configure the coupling port and the HIPER-Ring ports on different ports.

☐ Activate the function in the “Operation” frame (see fig. 41).
☐ You now connect the redundant line.

The displays in the “Select port” frame mean (see fig. 41):
– “Port mode”: The port is either active or in stand-by mode.
– “Port state”: The port is either connected or not connected.

The displays in the “Information” frame mean (see fig. 41):
– “Redundancy guaranteed”: One of the lines affected can fail, as a redundant line will then take over the function of the failed line.
– “Configuration failure”: The function is incomplete or incorrectly configured.

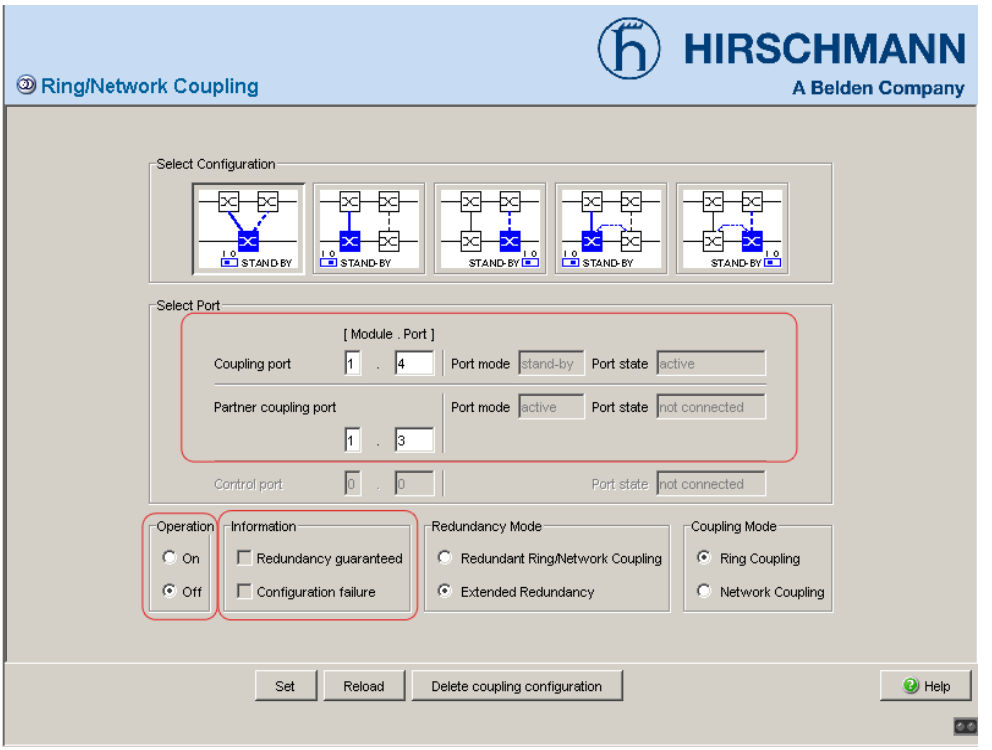


Figure 41: Selecting the port and enabling/disabling operation

Note: The following settings are required for the coupling ports (you select the `Basic Settings:Port Configuration` dialog):

– Port: on
– Automatic configuration (autonegotiation):
  on for twisted-pair connections
– Manual configuration: 100 Mbit/s FDX
  for glass fiber connections

Note: If VLANS are configured, note the VLAN configuration of the coupling and partner coupling ports.
In the Network/Ring Coupling configuration, select for the coupling and partner coupling ports

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

Redundancy mode

☐ In the “Redundancy Mode” frame, select (see fig. 42)
– “Redundant Ring/Network Coupling” or
– “Extended Redundancy”.

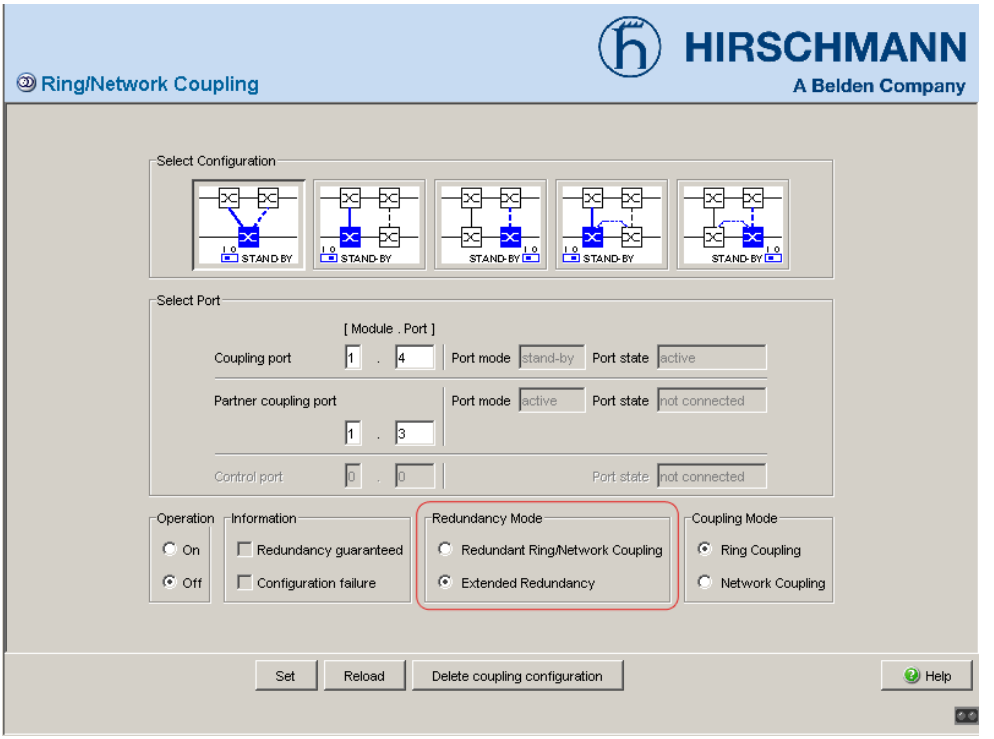


Figure 42: Selecting the redundancy mode

With the “Redundant Ring/Network Coupling” setting, either the main line or the redundant line is active. Both lines are never active simultaneously.

With the “Extended Redundancy” setting, the main line and the redundant line are simultaneously active if the connection line between the Switches in the connected network fails (see fig. 43).
During the reconfiguration period, there may be package duplications. Therefore, only select this setting if your application detects package duplications.

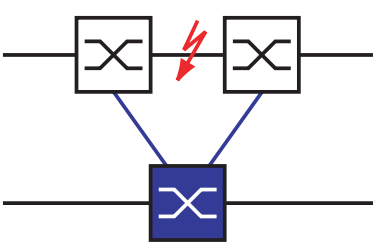


Figure 43: Extended redundancy

Coupling mode

The coupling mode indicates the type of the connected network.

☐ In the “Coupling Mode” frame, select (see fig. 44)
– “Ring Coupling” or
– “Network Coupling”

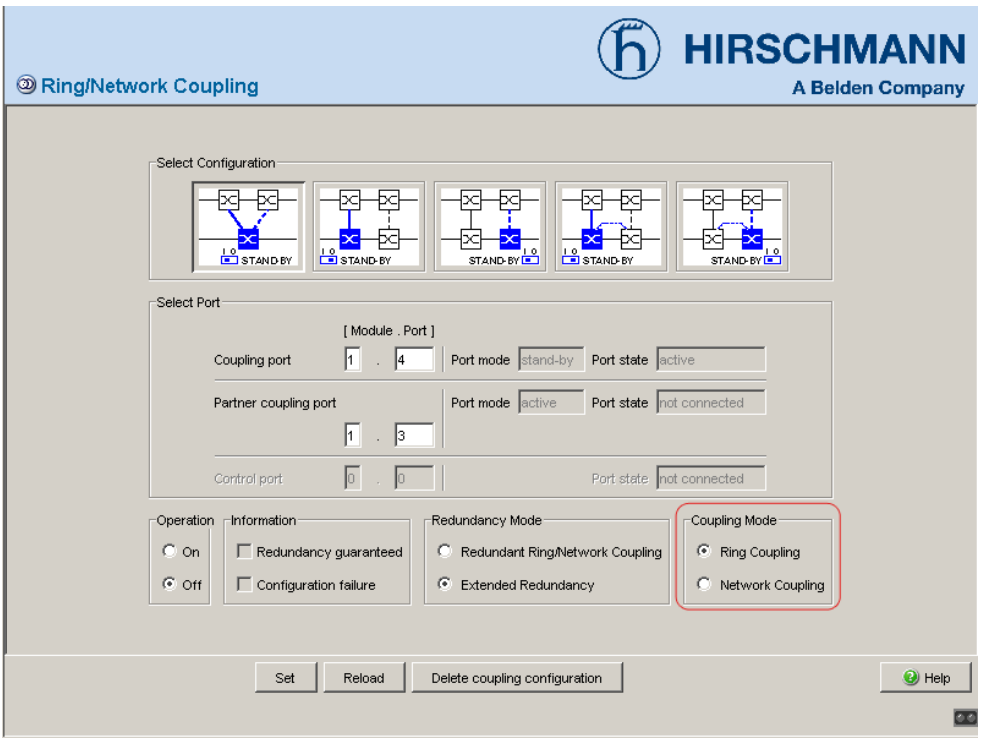


Figure 44: Selecting the coupling mode

☐ Select **“Ring coupling”** if you are connecting a HIPER-Ring.
☐ Select **“Network Coupling”** if you are connecting a line structure.

Delete coupling configuration

☐ The “Delete coupling configuration” button in the dialog allows you to reset all the coupling settings of the device to the state on delivery.

Two-Switch coupling

- ☐ Connect the two partners via their ring ports.
- ☐ Select the `Redundancy:Ring/Network Coupling` dialog.
- ☐ Select two-Switch main coupling (see fig. 45).

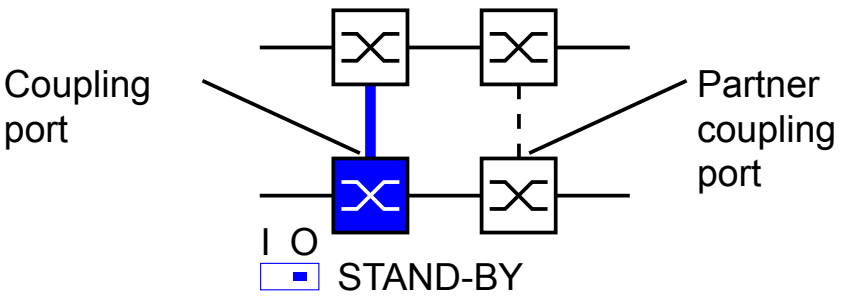


Figure 45: Two-Switch coupling

The following settings apply to the Switch displayed in blue in the selected graphic.

- ☐ Select the coupling port (see fig. 46), (see table 16).
  With “Coupling port” you specify at which port you are connecting the network segments.
- ☐ If the STANDBY DIP switch is OFF, connect the main line to the coupling port.

Switch	Coupling port
RS2-../..	Not possible
RS2-16M	Adjustable for all ports (default setting: port 1)
RS20	Adjustable for all ports (default setting: port 1.4)
RS30	Adjustable for all ports (default setting: port 1.4)
RS40	Adjustable for all ports (default setting: port 1.4)
MICE	Adjustable for all ports (default setting: port 1.4)
PowerMICE	Adjustable for all ports (default setting: port 1.4)
MS 20	Adjustable for all ports (default setting: port 1.4)
MS 30	Adjustable for all ports (default setting: port 2.4)
RSR20/30	Adjustable for all ports (default setting: port 1.4)
MACH 1000	Adjustable for all ports (default setting: port 1.4)
MACH 3000	Adjustable for all ports
MACH 4000	Adjustable for all ports (default setting: port 1.4)

Table 16: Port assignment for the redundant coupling

Note: Configure the coupling port and the HIPER-Ring ports on different ports.

☐ Activate the function in the “Operation” frame (see fig. 46).
☐ You now connect the redundant line.

The displays in the “Select port” frame mean (see fig. 46):
– “Port mode”: The port is either active or in stand-by mode.
– “Port state”: The port is either connected or not connected.
– “IP Address”: The IP address of the partner, if the partner is already operating in the network.

The displays in the “Information” frame mean (see fig. 46):
– “Redundancy guaranteed”: One of the lines affected can fail, as a redundant line will then take over the function of the failed line.
– “Configuration failure”: The function is incomplete or incorrectly configured.

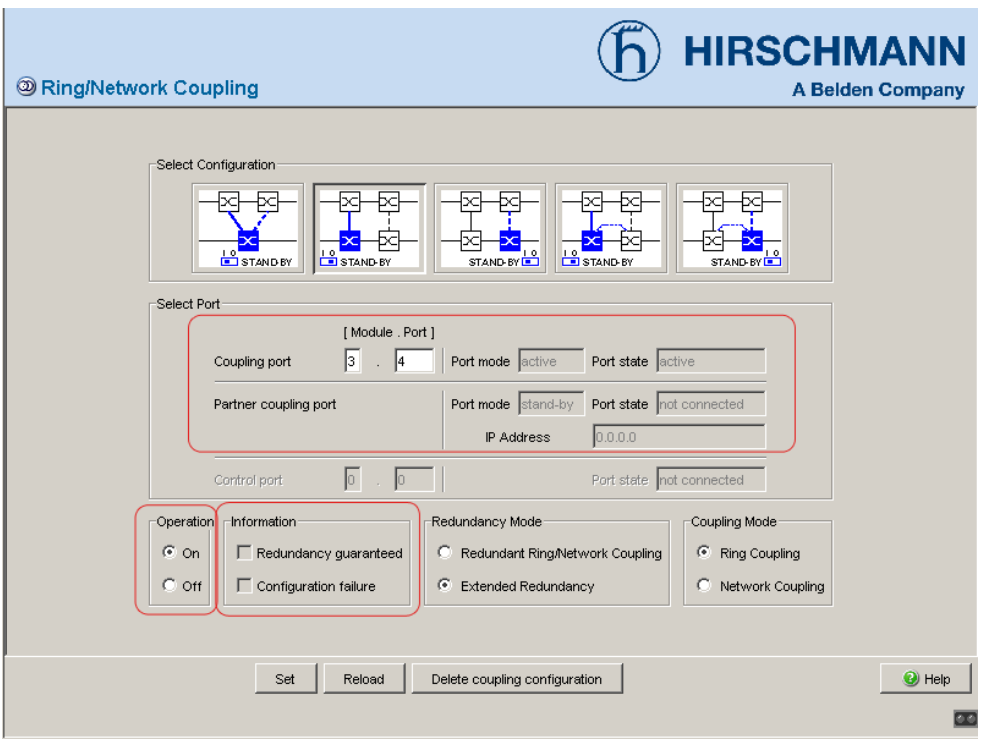


Figure 46: Selecting the port and enabling/disabling operation

To avoid continuous loops, the Switch sets the port state of the coupling port to “off” if you:
– switch off operation or
– change the configuration
while the connections are in operation at these ports.

Note: The following settings are required for the coupling ports (you select the `Basic Settings:Port Configuration` dialog):

– Port: on
– Automatic configuration (autonegotiation):
  on for twisted-pair connections
– Manual configuration: 100 Mbit/s FDX
  for glass fiber connections

Note: If VLANS are configured, note the VLAN configuration of the coupling and partner coupling ports.
In the Network/Ring Coupling configuration, select for the coupling and partner coupling ports
– VLAN ID 1 and “Ingress Filtering” disabled in the port table and
– VLAN membership U in the static VLAN table.

Note: Operating the redundancy manager and two-Switch coupling functions at the same time runs the risk of creating a loop.

☐ Select two-Switch redundant coupling (see fig. 47).

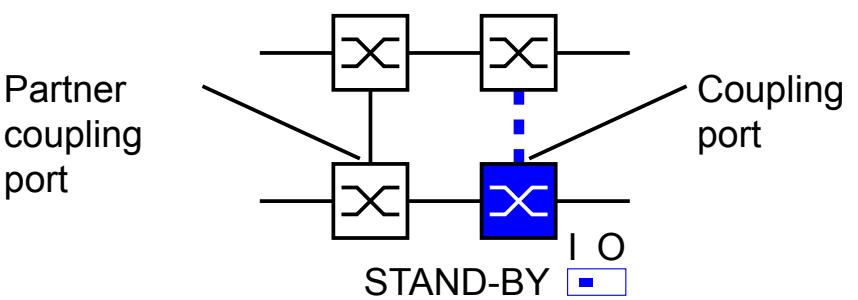


Figure 47: Two-Switch coupling

The following settings apply to the Switch displayed in blue in the selected graphic.
☐ Select the coupling port (see fig. 46), (see table 16).
  With “Coupling port” you specify at which port you are connecting the network segments.
☐ If the STANDBY DIP switch is ON, connect the main line to the coupling port.

Note: Configure the coupling port and the HIPER-Ring ports on different ports.

☐ Activate the function in the “Operation” frame (see fig. 46).

The displays in the “Select port” frame mean (see fig. 46):
– “Port mode”: The port is either active or in stand-by mode.

– “Port state”: The port is either connected or not connected.
– “IP Address”: The IP address of the partner, if the partner is already operating in the network.

The displays in the “Information” frame mean (see fig. 46):
– “Redundancy guaranteed”: One of the lines affected can fail, as a redundant line will then take over the function of the failed line.
– “Configuration failure”: The function is incomplete or incorrectly configured.

To avoid continuous loops, the Switch sets the port state of the coupling port to “off” if you:
– switch off operation or
– change the configuration
while the connections are in operation at these ports.

Note: The following settings are required for the coupling ports (you select the `Basic Settings:Port Configuration` dialog):
– Port: on
– Automatic configuration (autonegotiation):
on for twisted-pair connections
– Manual configuration: 100 Mbit/s FDX
for glass fiber connections

Note: If VLANS are configured, note the VLAN configuration of the coupling and partner coupling ports.
In the Network/Ring Coupling configuration, select for the coupling and partner coupling ports
– VLAN ID 1 and “Ingress Filtering” disabled in the port table and
– VLAN membership `U` in the static VLAN table.

Note: Operating the redundancy manager and two-Switch coupling functions at the same time runs the risk of creating a loop.

Redundancy mode

☐ In the “Redundancy Mode” frame, select (see fig. 48)
– “Redundant Ring/Network Coupling” or
– “Extended Redundancy”.

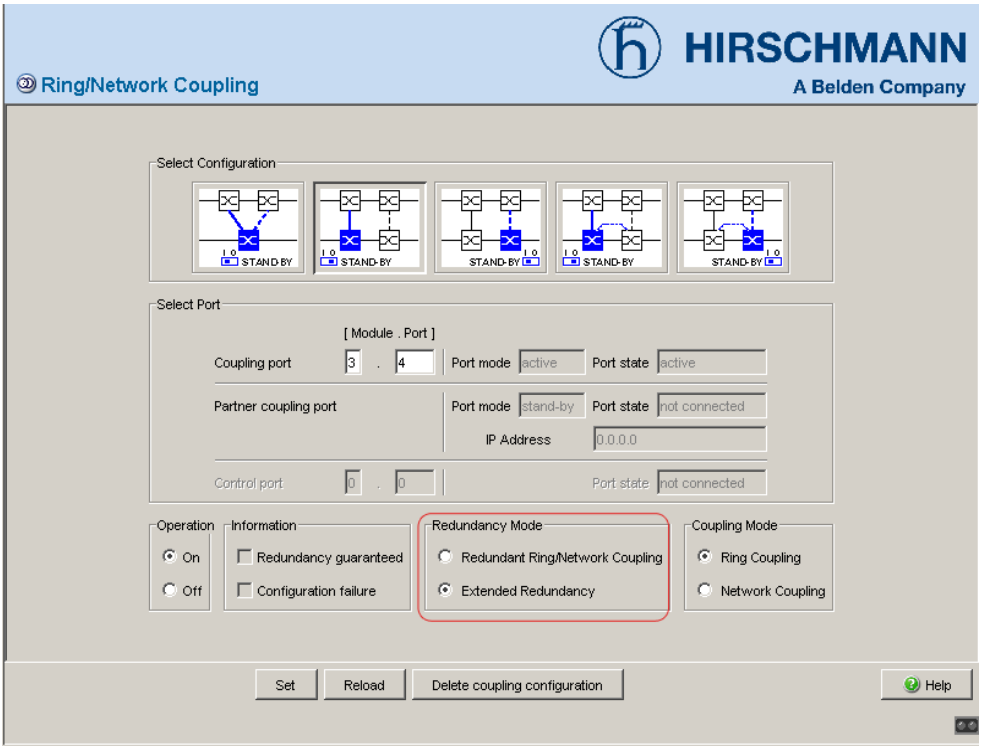


Figure 48: Selecting the redundancy mode

With the “Redundant Ring/Network Coupling” setting, either the main line or the redundant line is active. Both lines are never active simultaneously.

With the “Extended Redundancy” setting, the main line and the redundant line are simultaneously active if the connection line between the Switches in the connected network fails (see fig. 49).
During the reconfiguration period, there may be package duplications. Therefore, only select this setting if your application detects package duplications.

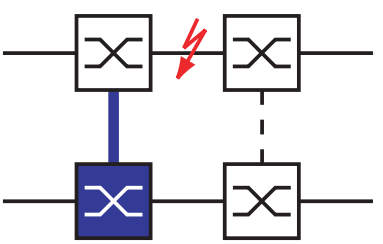


Figure 49: Extended redundancy

Coupling mode

The coupling mode indicates the type of the connected network.

☐ In the “Coupling Mode” frame, select (see fig. 50)

– “Ring Coupling” or

– “Network Coupling”

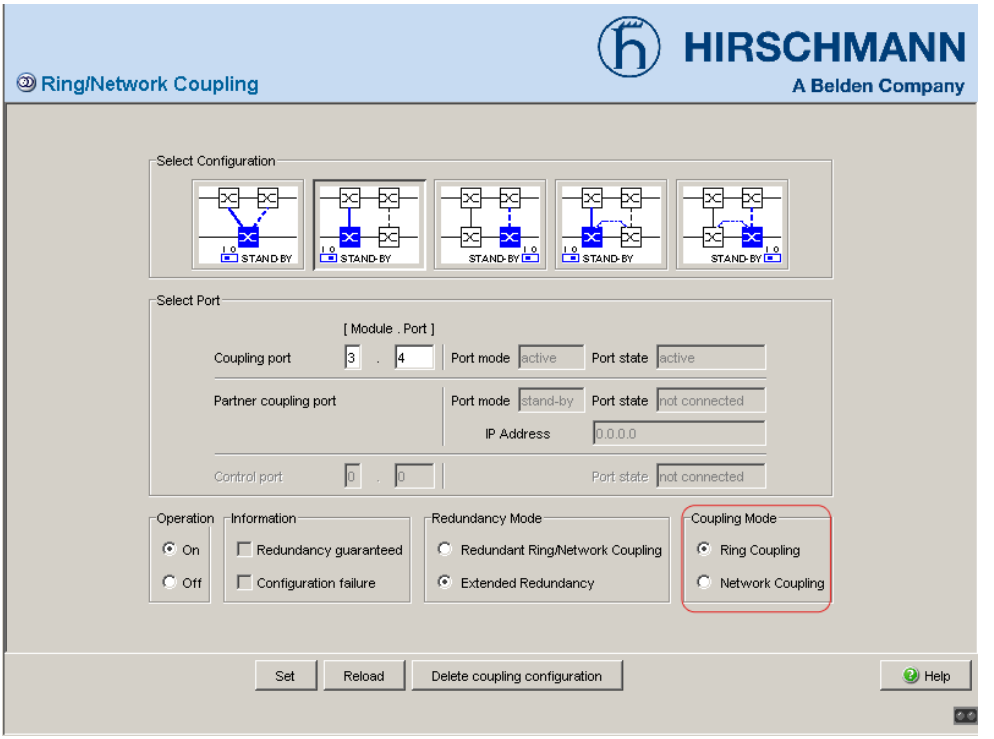


Figure 50: Selecting the coupling mode

☐ Select **“Ring coupling”** if you are connecting a HIPER-Ring.

☐ Select **“Network Coupling”** if you are connecting a line structure.

Delete coupling configuration

☐ The “Delete coupling configuration” button in the dialog allows you to reset all the coupling settings of the device to the state on delivery.

Two-Switch coupling with control line

- ☐ Connect the two partners via their ring ports.
- ☐ Select the `Redundancy:Ring/Network Coupling` dialog.
- ☐ Select two-Switch main coupling with control line (see fig. 51).

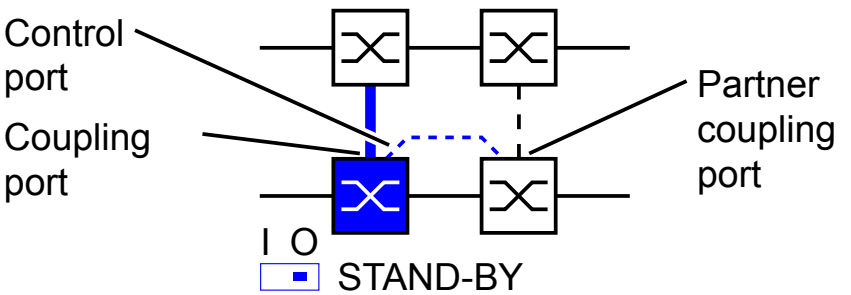


Figure 51: Two-Switch coupling with control line

The following settings apply to the Switch displayed in blue in the selected graphic.

- ☐ Select the coupling port (see fig. 52), (see table 17).
  With “Coupling port” you specify at which port you are connecting the redundant line.
- ☐ If the STANDBY DIP switch is OFF, connect the main line to the coupling port.
- ☐ Select the control port (see fig. 52), (see table 17).
  With “Control port” you specify at which port you are connecting the control line.

Switch	Coupling port	Control port
RS2-../..	Port 1	Stand-by port (can only be combined with RS2-../..)
RS2-16M	Adjustable for all ports (default setting: port 1)	Adjustable for all ports (default setting: port 2)
RS20	Adjustable for all ports (default setting: port 1.4)	Adjustable for all ports (default setting: port 1.3)
RS30	Adjustable for all ports (default setting: port 1.4)	Adjustable for all ports (default setting: port 1.3)
RS40	Adjustable for all ports (default setting: port 1.4)	Adjustable for all ports (default setting: port 1.3)
MICE	Adjustable for all ports (default setting: port 1.4)	Adjustable for all ports (default setting: port 1.3)
PowerMICE	Adjustable for all ports (default setting: port 1.4)	Adjustable for all ports (default setting: port 1.3)
MS 20	Adjustable for all ports (default setting: port 1.4)	Adjustable for all ports (default setting: port 1.3)
MS 30	Adjustable for all ports (default setting: port 2.4)	Adjustable for all ports (default setting: port 2.3)
RSR20/RSR30	Adjustable for all ports (default setting: port 1.4)	Adjustable for all ports (default setting: port 1.3)
MACH 1000	Adjustable for all ports (default setting: port 1.4)	Adjustable for all ports (default setting: port 1.3)
MACH 3000	Adjustable for all ports	Adjustable for all ports
MACH 4000	Adjustable for all ports (default setting: port 1.4)	Adjustable for all ports (default setting: port 1.3)

Table 17: Port assignment for the redundant coupling

Note: Configure the coupling port and the HIPER-Ring ports on different ports.

☐ Activate the function in the “Operation” frame (see fig. 52).
☐ You now connect the redundant line and the control line.

The displays in the “Select port” frame mean (see fig. 52):
– “Port mode”: The port is either active or in stand-by mode.
– “Port state”: The port is either connected or not connected.
– “IP Address”: The IP address of the partner, if the partner is already operating in the network.

The displays in the “Information” frame mean (see fig. 52):
– “Redundancy guaranteed”: One of the lines affected can fail, as a redundant line will then take over the function of the failed line.
– “Configuration failure”: The function is incomplete or incorrectly configured.

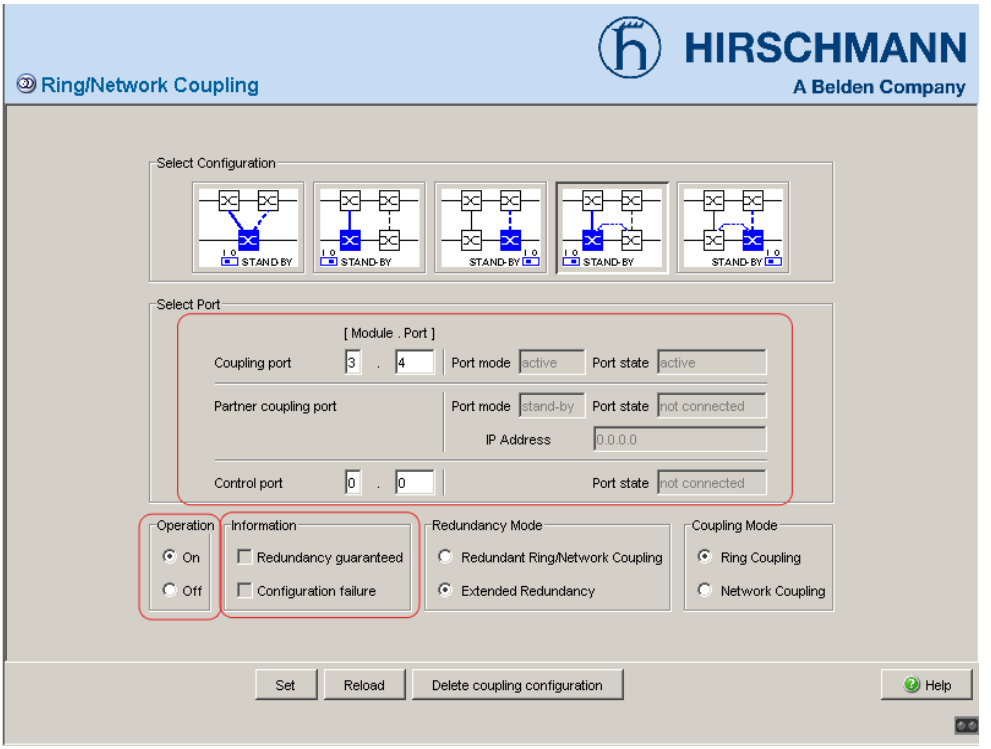


Figure 52: Selecting the port and enabling/disabling operation

To avoid continuous loops, the Switch sets the port state of the coupling port to “off” if you:
– switch off operation or
– change the configuration
while the connections are in operation at these ports.

Note: The following settings are required for the coupling ports (you select the `Basic Settings:Port Configuration` dialog):
– Port: on
– Automatic configuration (autonegotiation):
on for twisted-pair connections
– Manual configuration: 100 Mbit/s FDX
for glass fiber connections

Note: If VLANS are configured, note the VLAN configuration of the coupling and partner coupling ports.
In the Network/Ring Coupling configuration, select for the coupling and partner coupling ports
– VLAN ID 1 and “Ingress Filtering” disabled in the port table and
– VLAN membership `U` in the static VLAN table.

☐ Select two-Switch redundant coupling with control line (see fig. 53).

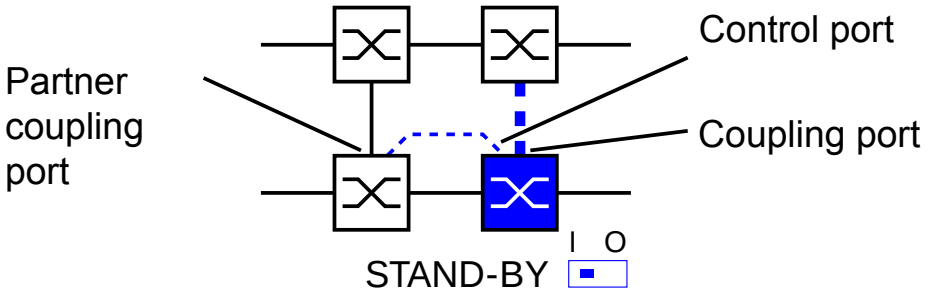


Figure 53: Two-Switch coupling with control line

The following settings apply to the Switch displayed in blue in the selected graphic.

☐ Select the coupling port (see fig. 52), (see table 17).
With “Coupling port” you specify at which port you are connecting the network segments.

☐ If the STANDBY DIP switch is ON, connect the main line to the coupling port.

☐ Select the control port (see fig. 52), (see table 17).
With “Control port” you specify at which port you are connecting the control line.

Note: Configure the coupling port and the HIPER-Ring ports on different ports.

☐ Activate the function in the “Operation” frame (see fig. 52).

☐ You now connect the redundant line and the control line.

The displays in the “Select port” frame mean (see fig. 52):

– “Port mode”: The port is either active or in stand-by mode.
– “Port state”: The port is either connected or not connected.
– “IP Address”: The IP address of the partner, if the partner is already operating in the network.

The displays in the “Information” frame mean (see fig. 52):

– “Redundancy guaranteed”: One of the lines affected can fail, as a redundant line will then take over the function of the failed line.
– “Configuration failure”: The function is incomplete or incorrectly configured.

To avoid continuous loops, the Switch sets the port state of the coupling port to “off” if you:
– switch off operation or
– change the configuration
while the connections are in operation at these ports.

Note: The following settings are required for the coupling ports (you select the `Basic Settings:Port Configuration` dialog):
– Port: on
– Automatic configuration (autonegotiation):
on for twisted-pair connections
– Manual configuration: 100 Mbit/s FDX
for glass fiber connections

Note: If VLANS are configured, note the VLAN configuration of the coupling and partner coupling ports.
In the Network/Ring Coupling configuration, select for the coupling and partner coupling ports
– VLAN ID 1 and “Ingress Filtering” disabled in the port table and
– VLAN membership `U` in the static VLAN table.

Redundancy mode

☐ In the “Redundancy Mode” frame, select (see fig. 54)
– “Redundant Ring/Network Coupling” or
– “Extended Redundancy”.

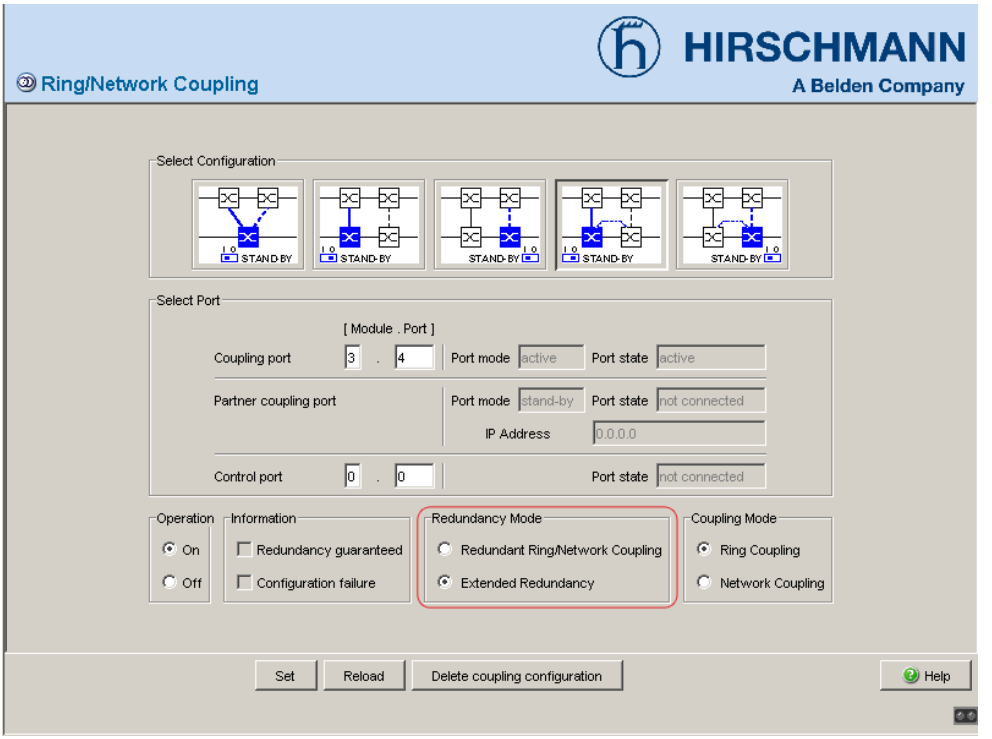


Figure 54: Selecting the redundancy mode

With the “Redundant Ring/Network Coupling” setting, either the main line or the redundant line is active. Both lines are never active simultaneously.

With the “Extended Redundancy” setting, the main line and the redundant line are simultaneously active if the connection line between the Switches in the connected network fails (see fig. 55).
During the reconfiguration period, there may be package duplications. Therefore, only select this setting if your application detects package duplications.

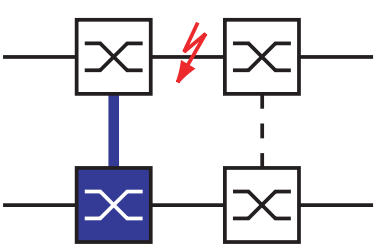


Figure 55: Extended redundancy

Coupling mode

The coupling mode indicates the type of the connected network.

☐ In the “Coupling Mode” frame, select (see fig. 56)

– “Ring Coupling” or

– “Network Coupling”

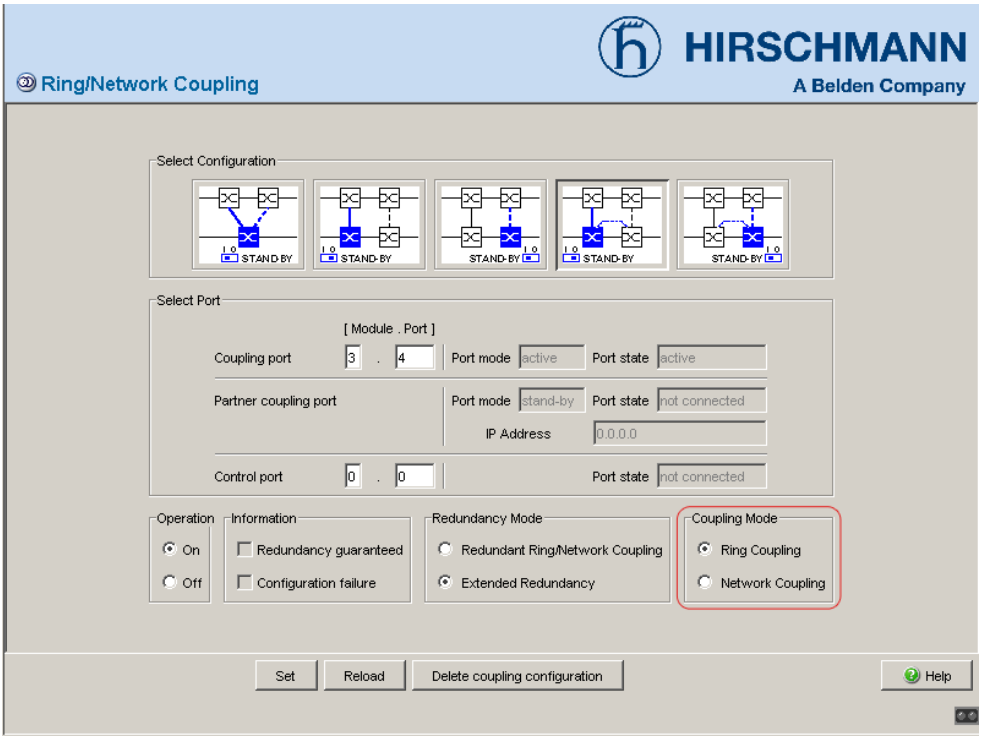


Figure 56: Selecting the coupling mode

☐ Select **“Ring coupling”** if you are connecting a HIPER-Ring.

☐ Select **“Network Coupling”** if you are connecting a line structure.

Delete coupling configuration

☐ The “Delete coupling configuration” button in the dialog allows you to reset all the coupling settings of the device to the state on delivery.

7.3 Rapid Spanning Tree

Note: The Spanning Tree protocol and the Rapid Spanning Tree protocol are protocols for MAC bridges. They are described in the standards IEEE 802.1D-2004 and IEEE 802.1w. For this reason, the following description of these protocols usually employs the term bridge instead of switch.

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

- to reduce the network load in subareas,
- 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 the total failure of the network. To prevent this, the (Rapid) Spanning Tree Algorithm was developed. The Rapid Spanning Tree Protocol (RSTP) enables redundancy by interrupting loops.

RSTP is a further development of the Spanning Tree Protocol (STP) and is compatible with it. If a connection or a bridge fails, the STP requires up to 30 seconds to reconfigure. This was no longer acceptable in time-sensitive applications. The STP was therefore developed into the RSTP, leading to reconfiguration times of less than a second.

Note: Standards dictate that all the bridges within a network work with the (Rapid) Spanning Tree Algorithm. However, if STP and RSTP are used at the same time, the advantages of faster reconfiguration with RSTP are lost.

7.3.1 Configuring the Rapid Spanning Tree

☐ Set up the network to meet your requirements.

Note: Before you connect the redundant lines, you must complete the configuration of the RSTP.
You thus avoid loops during the configuration phase.

☐ Select the `Redundancy:Rapid Spanning Tree:Global` dialog.

☐ Switch on RSTP on every device

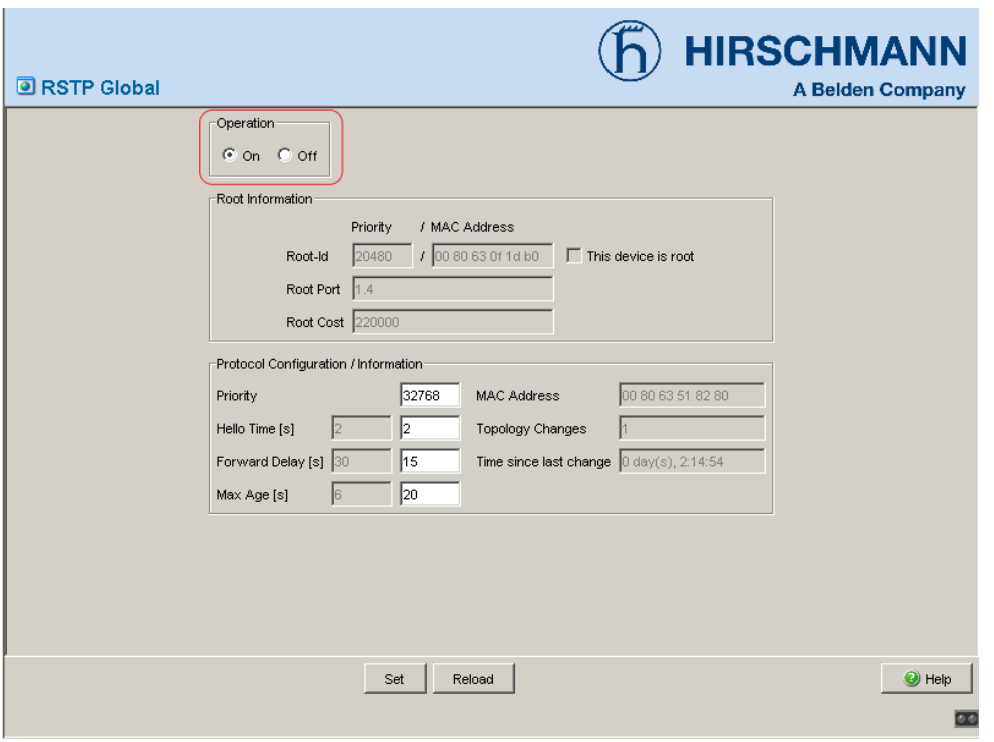


Figure 57: Operation on/off

☐ You now connect the redundant lines.

☐ Define the desired Switch as the root Switch by assigning it the lowest priority in the bridge information among all the Switches in the network, in the “Protocol Configuration/Information” frame. Note that only multiples of 4096 can be entered for this value (see table 18).
In the “Root Information” frame, the dialog shows this device as the root. A root switch has no root port and no root costs.

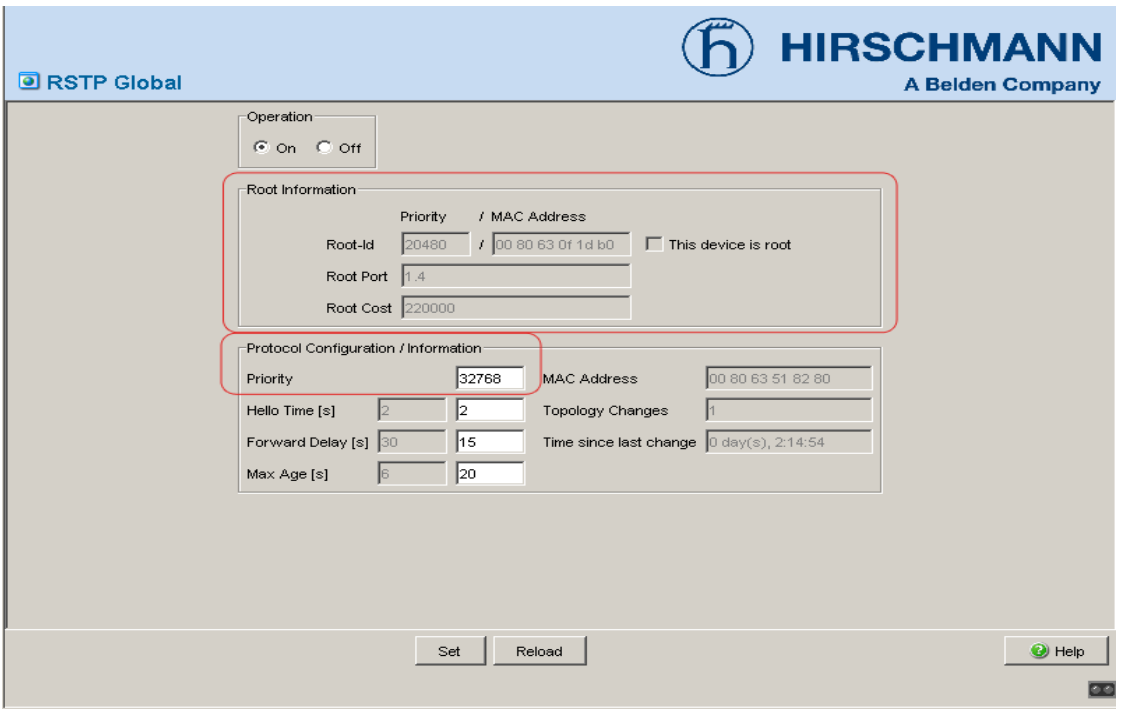


Figure 58: Assigning a priority. Display: Root Information

☐ As required, you change the default priority value of 32768 in other Switches in the network in the same way to the value you want (multiple of 4096).
For each of these Switches, check the display
in the “Root Information” frame:
– Root-Id: Displays the bridge identifier of the root Switch
– Root Port: Displays the port that leads to the root Switch
– Root Cost: Displays the root costs to the root Switch
in the “Protocol Configuration/Information” frame:
– Priority: Displays the priority in the bridge identifier for this Switch

– MAC Address: Displays the MAC address of this Switch
– Topology Changes: Displays the number of changes since the start of RSTP
– Time since last change: Displays the time that has elapsed since the last network reconfiguration

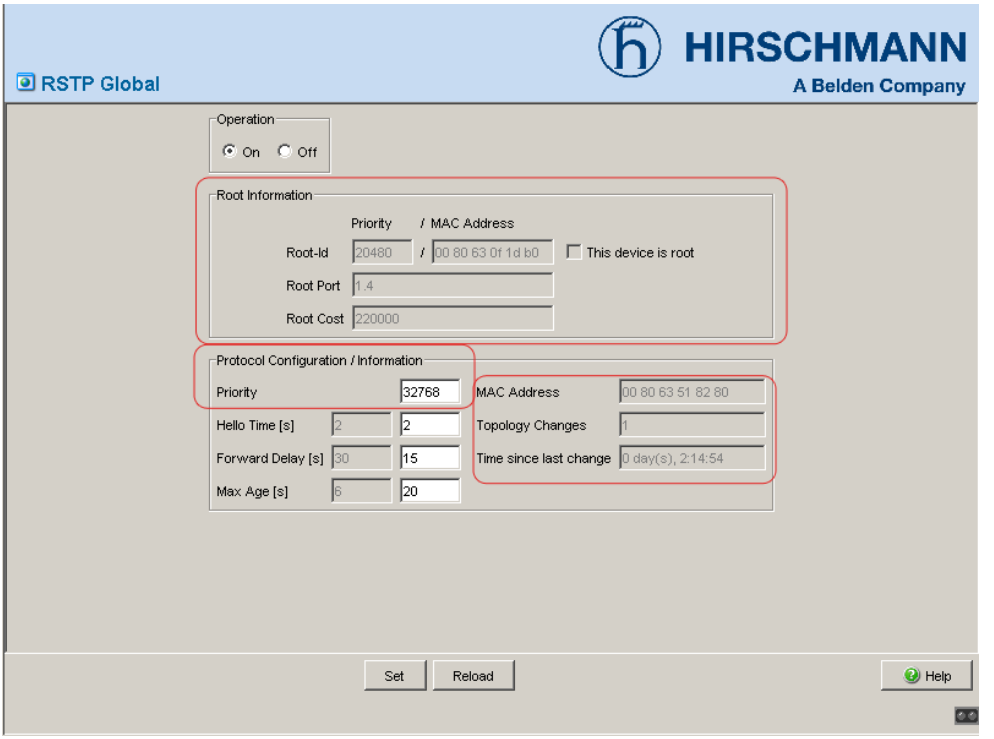


Figure 59: Display: Priority, MAC Address, Topology Changes and Time since last change

☐ If required, change the values for “Hello Time”, “Forward Delay” and “Max. Age” in the root Switch. The root Switch then transfers this data to the other Switches. The dialog displays the data received from the root Switch in the left column. In the right column you enter the values which shall apply when this Switch becomes a root Switch. For the configuration, take note of table 18.

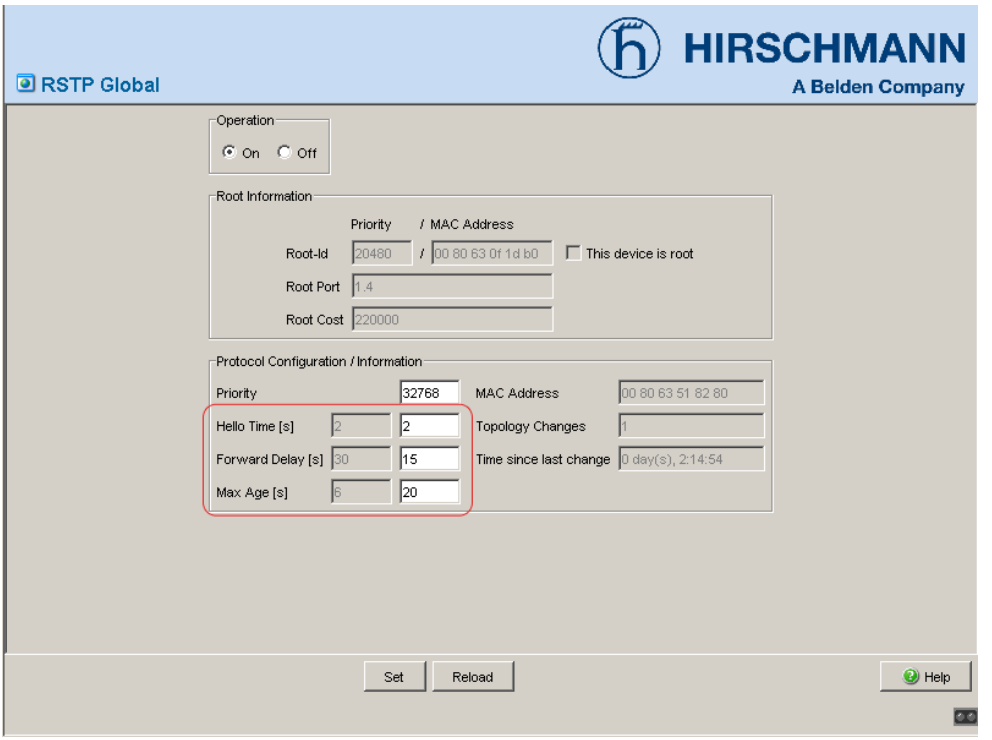


Figure 60: Assigning Hello Time, Forward Delay und Max. Age

The times entered in the dialog are in units of 1 s.
Example: Max Age = 20 corresponds to 20 seconds.

Variable	Meaning	Possible values	State on delivery
Priority	Priority and MAC address together make up the bridge identifier.	0 < n*4 096 < 61 440	32 768
Hello Time	The Switch periodically sends configuration messages (Hello packets, Configuration Bridge Protocol Data Units, CBPDU) if it is the root Switch. Hello Time is the time in seconds between the sending of two configuration messages (Hello packets, Configuration Bridge Protocol Data Units, CBPDU). This is the current value being used by the Switch.	1 - 10	2
Forward Delay	The state diagram of the Spanning Tree Protocol has four possible states: disabled, blocking, learning, forwarding. A certain amount of time passes when switching from one state to another. This is the current value being used by the Switch. The state change from forwarding to blocking occurs without a time lapse.	4 - 30	30
Max Age	After the “Max Age” elapses, a BPDU becomes invalid and is discarded.	6 - 40	6

Table 18: Global RSTP settings

☐ As required, change and verify the settings and displays that relate to each individual port (menu bar: Rapid Spanning Tree - Port).

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

Variable	Meaning	Possible values	State on delivery
STP status on	Switch RSTP on/off at this port. Switch STP off when connecting a terminal device in order to avoid unnecessary waiting times.	on, off	on
Port state	Display of the port state	disabled, forwarding, discarding, blocking, learning	-
Priority	Enter the first byte of the port identifier.	16 < n*16< 240	128
Admin Path Cost	Enter the path costs to indicate preference for redundant paths. If the value is “0”, the Switch automatically calculates the path costs depending on the transmission rate.	0 - 200 000 000	0
Admin Edge Port	Enter whether a terminal device (true) or an RSTP switch (false) is to be connected at this port. During reconfiguration, the edge port at a terminal device can switch to forwarding within 3 seconds.	true, false	false
Oper Edge Port	Shows whether an RSTP Switch is connected at this port. Independently of the value set under “Admin Edge Port”, the Switch detects a connected RSTP switch. Then it sets Edge Port = false .	true, false	-
Oper Point-ToPoint	Shows whether at this port the connection between two RSTP Switches is a half-duplex connection (true) or not (false). (The point-to-point connection is a direct connection between two RSTP Switches. The direct, decentralized communication between the two Switches results in a fast reconfiguration time.)	true, false	auto (is calculated): FDX = true HDX = false
Designated Root	Display of the bridge identifier of the designated root Switch for this port.	Bridge identifier (hexadecimal)	-
Designated Costs	Display of the costs of the path from this port to the root Switch.	Costs	-
Designated Port	Display of the port identifier of the port that creates the connection to the root Switch for this port (on the designated Switch).	Port identifier (hexadecimal) and port number	-

Table 19: Port-related RSTP settings and displays

☐ You now connect the redundant lines. You can avoid loops and network failures during the configuration phase by first configuring the Switches and only then connecting the redundant lines.

8 Diagnostics

The diagnostics menu contains the following tables and dialogs:

- Event log
- Ports (statistics, utilization, SFP modules)
- Topology discovery
- Port mirroring
- Device status
- Signal contact
- Alarms (traps)
- Report (log file, system information)
- IP address conflict detection
- Service-Mode

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

8.1 Event log

The table under Event Log lists all the events with a time stamp.
The "Delete" button allows you to delete the contents of the Event Log window.

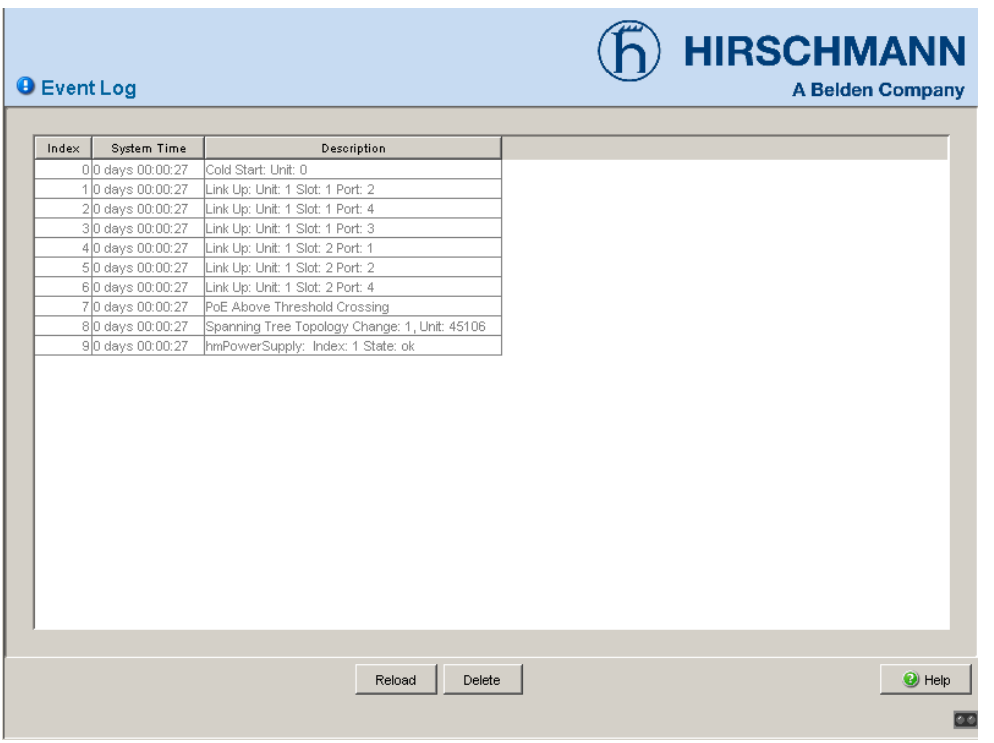


Figure 61: Event log table

8.2 Ports

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

- Statistics table
- Utilization
- SFP modules

8.2.1 Statistics table

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

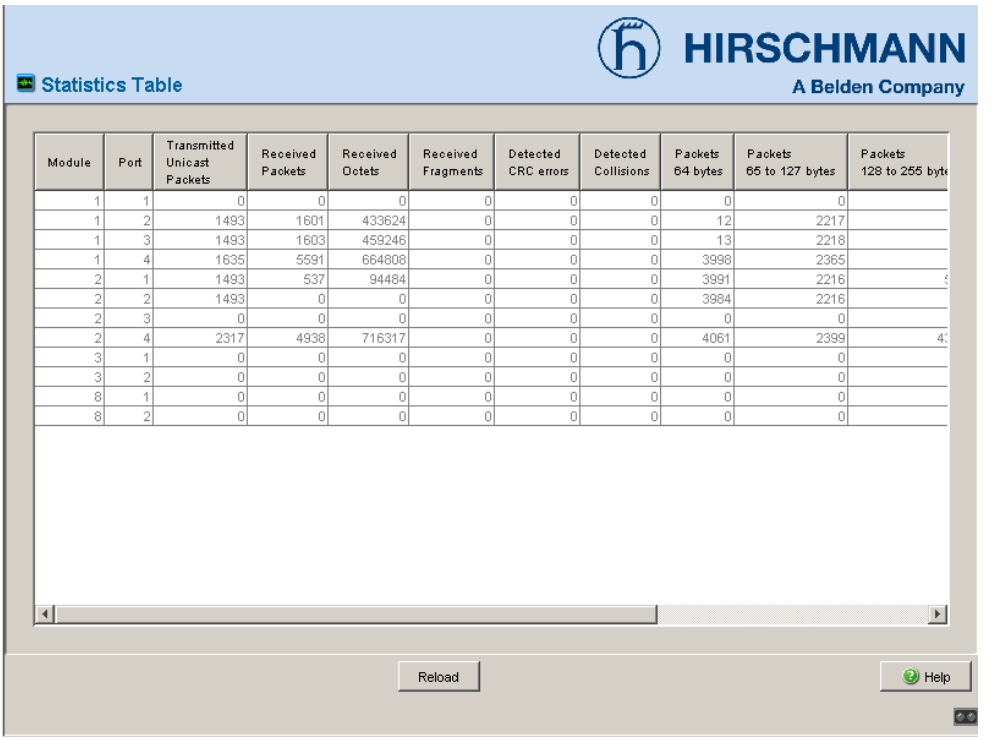


Figure 62: Port statistics table

8.2.2 Utilization

This table displays the network load of the individual ports.
In the “Upper Threshold[%]” column you enter the top threshold value for network load. If this threshold value is exceeded, the device sets a check mark in the “Alarm” field.
In the “Upper 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.

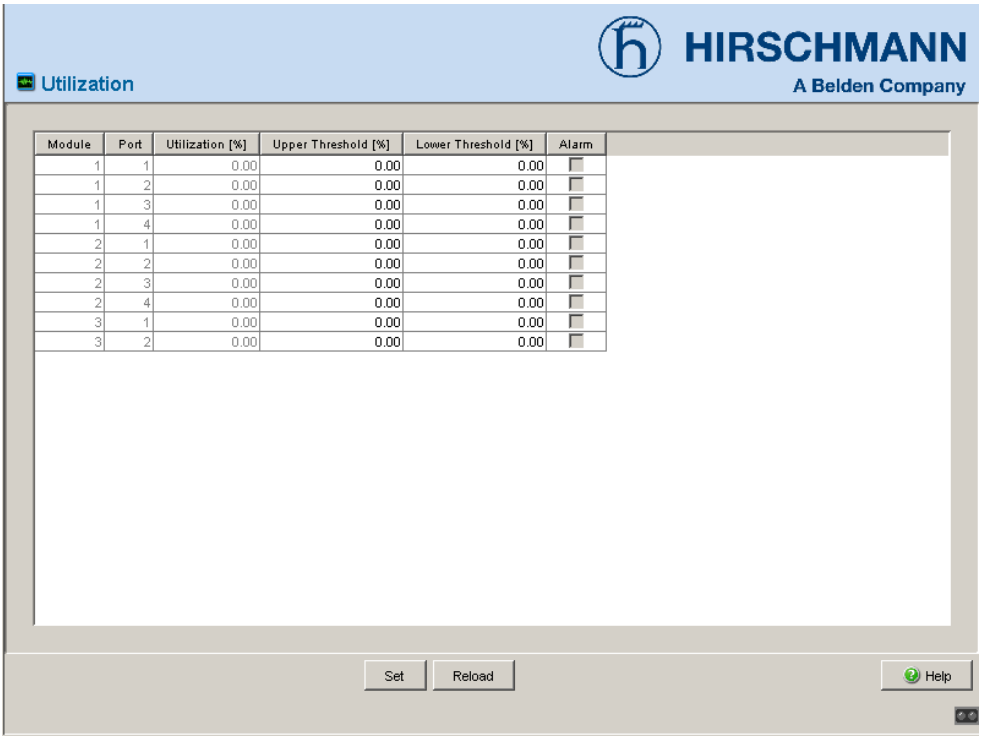


Figure 63: Network load dialog

8.2.3 SFP modules

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

- module type
- support provided in media module
- temperature in degrees Celsius
- transmission power in milliwatts
- reception power in milliwatts

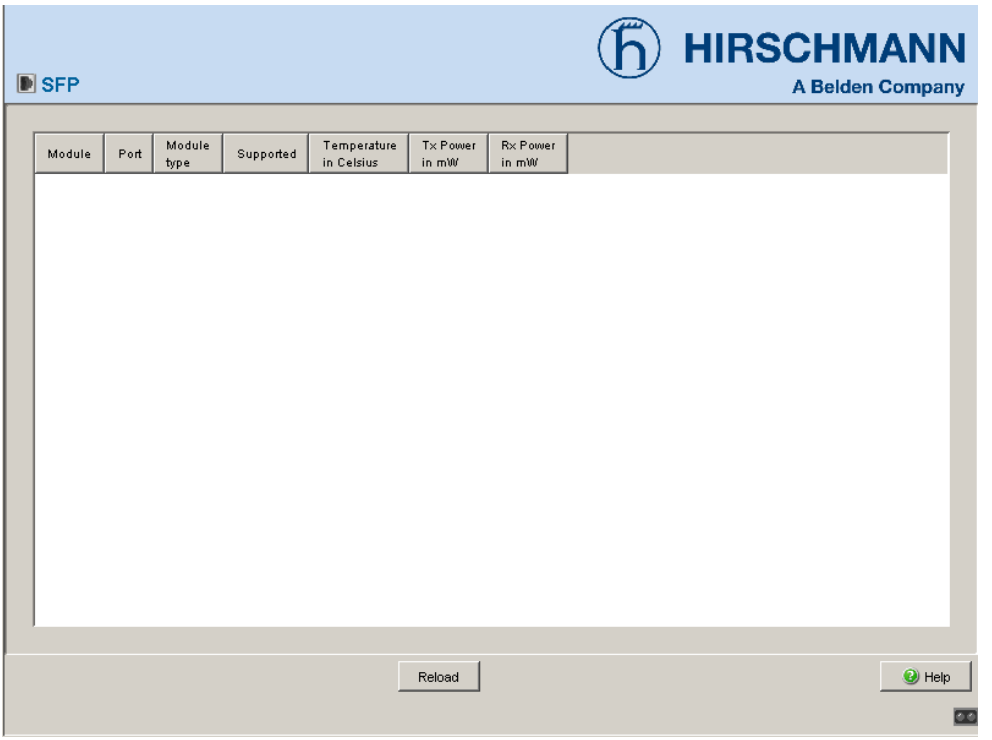


Figure 64: SFP Modules dialog

8.3 Topology Discovery

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

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

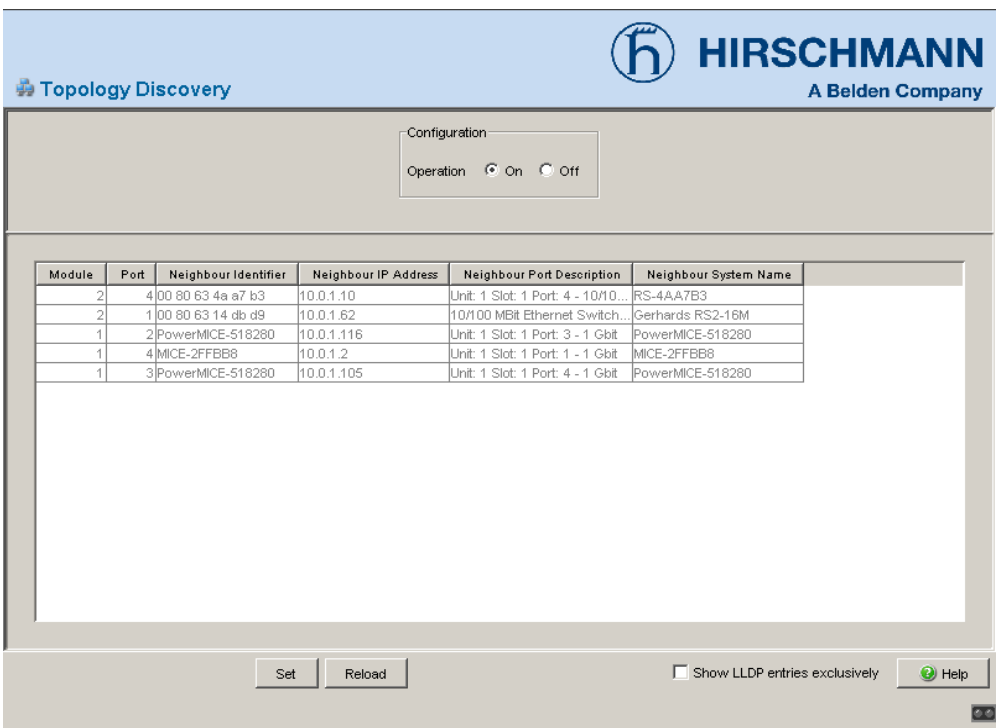


Figure 65: Topology discovery

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

If

- devices with active topology discovery function and

- devices without active topology discovery function
  are connected to a port, the topology table hides the devices without active topology discovery.

If

- only devices without active topology discovery are connected to a port, the table will contain one line for this port to represent all devices. This line contains the number of connected devices
  MAC addresses of devices that the topology table hides for the sake of clarity, are located in the address table (FDB), (see on page 61 „Filters for MAC addresses“).

8.4 Port Mirroring

This dialog allows you to configure and activate the port mirroring function of the device.
In port mirroring, the valid data packets of one port, the source port, are copied to another, the destination port. The data traffic at the source port is not influenced by port mirroring.
A management tool connected at the destination port, e.g. an RMON probe, can thus monitor the source port's data traffic in sending and receiving direction.
The destination port forwards the data to be sent and blocks data received.

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

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

☐ Select "enabled" to switch on the function.

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

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

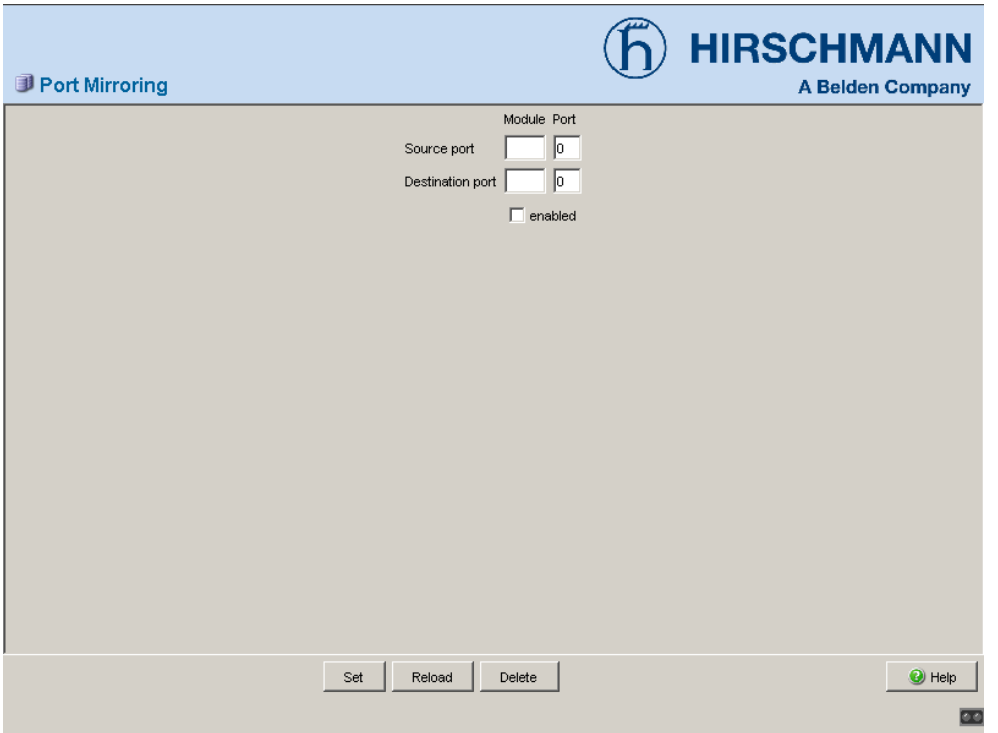


Figure 66: Port Mirroring dialog

8.5 Device Status

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

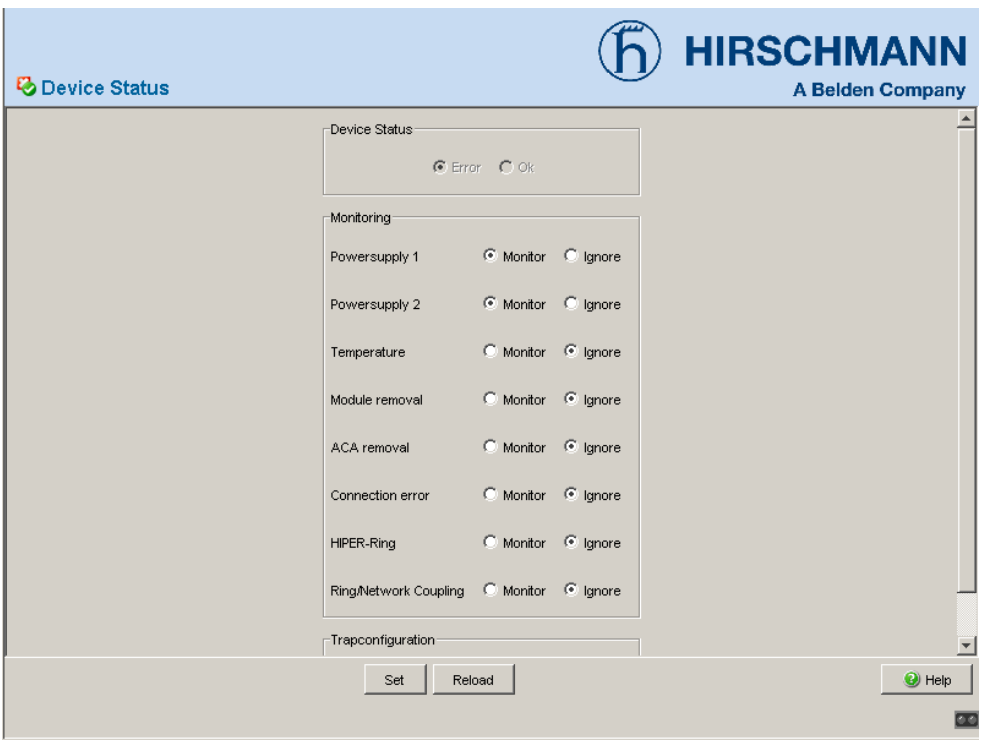


Figure 67: Device State dialog (for power MICE)

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

The events which can be selected are:

Name	Meaning
Power supply ...	Monitor/ignore supply voltage(s).
Temperature	Monitor/ignore the temperature threshold setting (see on page 16 „System“) for temperatures that are too high/too low.
Module removal	Monitor/ignore the removal of a module (for modular devices).
ACA removal	Monitor/ignore the removal of the ACA.
Connection error	Monitor/ignore the defective link status of at least one port. The reporting of the link status can be masked for each port by the management (see on page 24 „Port Configuration“). Link status is not monitored in the state on delivery.
HIPER-Ring	Monitor/ignore the failure of the redundancy (in redundancy manager mode). State on delivery: ring redundancy is not monitored.
Ring/network coupling	Monitor/ignore the failure of the redundancy. State on delivery: ring redundancy is not monitored. The following conditions are also reported by the device in standby mode: – Defective link status of the control line – Partner device is in standby mode.
Fan	Monitor/ignore fan function (for devices with fan).

Table 20: Device status

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

Note: With non-redundant voltage supply, the device reports the absence of a supply voltage. You can prevent this message by feeding the supply voltage over both inputs, or by switching off the monitoring (see on page 141 „Signal contact“).

8.6 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.

8.6.1 Manual setting

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

Application options:

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

8.6.2 Function monitoring

☐ Select the tab page “Alarm 1” or “Alarm 2” (for devices with two signal contacts).

☐ In the “Mode Signal contact” field, 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):

- Error during self-test (the contact remains open).
- Voltage supply 1/2 failure or continuous device malfunction (internal voltage). Select “Monitor” for Power Supply if the signal contact should report the failure of the voltage supply or the internal 3.3 V DC voltage.
- The temperature threshold has been exceeded or has not been reached (see on page 17 „System data“). Select “Monitor” for the temperature if the signal contact should report an impermissible temperature.
- Removing a module. Select “Monitor” for removing modules if the signal contact is to report the removal of a module (for modular devices).
- Fan failure (for devices with a fan).
- The removal of the ACA. Select “Monitor” for removing ACAs if the signal contact is to report the removal of an ACA (for devices which support ACAs).
- The defective link status of at least one port. The reporting of the link status can be masked via the management for each port in the device. Link status is not monitored in the state on delivery. Select “Monitor” for connection errors if the signal contact is to report a defective link status for at least one port.
- Loss of the redundancy guarantee in the HIPER-Ring (see on page 90 „HIPER-Ring“). Select “Monitor” for the HIPER-Ring if the signal contact is to report a redundancy that can no longer be guaranteed in the HIPER-Ring.
- Error in the Ring/Network coupling. Select “Monitor” for the Ring/Network coupling if the signal contact is to report an error in the Ring/Network coupling (see on page 99 „Configuring the redundant coupling“).

The following condition is also reported in RM mode:

- Redundancy guaranteed. State on delivery: ring redundancy is not monitored.

8.6.3 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 is used to monitor the status of the device (see on page 139 „Device Status“) and thereby makes remote diagnosis possible.
The device status “Error” (see on page 139 „Device Status“) is reported by means of a break in the contact via the potential-free signal contact (relay contact, closed circuit).

8.6.4 Configuring traps

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

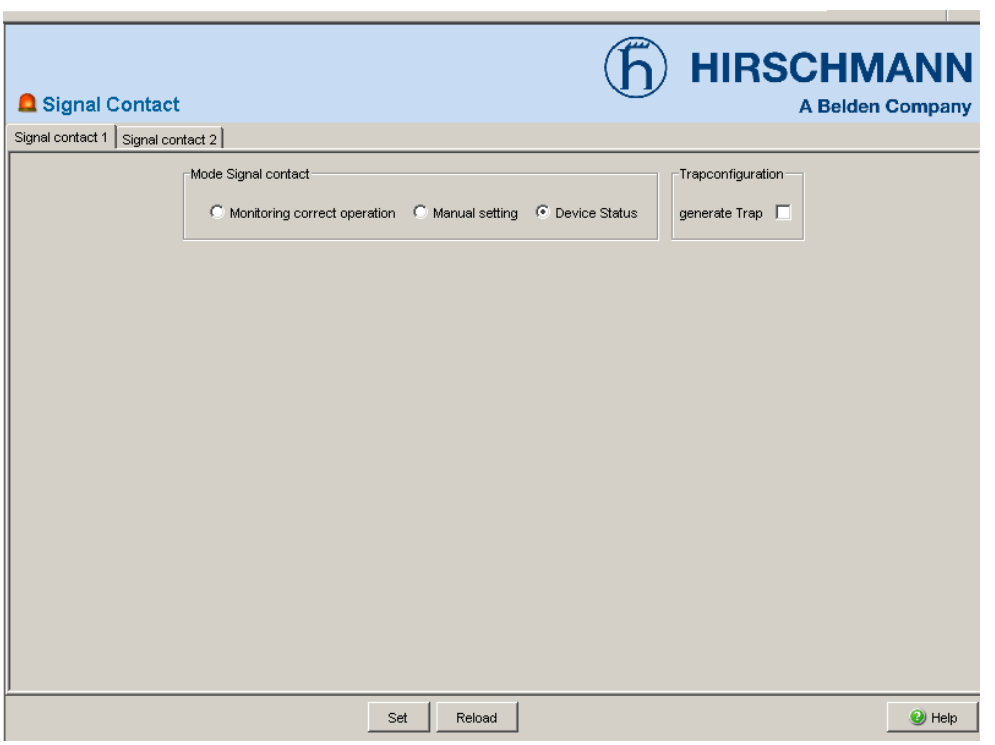


Figure 68: Signal contact dialog

8.7 Alarms (Traps)

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

☐ Select „Create entry“.
☐ In the „Address“ column, enter the IP address of the management station to which the traps should be sent.
☐ In the „Enabled“ column, you mark the entries which should be taken into account when traps are being sent.
☐ In the „Selection“ frame, select the trap categories from which you want to send traps.

The events which can be selected are:

Name	Meaning
Authentication	The device has rejected unauthorized access attempt, see dialog„SNMPv1/ v2 Access Setting“ on page 40 and „Port Mirroring“ on page 137.
Link Up/Down	At one port of the device, the link to a device connected there has been established/interrupted.
Spanning Tree	The topology of the Rapid Spanning Tree has changed.
Chassis	Encompasses 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. - The auto configuration adapter (ACA) has been added or removed. - The temperature threshold has been exceeded/not reached.
Redundancy	The redundancy status of the Hiper-Ring or the redundant ring/network coupling has changed.
Port security	On one port a data packet has been received from an unauthorized terminal device (see the `Port Security` dialog).

Table 21: Trap categories

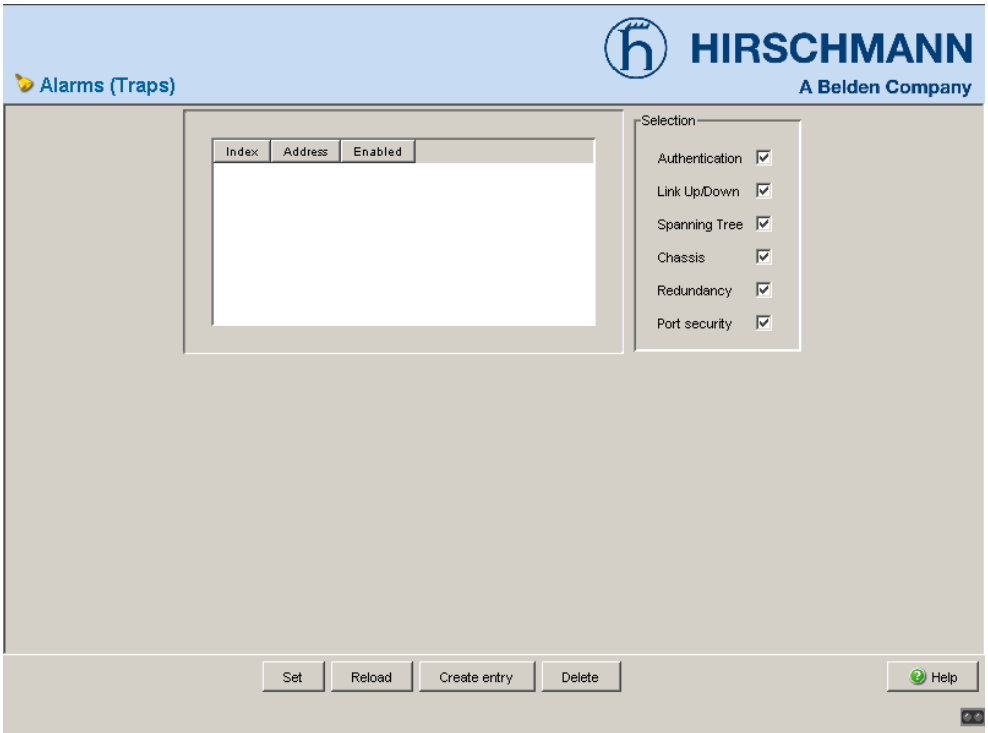


Figure 69: Alarms dialog

8.8 Report

The following reports are available for the diagnostics:

- Log file
  The log file is an HTML file in which the device writes all the important device-internal events
- System information.
  The system information is an HTML file containing all system-relevant data.
- System information.
  The security data sheet IAONA is a data sheet in the XML format that has been standardized by IAONA (Industrial Automation Open Networking Alliance). Among other data, it contains security-related information on the accessible ports and the associated protocols.

8.9 IP address conflict detection

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

☐ Select IP address conflict detection on/off under “Status” or select the mode (see table 22).

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

Table 22: Possible address conflict operation modes

- In the table the device logs IP address conflicts with its IP address.
  For each conflict the device logs:
  - the time
  - the conflicting IP address
  - the MAC address of the device with which the IP address conflicted.

  For each IP address, the device logs a line with the last conflict that occurred.

☐ You can delete this table by restarting the device.

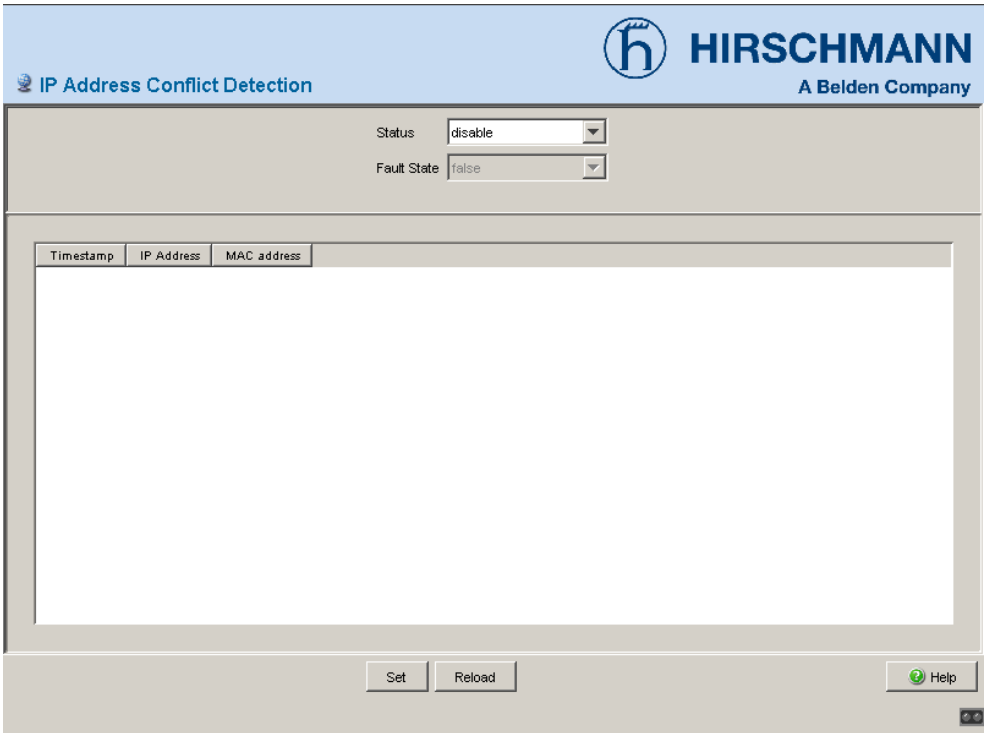


Figure 70: IP Address Conflict Detection dialog

8.10Self-test

This dialog allows you to activate/deactivate the RAM test when cold-starting the device. Deactivating the RAM tests shortens the booting time for a cold start of the device.

Figure 71: Self-test dialog

8.11 Service mode

The service mode enables you to divide the device into two transmission areas. You can thus, for example, perform test or service configurations in the field area of a network while the ongoing operation continues in the backbone area.

The device determines the two transmission areas via the HIPER-Ring ports: transmission area 1 only includes the HIPER-Ring ports of the device, while all other ports belong to transmission area 2. When the service mode is activated, the device creates a new VLAN in which all the ports of transmission area 2 are members. You use the redundant supply voltage (see below) to activate the service mode. You can view the configuration of the newly created VLAN in the dialogs under Switching/VLAN, but the device does not allow these entries to be changed, in order to keep the service configuration. By generating the VLAN, the device

- resets the port VLAN IDs for all the ports of this VLAN to the new VLAN ID
- deactivates GVRP at all ports of this VLAN. The device thus prevents GVRP from dynamically changing the service mode port settings.
- activates “ingress filtering” at all ports of this VLAN. Thus the device only transmits packets when the input and output ports belong to this VLAN.

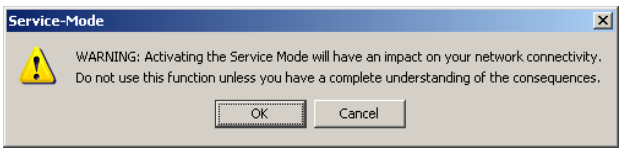
8.11.1 Activating the service mode

Prerequisites:

– HIPER-Ring ports are defined (HIPER-Ring version 1 or version 2).
– The supply voltage is redundant at P1 and P2.

Note: If there is no redundant voltage when the service mode is being activated (by clicking on “Set” - see below), the Switch immediately creates the two transmission areas. Depending on the settings already entered, this can break your link to the Switch.

☐ Select the `Diagnostics:Service Mode` dialog.
☐ Activate “Mode”.
☐ Enter a number not equal to 0 or 1 in the “VLAN” field. Enter a VLAN ID for a new VLAN in order to keep the settings for existing VLANs.
☐ Click on “Set”. The following warning appears:



☐ It you are sure that your link to the Switch will not be broken, click on “OK” to activate the service mode.

The device will indicate in all dialogs that the service mode is activated.

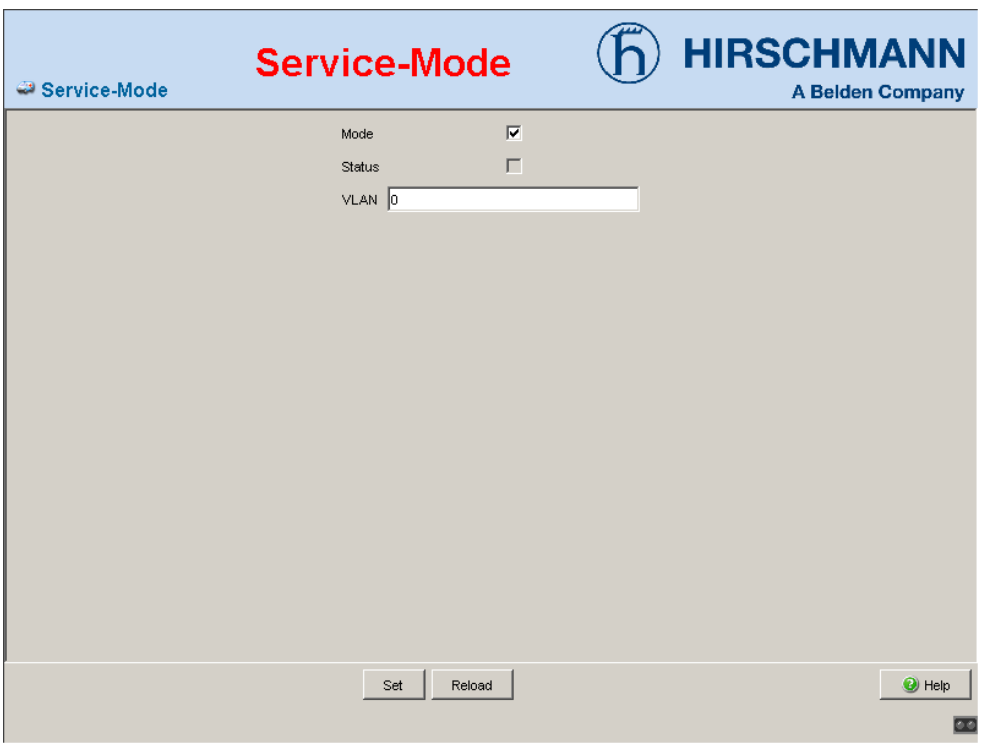


Figure 72: Service Mode dialog - mode activated

☐ Deactivate the redundant supply voltage.

The service mode is now activated, which the device indicates with a check-mark in the “Status” field.

Note: Deactivate the service mode (see below) when saving the device configuration (dialog: `Basics:Load/Save:Save:On the Switch`).

8.11.2 Deactivating the service mode

☐ Reactivate the redundant voltage.

The service mode is now deactivated.

☐ Select the `Diagnostics:Service Mode` dialog.
☐ Deactivate “Mode”.
☐ Click on “Set” to deactivate the service mode.
This prevents the device from switching to the service mode if the redundant voltage supply fails.

Note: After the service mode is deactivated, the device takes on its previous settings again.

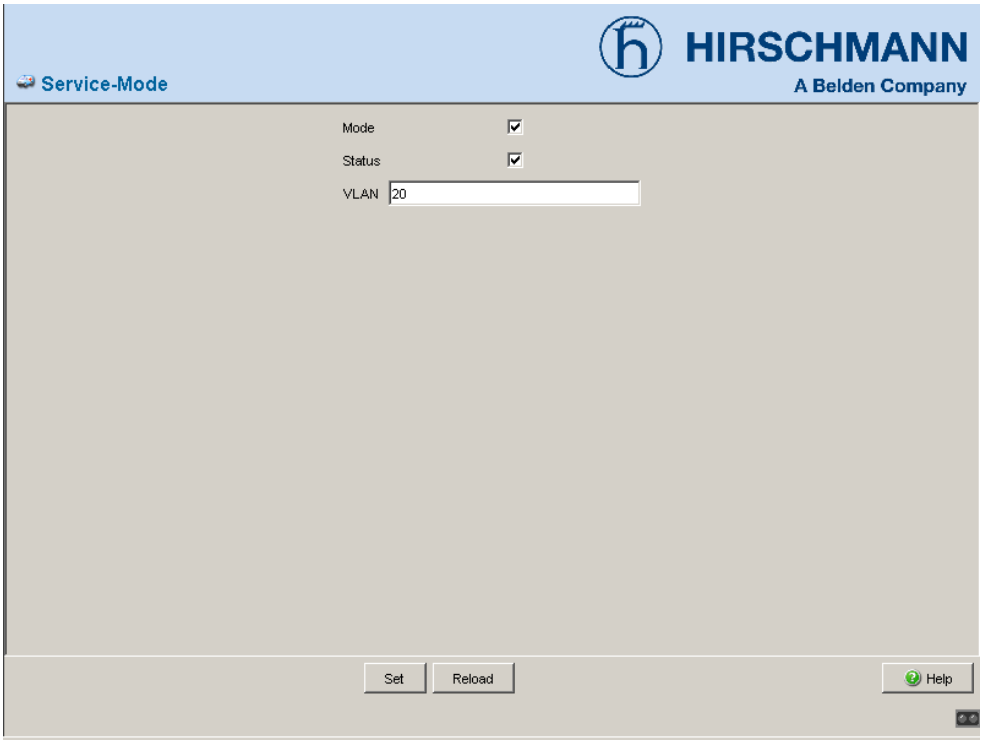


Figure 73: Service Mode dialog - mode deactivated

9 Advanced

The advanced menu contains the dialogs, displays and tables for:

- DHCP Relay Agent
- Industry Protocols
- Command Line

9.1 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, then you can enter up to three 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, that you can specify in the following rows).
"DHCP server RemoteID entry" shows you the value that you enter when configuring your DHCP server. "Type display" shows the device recognition in the selected form.

▶ The "Circuit ID" column shows you the value which you enter when configuring your DHCP server. The "Circuit ID" contains the port number and the ID of the VLAN from which the DHCP has been received.

Example of a configuration of your DHCP server:
Type: `mac`
RemoteID 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:
`B30600000100010100060080630006 1E`

☐ In the "Option 82 on/off" column, you can switch this function on/off for each port.

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

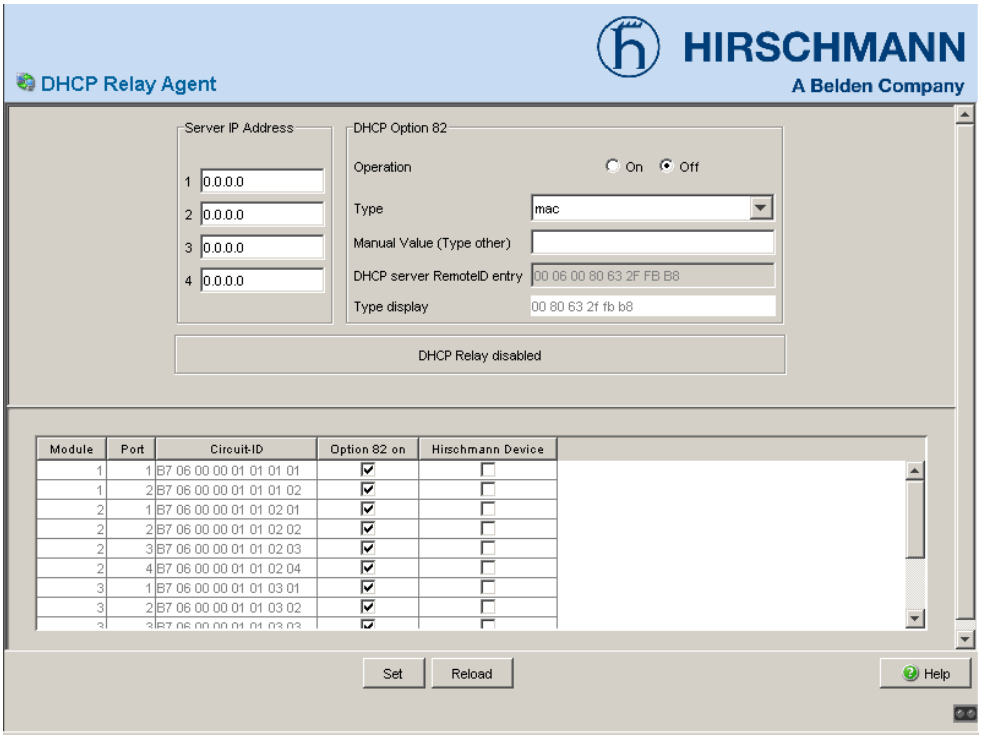


Figure 74: DHCP Relay Agent dialog

9.2 Industry Protocols

This dialog enables you to

- activate and deactivate the PROFINET IO or EtherNet/IP industry protocols
- download files for configuring the SPS from the Switch to your PC

☐ You will find detailed information on the industry protocols and on the configuration of the SPS in the "Industry Protocols" user manual.

Figure 75: Industry Protocols dialog

9.2.1 PROFINET IO

To integrate this into a control system,
☐ activate the function in the "ProfinetIO" frame
☐ click on "Download GSDML File" to load the GSDML file onto your PC
☐ in the `Basic Settings:Network` dialog, check whether `Local` is selected in the "Mode" frame (see on page 20 „Network“),
☐ in the `Switching:VLAN:Global` dialog, check whether "VLAN 0 Transparent Mode" is selected (see „Setting up the VLAN“ on page 73),
☐ configure the alarm settings and the threshold values for the alarms you want to monitor (see the „Device Status“ dialog on page 139,
☐ configure the SPS as described in the "Industry Protocols" user manual

9.2.2 EtherNet/IP

To integrate this into a control system,
☐ activate the function in the "EtherNet/IP" frame
☐ click on "Download EDS File" to load the EDS file onto your PC
☐ in the `Switching: Multicasts` dialog, check whether IGMP Snooping is activated (see on page 65 „Multicasts“),
☐ configure the SPS as described in the "Industry Protocols" user manual

9.3 Command Line

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

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

A Technical Data

VLAN	
VLAN ID	1 to 4042 (MACH 4000: 3966)
Number of VLANs	max. 256 simultaneously per device max. 256 simultaneously per port
Number of VLANs in GMRP in VLAN 1	max. 256 simultaneously per device max. 256 simultaneously per port

Switching	
Size of MAC address table (incl. static filters)	8000
Max. number of statically configured MAC address filters	100
Max. number of MAC address filters learnable via GMRP/IGMP Snooping	512
Max. length of over-long packets (from 03.0.00)	1632

B Reader´s 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:

	excellent	**good**	**satisfactory**	**mediocre**	**poor**
Accuracy	O	O	O	O	O
Readability	O	O	O	O	O
Comprehensibility	O	O	O	O	O
Examples	O	O	O	O	O
Structure/Layout	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 an error in the manual? If so, on what page?

Suggestions for improvement and additional information:

General comments:

Sender:

Company / Department:

Name / Telephone number:

Street:

Zip code / City:

Date / Signature:

Dear User,

Please fill out and return this page

- by fax to the number +49 (0)7127/14-1798 or
- by mail to

Hirschmann Automation and Control GmbH
Department AMM
Stuttgarter Str. 45-51

72654 NeckartenzlingenGermany
Germany

C Index

D Further support

Technical questions and training courses

In the event of technical queries, please talk to the Hirschmann contract partner responsible for looking after your account or directly to the Hirschmann office.
You can find the addresses of our contract partners on the Internet: www.hirschmann-ac.com.

Our support line is also at your disposal:

- Tel. +49 1805 14-1538
- Fax +49 7127 14-1551

Answers to Frequently Asked Questions can be found on the Hirschmann internet site (www.hirschmann-ac.com) at the end oft the product sites in the FAQ category.
The current training courses to technology and products can be found under http://www.hicomcenter.com.

Hirschmann Competence Center

In the long term, excellent products alone do not guarantee a successful customer relationship. Only comprehensive service makes a difference worldwide. In the current global competition scenario, the Hirschmann Competence Center is ahead of its competitors on three counts with its complete range of innovative services:

- Consulting incorporates comprehensive technical advice, from system evaluation through network planning to project planing.
- Training offers you an introduction to the basics, product briefing and user training with certification.
- 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 Company