



HIRSCHMANN

A **BELDEN** BRAND

Hirschmann Automation and Control GmbH

Classic L2E Rel. 09000

Reference Manuals

Graphical User Interface

Command Line Interface

User Manuals

Basic Configuration

Industry Protocols

Redundancy Configuration



HIRSCHMANN

A **BELDEN** BRAND

Reference Manual

**GUI Graphical User Interface
Industrial ETHERNET (Gigabit-)Switch
RS20/RS30/RS40, MS20/MS30**

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.

© 2015 Hirschmann Automation and Control GmbH

Manuals and software are protected by copyright. All rights reserved. The copying, reproduction, translation, conversion into any electronic medium or machine scannable form is not permitted, either in whole or in part. An exception is the preparation of a backup copy of the software for your own use. For devices with embedded software, the end-user license agreement on the enclosed CD/DVD applies.

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

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

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

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

Contents

	Safety Information	7
	About this Manual	9
	Key	11
	Graphical User Interface	13
1	Basic Settings	19
1.1	System	20
1.2	Modules (MS, PowerMICE, MACH102 and MACH4000)	24
1.3	Network	27
1.4	Software	30
1.4.1	View the software versions present on the device	31
1.4.2	Restoring the Backup Version	31
1.4.3	TFTP Software Update	31
1.4.4	TFTP Bootcode Update	32
1.4.5	HTTP Software Update	33
1.4.6	Automatic software update by ACA	33
1.5	Port Configuration	34
1.6	Power over ETHERNET	37
1.7	Load/Save	40
1.7.1	Loading a Configuration	41
1.7.2	Saving the Configuration	48
1.7.3	URL	50
1.7.4	Deleting a configuration	51
1.7.5	Using the AutoConfiguration Adapter (ACA)	51
1.7.6	Cancelling a configuration change	53
1.8	Restart	55
2	Security	57
2.1	Password / SNMPv3 access	58
2.2	SNMPv1/v2 Access Settings	61
2.3	Telnet/Web Access	64
2.3.1	Description of Telnet Access	65
2.3.2	Description of Web Access (http)	65

2.4	Port Security	67
2.5	Login/CLI Banner	74
2.5.1	Login Banner	75
2.5.2	CLI Banner	77
3	Time	79
3.1	Basic Settings	80
3.2	SNTP configuration	83
3.3	PTP (IEEE 1588)	87
3.3.1	PTP Global (MS20/MS30, PowerMICE, MACH 104, MACH 1040)	90
3.3.2	PTP Version 1 (MS20/MS30, PowerMICE, MACH 104, MACH 1040)	94
3.3.3	PTP Version 2 (BC) (MS20/MS30, PowerMICE, MACH 104, MACH 1040)	96
3.3.4	PTP Version 2 (TC) (MS20/MS30, PowerMICE, MACH 104, MACH 1040)	103
4	Switching	109
4.1	Switching Global	110
4.2	Filter for MAC addresses	114
4.3	Rate Limiter	117
4.3.1	Rate limiter settings	118
4.4	Multicasts	120
4.4.1	IGMP (Internet Group Management Protocol)	120
4.5	VLAN	127
4.5.1	VLAN Global	127
4.5.2	Current VLAN	131
4.5.3	VLAN Static	133
4.5.4	Port	136
5	QoS/Priority	139
5.1	Global	140
5.2	Port Configuration	144
5.2.1	Entering the port priority	145
5.3	802.1D/p mapping	146
5.4	IP DSCP mapping	148

6	Redundancy	151
6.1	Ring Redundancy	152
	6.1.1 Configuring the HIPER-Ring	154
	6.1.2 Configuring the MRP-Ring	158
6.2	Ring/Network Coupling	162
	6.2.1 Preparing a Ring/Network Coupling	162
6.3	Spanning Tree	168
	6.3.1 Global	170
	6.3.2 Port	176
7	Diagnostics	185
7.1	Syslog	186
7.2	Trap log	190
7.3	Ports	192
	7.3.1 Statistics table	192
	7.3.2 Network load (Utilization)	194
	7.3.3 SFP Transceiver	196
7.4	Topology Discovery	198
	7.4.1 LLDP Information from Neighbor Devices	198
7.5	Port Mirroring	200
7.6	Device Status	202
7.7	Signal contact	205
	7.7.1 Manual Setting	205
	7.7.2 Function monitoring	206
	7.7.3 Device status	207
	7.7.4 Configuring Traps	208
7.8	Alarms (Traps)	210
7.9	Report	213
	7.9.1 System Information	215
	7.9.2 Event Log	216
7.10	IP address conflict detection	217
7.11	MAC Notification	219
	7.11.1 Operation	219
	7.11.2 Configuration	220
	7.11.3 Table	220
7.12	Self Test	222

7.13	Service Mode	224
	7.13.1 Activating the service mode	225
	7.13.2 Deactivating the service mode	227
8	Advanced	229
8.1	DHCP Relay Agent	230
	8.1.1 Global	230
	8.1.2 Server	233
8.2	Industrial Protocols	235
	8.2.1 PROFINET	235
	8.2.2 EtherNet/IP	238
	8.2.3 IEC61850 MMS Protocol (RSR, MACH 1000)	239
8.3	Software DIP Switch overwrite (MICE, PowerMICE and RS)	241
8.4	Command Line	245
A	Appendix	247
A.1	Technical Data	248
A.2	List of RFCs	249
A.3	Underlying IEEE Standards	251
A.4	Underlying IEC Norms	252
A.5	Literature references	253
A.6	Copyright of Integrated Software	254
	A.6.1 Bouncy Castle Crypto APIs (Java)	254
	A.6.2 Broadcom Corporation	255
B	Readers' Comments	256
C	Index	259
D	Further Support	263

Safety Information



WARNING

UNCONTROLLED MACHINE ACTIONS

To avoid uncontrolled machine actions caused by data loss, configure all the data transmission devices individually.

Before you start any machine which is controlled via data transmission, be sure to complete the configuration of all data transmission devices.

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

About this Manual

The “GUI” reference manual contains detailed information on using the graphical interface to operate the individual functions of the device. In the following, the GUI (Graphical User Interface) will be referred as Web-based Interface.

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

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

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

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

The “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 or PROFINET IO.

The Industrial HiVision network management software provides you with additional options for smooth configuration and monitoring:

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

■ **Maintenance**

Hirschmann are continually working on improving and developing their software. Check regularly whether there is an updated version of the software that provides you with additional benefits. You find information and software downloads on the Hirschmann product pages on the Internet (www.hirschmann.com).

Key

The designations used in this manual have the following meanings:

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

Symbols used:

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

Key



Hub



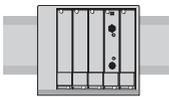
A random computer



Configuration Computer



Server



PLC -
Programmable logic
controller



I/O -
Robot

Graphical User Interface

■ **System requirements**

Use HiView to open the graphical user interface. This application offers you the possibility to use the graphical user interface without other applications such as a Web browser or an installed Java Runtime Environment (JRE).

Alternatively you have the option to open the graphical user interface in a Web browser, e.g. in Mozilla Firefox version 3.5 or higher or Microsoft Internet Explorer version 6 or higher. You need to install the Java Runtime Environment (JRE-7) in the most recently released version. You can find installation packages for your operating system at <http://java.com>.

■ **Starting the graphical user interface**

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

Starting the graphical user interface in HiView:

- Start HiView.
- In the URL field of the start window, enter the IP address of your device.
- Click "Open".

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

Start the graphical user interface in the Web browser:

- This requires that Java is enabled in the security settings of your Web browser.
- Start your Web browser.
- Write the IP address of the device in the address field of the Web browser. Use the following form: `https://xxx.xxx.xxx.xxx`

The Web browser sets up the connection to the device and displays the login window.

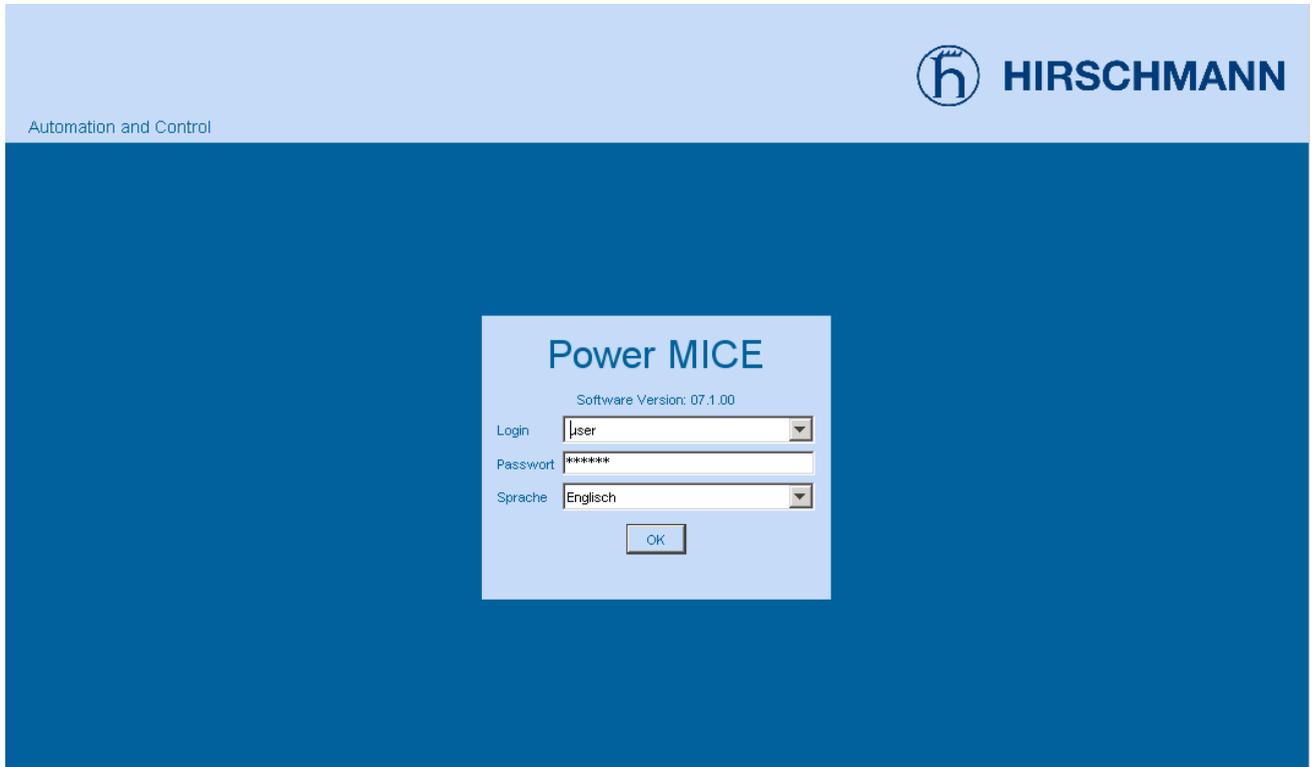


Figure 1: Login window

- Select the user name and enter the password.
- Select the language in which you want to use the graphical user interface.
- Click "Ok".

The Web browser displays the graphical user interface.

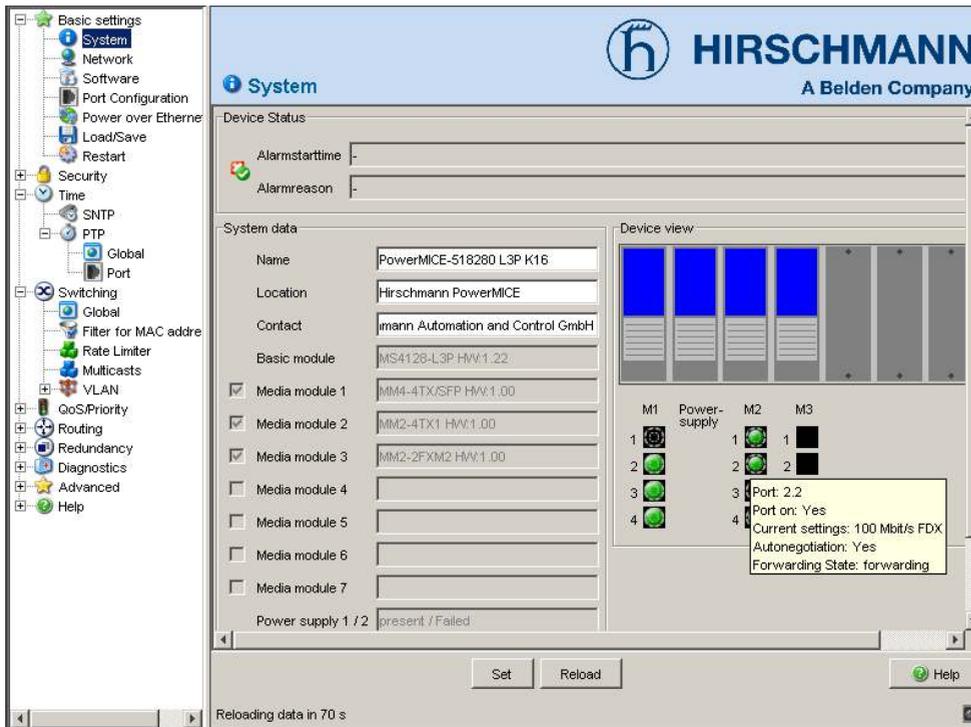
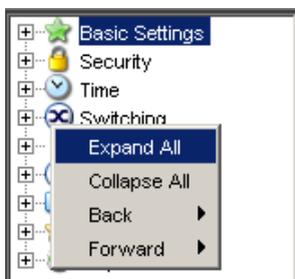


Figure 2: Web-based user interface of the device with tooltip.

■ Operating Instructions

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



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

Designation	Meaning
Expand All	Expands the nodes in the menu tree. The menu section displays the menu items for all levels.
Collapse All	Collapses the nodes in the menu tree. The menu section displays the menu items for the top level.
Expand Node	Expands the selected node and collapses the other nodes in the menu tree. This function allows you to expand a main node without scrolling and without collapsing other nodes manually.
Back	Allows you to quickly jump back to a previously selected menu item.
Forward	Allows you to quickly jump forward to a previously selected menu item when you have previously used the "Back" function.

Table 1: Menu section: Functions in the context menu

■ Notes on Saving the Configuration Profile

- To copy changed settings to the volatile memory, click the "Set" button.
- To update the display in the dialogs, click the "Load" button.
- To keep the changed settings even after restarting the device, open the `Basic Settings:Load/Save` dialog and click the "Set" button in the "Save" frame.

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

1 Basic Settings

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

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

Note: The graphical user interface uses Java 7.

Install the Software from www.java.com.

1.1 System

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

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

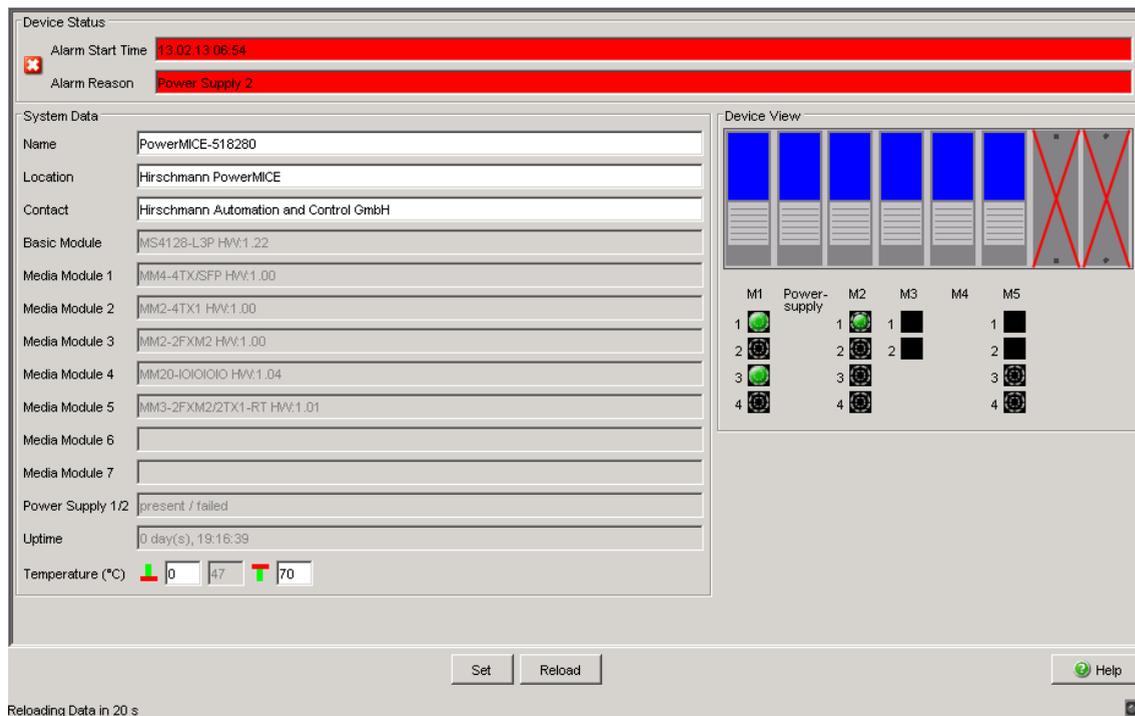


Figure 3: "System" Submenu

■ Device Status

This section of the graphical user interface provides information on the device status and the alarm states the device has detected.

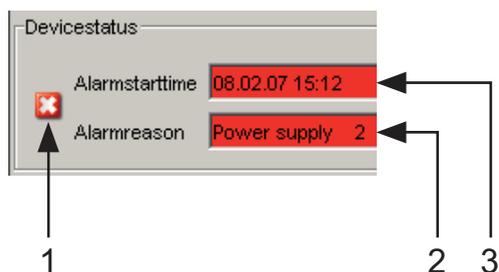


Figure 4: Device status and alarm display

- 1 - The symbol displays the device state
- 2 - Cause of the oldest existing alarm
- 3 - Start of the oldest existing alarm

■ System Data

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

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

Name	Meaning
Name	System name of this device If you use the PROFINET function of the device, the system name can only contain alphanumeric characters, hyphens, and periods.
Location	Location of this device
Contact	The contact for this device
Basic module	Hardware version of the device
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 module 5
Media module 6	Hardware version of media module 6
Media module 7	Hardware version of media module 7
Power supply (P1/P2)	Status of power units (P1/P2)

Table 2: System Data

Name	Meaning
Uptime	Shows the time that has elapsed since this device was last restarted.
Temperature (°C)	Temperature of the device. Lower/upper temperature threshold values. If the temperature goes outside this range, the device generates an alarm.

Table 2: System Data

■ Device View

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

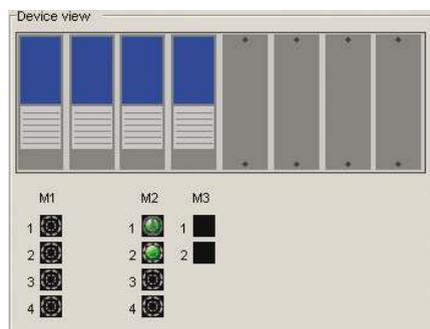


Figure 5: Device View

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 (100 MBit/s) is in the discarding mode of a redundancy protocol such as Spanning Tree or HIPER-Ring.
-  The port is in routing mode (100 Mbit/s).

■ Reloading

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

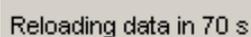


Figure 6: Time to next Reload

■ Buttons

Button	Meaning
Set	Transfers the changes to the volatile memory (RAM) of the device. To permanently save the changes, open the <code>Basic Settings:Load/Save</code> dialog, select the location to save the configuration, and click "Save".
Reload	Updates the fields with the values that are saved in the volatile memory (RAM) of the device.
Help	Opens the online help.

Table 3: Buttons

1.2 Modules (MS, PowerMICE, MACH102 and MACH4000)

When you plug a module in an empty slot of a modular device, the device configures the module with the port default settings. With the port default settings loaded on the module, access to the network is possible. Deny network access to modules by disabling the module slot. The device recognizes the module and port configuration is possible but, the ports remains in the disabled state.

Use the following work steps when deinstalling a module helps deny network access using an empty slot.

- Remove module and update the graphical user interface by clicking "Reload".
- The "Module Status" column for the removed module contains the value `configurable`. The device also grays out the removed module in the "Device View" frame of the `Basic Settings:System` dialog.
- Highlight the entry and click "Remove Module". The value in the "Module Status" column changes to `remove` and the slot is empty in the "Device View" frame in the `Basic Settings:System` dialog. Additionally, the "Type" column for this entry contains the value `none` and the device deletes the other module parameters.
- The selected "Enable" control box indicates that the slot is active. Disable the entry to deny further network access through the unused slot. Deactivating the control box disables the entry. After disabling an entry in this table, the device places a red „X“ over the slot in the "Device View" frame of the `Basic Settings:System` dialog.

Use the following work steps when installing a module in the slot.

- Place the module in the slot and update the graphical user interface by clicking "Reload". The device automatically configures the module with the default settings, detects the module parameters, and enters the values in the table.
- The "Status" value of the module changes to `physical`.
- You allow access to the network through the module by selecting the "Enable" control box.

- ▶ The "Serial Number" column list the serial number of the module.
- ▶ The "Status" column contains the status of the slot.
 - `physical` - indicates that a module is present in the slot.
 - `configurable` - indicates that the slot is empty and available for configuration.
 - `remove` - indicates that the slot is empty.

■ Buttons

Button	Meaning
Set	Transfers the changes to the volatile memory (RAM) of the device. To permanently save the changes, open the <code>Basic Settings:Load/Save</code> dialog, select the location to save the configuration, and click "Save".
Reload	Updates the fields with the values that are saved in the volatile memory (RAM) of the device.
Remove Module	Removes the module configuration from the device when the slot is empty.
Help	Opens the online help.

Table 4: Buttons

1.3 Network

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

Figure 8: Network parameters dialog

- Under “Mode”, you enter where the device gets its IP parameters:
 - ▶ In the BOOTP mode, the configuration is via a BOOTP or DHCP server on the basis of the MAC address of the device (see on page 40 “Load/Save”).
 - ▶ In the DHCP mode, the configuration is via a DHCP server on the basis of the MAC address or the name of the device (see on page 40 “Load/Save”).
 - ▶ 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 `Basic Settings:System` dialog of the graphical user interface.

- The “VLAN” frame enables you to assign a VLAN to the management CPU of the device. If you enter 0 here as the VLAN ID (not included in the VLAN standard version), the management CPU will then be accessible from all VLANs.
- The HiDiscovery protocol allows you to allocate an IP address to the device. Activate the HiDiscovery protocol if you want to allocate an IP address to the device from your PC with the enclosed HiDiscovery software (default setting: operation “on”, access “read-write”).

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

■ Buttons

Button	Meaning
Set	Transfers the changes to the volatile memory (RAM) of the device. To permanently save the changes, open the <code>Basic Settings:Load/Save</code> dialog, select the location to save the configuration, and click "Save".
Reload	Updates the fields with the values that are saved in the volatile memory (RAM) of the device.
Help	Opens the online help.

Table 5: Buttons

1.4 Software

The software dialog enables you to display the software versions in the device and to carry out a software update of the device via file selection, tftp or AutoConfiguration Adapter (ACA).

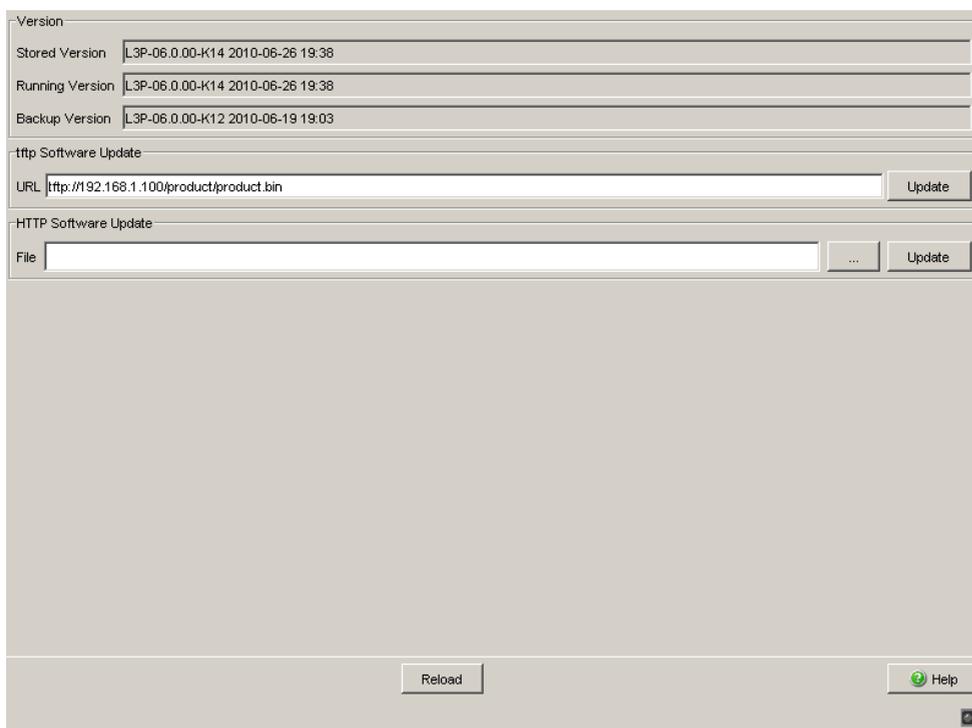


Figure 9: Software Dialog

1.4.1 View the software versions present on the device

The dialog shows the existing software versions:

- ▶ Stored Version:
The version of the software stored in the flash memory.
- ▶ Running Version:
The version of the software currently running.

1.4.2 Restoring the Backup Version

“Restore” replaces the software version stored with the backup version of the software. The relevant configuration files are replaced at the same time. A cold start is required to make the software versions effective. A warm start has no effect whatsoever.

- Once successfully replaced, activate the restored software:
Select the `Basic settings: Restart` dialog and perform a cold start. In a cold start, the device reloads the software from the non-volatile memory, restarts, and performs a self-test.
- Reload the graphical user interface in your browser to re-access the device after restarting.

1.4.3 TFTP Software Update

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

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

tftp://IP address of the tftp server/path name/file name
(e.g. tftp://192.168.1.1/device/device.bin).

- Select the “Firmware“ radio button.
- Enter the URL for the software location.
- To load the software from the tftp server to the device, click "Update".
- To start the new software after loading, cold start the device.

[See “Restart” on page 55.](#)

1.4.4 TFTP Bootcode Update

For a tftp update you need a tftp server to store the required bootcode. The URL identifies the path to the bootcode stored on the tftp server. The URL is in the format

tftp://IP address of the tftp server/path name/file name
(for example: tftp://192.168.1.1/device/device_bootrom.bin).

Note: If an interrupt occurs during a Bootcode update, the device is unrecoverable. Perform this update under the supervision of the Hirschmann support desk.

- Select the “Bootcode“ radio button.
- Enter the URL for the bootcode location.
- To load the bootcode from the tftp server to the device, click "Update".
- To start the new bootcode after loading, cold start the device.

[See “Restart” on page 55.](#)

1.4.5 HTTP Software Update

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

- Click on "..." in the "Software Update" frame.
- In the "Open" dialog select the device software image file with the suffix *.bin.
- Click on "Open".
- Click on "Update" to transfer the software to the device.
When the file is completely transferred, the device starts updating the device software. If the update was successful, the device displays the message "Successfully firmware update ...".

1.4.6 Automatic software update by ACA

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

■ Buttons

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

Table 6: Buttons

1.5 Port Configuration

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

- ▶ The column "Port" shows the number of the device port to which the table entry relates.
- ▶ In the "Port Name" column, you can enter a name for every port.
- ▶ In the "Port on" column, you can switch on the port by selecting it here.
- ▶ In the "Propagate connection error" column, you can specify that a link alarm will be forwarded to the device status and/or the the signal contact is to be opened.
- ▶ In the "Automatic Configuration" column, you can activate the automatic selection of the the operating mode (Autonegotiation) and the automatic assigning of the connections (Auto cable crossing) of a TP port by selecting the appropriate field. After the autonegotiation has been switched on, it takes a few seconds for the operating mode to be set.
- ▶ In the "Manual Configuration" column, you can set the operating mode for this port. The choice of operating modes depends on the media module. The possible operating modes are:
 - 10 Mbit/s half duplex (HDX)
 - 10 Mbit/s full duplex (FDX)
 - 100 Mbit/s half duplex (HDX)
 - 100 Mbit/s full duplex (FDX)
 - 1000 Mbit/s half duplex (HDX)
 - 1000 Mbit/s full duplex (FDX)
 - 10 Gbit/s full duplex (FDX)
- ▶ The "Link/Current Settings" column displays the current operating mode and thereby also an existing connection.

- ▶ In the “Manual Cable Crossing (Auto. Conf. off)” column, you assign the connections of a TP port, if “Automatic Configuration” is deactivated for this port. The possible settings are:
 - enable: the device does not swap the send and receive line pairs of the TP cable for this port (MDI).
 - disable: the device swaps the send and receive line pairs of the TP cable for this port (MDIX).
 - unsupported: the port does not support this function (optical port, TP SFP port).
- ▶ In the “Flow Control” column, you checkmark this port to specify that flow control is active here. You also activate the global “Flow Control” switch ([see on page 110 “Switching Global”](#)).

Note: The device supports gigabit interfaces on copper ports with auto negotiation enabled.

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

Note: When you are using a redundancy function, you deactivate the flow control on the participating device ports. If the flow control and the redundancy function are active at the same time, there is a risk that the redundancy function will not operate as intended.

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

Port type	Bit rate	Autonegotiation (automatic configuration)	Port setting	Duplex
TX	100 Mbit/s	off	on	full
TX	1 Gbit/s	on	on	-

Table 7: Port settings for ring ports

Port type	Bit rate	Autonegotiation (automatic configuration)	Port setting	Duplex
Optical	100 Mbit/s	off	on	full
Optical	1 Gbit/s	on	on	-

Table 7: 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.

■ Buttons

Button	Meaning
Set	Transfers the changes to the volatile memory (RAM) of the device. To permanently save the changes, open the <code>Basic Settings:Load/Save</code> dialog, select the location to save the configuration, and click "Save".
Reload	Updates the fields with the values that are saved in the volatile memory (RAM) of the device.
Help	Opens the online help.

Table 8: Buttons

1.6 Power over ETHERNET

Note: The following devices are equipped with Power over Ethernet (PoE) ports:

- ▶ RS20/30
- ▶ MS20/30
- ▶ PowerMICE
- ▶ OCTOPUS

You will learn in this section how these devices operate.

Devices with Power over ETHERNET (PoE) media modules or PoE ports enable you to supply current to terminal devices such as IP phones via the twisted-pair cable. PoE media modules and PoE ports support Power over ETHERNET in accordance with IEEE 802.3af.

The Power over ETHERNET function is globally active and the PoE-capable ports are active on delivery.

Nominal power for MS20/30, MACH 1000 and PowerMICE:

The device provides the nominal power for the sum of all PoE ports plus a surplus. Because the PoE media module gets its PoE voltage externally, the device does not know the possible nominal power.

The device therefore assumes a “nominal power” of 60 Watt per PoE media module for now.

Nominal power for OCTOPUS 8M-PoE and OCTOPUS 24M-8PoE:

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.

Frame "Operation":

- With "On/Off" you turn the PoE on or off.

Frame "Configuration":

- 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 on at least one port.
- Enter the power threshold in "Threshold". When the device exceeds or is below this value, the device will send a trap, provided that you enable the "Send Trap" function. For the power threshold you enter the power yielded as a percentage of the nominal power.
- "Budget [W]" displays the power that the device nominally provides to the PoE ports.
- "Reserved [W]" displays the maximum power that the device provides to the connected PoE devices on the basis of their classification.
- "Delivered [W]" shows how large the current power requirement is on the PoE ports.

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

Port Table:

The table only shows ports that support PoE.

- In the "POE enable" column, you can enable/disable PoE on this port.
- The "Status" column indicates the PoE status of the port.
- The "Class" column indicates the class of the connected device:
 - Class: Maximum delivered power
 - 0: 15.4 W = As-delivered state
 - 1: 4.0 W
 - 2: 7.0 W
 - 3: 15.4 W
 - 4: reserved, treated as Class 0
- The column „Consumption [W]“ displays the current power delivered at the respective port.
- The "Name" column indicates the name of the port, see `Basic settings:Port configuration`.

Port	PoE enable	Status	Priority	Class	Consumption [W]	Name
1.5	<input checked="" type="checkbox"/>	disabled	low	-	0.0	
1.6	<input checked="" type="checkbox"/>	disabled	low	-	0.0	
1.7	<input checked="" type="checkbox"/>	disabled	low	-	0.0	
1.8	<input checked="" type="checkbox"/>	disabled	low	-	0.0	

Figure 10: Power over Ethernet dialog

■ Buttons

Button	Meaning
Set	Transfers the changes to the volatile memory (RAM) of the device. To permanently save the changes, open the <code>Basic Settings:Load/Save</code> dialog, select the location to save the configuration, and click "Save".
Reload	Updates the fields with the values that are saved in the volatile memory (RAM) of the device.
Help	Opens the online help.

Table 9: Buttons

1.7 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.

The screenshot shows a configuration dialog box with the following sections:

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

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

Figure 11: Load/Save dialog

1.7.1 Loading a Configuration

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

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

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

■ Loading configuration of the offline configurator

Installing and starting the offline configurator

To create a configuration file in the offline configurator, proceed as follows:

- If you have not installed the offline configurator on your PC yet: Install the offline configurator by running the "Setup.exe" installation file from the "ocf_setup" folder included on the CD-ROM.
- Start the offline configurator by double-clicking the “Offline Management” desktop symbol.

Creating an XML configuration file with the offline configurator

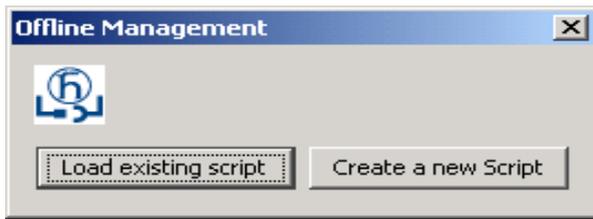


Figure 12: Offline Management selection

- ▶ Revising an existing script
 - Click on "Load existing script" to load a previously created script for revision in the offline configurator.
- ▶ Creating a new script
 - Click on "Create a new script" to create a new script with the aid of the offline configurator.
 - Then in the "Product Selection" list select the product that you want to create the script for.

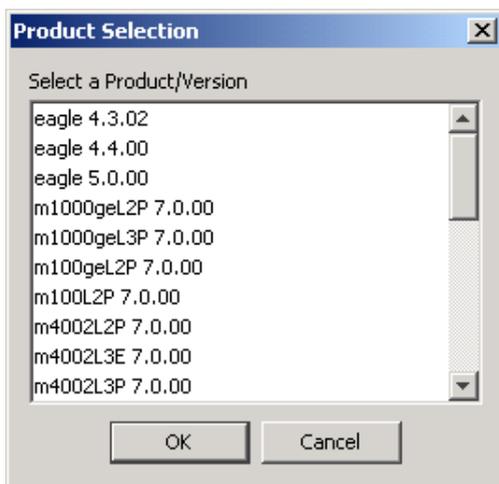


Figure 13: Creating New Script Dialog - Product Selection

- In the offline configurator interface, set the desired parameters appropriate to your requirements.

Note: The offline configurator interface contains only dialogs, tables and input fields for parameters writable to the device. You cannot read parameters from the device in the offline mode. The range of the offline configurator interface is reduced vis-à-vis that of the graphical user interface.

You can find a description of the settings you can make in the offline configurator interface in the respectively appropriate section of this manual.

► Example: Basic Settings Dialog - System

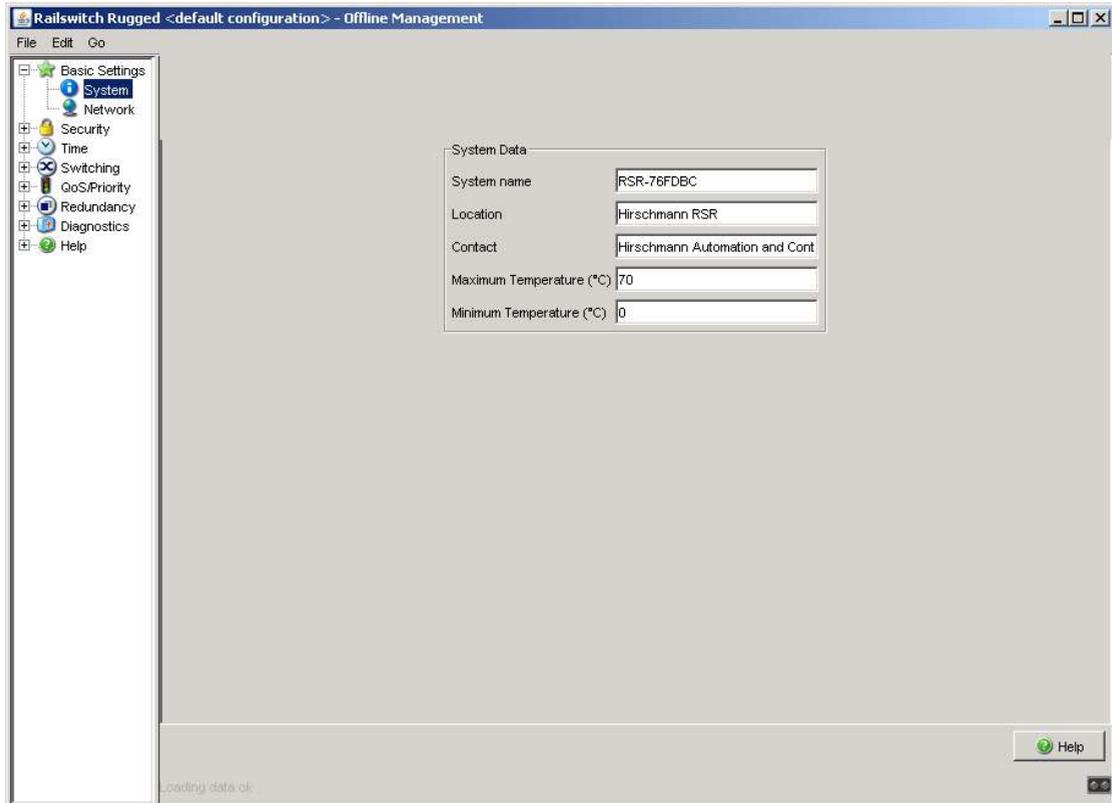


Figure 14: Basic Settings Dialog: System in the Offline Configurator

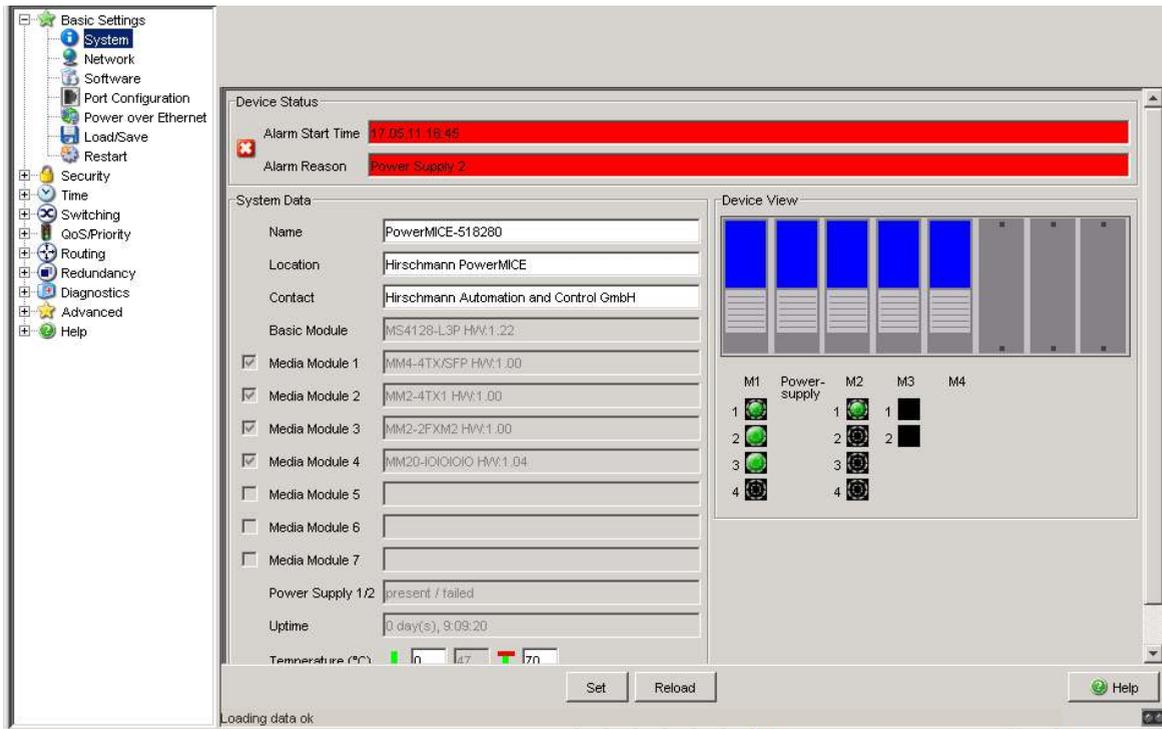


Figure 15: Basic Settings Dialog: System in the Graphical User Interface

The following applies to the above example: You can find a description of the parameters that can be set in the offline configurator `Basic Settings: System` dialog.

See “System” on page 20.

- Once you have set the desired parameters appropriate to your requirements in the offline configurator interface, save the configuration:

- ▶ File - Save as or
- ▶ File - Save

- Quit the offline configurator with File - Quit.

Loading an XML configuration file onto the device

- In the graphical user interface, select the `Basic Settings: Load/Save` menu item.

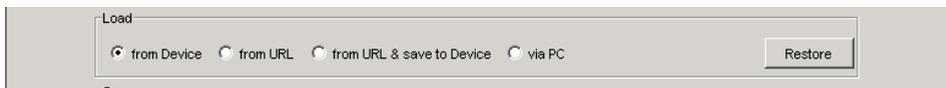


Figure 16: Loading the Configuration Dialog - Via PC

- To load a configuration saved on the PC with the offline configurator in XML format, check the "via PC" field in the "Load" frame with a click of the mouse and click on "Restore".
- Select the desired path in the "Open" window, from which the device is to load your configuration file. Specify in the "File Name" field the name of the desired file, including the .ocf (offline configurator) extension.

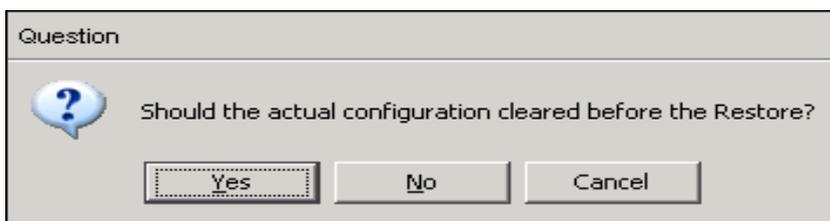


Figure 17: Query - Resetting Configuration

- To reset the current configuration on your device before loading the offline configuration file, click on "Yes".
- To retain the current configuration on your device before loading the offline configuration file and then to overwrite it with the contents of the offline configuration file, click on "No".

Once the offline configuration file has loaded successfully, the device returns in the subsequent "Configuration" window an overview of the configuration parameters that have loaded. By clicking in this window you can choose between the following two views:

- ▶ Tables View
- ▶ Text View

Tables View

Name	Index	Value	SNMP Error
sysContact	0	"4869727363686D616E6E204175746...	noError (0)
sysName	0	"506F7765724D4943452D353138323...	noError (0)
sysLocation	0	"4869727363686D616E6E20506F776...	noError (0)
hmTempUpLimit	0	"70"	noError (0)
hmTempLwrLimit	0	"0"	noError (0)
hmNetLocalIPAddr	0	"10.0.1.112"	noError (0)
hmNetGatewayIPAddr	0	"10.0.1.1"	noError (0)
hmNetMask	0	"255.255.255.0"	noError (0)
hmNetPPPOBaseIPAddr	0	"0.0.0.0"	noError (0)
hmNetPPPONetMask	0	"0.0.0.0"	noError (0)
hmNetVlanID	0	"1"	noError (0)
hmNetVlanPriority	0	"0"	noError (0)
hmNetIpDscpPriority	0	"0"	noError (0)
hmSysChassisName	0	"43686173736973353138323830"	noError (0)
hmSysStoFEnable	n	"1"	noError (0)

Figure 18: Information - Configuration - Tables View

In the Tables View you get an overview in tabular format of the configuration parameters that have loaded:

Parameters	Meaning	Possible values
Application date	Point in time (date and time of day) when you loaded the offline configuration file onto the device. Notation: yyyy-mm-dd hh-mm-ss	yyyy = valid year mm = 1 to 12 dd = 1 to 31 hh = 0 to 23 mm = 0 to 59 ss = 0 to 59
Name	Name of the configuration parameter (MIB variable)	see MIB
Index	Index of the configuration parameter (MIB variable)	see MIB

Table 10: Information - Configuration - Tables View

Parameters	Meaning	Possible values
Value	Value of the configuration parameter (MIB variable), which was set by loading the offline configuration file.	see MIB
SNMP error	The device's success at loading the respective configuration parameter	<ul style="list-style-type: none"> ▶ (0) = Success ▶ (1) = Response PDU Too Big ▶ (2) = Variable does not exist ▶ (3) = Cannot modify variable: Bad Value ▶ (4) = Cannot modify object, Read Only ▶ (5) = Cannot perform operation, General Error

Table 10: Information - Configuration - Tables View

Text View

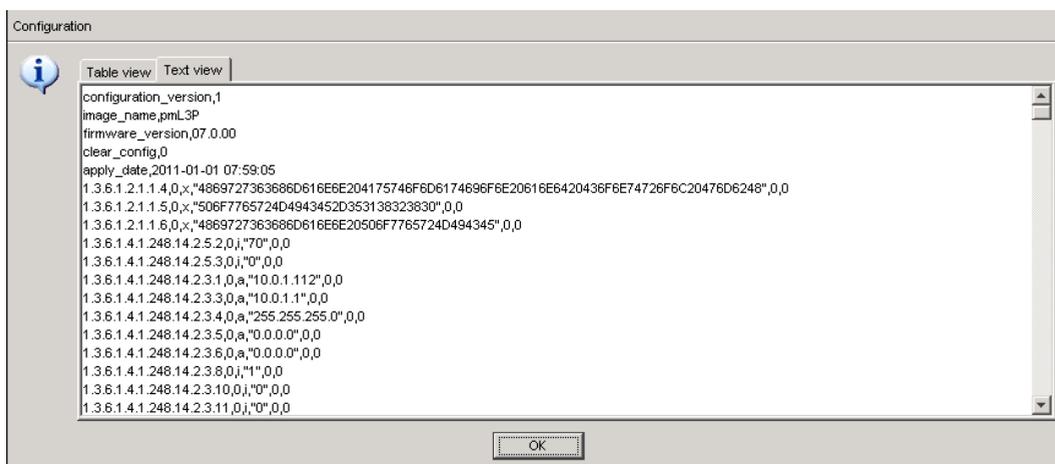


Figure 19: Information - Configuration - Text View

In the Text View you get an overview in textual format of the configuration parameters (MIB variables) that have loaded:

The device lists the individual configuration parameters in the following form. The data are separated by commas:

- ▶ Position in the MIB, e.g. 1.3.6.1.2.1.1.4
- ▶ Index
- ▶ Value
- ▶ SNMP error (see [table 10](#), "SNMP Error" parameter)
- ▶ The last parameter has the value of 0. It is included for future expansions.

1.7.2 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,
- ▶ save the current configuration for the offline configurator on the PC in XML format.

Note: For script configuration files, note the following characteristics:

- ▶ If you save the configuration in a binary file, the device saves all configuration settings in a binary file.
In contrast to this, the device only saves those configuration settings that deviate from the default setting when saving to a script file.
- ▶ When you load a configuration from a script file, delete the configuration on the device first so that the script that is being loaded overwrites the configuration default settings correctly.
If a configuration already exists on the device, the result is the loading of a script file in a configuration involving the union of the settings which differ from the default setting in the existing configuration or in the script file. If you use this feature, remember that loading a script sets configuration settings only to values that differ from the default setting.
- ▶ To delete the configuration on a device, select “Current configuration” in the “Delete” frame and click on “Delete configuration”. The device immediately deletes its current configuration from the volatile memory ([see on page 51 “Deleting a configuration”](#)). The configuration in the non-volatile memory is kept, along with the IP address. Thus the device remains reachable.

Note: The loading process started by DHCP/BOOTP ([see on page 27 “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, finish the loading process by loading the local configuration from the device in the “Load” frame.

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

After you have successfully saved the configuration on the device, the device sends a trap `hmConfigurationSavedTrap` together with the information about the AutoConfiguration Adapter (ACA), if one is connected. When you change the configuration for the first time after saving it, the device sends a trap `hmConfigurationChangedTrap`.

■ Saving configuration for the offline configurator

- In the graphical user interface, select the `Basic Settings:Load/Save` menu item.



Figure 20: Saving Configuration Dialog - On the PC (ocf)

- To save the current configuration for the offline configurator as an XML configuration file on the PC, check with a click of the mouse the "on the PC (ocf)" field in the "Save" frame and click on the "Save" button.
- Select the desired path in the "Save" window, on which the device is to save your configuration file. Specify the desired name in the "File name" field. The device saves your configuration in a file with the .ocf (offline configurator) extension.

■ Configuration Signature

A configuration signature as seen in the "Configuration Signature" frame of the `Basic Settings:Load/Save` dialog, uniquely identifies a particular configuration. Every time you save a configuration to the device, the device generates a random sequence of numbers and/or letters as a signature for the configuration. The signature changes every time you save the configuration to the device. The device stores the randomly generated signature with the configuration to assure the device loads appropriate configuration after a reboot.

1.7.3 URL

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

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

1.7.4 Deleting a configuration

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

- ▶ Reset the current configuration to the default settings. The configuration saved on the device is retained.
- ▶ Reset the device to the default settings. In this case, the device deletes its configuration in the volatile memory as well as in the non-volatile memory. This includes the IP address. The device will be reachable again over the network after it has obtained a new IP address, for example, via DHCP or the V.24 interface.

Note: With the exception of the watchdog configuration, the device stores user defined configurations in Non-volatile Memory. The device stores the watchdog configuration separately. Therefore, when you reset the configurations to the default settings, using the "Current Configuration" or "Current Configuration from the Device" delete functions, the watchdog configuration remains in the device.

1.7.5 Using the AutoConfiguration Adapter (ACA)

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

Note: When replacing a device with DIP switches, check the DIP switch settings to ensure that they are the same.

■ **Storing the current configuration data in the ACA:**

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

■ **Loading the Configuration file from the ACA:**

When you restart the device with ACA connected, the device adopts the configuration data from ACA and saves it permanently in the flash memory. If the connected ACA contains invalid data, for example, if the ACA contains an unchanged default configuration, the device loads the data from the flash memory.

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

The device loads the configuration data if

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

Status	Meaning
notPresent	No ACA present
ok	The configuration data from the ACA and the device match.
removed	The ACA was removed after booting.
notInSync	- The configuration data of the ACA and the device do not match, or only one file exists ^a , or - no configuration file is present on the ACA or on the device ^b .
outOfMemory	The local configuration data is too extensive to be stored on the ACA.

Table 11: *ACAstatus*

Status	Meaning
wrongMachine	The configuration data in external memory originates from a different device type and cannot be read or converted.
checksumErr	The configuration data is damaged.

Table 11: ACAstatus

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

1.7.6 Cancelling 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 you will then be reconnected if an incorrect configuration interrupts your connection to the device.
- Enter the “Period to undo while the connection is lost [s]” in seconds.
Possible values: 10-600 seconds.
Default setting: 600 seconds.

Note: Deactivate the function after you have successfully saved the configuration. In this way you help prevent the device from reloading the configuration after you close the web interface.

Note: When accessing the device via SSH, also note the TCP connection timeouts for the cancellation of the configuration.

■ 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.

■ Buttons

Button	Meaning
Set	Transfers the changes to the volatile memory (RAM) of the device. To permanently save the changes, open the <code>Basic Settings:Load/Save</code> dialog, select the location to save the configuration, and click "Save".
Reload	Updates the fields with the values that are saved in the volatile memory (RAM) of the device.
Help	Opens the online help.

Table 12: Buttons

1.8 Restart

This dialog provides you with the following functions:

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

Note: During the restart, the device temporarily does not transfer any data, and it cannot be accessed via the graphical user interface or other management systems such as Industrial HiVision.



Figure 21: Restart Dialog

■ Buttons

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

Table 13: Buttons

2 Security

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

- ▶ Password/SNMPv3 access
- ▶ SNMPv1/v2 access
- ▶ Telnet/Web access
- ▶ Port security
- ▶ RADIUS
- ▶ Login Banner

2.1 Password / SNMPv3 access

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

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

The graphical user interface and the command line interface (CLI) use the same passwords as SNMPv3 for the users “admin” and “user”.

Note: Passwords are case-sensitive.

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

- The device allows you to set the “Accept only encrypted requests” function differently for the access with the read password and with the read/write password.
- When logging in, the graphical user interface queries the current setting of the device and sends encrypted queries if the device requests this.

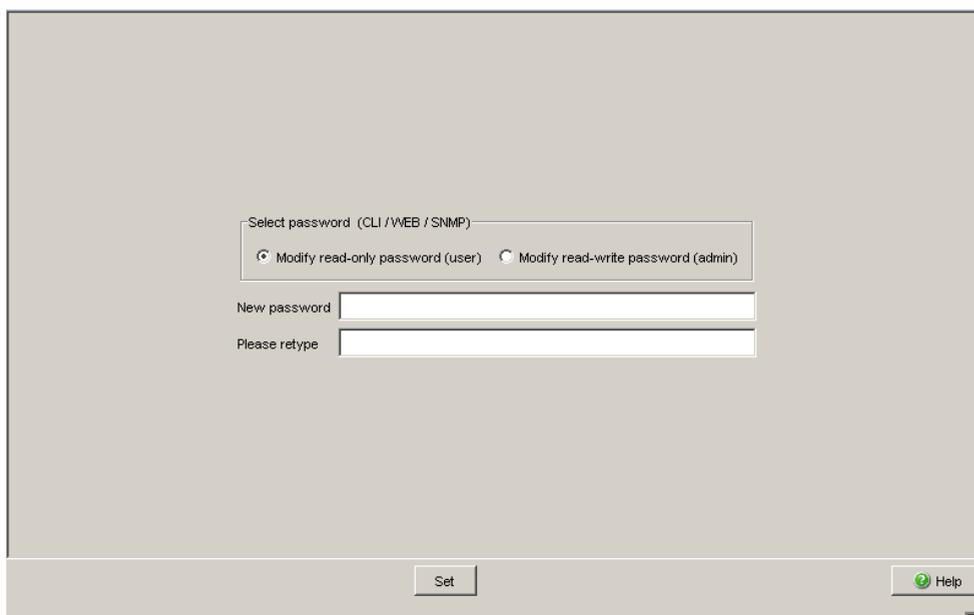


Figure 22: Dialog Password/SNMP Access

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

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

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

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

You can block access via a Web browser or Telnet client in a separate dialog. See [“Telnet/Web Access”](#) on page 64.

Access at IP address level is restricted in a separate dialog. See [“SNMPv1/v2 Access Settings”](#) on page 61.

■ Buttons

Button	Meaning
Set	Transfers the changes to the volatile memory (RAM) of the device. To permanently save the changes, open the <code>Basic Settings:Load/Save</code> dialog, select the location to save the configuration, and click "Save".
Reload	Updates the fields with the values that are saved in the volatile memory (RAM) of the device.
Help	Opens the online help.

Table 14: Buttons

2.2 SNMPv1/v2 Access Settings

With this dialog you can select access via SNMPv1 or SNMPv2. In the default setting, both protocols are activated.

You can thus manage the device with Industrial HiVision and communicate with earlier versions of SNMP.

Note: To be able to read and/or change the data in this dialog, log in to the graphical user interface with the user name `admin` and the relevant password.

- ▶ In the "Index" column, the device shows the sequential number.
- ▶ In the "Community Name" column, you enter the password with which a management station may access the device via SNMPv1/v2 from the specified address range.

Note: Passwords are case-sensitive.

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

Example:

255.255.255.255: a single IP address

255.255.255.240 with IP address = 172.168.23.20:

the IP addresses 172.168.23.16 to 172.168.23.31.

Binary notation of the mask 255.255.255.240:

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

Binary notation of the IP address 172.168.23.20:

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

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

```
1010 1100 1010 1000 0001 0111 0001 0000 bis
1010 1100 1010 1000 0001 0111 0001 1111
i.e.: 172.168.23.16 to 172.168.23.31
```

- ▶ In the "Access Mode" column, you specify whether this computer can access the device with the read password (access mode `readOnly`) or with the read/write password (access mode `readWrite`).
See ["Password / SNMPv3 access" on page 58](#).

Note: The password for the `readOnly` access mode is the same as the SNMPv3 password for read access.

The password for the `readWrite` access mode is the same as the SNMPv3 password for read/write access.

If you are changing one of the passwords, manually set the corresponding password for SNMPv3 to the same value. Alternatively mark the "Synchronize community to v3 password" checkbox in the "Configuration" frame. This way you ensure that you can also access with the same password via SNMPv3.

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

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

- ▶ With "Create" you create a new row in the table.
- ▶ With "Remove" you delete selected rows in the table.

The screenshot shows the 'SNMPv1/v2 Access Dialog' with a configuration section and a table of community names.

Configuration:

- SNMPv1 enabled
- SNMPv2 enabled
- Synchronize community to v3 password

Index	Community Name	IP Address	IP Mask	Access Mode	Active
0	public	0.0.0.0	0.0.0.0	readOnly	<input checked="" type="checkbox"/>
1	private	0.0.0.0	0.0.0.0	readWrite	<input checked="" type="checkbox"/>

Buttons at the bottom: Set, Reload, Create, Remove, Help.

Figure 23: SNMPv1/v2 Access Dialog

■ Buttons

Button	Meaning
Set	Transfers the changes to the volatile memory (RAM) of the device. To permanently save the changes, open the <code>Basic Settings:Load/Save</code> dialog, select the location to save the configuration, and click "Save".
Reload	Updates the fields with the values that are saved in the volatile memory (RAM) of the device.
Create	Adds a new table entry.
Remove	Removes the selected table entry.
Help	Opens the online help.

Table 15: Buttons

2.3 Telnet/Web Access

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

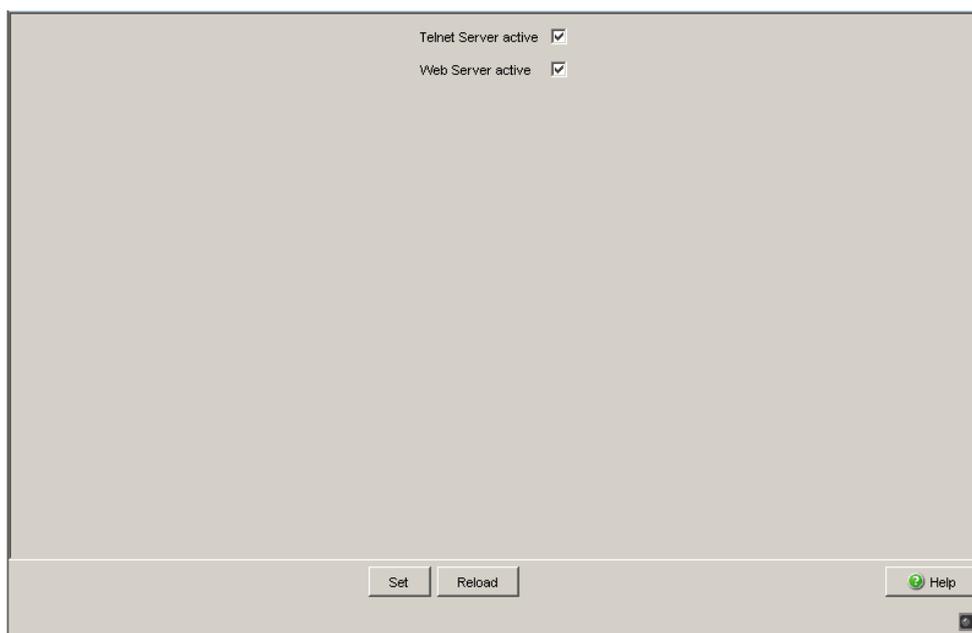


Figure 24: Telnet/Web Access dialog

Parameters	Meaning	Possible values	Default setting
Telnet server active	Activates or deactivates the Telnet service (Telnet access) for this device.	On Off	On
Web server (HTTP) active	Activates or deactivates the http service (Web server) for this device.	On Off	On

Table 16: Telnet/Web Access

2.3.1 Description of Telnet Access

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

The server is activated in its default setting.

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 retained.

Note: The Command Line Interface (out-of-band) and the `Security:Telnet/Web/SSH Access` dialog in the graphical user interface allows you to reactivate the Telnet server.

2.3.2 Description of Web Access (http)

The device's Web server allows you to configure the device by using the graphical user interface. You can deactivate the Web server to prevent Web access to the device.

The server is activated in its default setting.

After you switch the http Web server off, it is no longer possible to log in via a http Web browser. The http session in the open browser window remains active.

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

■ Buttons

Button	Meaning
Set	Transfers the changes to the volatile memory (RAM) of the device. To permanently save the changes, open the <code>Basic Settings:Load/Save</code> dialog, select the location to save the configuration, and click "Save".
Reload	Updates the fields with the values that are saved in the volatile memory (RAM) of the device.
Help	Opens the online help.

Table 17: Buttons

2.4 Port Security

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

If the device receives data packets at a port from an undesired sender, it performs the action defined for the port, e.g. send trap, disable port or auto-disable.

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

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

Table 18: Configuration of port security globally for all ports

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

With MAC-based port security, the device allows you either to define the permitted MAC addresses specifically or record the MAC addresses automatically.

With automatic recording, the device “learns” the MAC addresses of the sender by evaluating the received data packets. When the user-defined upper limit has been reached, the device performs the specified action.

Compared with the specific definition of MAC addresses, the automatic recording gives you the advantage of being able to replace the connected terminal devices at any time without having to modify the MAC address list in the device.

Name	Meaning
Port	Port identification using module and port numbers of the device, e.g. 2.1 for port one of module two.
Port Status	<p>enabled: Port is switched on and transmitting. disabled: Port is switched off and not transmitting.</p> <p>The port is switched on if</p> <ul style="list-style-type: none"> - an authorized address accesses the port <p>or</p> <ul style="list-style-type: none"> - an unauthorized address attempts to access the port and <code>trapOnly</code> or <code>none</code> is selected under "Action". <p>The port is switched off if</p> <ul style="list-style-type: none"> - an unauthorized address attempts to access the port and <code>portDisable</code> is selected under "Action".
Allowed MAC Addresses	<p>MAC addresses of the devices with which you allow data exchange on this port.</p> <p>The graphical user interface allows you to enter up to 50 MAC addresses, each separated by a space. After each MAC address you can enter a slash followed by a number identifying an address area. This number, between 2 and 47, indicates the number of relevant bits. Example:</p> <p>00:80:63:01:02:00/40 stands for 00:80:63:01:02:00 to 00:80:63:01:02:FF</p> <p>or</p> <p>00:80:63:00:00:00/24 stands for 00:80:63:00:00:00 to 00:80:63:FF:FF:FF</p> <p>If there is no entry, any number of devices can communicate via this port.</p>
Current MAC Address	Shows the MAC address of the device from which the port last received data. The graphical user interface allows you to copy an entry from the "Current MAC Address" column into the "Allowed MAC Addresses" column by dragging and dropping with the mouse button.
Allowed IP Addresses	<p>IP addresses of the devices with which you allow data exchange on this port.</p> <p>The graphical user interface allows you to enter up to 10 IP addresses, each separated by a space.</p> <p>If there is no entry, any number of devices can communicate via this port.</p>
Dynamic Limit	<p>Specifies the upper limit for the number of automatically recorded senders. When the upper limit is reached, the device performs the action defined in the "Action" column.</p> <p>Possible values:</p> <ul style="list-style-type: none"> ▶ 0 or – (default setting: –) Deactivates the automatic recording of the senders on this port. ▶ 1 . . 50 Upper limit for the automatic recording of senders. Adjust the value to the number of expected senders. In this way you make MAC flooding attacks more difficult.

Table 19: Configuration of port security for a single port

Name	Meaning
Dynamic Count	Shows how many senders the device has automatically recorded.
Action	<p>Action performed by the device after an unauthorized access.</p> <p>Possible values:</p> <ul style="list-style-type: none"> ▶ <code>none</code> (default setting) No action. ▶ <code>trapOnly</code> Send alarm. ▶ <code>portDisable</code> Disables the port. Then the port LED on the device blinks green 3 times per period. The device re-enables the port when you have defined the following settings in the <code>Diagnostics:Ports:Auto Disable</code> dialog: <ul style="list-style-type: none"> – In the "Configuration" frame, the checkbox for the "Port Security" triggering event is marked. – The reset timer is defined >0 for the port. ▶ <code>autoDisable</code> Disables the port depending on the settings in the <code>Diagnostics:Ports:Auto Disable</code> dialog, "Configuration" frame. <ul style="list-style-type: none"> – The device disables the port when the checkbox for the "Port Security" triggering event is marked. Then the port LED on the device blinks green 3 times per period. The device re-enables the port when the reset timer is defined >0 for the port in the <code>Diagnostics:Ports:Auto Disable</code> dialog for the port. – The port remains enabled when the checkbox for the "Port Security" triggering event is unmarked.

- Note:** Prerequisites for the device to be able to send an alarm (trap):
- You have entered at least one recipient
 - You have selected at least one recipient in the "Active" column
 - In the "Selection" frame, you have selected "Port Security"

Table 19: Configuration of port security for a single port

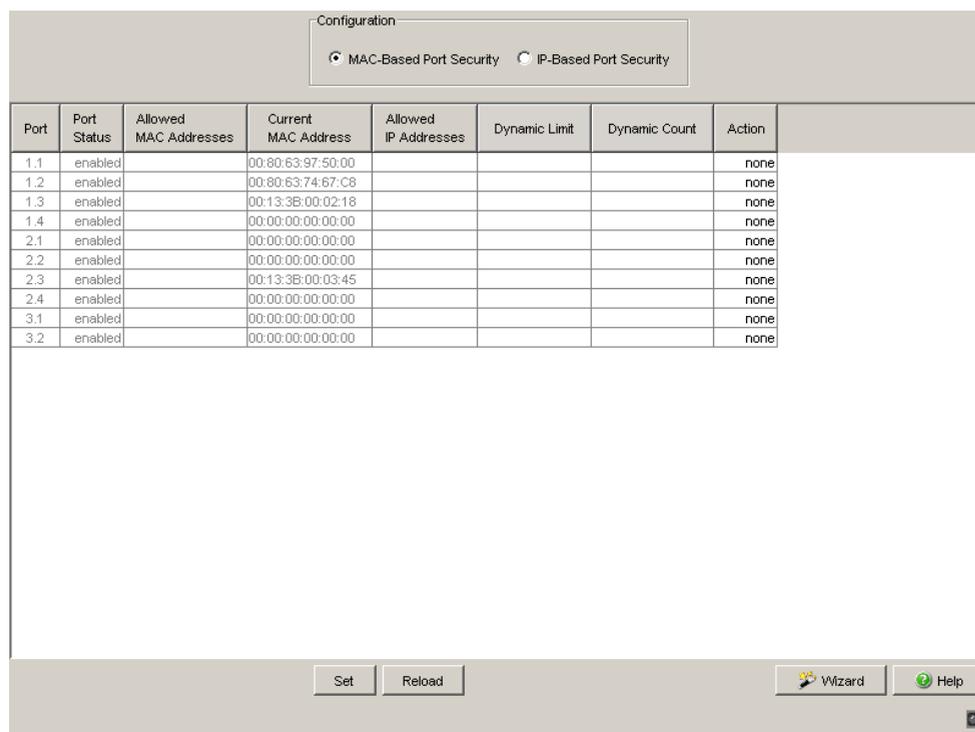


Figure 25: Port Security dialog

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

Prerequisites for the IP-based port security:

- The device with the allowed IP address supports ARP,
- The device is accessible during the configuration of IP port security,
- The MAC address to which the IP address is assigned is unique and remains unchanged after the IP address is entered.

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

If a connected device sends packets with the allowed IP address but a different MAC address, the Switch denies this data traffic. If you replace the device with the allowed IP address with a different one having the same IP address, enter the IP address in the Switch again so that the Switch can learn the new MAC address.

■ Buttons

Button	Meaning
Set	Transfers the changes to the volatile memory (RAM) of the device. To permanently save the changes, open the <code>Basic Settings:Load/Save</code> dialog, select the location to save the configuration, and click "Save".
Reload	Updates the fields with the values that are saved in the volatile memory (RAM) of the device.
Wizard	Opens the "Wizard". With the "Wizard" you assign the permitted MAC addresses to a port.
Help	Opens the online help.

Table 20: Buttons

■ Wizard – Select Port

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

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

Table 21: Wizard in the `Security:Port Security` dialog, "Select Port" page

■ Wizard – Addresses

The "Wizard" helps you to connect the device ports with one or more desired senders. When you have defined the settings, click "Finish". To save the changes afterwards, click `Set` in the "Security:Port Security" dialog.

Parameters	Meaning
Allowed MAC Addresses	<p>Lists the MAC Addresses allowed access to the port.</p> <p>Possible values:</p> <ul style="list-style-type: none"> ▶ Valid Unicast MAC addresses <p>Click "Add" to transfer the MAC address to the "Allowed MAC Addresses" field.</p>
MAC Address	<p>Defines the MAC address allowed access to the port.</p> <p>Possible values:</p> <ul style="list-style-type: none"> ▶ Valid Unicast MAC address <p>Enter the value in one of the following formats:</p> <ul style="list-style-type: none"> – without a separator, e.g. 001122334455 – separated by spaces, e.g. 00 11 22 33 44 55 – separated by colons, e.g. 00:11:22:33:44:55 – separated by hyphens, e.g. 00-11-22-33-44-55 – separated by points, e.g. 00.11.22.33.44.55 – separated by points after every 4th character, e.g. 0011.2233.4455 <p>Click "Add" to transfer the MAC address to the "Allowed MAC Addresses" field.</p>
Mask	<p>Defines number of significant digits in the MAC address range.</p> <p>Possible values:</p> <ul style="list-style-type: none"> ▶ 1..48 <p>Used this field to indicate the significant digits as with CIDR notation. For example, 00:11:22:33:44:00/40 indicates that the port allows devices with a MAC Address matching the first 5 groups of hexadecimal digits to access the network.</p>
Add	Transfers the values specified in the "MAC Address" fields to the "Allowed MAC Addresses" field.
Remove	Removes the entries selected in the "Allowed MAC Addresses" field.

Table 22: Wizard in the *Security:Port Security* dialog, "Addresses" page

■ Wizard – Action

This dialog defines the actions that the device performs in the event of unauthorized access to the port.

Name	Meaning
Action	<p>Action performed by the device after an unauthorized access.</p> <p>Possible values:</p> <ul style="list-style-type: none"> ▶ none (default setting) No action. ▶ trapOnly Send alarm. ▶ portDisable Disables the port. Then the port LED on the device blinks green 3 times per period. The device re-enables the port when you have defined the following settings in the <code>Diagnostics:Ports:Auto Disable</code> dialog: <ul style="list-style-type: none"> – In the "Configuration" frame, the checkbox for the "Port Security" triggering event is marked. – The reset timer is defined >0 for the port. ▶ autoDisable Disables the port depending on the settings in the <code>Diagnostics:Ports:Auto Disable</code> dialog, "Configuration" frame. <ul style="list-style-type: none"> – The device disables the port when the checkbox for the "Port Security" triggering event is marked. Then the port LED on the device blinks green 3 times per period. The device re-enables the port when the reset timer is defined >0 for the port in the <code>Diagnostics:Ports:Auto Disable</code> dialog for the port. – The port remains enabled when the checkbox for the "Port Security" triggering event is unmarked. <p>Note: Prerequisites for the device to be able to send an alarm (trap):</p> <ul style="list-style-type: none"> – You have entered at least one recipient, – You have selected at least one recipient in the "Active" column – In the "Selection" frame, you have selected "Port Security".

Table 23: Wizard in the `Security:Port Security` dialog, "Action" page

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

■ Buttons

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

Table 24: Buttons

2.5 Login/CLI Banner

This dialog allows you to display a greeting or information text to users before they login to the device.

The dialog contains the following tabs:

- ▶ [Login Banner](#)
- ▶ [CLI Banner](#)

2.5.1 Login Banner

This tab allows you to show the users a greeting or information text in the login dialog of the graphical user interface and in the command line interface before the users login.

Users logging in in the command line interface with SSH see the text - regardless of the client used - before or during the login.

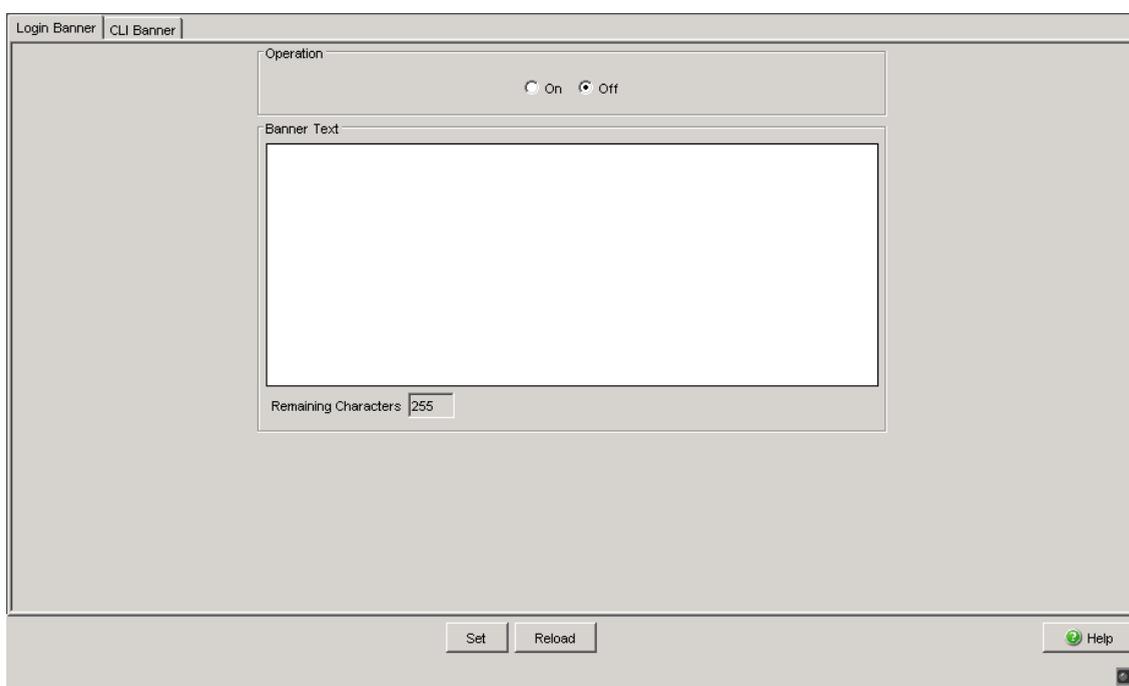


Figure 26: "Login/CLI Banner" dialog, "Login Banner" tab

■ Function

Parameter	Meaning
Operation	<p>When this function is switched on, the device shows the text defined in the "Banner Text" field to the users that login in the login dialog of the graphical user interface or in the command line interface.</p> <p>Possible values:</p> <ul style="list-style-type: none"> ▶ Off (default setting) ▶ On

■ Banner Text

Parameter	Meaning
Banner Text	<p>Specifies the text that the device displays in the login dialog of the graphical user interface and in the command line interface.</p> <p>Possible values:</p> <ul style="list-style-type: none">▶ Alphanumeric ASCII character string with 0..255 characters (0x20..0x7E) including spaces▶ Tab \t▶ Line break \n
Remaining Characters	<p>Shows how many characters are still available in the "Banner Text" field.</p> <p>Possible values:</p> <ul style="list-style-type: none">▶ 255..0

2.5.2 CLI Banner

This tab page allows you to display an individual text only in the command line interface.

In the default setting, the CLI start screen shows information about the device, such as the software version and the device settings. With the function on this tab page, you deactivate this information and replace it with an individually definable text.

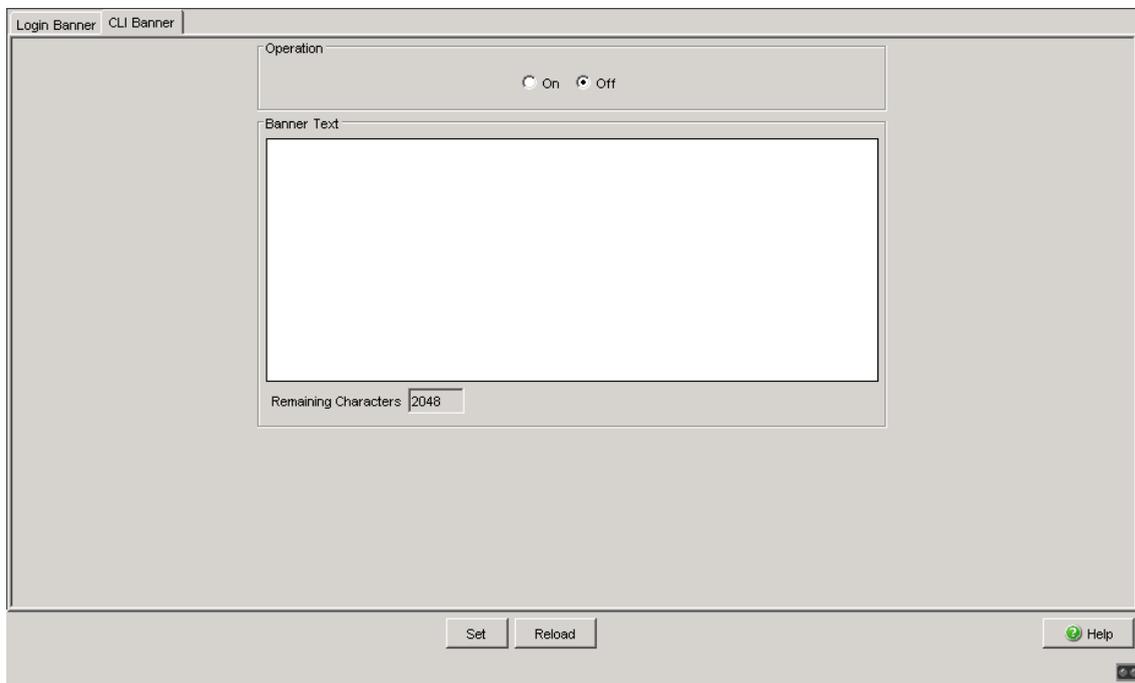


Figure 27: "Login/CLI Banner" dialog, "CLI Banner" tab

■ Function

Parameter	Meaning
Operation	<p>When this function is switched on, the device shows the text information defined in the "Banner Text" field to the users that login to the device via the command line interface.</p> <p>When the function is switched off, the CLI start screen shows information about the device. The text information in the "Banner Text" field is retained.</p> <p>Possible values:</p> <ul style="list-style-type: none"> ▶ Off (default setting) ▶ On

■ Banner Text

Parameter	Meaning
Banner Text	<p>Defines the text information that the device displays to the users instead of the default information.</p> <p>Possible values:</p> <ul style="list-style-type: none"> ▶ Alphanumeric ASCII character string with 0..2048 characters (0x20..0x7E) including spaces ▶ Tab \t ▶ Line break \n
Remaining Characters	<p>Shows how many characters are still remaining in the "Banner Text" field for the text information.</p> <p>Possible values:</p> <ul style="list-style-type: none"> ▶ 2048..0

■ Buttons

Button	Meaning
Set	Transfers the changes to the volatile memory (RAM) of the device. To permanently save the changes afterwards, you open the <code>Basic Settings:Load/Save</code> dialog and click "Save".
Reload	Updates the fields with the values that are saved in the volatile memory (RAM) of the device.
Help	Opens the online help.

Table 25: Buttons

3 Time

3.1 Basic Settings

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

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

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

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

Interaction of PTP and SNTP

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

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

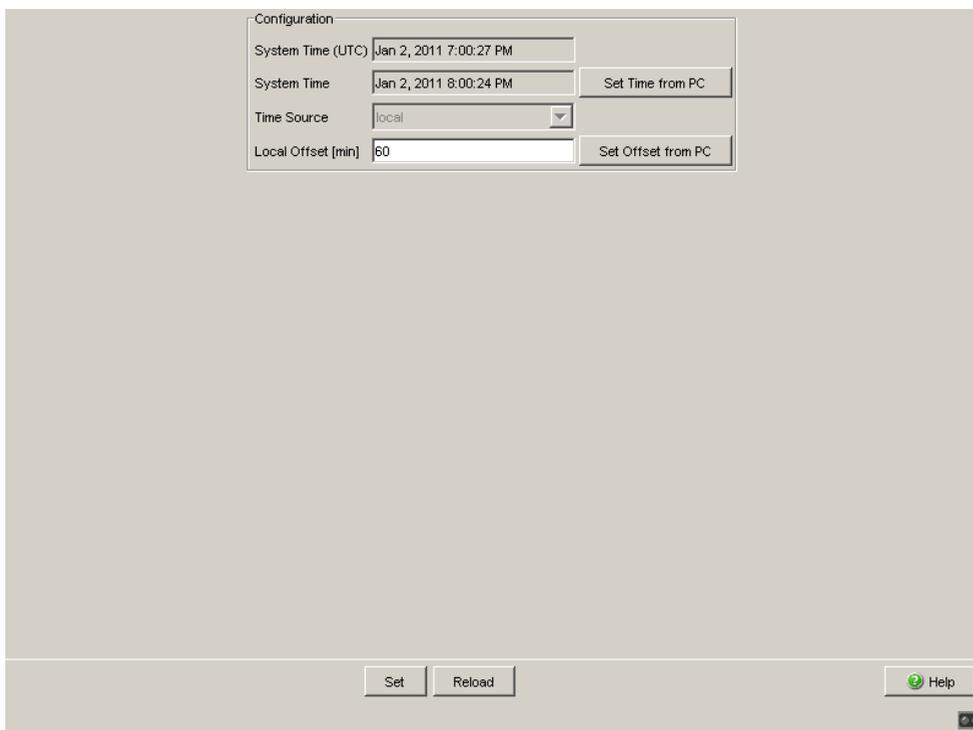


Figure 28: Time Dialog:Basic Settings

■ Buttons

Button	Meaning
Set	Transfers the changes to the volatile memory (RAM) of the device. To permanently save the changes, open the <code>Basic Settings:Load/Save</code> dialog, select the location to save the configuration, and click "Save".
Reload	Updates the fields with the values that are saved in the volatile memory (RAM) of the device.
Help	Opens the online help.

Table 26: Buttons

3.2 SNTP configuration

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

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

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

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

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

Parameters	Meaning	Possible values	Default setting
Operation	Switches the SNTP function on and off globally.	On, Off	Off

Table 27: Switches SNTP on and off globally

Parameters	Meaning	Possible values	Default setting
SNTP Status	Displays conditions such as "Server - cannot be reached".	-	-

Table 28: SNTP Status

Parameters	Meaning	Possible values	Default setting
Client Status	Switches the SNTP client on and off.	On, Off	On
External Server Address	IP address of the SNTP server from which the device periodically requests the system time.	Valid IPv4 address	0.0.0.0
Redundant Server Address	IP address of the SNTP server from which the device periodically requests the system time if it does not receive a response to a request from the “External server address” within 0.5 seconds.	Valid IPv4 address	0.0.0.0
Server Request Interval	Time interval at which the device requests SNTP packets.	1 s - 3600 s	30 s
Accept SNTP Broadcasts	Specifies whether the device accepts the system time from SNTP Broadcast/Multicast packets that it receives.	On, Off	On
Threshold for obtaining the UTC [ms]	The device changes the time as soon as the deviation from the server time is above this threshold in milliseconds. This reduces the frequency of time changes.	0 - 2147483647 (2 ³¹ -1)	0
Disable Client after successful Synchronization	Enable/disable further time synchronizations once the client, after its activation, has synchronized its time with the server.	On, Off	Off

Table 29: Configuration SNTP Client

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

Note: If you are receiving the system time from an external/redundant server address, switch off the reception of SNTP Broadcasts (see “Accept SNTP Broadcasts”). You thus ensure that the device only takes the time from a defined SNTP server.

Parameters	Meaning	Possible values	Default setting
Server Status	Switches the SNTP server on and off.	On, Off	On
Anycast Destination Address	IP address, to which the SNTP server of the device sends the SNTP packets (see table 31).	Valid IPv4 address	0.0.0.0
VLAN ID	VLANs to which the device periodically sends SNTP packets.	1-4042	1
Anycast Send Interval	Time interval at which the device sends SNTP packets.	1 - 3600	120
Disable Server at local Time Source	Enables/disables the SNTP server function if the status of the time source is <code>local</code> (see Time dialog).	On, Off	Off

Table 30: Configuration SNTP-Server

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

Table 31: Destination address classes for SNTP and NTP packets

Figure 29: SNTP Dialog

■ Buttons

Button	Meaning
Set	Transfers the changes to the volatile memory (RAM) of the device. To permanently save the changes, open the <code>Basic Settings:Load/Save</code> dialog, select the location to save the configuration, and click "Save".
Reload	Updates the fields with the values that are saved in the volatile memory (RAM) of the device.
Help	Opens the online help.

Table 32: Buttons

3.3 PTP (IEEE 1588)

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

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

■ Devices without PTP hardware support

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

With these devices

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

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

■ Devices with PTP hardware support

Devices with PTP hardware support, which have ports with a time stamp unit, support other modes subject to the version of the time stamp unit.

▶ MS20, MS30 and PowerMICE devices with the modules

- MM3-4TX1-RT
- MM3-2FXM2/2TX1-RT
- MM3-2FXS2/2TX1-RT
- MM3-2FLM4/2TX1-RT

support the modes

- v1-boundary-clock
- v1-simple-mode
- v2-boundary-clock-twostep, only with the network protocol UDP/IPv4 and the runtime measurement E2E

▶ MS20, MS30 and PowerMICE devices with the modules

- MM23
- MM33

support the modes:

- v1-boundary-clock
- v1-simple-mode
- v2-boundary-clock-onestep
- v2-boundary-clock-twostep
- v2-transparent-clock
- v2-simple-mode

▶ MACH 104 and MACH 1040 devices support the modes

- v1-boundary-clock
- v1-simple-mode
- v2-boundary-clock-twostep
- v2-transparent-clock
- v2-simple-mode

The following sections relate exclusively to devices **with** PTP hardware support.

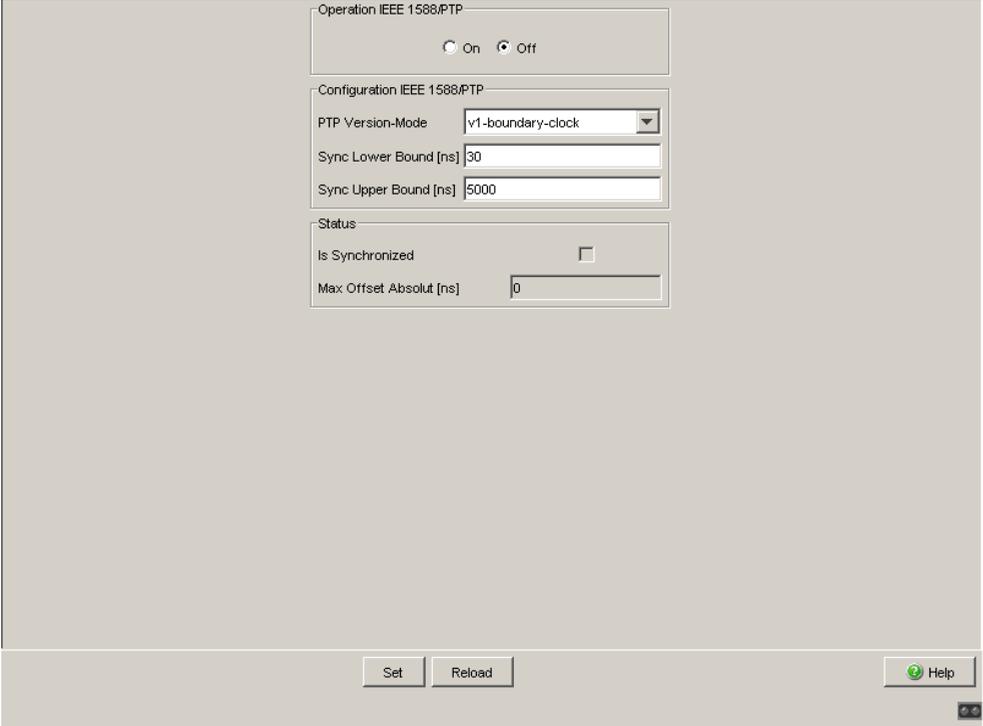


Figure 30: PTP Global Dialog

3.3.1 PTP Global (MS20/MS30, PowerMICE, MACH 104, MACH 1040)

The table below helps you to select the PTP version and the PTP mode.

Version	Mode	Reference clock used	Device with timestamp	PTP messages
Version 1	v1-simple-mode	Version 1	No	—
	v1-boundary-clock	Version 1	Yes	Process
Version 2	v2-simple-mode	Version 2	No	—
	v2-boundary-clock-onestep	Version 2	Yes	Process
	v2-boundary-clock-twostep	Version 2	Yes	Process
	v2-transparent-clock	Version 2	Yes	Forward

Note: For the MS20, MS30 and PowerMICE devices with MM23 or MM33 modules, see sections [“Devices without PTP hardware support” on page 87](#) and [“Devices with PTP hardware support” on page 88](#).

Table 33: Selecting the PTP version and the PTP mode

The PTP modes

- ▶ v1-boundary-clock
- ▶ v2-boundary-clock-onestep¹
- ▶ v2-boundary-clock-twostep
- ▶ v2-transparent-clock

enable you to optimize time division accuracy.

You use these dialogs for this purpose

- ▶ Version 1
- ▶ Version 2 (Boundary Clock, BC)
- ▶ Version 2 (Transparent Clock, TC)

The PTP modes

- ▶ v1-simple-mode
- ▶ v2-simple-mode

allow you to use the plug-and-play start-up.

Parameters	Meaning	Possible values	Default setting
Operation on/off	Enable/disable the PTP function	On, Off	Off

Table 34: Function IEEE 1588/PTP

Parameters	Meaning	Possible values	Default setting
PTP Version-Mode	Version and mode of the local clock.	v1-boundary-clock v1-simple-mode v2-boundary-clock-onestep v2-boundary-clock-twostep v2-transparent-clock v2-simple-mode	v1-boundary-clock

Table 35: Configuration IEEE 1588/PTP, PTP version and mode, overview

1. For the MS20, MS30 and PowerMICE devices with MM23 or MM33 modules, see sections [“Devices without PTP hardware support”](#) on page 87 and [“Devices with PTP hardware support”](#) on page 88.

Value for PTP version and PTP mode	Meaning
v1-boundary-clock	<p>Boundary Clock function based on IEEE1588-2002 (PTPv1).</p> <p>For the MS20, MS30 and PowerMICE devices with realtime modules and for MACH 104 and MACH 1040, see sections “Devices without PTP hardware support” on page 87 and “Devices with PTP hardware support” on page 88.</p>
v1-simple-mode	<p>Support for PTPv1 without special hardware. The device synchronizes itself with PTPv1 messages received. This mode does not provide any other functions, such as PTP management or runtime measuring.</p> <p>Select this mode if the device only has ports absent a timestamp unit.</p>
v2-boundary-clock-onestep	<p>Boundary Clock function based on IEEE 1588-2008 (PTPv2).</p> <p>The one-step mode determines the precise PTP time with 1 message.</p> <p>For the MS20, MS30 and PowerMICE devices with MM23 or MM33 modules, see sections “Devices without PTP hardware support” on page 87 and “Devices with PTP hardware support” on page 88.</p>
v2-boundary-clock-twostep	<p>Boundary Clock function based on IEEE 1588-2008 (PTPv2).</p> <p>The two-step mode determines the precise PTP time with 2 messages.</p>
v2-transparent-clock	<p>Transparent Clock function based on IEEE 1588-2008 (PTPv2).</p> <p>Here, the MS20, MS30 and PowerMICE devices with MM23 or MM33 modules use only the one-step mode.</p> <p>Here, the MACH 104 and MACH 1040 devices use only the two-step mode. They support a receive rate of 8 frames/s max.</p>
v2-simple-mode	<p>Support for PTPv2 without special hardware. The device synchronizes itself with PTPv2 messages received. This mode does not provide any other functions, such as PTP management or runtime measuring.</p> <p>Select this mode if the device only has ports absent a timestamp unit.</p>

Table 36: Configuration IEEE 1588/PTP, PTP version and mode, details

Parameters	Meaning	Possible values	Default setting
Sync Lower Bound [ns]	Bottom PTP synchronization threshold value, specified in nanoseconds. If the result 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.	0-999999999	30
Sync Upper Bound [ns]	Top PTP synchronization threshold value, specified in nanoseconds. If the result 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.	31-1000000000	5000

Table 37: Configuration IEEE 1588/PTP, synchronization thresholds

Parameters	Meaning	Possible values	Default setting
Is Synchronized	Local clock synchronized with reference clock; compare Bottom synchronization threshold and Top synchronization threshold.	true, false	-
Max Offset Absolute [ns]	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.		-

Table 38: IEEE 1588/PTP status

■ Buttons

Button	Meaning
Set	Transfers the changes to the volatile memory (RAM) of the device. To permanently save the changes, open the Basic Settings:Load/Save dialog, select the location to save the configuration, and click "Save".
Reload	Updates the fields with the values that are saved in the volatile memory (RAM) of the device.
Help	Opens the online help.

Table 39: Buttons

3.3.2 PTP Version 1 (MS20/MS30, PowerMICE, MACH 104, MACH 1040)

You select the PTP version you will use in the `Time:PTP:Global` dialog.

■ PTP Version 1, Global Settings

Parameters	Meaning	Possible values	Default setting
Sync Interval	Period for sending synchronization messages. Entered in seconds. In order for changes to take effect, click "Reinitialize".	- sec-1 - sec-2 - sec-8 - sec-16 - sec-64	sec-2
Subdomain Name	Name of the PTP subdomain to which the local clock belongs. In order for changes to take effect, click "Reinitialize".	1 to 16 ASCII characters, hex value 0x21 (!) through 0x7e (~)	_DFLT
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.	true false	false

Table 40: Function IEEE 1588/PTPv1

Parameters	Meaning	Possible values	Default setting
Offset to Master [ns]	Deviation of the local clock from the reference clock in nanoseconds.		
Delay to Master [ns]	Single signal runtime between the local device and reference clock in nanoseconds.		
Grandmaster UUID	MAC address of the grandmaster clock (Unique Universal Identifier).		
Parent UUID	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.).		

Table 41: Status IEEE 1588/PTPv1

Note: PTPv1 uses as the device UUID 48 bits which are identical to the MAC address of the particular device.

■ Buttons

Button	Meaning
Set	Transfers the changes to the volatile memory (RAM) of the device. To permanently save the changes, open the <code>Basic Settings:Load/Save</code> dialog, select the location to save the configuration, and click "Save".
Reload	Updates the fields with the values that are saved in the volatile memory (RAM) of the device.
Reinitialize	Restarts synchronization after changing the interval time and sets the Subdomain Name.
Help	Opens the online help.

Table 42: Buttons

■ PTP Version 1, Port Settings

Parameters	Meaning	Possible values	Default setting
Port	Port to which this entry applies. The table remains empty if the device does not support the PTP mode selected		
PTP enable	Port sends/receives PTP synchronization messages	on	on
	Port blocks PTP synchronization messages.	off	
PTP Burst enable	on: 2 to 8 synchronization runs take place during the synchronization interval. This enables faster synchronization with a correspondingly higher network load.	on	off
	off: One synchronization run is performed in a synchronization interval.	off	

Table 43: Port dialog version 1

Parameters	Meaning	Possible values	Default setting
PTP Status	Port is in the initialization phase.	initializing	
	Port is in the faulty mode. Error in the PTP protocol.	faulty	
	PTP function is switched off at this port.	disabled	
	Port has not received any information and is waiting for synchronization messages.	listening	
	Port is in PTP pre-master mode.	pre-master	
	Port is in PTP master mode.	master	
	Port is in PTP passive mode.	passive	
	Port is in PTP uncalibrated mode.	uncalibrated	
	Port is in PTP slave mode.	slave	

Table 43: Port dialog version 1

■ Buttons

Button	Meaning
Set	Transfers the changes to the volatile memory (RAM) of the device. To permanently save the changes, open the <code>Basic Settings:Load/Save</code> dialog, select the location to save the configuration, and click "Save".
Reload	Updates the fields with the values that are saved in the volatile memory (RAM) of the device.
Help	Opens the online help.

Table 44: Buttons

3.3.3 PTP Version 2 (BC) (MS20/MS30, PowerMICE, MACH 104, MACH 1040)

PTP version 2 provides considerably more settings. These support

- faster reconfiguration of the PTP network than in PTP version 1
- greater precision in some environments.

You select the PTP version you will use in the `Time:PTP:Global` dialog.

■ Global

Parameters	Meaning	Possible values	Default setting
Priority 1	The clock with the lowest priority 1 becomes the reference clock (grandmaster).	0-255	128
Priority 2	If all the relevant values for selecting the reference clock are the same for multiple devices, the clock with the lowest priority 2 is selected as the reference clock (grandmaster).	0-255	128
Domain Number	Assignment of the clock to a PTPv2 domain. Only clocks with the same domain are synchronized.	0-255	0

Table 45: Function IEEE 1588/PTPv2 BC

Parameters	Meaning	Possible values	Default setting
Two-Step	Displays the device's clock mode	Off (select v2-boundary-clock-onestep in PTP Global dialog) On (select v2-boundary-clock-twostep in PTP Global dialog)	
Steps Removed	Number of boundary clocks between this device and the PTP reference clock.		
Offset to Master [ns]	Deviation of the local clock from the reference clock in nanoseconds.		
Delay to Master [ns]	Single signal runtime (end-to-end) between the local device and reference clock in nanoseconds. Prerequisite: The slave port's runtime mechanism is set to E2E.		

Table 46: IEEE 1588/PTPv2 BC Status

Parameters	Meaning	Possible values	Default setting
Clock identify	Own device UUID (unique identification number)		

Table 47: PTP Clock Identities

Parameters	Meaning	Possible values	Default setting
Parent Port identity	Port UUID of the direct master		
Grandmaster identity	Device UUID of the reference clock		

Table 47: PTP Clock Identities

Note: PTPv2 uses as the device UUID 64 bits, consisting of the device's MAC address, between whose No. 3 and No. 4 bytes the values ff and fe are added.

A port UUID consists of the device UUID followed by a 16-bit port ID.

The device displays UUIDs as a byte sequence in hexadecimal notation.

Parameters	Meaning	Possible values	Default setting
Priority 1	Display priority 1 of the current reference clock.		
Priority 2	Display priority 2 of the current reference clock.		
Class	Class of the reference clock		
Precision	Estimated accuracy with regard to the UTC, indicated by the reference clock (the Grandmaster).		
Variance	Variance as described in the IEEE 1588-2008 standard		

Table 48: Grandmaster (reference clock)

Parameters	Meaning	Possible values	Default setting
Time source	Source selected for own clock.	atomicClock gps terrestrialRadio ptp ntp handset other internalOscillator	internalOscillator
UTC Offset [s]	Current difference between the PTP time scale (see below) and the UTC.	-32768 to 32767	35 (since 2012-07-01)
UTC Offset valid	Specifies whether value of UTC offset is valid or not.	Yes No	No
Time Traceable	The device gets the time from a primary UTC reference, e.g. from an NTP server.	Yes No	

Table 49: Properties of the local time

Parameters	Meaning	Possible values	Default setting
Frequency Traceable	The device gets the frequency from a primary UTC reference, e.g. NTP server, GPS.	Yes No	
PTP Time Scale	The device uses the PTP time scale. According to IEEE 1588, the PTP time scale is the TAI atomic time started on 01.01.1970. In contrast to UTC, TAI does not use leap seconds. On 01.01.2009, the difference between UTC and TAI was +34 seconds.	Yes No	

Table 49: Properties of the local time

■ Buttons

Button	Meaning
Set	Transfers the changes to the volatile memory (RAM) of the device. To permanently save the changes, open the <code>Basic Settings:Load/Save</code> dialog, select the location to save the configuration, and click "Save".
Reload	Updates the fields with the values that are saved in the volatile memory (RAM) of the device.
Help	Opens the online help.

Table 50: Buttons

■ Port

Parameters	Meaning	Possible values	Default setting
Port	Port to which this entry applies. If the device does not support the PTP mode selected, the table is empty.		
PTP enable	Port sends/receives PTP synchronization messages	on	on
	Port blocks PTP synchronization messages.	off	

Table 51: Port Dialog Version 2(BC)

Parameters	Meaning	Possible values	Default setting
PTP Status	Port is in the initialization phase.	initializing	
	Port is in the faulty mode. Error in the PTP protocol.	faulty	
	PTP function is switched off at this port.	disabled	
	Port has not received any information and is waiting for synchronization messages.	listening	
	Port is in PTP pre-master mode.	pre-master	
	Port is in PTP master mode.	master	
	Port is in PTP uncalibrated mode.	uncalibrated	
	Port is in PTP passive mode.	passive	
	Port is in PTP slave mode.	slave	
Sync Interval [s]	Interval in seconds for the synchronization messages	0,5; 1; 2	1
Runtime Measuring Mechanism	Mechanism for measuring the message runtime. Enter the same mechanism for the PTP device connected to this port.		
	A PTP slave port measures the runtime of the entire transmission path to the master. The device displays the measured value in the PTP:Version 2(BC):Global dialog (see on page 97 “Global”).	E2E (end-to-end):	
	The device measures the runtime to all the PTP devices connected. If a reconfiguration is performed, this mechanism eliminates the need to determine the runtime again, provided all these devices support P2P.	P2P (peer-to-peer)	
	The MS20, MS30 and PowerMICE devices with MM23 or MM33 modules, as well as the MACH 104 and MACH 1040 devices support these mechanisms.		
	No runtime determination.	Disabled	Disabled
P2P Runtime	Measured P2P (peer-to-peer) runtime. Prerequisite: You have selected the P2P runtime measuring mechanism.		

Table 51: Port Dialog Version 2(BC)

Parameters	Meaning	Possible values	Default setting
P2P Runtime Measuring Interval	Interval for peer-to-peer runtime measurements at this port. Prerequisite: You have selected the P2P runtime measuring mechanism on the device itself and on the PTP device connected.		
Network Protocol	Transport protocol for PTP messages.	802.3 Ethernet, UDP/IPv4	UDP/IPv4
Announce Interval	Message interval for PTP topology discovery (selection of the reference clock). Select the same value for all devices within a PTP domain.	1, 2, 4, 8, 16	2
Announce Timeout	Announce interval timeout for PTP topology discovery in number of announce intervals. The standard settings of announce interval = 2 (2 per second) and announce timeout = 3 result in a timeout of 3 x 2 seconds = 6 seconds. Select the same value for all devices within a PTP domain.	2-10	3
E2E Runtime Measuring Interval	Displays in seconds the interval for E2E (end-to-end) runtime measurements at this port. This is a device variable and is assigned to ports with PTP slave status by the master connected. If the port itself is the master, then the device assigns the port the value 8 (state on delivery).		8
V1 Hardware Compatibility	Some devices from other manufacturers require PTP messages of specific length. If the UDP/IPv4 network protocol is selected and the function is active, the device extends the PTP messages.	auto, on, off	auto
Asymmetry	Correction of the runtime asymmetry in ns. A runtime measurement value of x ns corrupted by asymmetrical transmission values corresponds to an asymmetry of x·2 ns		

Table 51: Port Dialog Version 2(BC)

Parameters	Meaning	Possible values	Default setting
VLAN	The VLAN ID with which the device sends PTP frames to this port.	none, 0 - 4042	none
	<p>Note:</p> <ul style="list-style-type: none"> ▶ Also take the port's VLAN setting (see on page 133 "VLAN Static") into account here, in particular whether the VLAN exists and if the port is a tagged or untagged member in the VLAN. ▶ none: The device always sends PTP frames absent a VLAN tag, even if the port is a tagged member of the VLAN. ▶ You can select VLANs that you have already set up using of the table row drop-down list. 		
VLAN Priority	The VLAN priority (Layer 2, IEEE 802.1p) with which the device sends PTP frames to this port. If you have set the VLAN ID to none, the device ignores the VLAN priority.	0 - 7	0

Table 51: Port Dialog Version 2(BC)

■ Buttons

Button	Meaning
Set	Transfers the changes to the volatile memory (RAM) of the device. To permanently save the changes, open the <code>Basic Settings:Load/Save</code> dialog, select the location to save the configuration, and click "Save".
Reload	Updates the fields with the values that are saved in the volatile memory (RAM) of the device.
Help	Opens the online help.

Table 52: Buttons

3.3.4 PTP Version 2 (TC) (MS20/MS30, PowerMICE, MACH 104, MACH 1040)

In strongly cascaded networks in particular, the transparent clock (TC) introduced in PTP Version 2 provides a noticeable increase in precision. The combination with the P2P runtime mechanism (simultaneous runtime measurement at all ports) enables “seamless” reconfiguration.

For the MS20, MS30 and PowerMICE devices with MM23 or MM33 modules:

The following settings enable you to also use the TC for Unicast PTP messages:

- Selecting the E2E mechanism
- Syntonize disabled
- PTP Management disabled.

You select the PTP version you will use in the `Time:PTP:Global` dialog.

■ PTP Version 2 (TC), Global Settings

Parameters	Meaning	Possible values	Default setting
Profile	Defines relevant PTP parameters to a specific profile.	E2E-Defaults P2P-Defaults Power-Defaults	

Table 53: PTP Version 2(TC) Profile Presets

Parameters	Meaning	Possible values	Default setting
Runtime Measuring Mechanism	Mechanism for measuring the message runtime. Enter the same mechanism for the PTP device connected to this port.		
	A PTP slave port measures the runtime of the entire transmission path to the master. The device displays the measured value in the PTP:Version 2(BC):Global dialog (see on page 97 “Global”).	E2E (end-to-end):	
	The device itself measures the runtime to all the PTP devices connected. If a reconfiguration is performed, this eliminates the need to determine the runtime again.	P2P (peer-to-peer)	
	For the MACH 104 and MACH 1040 devices: Such as E2E with the following characteristics: <ul style="list-style-type: none"> ▶ The device only transmits the PTP slaves' delay queries to the master, even though these queries are multicast frames. In this way, the device relieves the other clients from unnecessary multicast queries. ▶ With changes in the PTP master-slave topology, the device relearns the port for the PTP master as soon as it has received a frame from another PTP master. ▶ If the device does not recognize a PTP master, it also floods delay queries received in the E2E Optimized mode. 	E2E Optimized (end-to-end, optimized)	
	For the MACH 104 and MACH 1040 devices: The device does not allow runtime measurement, i.e., it discards frames received, which are used for measuring runtime.	Disabled	
Primary Domain	Assignment of the clock to a PTPv2 domain.	0-225	0
Network Protocol	Network protocol for P2P and management messages.	UDP/IPv4, IEEE 802.3	UDP/IPv4

Table 54: Function IEEE 1588 / PTPv2 TC

Parameters	Meaning	Possible values	Default setting
Syntonize	Synchronize frequency.	On Off	For the MS20, MS30 and PowerMICE devices: Off For devices MACH 104 and MACH 1040: On
Synchronizing local time	The device synchronizes its local time with the time received via the PTP. Prerequisite: the Syntonize setting is activated.	On Off	Off
PTP Management	Activate/deactivate PTP management. To reduce the load on the device, deactivate PTP Management and Syntonize - at high synchronization rates and - in Unicast mode.	On Off	Off
Multi Domain Mode	On: TC corrects messages from all domains. Off: TC only corrects messages from the primary domain.	On Off	Off
Power TLV Check	Activate/deactivate the Power TLV check. On: The device ignores announce messages without the Power Profile TLV.	On Off	Off

Table 54: Function IEEE 1588 / PTPv2 TC

Parameters	Meaning	Possible values	Default setting
VLAN	The VLAN ID with which the device sends its own frames (like PTP Management frames or P2P frames) to this port.	none, 0 - 4042	none
	<p>Note:</p> <ul style="list-style-type: none"> ▶ Also take the port's VLAN setting (see on page 133 “VLAN Static”) into account here, in particular whether the VLAN exists and if the the port is a tagged or untagged member in the VLAN. ▶ none: The device always sends PTP frames absent a VLAN tag, even if the port is a tagged member of the VLAN. ▶ You can select VLANs that you have already set up using of the table row drop-down list. 		
VLAN Priority	The VLAN priority (Layer 2, IEEE 802.1p) with which the device sends tagged PTP frames. If you have set the VLAN ID to none, the device ignores the VLAN priority.	0 - 7	0

Table 54: Function IEEE 1588 / PTPv2 TC

Parameters	Meaning	Possible values	Default setting
Clock identifier	Device UUID of the TC (transparent clock)		
Current master	When the Syntonize function is enabled, the master's port UUID, with which the device synchronizes its frequency, is displayed. A value consisting of zeros means that: <ul style="list-style-type: none"> ▶ the Syntonize function is deactivated or ▶ the device has not found a master 		

Table 55: Status IEEE 1588 / PTPv2 TC

Note: PTPv2 uses as the device UUID 64 bits, consisting of the device's MAC address, between whose No. 3 and No. 4 bytes the values ff and fe are added.

A port UUID consists of the device UUID followed by a 16-bit port ID. The device displays UUIDs as a byte sequence in hexadecimal notation.

■ Buttons

Button	Meaning
Set	Transfers the changes to the volatile memory (RAM) of the device. To permanently save the changes, open the <code>Basic Settings:Load/Save</code> dialog, select the location to save the configuration, and click "Save".
Reload	Updates the fields with the values that are saved in the volatile memory (RAM) of the device.
Help	Opens the online help.

Table 56: Buttons

■ PTP Version 2 (TC), Port Settings

Parameters	Meaning	Possible values	Default setting
Module	Module number for modular devices, otherwise 1.		
Port	Port to which this entry applies. If the device does not support the PTP mode selected, the table is empty.		
PTP enable	Port sends/receives PTP synchronization messages	on	on
	Port blocks PTP synchronization messages. The device does not process any PTP messages it receives at this port.	off	
P2P Runtime Measuring Interval	Interval for peer-to-peer runtime measurements at this port. Prerequisite: You have selected the P2P runtime measuring mechanism on the device itself and on the PTP device connected.		

Table 57: Port Dialog Version 2(TC)

Parameters	Meaning	Possible values	Default setting
P2P Runtime	Measured P2P (peer-to-peer) runtime. Prerequisite: You have selected the P2P runtime measuring mechanism.		
Asymmetry	Correction of the runtime asymmetry in ns. A runtime measurement value of x ns corrupted by asymmetrical transmission values corresponds to an asymmetry of x·2 ns		

Table 57: Port Dialog Version 2(TC)

■ Buttons

Button	Meaning
Set	Transfers the changes to the volatile memory (RAM) of the device. To permanently save the changes, open the <code>Basic Settings:Load/Save</code> dialog, select the location to save the configuration, and click "Save".
Reload	Updates the fields with the values that are saved in the volatile memory (RAM) of the device.
Help	Opens the online help.

Table 58: Buttons

4 Switching

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

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

4.1 Switching Global

Parameters	Meaning	Possible values	Default setting
MAC address (read only)	Display the MAC address of the device		
Aging Time (s)	Enter the Aging Time in seconds for dynamic MAC address entries. In connection with the router redundancy, select a time \geq 30 s.	15-3825	30
Activate Flow Control	Activate/deactivate the flow control	On, Off	Off

Table 59: Switching:Global dialog

Note: When you are using a redundancy function, you deactivate the flow control on the participating device ports. If the flow control and the redundancy function are active at the same time, there is a risk that the redundancy function will not operate as intended.

Parameters	Meaning	Possible values	Default setting
Address learning	Activate/deactivate the learning of MAC source addresses.	On, Off	On
Frame size	Set the maximum packet size (frame size) in bytes.	1522, 1632	1522
Activate Address Relearn Detection	Enable/disable whether the device detects whether it has repeatedly learned the same MAC source addresses at different ports. This process very probably indicates a loop situation in the network. If the device detects this process, it creates an entry in the log file and sends an alarm (trap).	On, Off	Off

Table 60: Switching:Global dialog

Parameters	Meaning	Possible values	Default setting
Address Relearn Threshold	Number of learned MAC addresses on different ports within a checking interval. If the number of learned addresses reach this threshold, the device sees this as a relevant event. The interval for this check is a few seconds.	1 - 1024	1
Activate Duplex Mismatch Detection	Enable/disable whether the device reports a duplex problem at a port for specific error events. This means that the duplex mode of the port might not match that of the remote port. If the device detects a potential non-match, it creates an entry in the trap log and sends an alarm (trap). To detect potential non-matches, the device evaluates the error counters of the port after the connection is set up, in the context of the port settings (see table 61).	On, Off	On

Table 60: Switching:Global dialog

The following table lists the duplex operating modes for TX ports, with the possible fault events. The meanings of terms used in the table are as follows:

- ▶ Collisions: In half-duplex mode, collisions mean normal operation.
- ▶ Duplex problem: Mismatching duplex modes.
- ▶ EMI: Electromagnetic interference.
- ▶ Network extension: The network extension is too great, or too many cascading hubs.
- ▶ Collisions, late collisions: In full-duplex mode, no incrementation of the port counters for collisions or late collisions.
- ▶ CRC error: The device evaluates these errors as non-matching duplex modes in the manual full duplex mode.

No.	Automatic configuration	Current duplex mode	Detected error events (≥ 10 after link up)	Duplex modes	Possible causes
1	On	Half duplex	None	OK	
2	On	Half duplex	Collisions	OK	
3	On	Half duplex	Late collisions	Duplex problem detected	Duplex problem, EMI, network extension

Table 61: Evaluation of non-matching of the duplex mode

No.	Automatic configuration	Current duplex mode	Detected error events (≥ 10 after link up)	Duplex modes	Possible causes
4	On	Half duplex	CRC error	OK	EMI
5	On	Full duplex	None	OK	
6	On	Full duplex	Collisions	OK	EMI
7	On	Full duplex	Late collisions	OK	EMI
8	On	Full duplex	CRC error	OK	EMI
9	Off	Half duplex	None	OK	
10	Off	Half duplex	Collisions	OK	
11	Off	Half duplex	Late collisions	Duplex problem detected	Duplex problem, EMI, network extension
12	Off	Half duplex	CRC error	OK	EMI
13	Off	Full duplex	None	OK	
14	Off	Full duplex	Collisions	OK	EMI
15	Off	Full duplex	Late collisions	OK	EMI
16	Off	Full duplex	CRC error	Duplex problem detected	Duplex problem, EMI

Table 61: Evaluation of non-matching of the duplex mode (cont.)

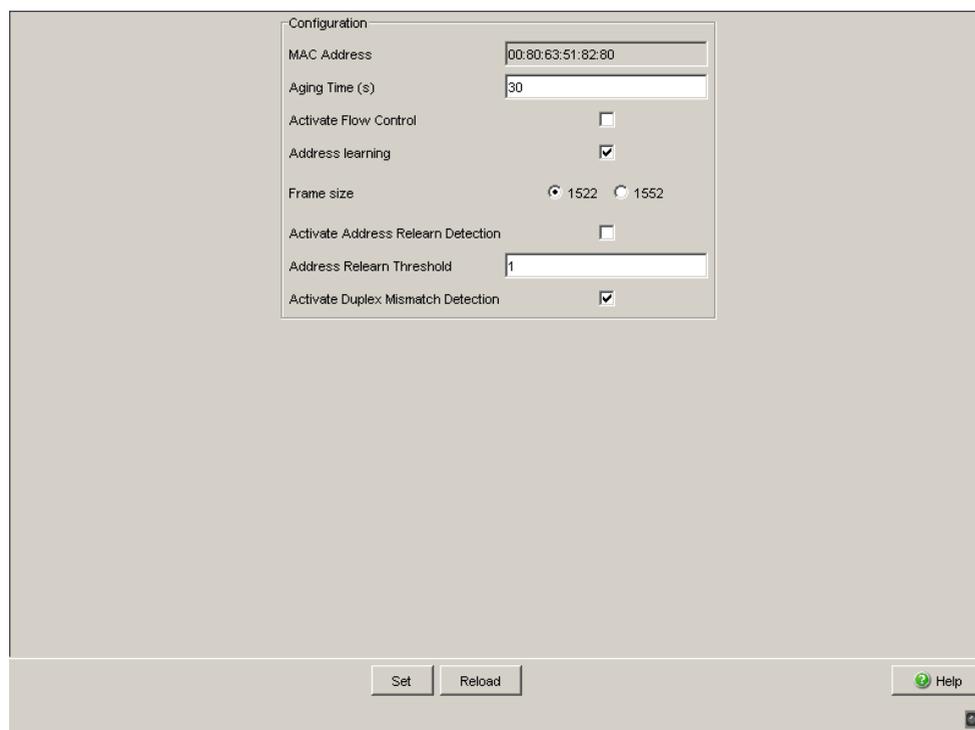


Figure 31: Dialog Switching Global

■ Buttons

Button	Meaning
Set	Transfers the changes to the volatile memory (RAM) of the device. To permanently save the changes, open the <code>Basic Settings:Load/Save</code> dialog, select the location to save the configuration, and click "Save".
Reload	Updates the fields with the values that are saved in the volatile memory (RAM) of the device.
Help	Opens the online help.

Table 62: Buttons

4.2 Filter for MAC addresses

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

- ▶ **learned**: The filter was created automatically by the device.
- ▶ **invalid**: With this status you delete a manually created filter.
- ▶ **permanent**: The filter is stored permanently in the device or on the URL (see on page 40 “Load/Save”).
- ▶ **igmp**: The filter was created by IGMP Snooping.

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

Address A	Status	VLAN-ID	1.1	1.2	1.3	1.4	2.1	2.2	2.3	2.4	3.1	3.2	8.1	8.2
00 15 58 7c f5 15	learned	1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
00 80 63 14 db df	learned	1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
00 80 63 2f fb c0	learned	1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
00 80 63 4a a7 be	learned	1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
00 80 63 51 74 0b	learned	1	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
00 80 63 51 7a 8a	learned	1	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
00 80 63 51 82 80	mgmt	1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Buttons: Set, Reload, Create, Help

Figure 32: Filter Table dialog

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

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

■ Create

To set up a filter manually, click the "Create" button.

Parameters	Meaning
VLAN ID	<p>Defines the ID of the VLAN to which the table entry applies.</p> <p>Possible values:</p> <ul style="list-style-type: none"> ▶ All VLAN IDs that are set up
Address	<p>Defines the destination MAC address to which the table entry applies.</p> <p>Possible values:</p> <ul style="list-style-type: none"> ▶ Valid MAC address <p>Enter the value in one of the following formats:</p> <ul style="list-style-type: none"> – without a separator, e.g. 001122334455 – separated by spaces, e.g. 00 11 22 33 44 55 – separated by colons, e.g. 00:11:22:33:44:55 – separated by hyphens, e.g. 00-11-22-33-44-55 – separated by points, e.g. 00.11.22.33.44.55 – separated by points after every 4th character, e.g. 0011.2233.4455
Possible Ports	<p>Defines the device ports to which the device transmits data packets with the destination MAC address:</p> <ul style="list-style-type: none"> <input type="checkbox"/> Select one port if the destination MAC address is a Unicast address. <input type="checkbox"/> Select one or more ports if the destination MAC address is a Multicast address. <input type="checkbox"/> Select no port to set up a discard filter. The device discards data packets with the destination MAC address specified in the table entry.

Table 63: "Create" window

■ Edit Entry

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

Parameters	Meaning
Possible Ports	This column contains the ports available in the device.
Dedicated Ports	This column contains the device ports that are assigned to the table entry. <ul style="list-style-type: none"> <input type="checkbox"/> Select one port if the destination MAC address is a Unicast address. <input type="checkbox"/> Select one or more ports if the destination MAC address is a Multicast address. <input type="checkbox"/> Select no port to set up a discard filter. The device discards data packets with the destination MAC address specified in the table entry.

Table 64: "Edit Entry" window in the *Switching:Filters for MAC Addresses* dialog

■ Buttons

Button	Meaning
Set	Transfers the changes to the volatile memory (RAM) of the device. To permanently save the changes afterwards, you open the <i>Basic Settings:Load/Save</i> dialog and click "Save".
Reload	Updates the fields with the values that are saved in the volatile memory (RAM) of the device.
Create	Adds a new table entry.
Edit Entry	Opens the "Edit Entry" window.
Help	Opens the online help.
>	Moves the selected entry to the right column.
>>	Moves all entries to the right column.
<	Moves the selected entry to the left column.
<<	Moves all entries to the left column.

Table 65: *Buttons*

4.3 Rate Limiter

To ensure reliable operation at a high level of traffic, the device allows you to limit the rate of traffic at the ports.

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

If the traffic at this port exceeds the maximum rate entered, then the device suppresses the overload at this port.

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

Note: The limiter functions only work on Layer 2 and are used to limit the effect of storms by frame types that the Switch floods (typically broadcasts). In doing so, the limiter function disregards the protocol information of higher layers, such as IP or TCP. This can affect on TCP traffic, for example.

To minimize these effects, use the following options:

- ▶ limiting the limiter function to particular frame types (e.g. to broadcasts, multicasts and unicasts with unlearned destination addresses) and receiving unicasts with destination addresses established by the limitation,
- ▶ using the output limiter function instead of the input limiter function because the former works slightly better together with the TCP flow control due to switch-internal buffering.
- ▶ increasing the aging time for learned unicast addresses.

4.3.1 Rate limiter settings

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

Setting options per port:

- ▶ "Ingress Packet Types" allows you to select the packet type for which the limit is to apply:
 - ▶ ALL, limits the total ingress data volume at this port.
 - ▶ BC, limits the broadcast packets received at this port.
 - ▶ BC + MC, limits broadcast packets and multicast packets received on this port.
 - ▶ BC + MC + uUC, limits broadcast packets, multicast packets, and unknown unicast packets received on this port.
- ▶ "Ingress Limiter Rate (kbit/s)" for the ingress packet type selected:
 - ▶ = 0, no ingress limit at this port.
 - ▶ > 0, maximum ingress traffic rate in kbit/s that can be received on this port.
- ▶ "Egress Limit (Pkt/s)" for broadcast packets:
 - ▶ = 0, no rate limit for egress broadcast packets at this port.
 - ▶ > 0, maximum number of egress broadcasts per second that can be sent on this port.
- ▶ "Egress Limit (kbit/s)" for the entire data stream:
 - ▶ = 0, no rate limit for egress data stream at this port.
 - ▶ > 0, maximum egress traffic rate in kbit/s sent on this port.

Note: If applicable, the device rounds the values entered up to the next value that the hardware can process. After entering the values, to see which values the device actually uses, click "Set" and then "Reload".

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

Figure 33: Rate Limiter Dialog

■ Buttons

Button	Meaning
Set	Transfers the changes to the volatile memory (RAM) of the device. To permanently save the changes afterwards, you open the <code>Basic Settings:Load/Save</code> dialog and click "Save".
Reload	Updates the fields with the values that are saved in the volatile memory (RAM) of the device.
Help	Opens the online help.

Table 66: Buttons

4.4 Multicasts

4.4.1 IGMP (Internet Group Management Protocol)

With this dialog you can

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

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

Figure 34: IGMP Snooping dialog

■ Operation

In this frame you can:

- ▶ activate/deactivate the IGMP Snooping protocol.

Parameters	Meaning	Possible values	Default setting
Operation	Activate/deactivate IGMP Snooping globally for the device. If IGMP Snooping is switched off: <ul style="list-style-type: none"> ▶ 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. 	On Off	Off

Table 67: IGMP Snooping, global function

■ IGMP Querier and IGMP settings

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

Prerequisite: The IGMP Snooping function is activated globally.

Parameters	Meaning	Possible values	Default setting
IGMP Querier			
IGMP Querier active	Switch query function on/off	on off	off
Protocol Version	Select IGMP version 1, 2 or 3.	1, 2, 3	2
Transmit Interval [s]	Enter the interval at which the switch sends query packets. All IGMP-capable terminal devices respond to a query with a report message.	2-3599 s ^a	125 s
IGMP settings			
Current querier IP address	Display the IP address of the router/switch that has the query function.		

Table 68: IGMP Querier and IGMP settings

Parameters	Meaning	Possible values	Default setting
Max. Response Time	Enter the time within which the multicast group members are to respond to a query. The multicast group members select a random value within the response time for their response to prevent all multicast group members from responding to the query at the same time.	Protocol Version - 1, 2: 1-25 s - 3: 1-3598 s ^a	10 s
Group Membership Interval	Enter the period for which a dynamic Multicast group remains entered in the device if it does not receive any report messages.	3-3600 s ^a	260 s

Table 68: IGMP Querier and IGMP settings

- a. Note the connection between the parameters Max. Response Time, Transmit interval and Group Membership Interval ([see table 69.](#))

The parameters

- Max. Response Time,
- Transmit Interval and
- Group Membership Interval

have a relationship to one another:

Max. Response Time < Transmit Interval < Group Membership Interval.

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

Parameters	Protocol Version	Possible values	Default setting
Max. Response Time	1, 2 3	1-25 seconds 1-3,598 seconds	10 seconds
Transmit Interval	1, 2, 3	2-3,599 seconds	125 seconds
Group Membership Interval	1, 2, 3	3-3,600 seconds	260 seconds

Table 69: Value range for Max. Response Time, Transmit Interval and Group Membership Interval

For “Transmit interval” and “Max. Response Time”,

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

■ Multicasts

In this frame you specify how the device transmits packets with

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

Prerequisite: The IGMP Snooping function is activated globally.

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

Table 70: Known and unknown Multicasts

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

■ Settings per Port (Table)

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

Parameters	Meaning	Possible values	Default setting
Port	Module and port numbers to which this entry applies.	-	-
IGMP enabled	Switch IGMP on/off for each port. Switching IGMP off at a port prevents registration for this port. Prerequisite: The IGMP Snooping function is activated globally.	On Off	On
IGMP Forward All	Switch the IGMP Snooping function Forward All on/off. With the IGMP Forward All setting, the device sends to this port all data packets with a Multicast address in the destination address field. Prerequisite: The IGMP Snooping function is activated globally.	On Off	Off
<p>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.</p> <p>Note: If you use IGMP version 1 in a subnetwork, then you must also use IGMP version 1 in the entire network.</p>			
IGMP Automatic Query Port	Displays which ports the device has learned as query ports if <code>automatic</code> is selected in "Static Query Port". Prerequisite: The IGMP snooping function is activated globally.	yes, no	-

Table 71: Settings per port

Parameters	Meaning	Possible values	Default setting
Static Query Port	The device sends IGMP report messages to the ports at which it receives IGMP queries (default setting). This column allows you to also send IGMP report messages to: other selected ports (enable) or connected Hirschmann devices (automatic). Prerequisite: The IGMP snooping function is activated globally.	enable, disable, automatic	disable
Learned Query Port	Shows at which ports the device has received IGMP queries if “disable” is selected in “Static Query Port”. Prerequisite: The IGMP Snooping function is activated globally.	Yes No	-

Table 71: Settings per port

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

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

■ Buttons

Button	Meaning
Set	Transfers the changes to the volatile memory (RAM) of the device. To permanently save the changes afterwards, you open the <i>Basic Settings:Load/Save</i> dialog and click "Save".
Reload	Updates the fields with the values that are saved in the volatile memory (RAM) of the device.
Help	Opens the online help.

Table 72: Buttons

4.5 VLAN

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

4.5.1 VLAN Global

With this dialog you can:

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

Parameter	Meaning
Max. VLAN ID	Displays the biggest possible VLAN ID (see on page 133 “VLAN Static”)
Max. supported VLANs	Displays the maximum number of VLANs (see on page 133 “VLAN Static”).
Number of VLANs	Displays the number of VLANs configured (see on page 133 “VLAN Static”).

Table 73: VLAN Displays

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

Parameters	Meaning	Possible values	Default setting
VLAN 0 Transparent Mode	When the VLAN 0 Transparent Mode is activated, the device accepts a VLAN ID of 0 in the packet when it receives it, regardless of the setting for the port VLAN ID in the dialog (see on page 136 “Port”). Activate “VLAN 0 Transparent Mode” to transmit packets with a priority TAG without VLAN membership, i.e. with a VLAN ID of 0.	On, Off	Off
Double VLAN Tag Ethertype	Defines the value of the outer VLAN tag which a core port uses when sending a frame. The selectable values have the following meaning: – 0x8100 (802.1Q): VLAN tag – 0x88A8 (vman): Provider Bridging	0 - 65535	33024 (8100 _H)

Note: This setting is only effective for a core port. Access ports and normal ports ignore this setting and always use 8100_H.

Table 74: VLAN settings

Note: If you are using the GOOSE protocol in accordance with IEC61850-8-1, then you activate the “VLAN 0 transparent mode”. In this way, the prioritizing information remains in the data packet in accordance with IEEE802.1D/p when the device forwards the data packet. This also applies to other protocols that use this prioritizing in accordance with IEEE 802.1D/p, but do not require any VLANs according to IEEE 802.1Q.

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

- ▶ For RS20/RS30/RS40, MS20/MS30, RSR20/RSR30, MACH 100, MACH 1000 and OCTOPUS:
In “Transparent mode”, the devices ignore the port VLAN ID set. Set the VLAN membership of the ports of VLAN 1 to U (Untagged) or T (Tagged), ([see on page 133 “VLAN Static”](#)).

Parameters	Meaning	Possible values	Default setting
Mode	<p>Selecting the VLAN Mode. “Independent VLAN” subdivides the forwarding database (see on page 114 “Filter for MAC addresses”) virtually into one independent forwarding database per VLAN. The device cannot assign data packets with a destination address in another VLAN and it floods them to all the ports of the VLAN.</p> <p>Application area: Setting up identical networks that use the same MAC addresses. “Shared VLAN” uses the same forwarding database for all VLANs (see on page 114 “Filter 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.</p> <p>Application area: In the case of overlapping groups, the device can distribute directly across VLANs, as long as the ports involved belong to a VLAN that can be reached. Changes to the mode are only applied after a warm start (see on page 55 “Restart”) is performed on the device, and the changes are then displayed in the line below under “Status”.</p>	Independent VLAN, Shared VLAN	Independent VLAN
Status	Displays the current status. After a warm start (see on page 55 “Restart”) on the device, the device take the setting for the “Mode” into the status line.	Independent VLAN, Shared VLAN	

Table 75: Settings and displays in the “Learning” frame

Figure 35: VLAN Global dialog

■ Buttons

Button	Meaning
Set	Transfers the changes to the volatile memory (RAM) of the device. To permanently save the changes afterwards, you open the <code>Basic Settings:Load/Save</code> dialog and click "Save".
Reload	Updates the fields with the values that are saved in the volatile memory (RAM) of the device.
Clear...	Resets the VLAN settings of the device to the state on delivery. Caution: You block your access to the device if you have changed the VLAN ID for the management functions of the device in the <code>Basic Settings:Network</code> dialog.
Help	Opens the online help.

Table 76: Buttons

4.5.2 Current VLAN

This dialog gives you the option of displaying the current VLAN parameters

The Current VLAN table shows all

- ▶ manually configured VLANs
- ▶ VLANs configured via redundancy mechanisms

The Current VLAN Table is only used for display purposes. You can make changes to the entries in the `VLAN:Static` dialog ([see on page 133 “VLAN Static”](#)).

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

Table 77: Current VLAN

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

Buttons: Reload, Help

Figure 36: Current VLAN dialog

■ Buttons

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

Table 78: Buttons

4.5.3 VLAN Static

With this dialog you can:

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

Parameters	Meaning	Possible values	Default setting
VLAN ID	Displays the ID of up to 255 VLANs that are simultaneously possible.	1-4042	
Name	Enter the name of your choice for this VLAN.	Maximum 32 characters	VLAN 1: default
Ports x.x	Select the membership of the ports to the VLANs.	-: currently not a member (GVRP allowed). T: Member of the VLAN; send data packets with tag (tagged). U: Member of the VLAN; send data packets without tag (untagged). F: Membership forbidden, so no entry possible via GVRP either.	VLAN 1: U, new VLANs: -

Table 79: VLAN Static dialog

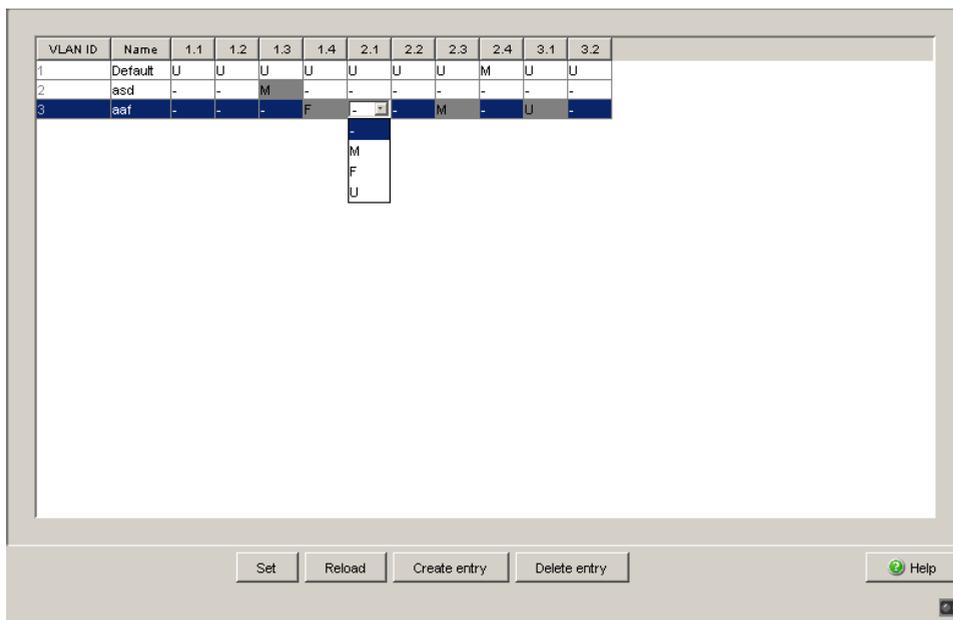


Figure 37: VLAN Static Dialog

Note: When configuring the VLAN, ensure that the management station still has access to the device after the VLAN configuration is saved. Connect the management station to a port that is a member of the VLAN that is selected as the management VLAN. In the state on delivery, the device transmits the management data in VLAN 1.

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

Note: Note the tagging settings for ports that are part of a redundant Ring or of the Ring/network coupling.

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

Table 80: Required VLAN settings for ports that are part of redundant Rings or Ring/Network coupling.

Note: In a redundant ring with VLANs, you should only operate devices whose software version supports VLANs:

- ▶ RS2 xx/xx (from rel. 7.00)
- ▶ RS2-16M
- ▶ RS20, RS30, RS40 (with software variants L2E, L2P)
- ▶ MICE (from rel. 3.0)
- ▶ PowerMICE
- ▶ MS20, MS30
- ▶ RSR20, RSR30
- ▶ MACH 100
- ▶ MACH 1000
- ▶ MACH 4000
- ▶ MACH 3000 (from Rel. 3.3),
- ▶ OCTOPUS

■ Buttons

Button	Meaning
Set	Transfers the changes to the volatile memory (RAM) of the device. To permanently save the changes afterwards, you open the <code>Basic Settings:Load/Save</code> dialog and click "Save".
Reload	Updates the fields with the values that are saved in the volatile memory (RAM) of the device.
Create	Adds a new table entry.
Remove	Removes the selected table entry.
Help	Opens the online help.

Table 81: Buttons

4.5.4 Port

With this dialog you can:

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

Parameters	Meaning	Possible values	Default setting
Port	Port to which this entry applies.		
Port VLAN ID	Specifies which VLAN the port assigns a received, untagged data packet to.	All allowed VLAN IDs	1
Acceptable Frame Types	Specifies whether the port can also receive untagged data packets. admitAll: The device accepts frames received on this port and assigns untagged or Priority-tagged frames to the port PVID. admitOnlyVlanTagged: The device discards untagged frames received on this port. admitOnlyUntagged: The device discards frames with a VLAN tag. This value is available on MS, RS, Octopus, MACH102, MACH1020/30, and RSR devices.	admitAll admitOnlyVlanTagged admitOnlyUntagged	admitAll

Table 82: *Switching:VLAN:Port dialog*

Parameters	Meaning	Possible values	Default setting
Ingress Filtering	Specifies whether the port evaluates the received tags.	on, off	off
DVLAN Tag Mode	<p>- normal: The port is not involved in DVLAN tagging.</p> <p>- core: The port sends a double-tagged frame with the Ether type selected under “Double VLAN Ether type”. For this, you include the port as a tagged member in all tunnel VLANs.</p> <p>- access: The port assigns its port VLAN ID to a received frame, even for an already tagged frame. The port sends the originally received frame back out (tagged or untagged). You assign the port the tunnel VLAN ID as port VLAN ID and include it as an untagged member in this VLAN.</p>	normal, core, access	normal

Table 82: Switching:VLAN:Port dialog

Note: Note the following:

- ▶ **HIPER-Ring**
Select the port VLAN ID 1 for the ring ports and deactivate “Ingress Filtering”.
- ▶ **MRP-Ring**
 - If the MRP-Ring configuration ([see on page 158 “Configuring the MRP-Ring”](#)) is not assigned to a VLAN, select the port VLAN ID 1.
 - If the MRP-Ring configuration ([see on page 158 “Configuring the MRP-Ring”](#)) is assigned to a VLAN, the device automatically performs the VLAN configuration for this port.
- ▶ **Network/Ring coupling**
Select the VLAN ID 1 for the coupling and partner coupling ports and deactivate “Ingress Filtering”.

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

Figure 38: Switching:VLAN:Port dialog

■ Buttons

Button	Meaning
Set	Transfers the changes to the volatile memory (RAM) of the device. To permanently save the changes afterwards, you open the Basic Settings:Load/Save dialog and click "Save".
Reload	Updates the fields with the values that are saved in the volatile memory (RAM) of the device.
Help	Opens the online help.

Table 83: Buttons

5 QoS/Priority

The device enables you to set

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

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

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

5.1 Global

With this dialog you can:

- ▶ enter the VLAN priority for management packets in the range 0 to 7 (default setting: 0).
In order for you to have full access to the management of the device, even when there is a high network load, the device enables you to prioritize management packets.
In prioritizing management packets (SNMP, Telnet, etc.), the device sends the management packets with priority information.
Note the assignment of the VLAN priority to the traffic class ([see table 89](#)).
- ▶ 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 87](#)).

Note: Certain DSCP values have DSCP names, such as be/cs0 to cs7 (class selector) or af11 to af43 (assured forwarding) and ef (expedited forwarding).

- ▶ display the maximum number of queues possible per port.
The device supports 4 (8 for MACH 4000, MACH 104, MACH 1040 and PowerMICE) priority queues (traffic classes in compliance with IEEE 802.1D).
- ▶ select the trust mode globally. You use this to specify how the device handles received data packets that contain priority information.
 - ▶ “untrusted”
The device ignores the priority information in the packet and always assigns the packets the port priority of the receiving port.
 - ▶ “trustDot1p”:
The device prioritizes received packets that contain VLAN tag information according to this information (assigning them to a traffic class - see [“802.1D/p mapping”](#)).
The device prioritizes received packets that do not contain any tag information (assigning them to a traffic class - see [“Entering the port priority”](#)) according to the port priority of the receiving port .
 - ▶ “trustIpDscp”:
The device prioritizes received IP packets (assigning them to a traffic class - see [“IP DSCP mapping”](#)) according to their DSCP value.
The device prioritizes received packets that are not IP packets (assigning them to a traffic class - see [“Entering the port priority”](#)) according to the port priority of the receiving port .
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 133 “VLAN Static”](#)).
Based on the traffic class to which the IP packet was assigned (see above), the device assigns the new VLAN priority to the IP packet in accordance with [table 91](#).
Example: A received IP packet with a DSCP value of 32 (cs4) is assigned to traffic class 2 (default setting). The packet was received at a port with port priority 2. Based on [table 91](#), the VLAN priority is set to 4.

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

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

Traffic class	New VLAN priority when receiving port has an even port priority	New VLAN priority when receiving port has an odd port priority
0	0	1
1	2	3
2	4	5
3	6	7

Table 84: VLAN priority remarking

VLAN Priority for Management packets: 0

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

Number of Queues per Port: 4

Trust Mode: trustDot1p

Buttons: Set, Reload, Help

Figure 39: Global dialog

■ Buttons

Button	Meaning
Set	Transfers the changes to the volatile memory (RAM) of the device. To permanently save the changes afterwards, you open the <code>Basic Settings:Load/Save</code> dialog and click "Save".
Reload	Updates the fields with the values that are saved in the volatile memory (RAM) of the device.
Help	Opens the online help.

Table 85: Buttons

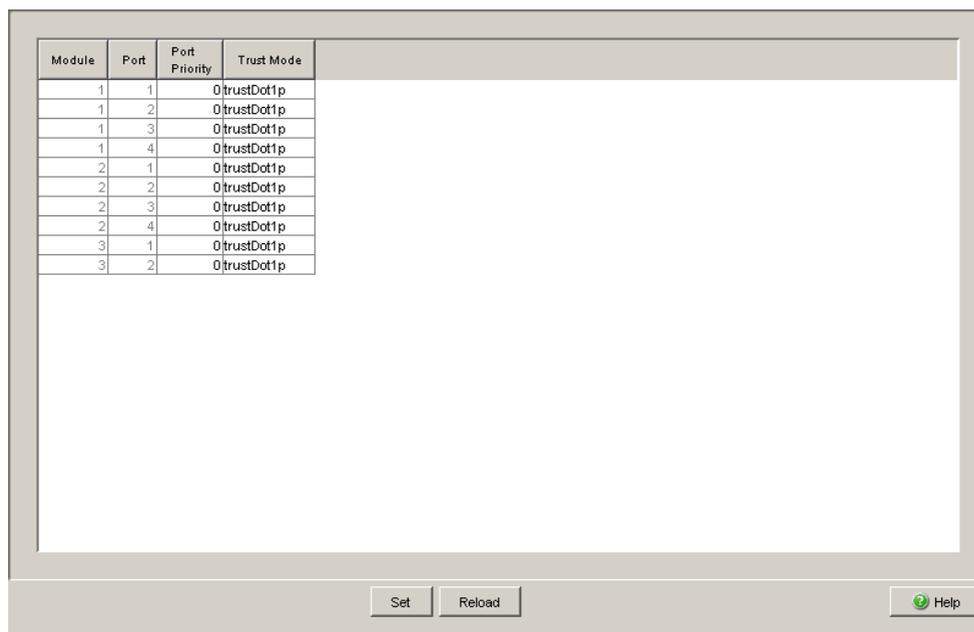
5.2 Port Configuration

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

- assign a port priority to a port.

Parameter	Meaning
Module.Port	Port identification using module and port numbers of the device, e.g. 2.1 for port one of module two.
Port priority	Enter the port priority.

Table 86: Port configuration table



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

Figure 40: Port configuration dialog

5.2.1 Entering the port priority

- Double-click a cell in the “Port priority” column and enter the priority (0-7). According to the priority entered, the device assigns the data packets that it receives at this port to a traffic class (see table 87).

Prerequisite:

Setting in the dialog `Global: Trust Mode: untrusted` (see on page 140 “Global”) or

Setting in the dialog `Global: Trust Mode: trustDot1p` (see on page 140 “Global”) and the data packets do not contain a VLAN tag or

Setting in the dialog `Global: Trust Mode: trustIpDscp` (see on page 140 “Global”) and the data packets are not IP packets.

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

Table 87: Assigning the port priority to the 4 traffic classes

■ Buttons

Button	Meaning
Set	Transfers the changes to the volatile memory (RAM) of the device. To permanently save the changes afterwards, you open the <code>Basic Settings:Load/Save</code> dialog and click "Save".
Reload	Updates the fields with the values that are saved in the volatile memory (RAM) of the device.
Help	Opens the online help.

Table 88: Buttons

5.3 802.1D/p mapping

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

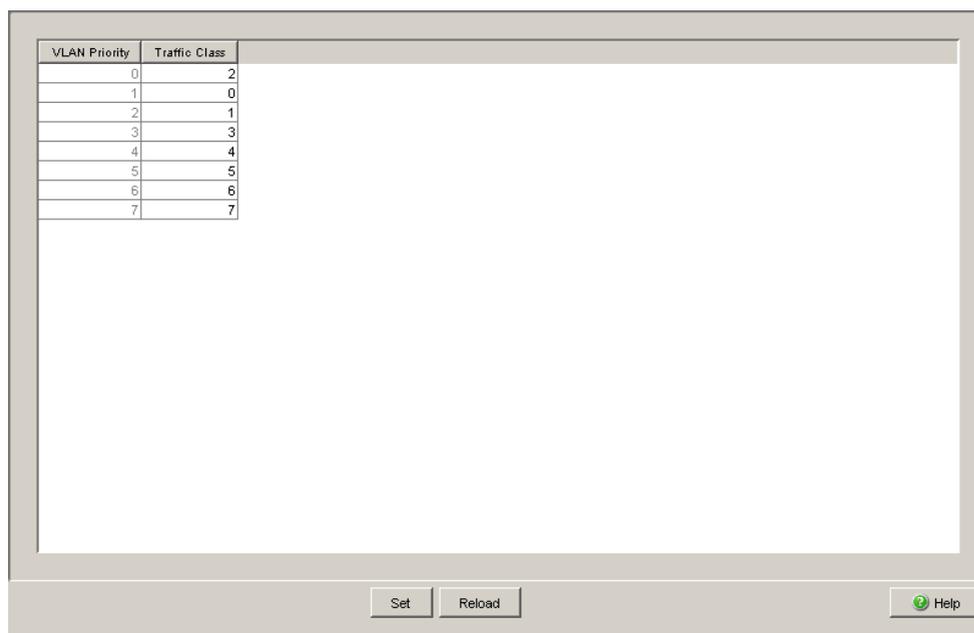


Figure 41: 802.1D/p Mapping dialog

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

Port priority	Traffic class (default setting)	IEEE 802.1D traffic type
0	1	Best effort (default)
1	0	Background

Table 89: Assigning the VLAN priority to the 4 traffic classes

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

Table 89: Assigning the VLAN priority to the 4 traffic classes

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

■ Buttons

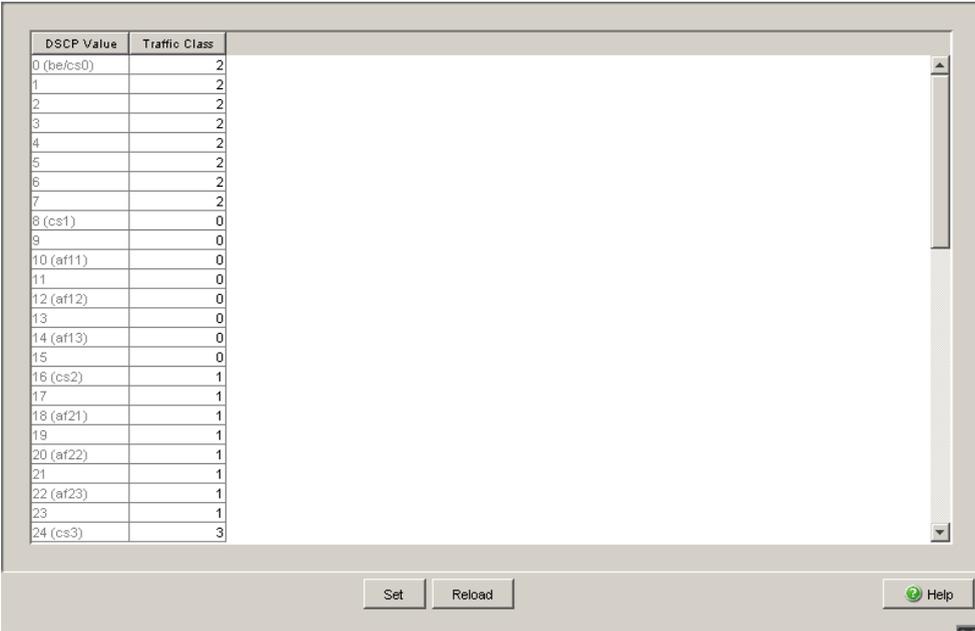
Button	Meaning
Set	Transfers the changes to the volatile memory (RAM) of the device. To permanently save the changes afterwards, you open the <code>Basic Settings:Load/Save</code> dialog and click "Save".
Reload	Updates the fields with the values that are saved in the volatile memory (RAM) of the device.
Help	Opens the online help.

Table 90: Buttons

5.4 IP DSCP mapping

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

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



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

Figure 42: IP DSCP mapping table

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

PHB classes:

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

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

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

Table 91: Mapping the DSCP values onto the traffic classes

■ Buttons

Button	Meaning
Set	Transfers the changes to the volatile memory (RAM) of the device. To permanently save the changes afterwards, you open the <code>Basic Settings:Load/Save</code> dialog and click "Save".

Table 92: Buttons

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

Table 92: Buttons (cont.)

6 Redundancy

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

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

Note: The “Redundancy Configuration User Manual” document contains detailed information that you require to select the suitable redundancy procedure and configure it.

6.1 Ring Redundancy

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

If a section is down, the ring structure of a

- ▶ **HIPER-(HIGH PERFORMANCE REDUNDANCY)** Ring with up to 50 devices typically transforms back to a line structure within 80 ms (possible settings: standard/accelerated).
- ▶ **MRP (Media Redundancy Protocol)** Ring (IEC 62439) of up to 50 devices typically transforms back to a line structure within 80 ms (adjustable to max. 200 ms/500 ms).

With the aid of a device's **Ring Manager (RM)** function you can close both ends of a backbone in a line-type configuration to form a redundant ring.

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

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

- ▶ Select one of the available Ring Redundancy versions, or change it.
- ▶ Display an overview of the current Ring Redundancy configuration.

- ▶ Create new Ring Redundancies.
- ▶ Configure existing Ring Redundancies.
- ▶ Enable/disable the Ring Manager function.
- ▶ Receive Ring information.
- ▶ Delete the Ring Redundancy.

Note: Only one Ring Redundancy method can be enabled on one device at any one time. When changing to another Ring Redundancy method, deactivate the function for the time being.

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

Table 93: Ring Redundancy basic configuration

6.1.1 Configuring the HIPER-Ring

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

Port type	Bit rate	Autonegotiation (automatic configuration)	Port setting	Duplex
TX	100 Mbit/s	off	on	100 Mbit/s full duplex (FDX)
TX	1 Gbit/s	on	on	-
Optical	100 Mbit/s	off	on	100 Mbit/s full duplex (FDX)
Optical	1 Gbit/s	on	on	-

Table 94: Port settings for ring ports

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

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

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

Table 95: HIPER-Ring configuration

The screenshot shows a configuration window for Ring Redundancy. At the top, there are radio buttons for 'HIPER-Ring' and 'MRP', with 'MRP' selected. Below this are two columns for 'Ring Port 1' and 'Ring Port 2', each containing input fields for 'Module', 'Port', and 'Operation'. The 'Configuration Redundancy Manager' section has a checkbox for 'Advanced Mode'. The 'Redundancy Manager' section has radio buttons for 'Mode On' and 'Mode Off', with 'Mode Off' selected. The 'Operation' section has radio buttons for 'On' and 'Off', with 'Off' selected. The 'Ring Recovery' section has radio buttons for '500ms' and '200ms', with '200ms' selected. There is a 'VLAN' section with a 'VLAN ID' input field. At the bottom, there are buttons for 'Set', 'Reload', 'Delete ring configuration', and 'Help'.

Figure 43: Selecting ring redundancy, entering ring ports, enabling/disabling ring manager and selecting ring recovery.

Note: Deactivate the Spanning Tree protocol (STP) for the ports connected to the redundant ring, because the Spanning Tree and the Ring Redundancy work with different reaction times (`Redundancy:Spanning Tree:Port`). If you used the DIP switch to activate the HIPER-Ring function, STP is automatically switched off.

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

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

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

Note: If you are also using redundant ring/network coupling, make sure that the device is transmitting VLAN 1 packets tagged on the two ring ports.

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

6.1.2 Configuring the MRP-Ring

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

Port type	Bit rate	Autonegotiation (automatic configuration)	Port setting	Duplex
TX	100 Mbit/s	off	on	100 Mbit/s full duplex (FDX)
TX	1 Gbit/s	on	on	-
Optical	100 Mbit/s	off	on	100 Mbit/s full duplex (FDX)
Optical	1 Gbit/s	on	on	-

Table 96: Port settings for ring ports

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

Note: If you have configured VLANs and you want to assign the MRP-Ring configuration to a VLAN.

- Select a VLAN-ID > 0 in the `VLAN` field in the `Redundancy:Ring Redundancy` dialog. Select this VLAN ID in the MRP-Ring configuration for all devices in this MRP-Ring.
- Check the VLAN configuration of the ring ports: For all ring ports in this MRP-Ring, select this corresponding VLAN ID and the VLAN membership `T` in the static VLAN table.
- Avoid the VLAN ID = 0.

Note: If you are also using redundant ring/network coupling, make sure that the device is transmitting VLAN 1 packets tagged on the two ring ports.

Parameter	Meaning
Ring port X.X operation	Display in “Operation” field: <i>forwarding</i> : This port is switched on and has a link. <i>blocked</i> : This port is blocked and has a link. <i>disabled</i> : This port is switched off. <i>not connected</i> : This port has no link.
Ring Manager Configuration	Deactivate the advanced mode if a device in the ring does not support the advanced mode for fast switching times. Otherwise you activate the advanced mode.
Note: All Hirschmann devices that support the MRP-Ring also support the advanced mode.	
Operation	When you have configured all the parameters for the MRP-Ring, you switch the operation on with this setting. When you have configured all the devices in the MRP-Ring, you close the redundant line.
Ring Recovery	For the device for which you have activated the ring manager, select the value 200 ms if the stability of the ring meets the requirements for your network. Otherwise select 500 ms. <i>Note</i> : Settings in the “Ring Recovery” frame are only effective for devices that are ring managers.
VLAN ID	If you have configured VLANs, then here you select: <ul style="list-style-type: none"> ▶ <i>VLAN ID 0</i> if you do not want to assign the MRP-Ring configuration to any VLAN. Note the VLAN configuration of the ring ports: Select VLAN ID 1 and VLAN membership <i>U</i> in the static VLAN table for the ring ports. ▶ <i>VLAN ID > 0</i> if you want to assign the MRP-Ring configuration to this VLAN. Select this VLAN ID in the MRP-Ring configuration for all devices in this MRP-Ring. Note the VLAN configuration of the ring ports: For all ring ports in this MRP-Ring, select this corresponding VLAN ID and the VLAN membership <i>T</i> in the static VLAN table.
Information	If the device is a ring manager: The displays in this frame mean: “Redundancy working”: When a component of the ring is down, the redundant line takes over its function. “Configuration failure”: You have configured the function incorrectly, or there is no ring port connection.

Table 97: MRP-Ring configuration

Version
 HIPER-Ring MRP

Ring Port 1
Module: 1
Port: 1
Operation: []

Ring Port 2
Module: 1
Port: 2
Operation: []

Configuration Redundancy Manager
 Advanced Mode

Redundancy Manager
Mode: On Off

Operation: On Off

Ring Recovery: 500ms 200ms

VLAN
VLAN ID: 1

Information

Set Reload Delete ring configuration Help

Figure 44: Selecting MRP-Ring version, entering ring ports and enabling/disabling ring manager

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

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

■ Buttons

Button	Meaning
Set	Transfers the changes to the volatile memory (RAM) of the device. To permanently save the changes, open the <code>Basic Settings:Load/Save</code> dialog, select the location to save the configuration, and click "Save".
Reload	Updates the fields with the values that are saved in the volatile memory (RAM) of the device.
Delete ring configuration	Switches off the redundancy function and resets all the settings in the dialog to the state on delivery.
Help	Opens the online help.

Table 98: Buttons

6.2 Ring/Network Coupling

Use the ring/network coupling to redundantly couple an existing ring (HIPER-Ring, MRP, Fast HIPER-Ring) to another network or another ring. Make sure the coupling partners are Hirschmann devices.

Note: Two-Switch coupling

Make sure you have configured a ring (HIPER-Ring, MRP, Fast HIPER-Ring) before setting up the ring/network coupling.

With this dialog you can:

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

6.2.1 Preparing a Ring/Network Coupling

■ **STAND-BY switch**

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

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

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

Device type	STAND-BY switch type
RS2-./.	DIP switch
RS2-16M	DIP switch
RS20/RS30/RS40	Selectable: DIP switch and software setting
MS20/MS30	Selectable: DIP switch and software setting

Table 99: Overview of the STAND-BY switch types

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

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

Table 100: Setting the STAND-BY switch

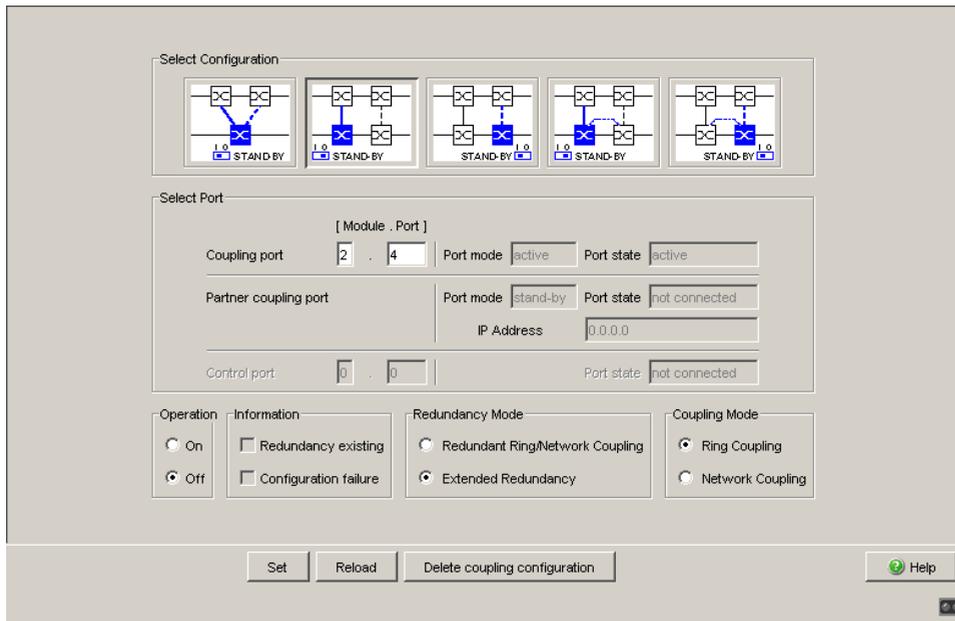


Figure 45: Software configuration of the STAND-BY switch

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

One-Switch coupling

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

Two-Switch coupling

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

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

■ Ring/Network Coupling dialog

Parameter	Meaning
Selecting the configuration	<p>Depending on your local conditions, select “One-Switch coupling”, “Two-Switch coupling, Slave”, “Two-Switch coupling, Master”, “Two-Switch coupling with control line, Slave” or “Two-Switch coupling with control line, Master”. These options are presented as buttons from left to right.</p> <p>Depending on the device type (see table 99), you make this setting:</p> <ul style="list-style-type: none"> – only using DIP switches – only using software – using DIP switch and software <p>You will find details on the DIP switches on the devices in the “Installation” user manual.</p> <ul style="list-style-type: none"> – For devices configured only using DIP switches, you use these switches to make the settings. In this case, the buttons in the dialog are only for display purposes. – For devices without DIP switches, you only use the software to make settings. You can select the configuration using the buttons. – For devices that can be configured using DIP switches and software, you can activate or deactivate the DIP switches. If you have activated the DIP switches, you cannot overwrite the DIP switch settings using the software - settings that cannot be selected using the software are grayed-out in the dialog. <p>To configure using the software, select the relevant Ring/Network coupling constellation by pressing the corresponding button.</p>
Coupling port	<p>This is the port to which you have connected a redundant connection.</p> <p>Note: Configure the coupling port and the ring ports, if there are any ring ports, on different ports.</p> <p>Note: To avoid continuous loops, the device sets the port status of the coupling port to “off” if you switch off the function or change the configuration while the connections are operating at these ports.</p>
Port mode	<ul style="list-style-type: none"> - <code>active</code>: You have switched the port on. - <code>stand-by</code>: The port is in stand-by mode.
Port State	<ul style="list-style-type: none"> - <code>active</code>: You have switched the port on. - <code>stand-by</code>: The port is in stand-by mode. - <code>not connected</code>: You have not connected the port.
Partner coupling port	<p>This is the port at which the partner has made its connection. It is only possible and necessary to enter a port if “One-Switch coupling” is being set up.</p> <p>Note: Configure the partner coupling port and the ring ports, if there are any ring ports, on different ports.</p>
IP address	<p>If you have selected “Two-Switch coupling”, the device displays the IP address of the partner here, once you have already started operating the partner in the network.</p>
Control port	<p>This is the port to which you connect the control line.</p>

Table 101: Ring/Network Coupling dialog

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

Table 101: Ring/Network Coupling dialog

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

Port type	Bit rate	Autonegotiation (automatic configuration)	Port setting	Duplex
TX	100 Mbit/s	off	on	100 Mbit/s full duplex (FDX)
TX	1 Gbit/s	on	on	-
Optical	100 Mbit/s	off	on	100 Mbit/s full duplex (FDX)
Optical	1 Gbit/s	on	on	-

Table 102: Port settings for ring ports

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

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

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

Note: Independently of the VLAN settings, the device sends the ring coupling frames with VLAN ID 1 and priority 7. Make sure that the device sends VLAN 1 packets tagged in the local ring and in the connected network. This maintains the priority of the ring coupling frames.

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

Note: The Ring/Network coupling operates with test packets (Layer 2 frames). The devices subscribed always send their test packets VLAN-tagged, including the VLAN ID 1 and the highest VLAN priority 7. This also applies if the send port is an untagged member in VLAN 1.

■ Buttons

Button	Meaning
Set	Transfers the changes to the volatile memory (RAM) of the device. To permanently save the changes, open the <code>Basic Settings:Load/Save</code> dialog, select the location to save the configuration, and click "Save".
Reload	Updates the fields with the values that are saved in the volatile memory (RAM) of the device.
Delete Coupling configuration	Removes the coupling configuration.
Help	Opens the online help.

Table 103: Buttons

6.3 Spanning Tree

Under Spanning Tree you will find the dialogs and views for configuring and monitoring of the Spanning Tree function according to the IEEE 802.1Q-2005 standard, Rapid Spanning Tree (RSTP).

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

Introduction

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

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

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

Rapid Spanning Tree Protocol (RSTP)

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

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

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

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

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

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

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

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

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

Note: The following text uses the term Spanning Tree (STP) to describe settings or behavior that applies to STP, RSTP or MSTP.

6.3.1 Global

With this dialog you can:

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

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

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

Parameter	Meaning	Possible values	Default settings
Frame „Function“	Switches the Spanning Tree function for this device “On” or “Off”. If you switch off the Spanning Tree for a device globally, the device floods the Spanning Tree packets received like normal Multicast packets to the ports. Thus the device behaves transparently with regard to Spanning Tree packets.	On, Off	On

Table 104: Global Spanning Tree settings, basic function

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

Parameter	Meaning	Possible values	Default settings
Column „Bridge“	Information and configuration parameters of the local device		
Bridge ID (read only)	The local Bridge ID, made up of the local priority and its own MAC address. The format is ppppp / mm mm mm mm mm mm, with: ppppp: priority (decimal) and mm: the respective byte of the MAC address (hexadecimal).		
Priority	Sets the local bridge priority. The bridge priority and its own MAC address make up this separate Bridge ID. The device with the best (numerically lowest) priority assumes the role of the root bridge. Define the root device by assigning the device the best priority in the Bridge ID among all the devices in the network. Enter the value as a multiple of 4096.	$0 \leq n \cdot 4096 \leq$ 61440	32768

Table 105: Global Spanning Tree settings, local bridge parameters

Parameter	Meaning	Possible values	Default setting
Hello Time	Sets the Hello Time. The local <code>Hello Time</code> is the time in seconds between the sending of two configuration messages (Hello packets). If the local device has the root function, the other devices in the entire network take over this value. Otherwise the local device uses the value of the root bridge in the "Root" column on the right.	1 - 2	2
Forward Delay	Sets the Forward Delay parameter. In the previous STP protocol, the Forward Delay parameter was used to delay the status change between the statuses <code>disabled</code> , <code>discarding</code> , <code>learning</code> , and <code>forwarding</code> . Since the introduction of RSTP, this parameter has a subordinate role, because the RSTP bridges negotiate the status change without any specified delay. If the local device is the root, the other devices in the entire network take over this value. Otherwise the local device uses the value of the root bridge in the "Root" column on the right.	4 - 30 s See the note following this table.	15 s
Max Age	Sets the Max Age parameter. In the previous STP protocol, the Max Age parameter was used to specify the validity of STP BPDUs in seconds. For RSTP, Max Age signifies the maximum permissible branch length (number of devices to the root bridge). If the local device is the root, the other devices in the entire network take over this value. Otherwise the local device uses the value of the root bridge in the "Root" column on the right.	6 - 40 s See the note following this table.	20 s
Tx Hold Count	Sets the Hx Hold Count parameter. If the device sends a BPDU, it increments a counter at this port. When the counter reaches the value of the Tx Hold Count, the port stops sending any more BPDUs. The counter is decremented by 1 every second. The device sends a maximum of 1 new BPDU in the following second.	1 - 40 (based on RSTP standard: 1 - 10)	10

Table 105: Global Spanning Tree settings, local bridge parameters

Parameter	Meaning	Possible values	Default setting
MRP compatibility	Switches the MRP compatibility on/off. MRP compatibility enables RSTP to be used within an MRP-Ring and when coupling RSTP segments to an MRP-Ring. The prerequisite is that all devices in the MRP-Ring must support MRP compatibility.	On, Off	Off
BPDU Guard	Switches the BPDU Guard function on/off. If BPDU Guard is switched on, the device automatically activates the function for edge ports (with the setting “Admin Edge Port” true). When such a port receives any STP-BPDU, the device sets the port status “BPDU Guard Effect” to true and the transmission status of the port to discarding(see table 111). Thus the device helps you protect your network at terminal device ports from incorrect configurations or attacks with STP-BPDUs that try to change the topology.	On, Off	Off

Table 105: Global Spanning Tree settings, local bridge parameters

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

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

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

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

Parameter s	Meaning	Possible values	Default setting
Column „Root“	Information on the device that is currently the root bridge		
Bridge ID	The <code>Bridge ID</code> of the current root bridge. The format is ppppp / mm mm mm mm mm mm, with: ppppp: priority (decimal) and mm: the respective byte of the MAC address (hexadecimal).		
Priority	The <code>Priority</code> of the current root bridge.	$0 \leq n * 4096 \leq 61440$	32768
Hello Time	The <code>Hello Time</code> of the current root bridge.	1 - 2	2
Forward Delay	The <code>Forward Delay</code> of the current root bridge.	4 - 30 s	15 s
Max Age	The <code>Max Age</code> of the current root bridge.	6 - 40 s	20 s

Table 106: Global Spanning Tree settings, root bridge information

Parameters	Meaning	Possible values
Column „Topology“	Spanning Tree topology information	
Bridge is root	If the local device is currently the root bridge, the device displays this box as selected, and otherwise as empty.	Selected, not selected.
Root Port	The port of the device from which the current path leads to the root bridge. 0: the local bridge is the root.	Valid port ID or 0.
Root path costs	Path costs from the root port of the device to the current root bridge of the entire layer 2 network. 0: the local bridge is the root.	0-200000000
Topology change count	Counts how often the device has put a port into the <code>Forwarding</code> status via Spanning Tree since it was started.	
Time since last change	Time since the last topology change.	

Table 107: Global Spanning Tree settings, topology information

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

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

Table 108: Global Spanning Tree settings, Information frame

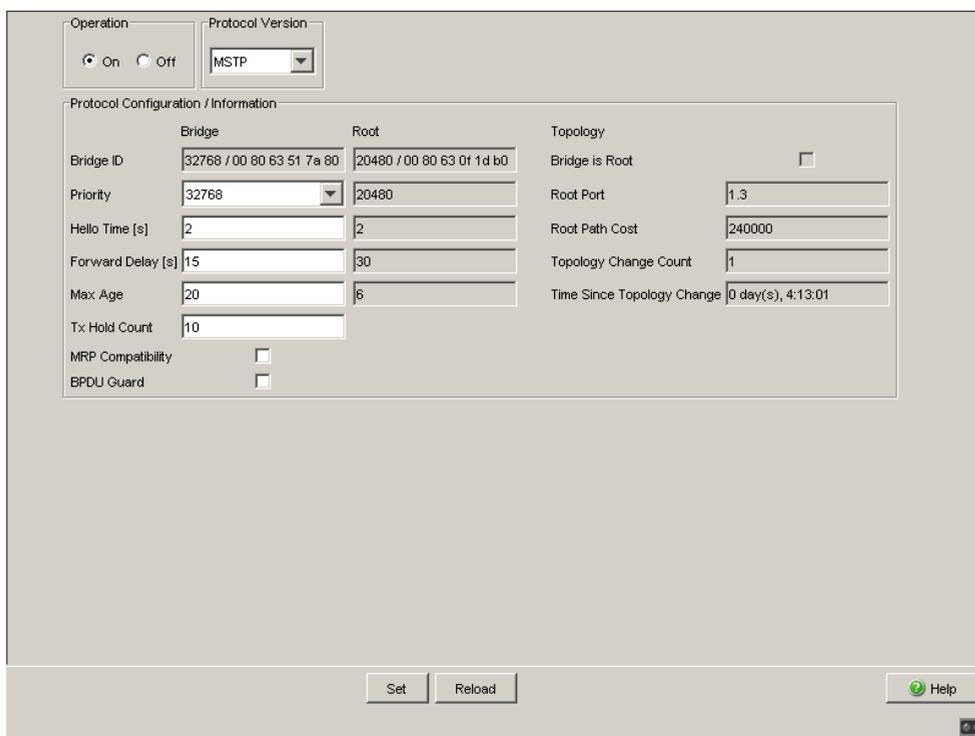


Figure 46: Dialog Spanning Tree, Global

■ Buttons

Button	Meaning
Set	Transfers the changes to the volatile memory (RAM) of the device. To permanently save the changes, open the <code>Basic Settings:Load/Save</code> dialog, select the location to save the configuration, and click "Save".
Reload	Updates the fields with the values that are saved in the volatile memory (RAM) of the device.
Help	Opens the online help.

Table 109: Buttons

6.3.2 Port

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

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

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

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

Parameters	Meaning	Possible values	Default setting
Tab „CIST“	Port configuration and information on the global MSTI (IST) and the CST.		
Module.Port	Port identification using module and port numbers of the device, e.g. 2.1 for port one of module two.		
STP active	Here you can switch Spanning Tree on or off for this port. If Spanning Tree is activated globally and switched off at one port, this port does not send STP-BPDUs and drops any STP-BPDUs received.	On, Off	On
	<p>Note: If you want to use other layer 2 redundancy protocols such as HIPER-Ring or Ring/Network coupling in parallel with Spanning Tree, make sure you switch off the ports participating in these protocols in this dialog for Spanning Tree. Otherwise the redundancy may not operate as intended or loops can result.</p>		
Port status (read only)	Displays the STP port status with regard to the global MSTI (IST).	discarding, learning, forwarding, disabled, manualForwarding, notParticipate	-
Port Role (read only)	Displays the STP port role with regard to the global MSTI (IST).	root alternate designated backup master disabled	-

Table 110: Port-related STP settings and displays, CIST

Parameters	Meaning	Possible values	Default setting
Port path costs	Enter the path costs with regard to the global MSTI (IST) to indicate preference for redundant paths. If the value is 0, the Switch automatically calculates the path costs for the global MSTI (IST) depending on the transmission rate.	0 - 200000000	0 (automatically)
Port priority	Here you enter the port priority (the four highest bits of the port ID) with regard to the global MSTI (IST) as a decimal number of the highest byte of the port ID.	$16 \leq n \cdot 16 \leq 240$	128
Received bridge ID (read only)	Displays the remote bridge ID from which this port last received an STP-BPDU. ^a	Bridge identification (format ppppp / mm mm mm mm mm mm)	-
Received port ID (read only)	Displays the port ID at the remote bridge from which this port last received an STP-BPDU. ^a	Port ID, format pn nn, with p: port priority / 16, nnn: port No., (both hexadecimal)	-
Received path costs (read only)	Displays the path costs of the remote bridge from its root port to the CIST root bridge. ^a	0-200000000	-
Admin Edge Port	Only activate this setting when a terminal device is connected to the port (administrative: default setting). Then the port immediately has the forwarding status after a link is set up, without first going through the STP statuses. If the port still receives an STP-BPDU, the device blocks the port and clarifies its STP port role. In the process, the port can switch to a different status, e.g. forwarding, discarding, learning. Deactivate the setting when the port is connected to a bridge. After a link is set up, the port then goes through the STP statuses first before taking on the forwarding status, if applicable. This setting applies to all MSTIs.	active (box selected), inactive (box empty)	inactive

Table 110: Port-related STP settings and displays, CIST

Parameters	Meaning	Possible values	Default setting
Auto Edge Port	The device only considers the Auto Edge Port setting when the Admin Edge Port parameter is deactivated. If Auto Edge Port is active, after a link is set up the device sets the port to the forwarding status after $1.5 \cdot \text{Hello Time}$ (in the default setting 3 s). If Auto Edge Port is deactivated, the device waits for the <code>Max Age</code> instead (in the default setting 20 s). This setting applies to all MSTIs.	<code>active</code> (box selected), <code>inactive</code> (box empty)	<code>active</code>
Oper Edge Port	The device sets the “Oper Edge Port” condition to <code>true</code> if it has not received any STP-BPDUs, i.e. a terminal device is connected. It sets the condition to <code>false</code> if it has received STP-BPDUs, i.e. a bridge is connected. This condition applies to all MSTIs.	<code>true</code> , <code>false</code>	-
Oper PointToPoint	The device sets the “Oper point-to-point” condition to <code>true</code> if this port has a full duplex condition to an STP device. Otherwise it sets the condition to <code>false</code> (e.g. if a hub is connected). The point-to-point connection makes a direct connection between 2 RSTP devices. The direct, decentralized communication between the two bridges results in a short reconfiguration time. This condition applies to all MSTIs.	<code>true</code> , <code>false</code> The device determines this condition from the duplex mode: FDX: <code>true</code> HDX: <code>false</code>	

Table 110: Port-related STP settings and displays, CIST

- ^a These columns show you more detailed information than that available up to now:
For designated ports, the device displays the information for the STP-BPDU last received by the port. This helps with the diagnosis of possible STP problems in the network.
For the port roles alternative, back-up, master and root, in the stationary

condition (static topology), this information is identically to the designated information.

If a port has no link, or if it has not received any STP-BDPUs for the current MSTI, the device displays the values that the port would send as a designated port.

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

Figure 47: Multiple Spanning Tree dialog, Port, CIST tab

Parameters	Meaning	Possible values	Default setting
------------	---------	-----------------	-----------------

Tab „Guards“ Protective settings for the ports.

Module.Port Port identification using module and port numbers of the device, e.g. 2.1 for port one of module two.

Table 111: Port-related STP settings and displays, guards

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

Table 111: Port-related STP settings and displays, guards

Parameters	Meaning	Possible values	Default setting
Loop Guard	<p>The “Loop Guard” setting is only meaningful for ports with the STP role <code>alternate</code>, <code>backup</code> or <code>root</code>. If the “Loop Guard” setting is active and the port has not received any STP-BPDUs for a while, the device sets the port to the <code>discarding</code> condition (port sends no more data).</p> <p>The device also sets the port to what is known as the “loop inconsistent status” and displays this in the “Loop Status” column.</p> <p>The device prevents a potential loop if no more STP-BPDUs are received if, for example, you switch STP off on the remote device, or the link only fails in the receiving direction.</p> <p>When the port receives BPDUs again, the device resets the loop status of the port to <code>false</code>, and the transmission status of the port according to the port role.</p> <p>If the “Loop Guard” setting is inactive, however, the device sets the port to the <code>forwarding</code> status when STP-BPDUs have not been received.</p>	<p><code>active</code> (box selected),</p> <p><code>inactive</code> (box empty)</p>	<code>inactive</code>
<p>Note: The “Root Guard” and “Loop Guard” settings are mutually exclusive. If you activate one setting when the other is already active, the device switches off the other one.</p>			
Loop State (read only)	<p>Display the status of the Loop Status.</p> <p>The device sets the loop status of the port to <code>true</code> if the “Loop Guard” setting is active at the port and the port is not receiving any more STP-BPDUs.</p> <p>Here the device leaves the port in the <code>discarding</code> transmission status, thus helping to prevent a potential loop.</p> <p>When the port receives STP-BPDUs again, the device resets the loop status to <code>false</code>.</p>	<code>true, false</code>	-
Transitions to Loop Status (read only)	Counts how often the device has set the port to the loop status (“Loop Status” column <code>true</code>).	0 - 4294967295 (2 ³² -1)	0

Table 111: Port-related STP settings and displays, guards

Parameters	Meaning	Possible values	Default setting
Transitions from Loop Status	Counts how often the device has set the port out of the loop status ("Loop Status" column <code>true</code>).	0 - 4294967295 ($2^{32}-1$)	0
BPDU Guard Effect (read only)	<p>The "BPDU Guard Effect" status is only relevant for edge ports (ports with the "Admin Edge Port" status <code>true</code>), and only if the "BPDU Guard" global function is active (see table 105).</p> <p>When such a port receives any random STP-BPDU, the device sets the port's "BPDU Guard Effect" status to <code>true</code> and its transmission status to <code>discarding</code>.</p> <p>Thus the device helps you protect your network at terminal device ports from incorrect configurations or attacks with STP-BPDUs that try to change the topology.</p> <p>To return the port to a normal transmitting status from the locked status, break and reconnect the link, or switch the "Admin Edge Port" port setting off and on again.</p>	<code>true</code> , <code>false</code>	-

Table 111: Port-related STP settings and displays, guards

Port	Root Guard	TCN Guard	Loop Guard	Loop State	Trans. into Loop	Trans. out of Loop	BPDU Guard Effect
1.1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	false	0	0	disable
1.2	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	false	0	0	disable
1.3	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	false	0	0	disable
1.4	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	false	0	0	disable
2.1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	false	0	0	disable
2.2	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	false	0	0	disable
2.3	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	false	0	0	disable
2.4	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	false	0	0	disable
3.1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	false	0	0	disable
3.2	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	false	0	0	disable

Figure 48: Multiple Spanning Tree dialog, Port, Guards tab

Buttons

Button	Meaning
Set	Transfers the changes to the volatile memory (RAM) of the device. To permanently save the changes, open the <code>Basic Settings:Load/Save</code> dialog, select the location to save the configuration, and click "Save".
Reload	Updates the fields with the values that are saved in the volatile memory (RAM) of the device.
Help	Opens the online help.

Table 112: Buttons

7 Diagnostics

The diagnostics menu contains the following tables and dialogs:

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

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

7.1 Syslog

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

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

Note: You will find the actual events that the device has logged in the “Trap Log” dialog ([see on page 190 “Trap log”](#)) and in the log file ([see on page 216 “Event Log”](#)). The device evaluates SNMP requests as events if you have activated “Log SNMP Set/Get Request” ([see table 114](#)).

Parameters	Meaning	Possible values	Default setting
“Operation” Frame	Switches the syslog function for this device “On” or “Off”	On Off	Off
“SNMP Logging” Frame	Settings for sending SNMP requests to the device as events to the list of syslog servers.		
Log SNMP Get Request	Creates events for the syslog for SNMP Get requests with the specified “severity”.	Active inactive	inactive
Severity (for logs of SNMP Get Requests)	Specifies the level for which the device creates the event “SNMP Get Request received” for the list of the syslog servers.	debug informational notice warning error critical alert emergency	notice

Table 113: Syslog and SNMP Logging settings

Parameters	Meaning	Possible values	Default setting
Log SNMP Set Request	Creates events for the syslog for SNMP Set requests with the specified "severity".	Active inactive	inactive
Severity (for logs of SNMP Set Requests)	Specifies the level for which the device creates the event "SNMP Set Request received" for the list of the syslog servers.	debug informational notice warning error critical alert emergency	notice

Table 113: Syslog and SNMP Logging settings

Parameters	Meaning	Possible values	Default setting
Syslog server entries			
Index	Sequential number of the syslog server entry in the table. When you delete an entry, this leaves a gap in the numbering. When you create a new entry, the device fills the first gap.	1 - 8	-
IP-Address	Address of a syslog server to which the device sends its log entries.	Valid IPv4 address	0.0.0.0
Port	UDP port at which your syslog server receives entries.	1 - 65535	514
Minimum Severity	Minimum severity for an event for the device to sent a log entry for it to this syslog server.	debug informational notice warning error critical alert emergency	critical
Active	Activate or deactivate the current syslog server entry in the table.	active (box selected) inactive (box empty)	inactive

Table 114: Syslog server entries

Note: When you activate the logging of SNMP requests, the device sends these as events with the preset severity `notice` to the list of syslog servers. The preset minimum severity for a syslog server entry is `critical`.

To send SNMP requests to a syslog server, you have a number of options to change the default settings. Select the ones that meet your requirements best.

- ▶ Set the severity for which the device creates SNMP requests as events to `warning` or `error` and change the minimum severity for a syslog entry for one or more syslog servers to the same value. You also have the option of creating a separate syslog server entry for this.
- ▶ When you set the severity for SNMP requests to `critical` or higher. The device then sends SNMP requests as events with the severity `critical` or higher to the syslog servers.
- ▶ When you set the minimum severity for one or more syslog server entries to `notice` or lower. Then it is possible that the device sends many events to the syslog servers.

Operation

On Off

SNMP Logging

Log SNMP Get Request Severity notice

Log SNMP Set Request Severity notice

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

Set
Reload
Create
Remove

Help

Figure 49: Syslog dialog

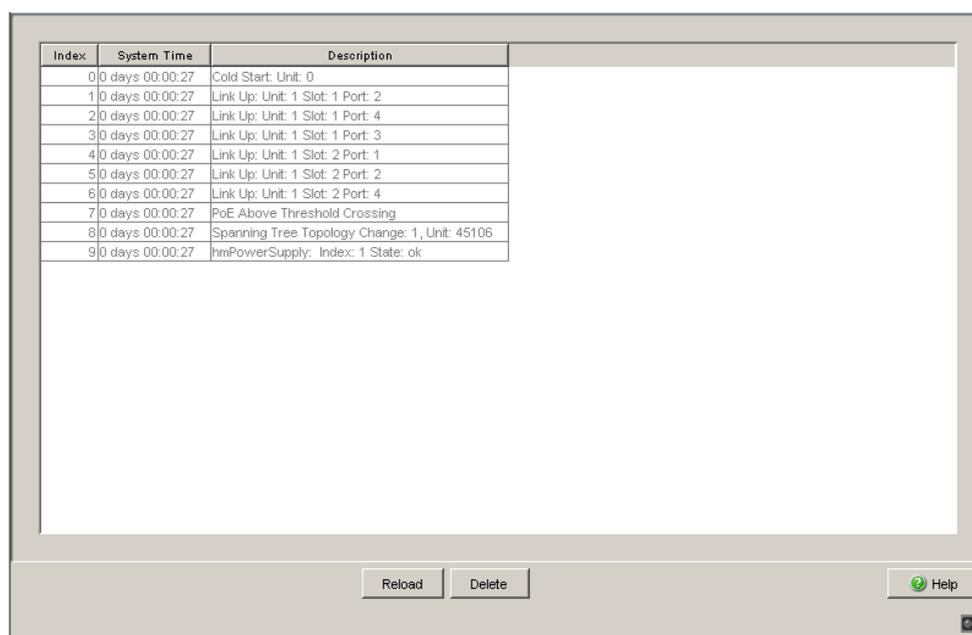
■ Buttons

Button	Meaning
Set	Transfers the changes to the volatile memory (RAM) of the device. To permanently save the changes, open the <code>Basic Settings:Load/Save</code> dialog, select the location to save the configuration, and click "Save".
Reload	Updates the fields with the values that are saved in the volatile memory (RAM) of the device.
Create	Adds a new table entry.
Remove	Removes the selected table entry.
Help	Opens the online help.

Table 115: Buttons

7.2 Trap log

The table lists the logged events with a time stamp. You update the content of the trap log via the “Reload” button. You delete the content of the trap log via the “Clear” button.



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

Figure 50: Trap log table

Parameters	Meaning	Possible values	Default setting
Index	Shows a sequential number to which the table entry relates. The device automatically defines this number.	0, 1, 2, ...	
System Time	Displays the time elapsed since the logged event.	d days hh:mm:ss	
Description	Displays a short description of the logged event.	-	

Table 116: Trap log table

You have the option to also send the logged events to one or more syslog servers ([see on page 186 “Syslog”](#)).

■ Buttons

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

Table 117: Buttons

7.3 Ports

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

- ▶ Statistics table
- ▶ Utilization
- ▶ SFP Modules

7.3.1 Statistics table

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

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

Port	Transmitted Packets	Transmitted Unicast Packets	Transmitted Non Unicast Packets	Received Packets	Received Octets	Received Fragments	Detected CRC errors	Detected Collisions	Detected Late Collisions	Packets 64 bytes	P 6
1.1	2246	4	2242	433	50632	0	0	0	0	2192	
1.2	2497	4	2493	180	42600	0	0	0	0	2189	
1.3	5045	2738	2307	3210	515117	0	0	0	0	2936	
1.4	635	2	633	2485	316216	0	0	0	0	2153	
2.1	2473	5	2468	253	42860	0	0	0	0	2135	
2.2	2552	5	2547	142	34648	0	0	0	0	2164	
2.3	2514	2	2512	136	26297	0	0	0	0	2179	
2.4	2615	5	2610	124	28936	0	0	0	0	2166	
3.1	0	0	0	0	0	0	0	0	0	0	
3.2	0	0	0	0	0	0	0	0	0	0	

Figure 51: Port statistics, table

■ Buttons

Button	Meaning
Reload	Updates the fields with the values that are saved in the volatile memory (RAM) of the device.
Reset port counters	Resets the counter for the port statistics to 0.
Help	Opens the online help.

Table 118: Buttons

7.3.2 Network load (Utilization)

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

The upper and lower thresholds work together controlling utilization alarms for a port. The device sends an alarm when utilization exceeds the upper threshold. Then, when the utilization is below the lower threshold the alarm is reset. A wide range between the upper and lower thresholds keeps the device from sending multiple alarms.

Port	Utilization [%]	Lower Threshold [%]	Upper Threshold [%]	Alarm
1.1	0.0	0.0	0.0	<input type="checkbox"/>
1.2	0.0	0.0	0.0	<input type="checkbox"/>
1.3	0.0	0.0	0.0	<input type="checkbox"/>
1.4	0.0	0.0	0.0	<input type="checkbox"/>
2.1	0.0	0.0	0.0	<input type="checkbox"/>
2.2	0.0	0.0	0.0	<input type="checkbox"/>
2.3	0.0	0.0	0.0	<input type="checkbox"/>
2.4	0.0	0.0	0.0	<input type="checkbox"/>
3.1	0.0	0.0	0.0	<input type="checkbox"/>
3.2	0.0	0.0	0.0	<input type="checkbox"/>

Set Reload Help

Figure 52: Network load dialog

Parameters	Meaning	Possible values	Default setting
Port	Number of the device port to which the table entry relates.	1.1, 1.2, 1.3 etc.	
Utilization [%]	Shows the current utilization in percent which the device port has received within the last 30 s. The utilization is the relationship of the received data quantity to the maximum possible data quantity at the currently configured data rate.	0.00..100.00	0.00
Lower Threshold [%]	Defines the lower threshold for utilization. When the utilization of the device port falls below this value, the alarm is reset. The value 0 deactivates the lower threshold.	0.00..100.00	0.00
Upper Threshold [%]	Defines an upper threshold for the utilization. If the utilization of the device port exceeds this value, the Alarm field shows an alarm. The value 0 deactivates the upper threshold.	0.00..100.00	0.00
Alarm	Indicates the alarm status for the utilization. – Selected The utilization of the device port is below the value defined in the Lower Threshold [%] field or above the value defined in the Upper Threshold [%] field. The device sends an SNMP message (trap). – Not selected The utilization of the device port is above the value defined in the Lower Threshold [%] field or below the value defined in the Upper Threshold [%] field.	Selected Not selected	Not selected

Table 119: Network load (Utilization) table

■ Buttons

Button	Meaning
Set	Transfers the changes to the volatile memory (RAM) of the device. To permanently save the changes, open the <code>Basic Settings:Load/Save</code> dialog, select the location to save the configuration, and click "Save".
Reload	Updates the fields with the values that are saved in the volatile memory (RAM) of the device.
Help	Opens the online help.

Table 120: Buttons

7.3.3 SFP Transceiver

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

Parameters	Meaning
Port	Port identification using module and port numbers of the device, e.g. 2.1 for port one of module two.
Module type	Type of SFP module, e.g. M-SFP-SX/LC.
Supported	Shows whether the media module supports the SFP module.
Temperature in °C	Shows the SFP's operating temperature.
Tx Power in mW	Shows the transmission power in mW.
Rx Power in mW	Shows the receive power in mW.
Tx power in dBm	Shows the transmission power in dBm.
Rx power in dBm	Shows the receive power in dBm.

Table 121: SFP Modules dialog

Port	Modultyp	Unterstützt	Temperatur in °Celsius	Sendeleistung in mW	Empfangsleistung in mW	Sendeleistung in dBm	Empfangsleistung in dBm
1.4	M-SFP-SX/LC	<input checked="" type="checkbox"/>	40	0.2488	0.0138	-6.0	-18.6

Laden
Hilfe

Figure 53: SFP Modules dialog

■ Buttons

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

Table 122: Buttons

7.4 Topology Discovery

This dialog enables you to activate/deactivate the function for Topology Recognition (LLDP) and to display the LLDP information received in the form of a table.

7.4.1 LLDP Information from Neighbor Devices

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

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

The table shows you which LLDP-MED information the device received on its ports from other devices.

Parameters	Meaning
Port	Port identification using module and port numbers of the device, e.g. 2.1 for port one of module two.
Neighbor Identifier	Chassis ID of the neighboring device. This can be the basis MAC address of the neighboring device, for example.
Neighbor IP Address	Management address of the neighboring device. This can be an IPv4 address, for example.
Neighbor Port Description	Port description of the neighboring device. The port description is an alphanumeric string.
Neighbor System Name	System name of the neighboring device. The system name is an alphanumeric string.
Neighbor System Description	System description of the neighbor device, according to IEEE 802.1AB.

Table 123: Topology discovery (LLDP information)

Operation
 On Off

LLDP | LLDP-MED

Port	Neighbor Identifier	Neighbor IP Address	Neighbor Port Description	Neighbor System Name	Neighbor System Description
1.3	ec e5 55 49 1d 00	10.0.1.120	Module: 1 Port: 1 - 1 Gbit	MACH-491D00	Hirschmann MACH - SW: L3P-08.0.00-B1
2.2	00 80 63 51 7a 80	10.0.1.116	Module: 2 Port: 1 - 10/100 Mbit TX	PowerMICE-517A80	Hirschmann PowerMICE - SW: L3E-07.0.00-
2.4	00 80 63 4a a7 b3	10.0.1.10	Module: 1 Port: 4 - 10/100 Mbit TX	RS-4AA7B3	Hirschmann Railswitch - SW: L2B-05.0.1
1.1	00 80 63 2f fb b8	10.0.1.2	Module: 1 Port: 1 - 1 Gbit	MICE-2FFBB8	Hirschmann MICE - SW: L2P-08.0.00-B10
2.1	00 80 63 14 db d9	10.0.1.62	10/100 MBit Ethernet Switch Interfa...	Gerhards RS2-16M	Hirschmann Ethernet Railswitch 2

Display FDB Entries

Set Reload Help

Figure 54: Topology Discovery

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

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

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

You can find the MAC addresses of devices, which the topology table hides for clarity's sake, in the address table (FDB), ([see on page 114 "Filter for MAC addresses"](#)).

7.5 Port Mirroring

The port mirroring function enables you to review the data traffic from a group of ports on the device for diagnostic purposes. The device forwards (mirrors) the data for the source ports to the destination. A management tool connected at the destination port, e.g. an RMON probe, can thus monitor the data traffic of the source ports in the sending and receiving directions. The device does not affect the data traffic on the source ports during port mirroring.

Note: The destination port needs sufficient bandwidth to receive the data stream. When the copied data stream exceeds the bandwidth of the destination port, the device discards surplus data packets on the destination port.

You use physical ports as source or destination ports.
The device supports up to 8 source ports.

- Select the source ports whose data traffic you want to review from the physical ports list. Mark the relevant checkboxes.
The device displays the port currently used as the "Destination Port" as grayed out in the table. Default setting: (no source ports)
- In the "Destination Port" frame, select the destination port to which you have connected your management tool.
The drop-down list displays available ports exclusively. For example, the list excludes the ports currently in use as source ports. Default setting: (no destination port)
- To enable the function, select `On` in the "Operation" frame and click "Set".
Default setting: `Off`.

■ Buttons

Button	Meaning
Set	Transfers the changes to the volatile memory (RAM) of the device. To permanently save the changes afterwards, you open the <code>Basic Settings:Load/Save</code> dialog and click "Save".
Reload	Updates the fields with the values that are saved in the volatile memory (RAM) of the device.
Reset Config	Resets the settings in the dialog to the default settings.
Help	Opens the online help.

Table 124:Buttons

7.6 Device Status

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

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

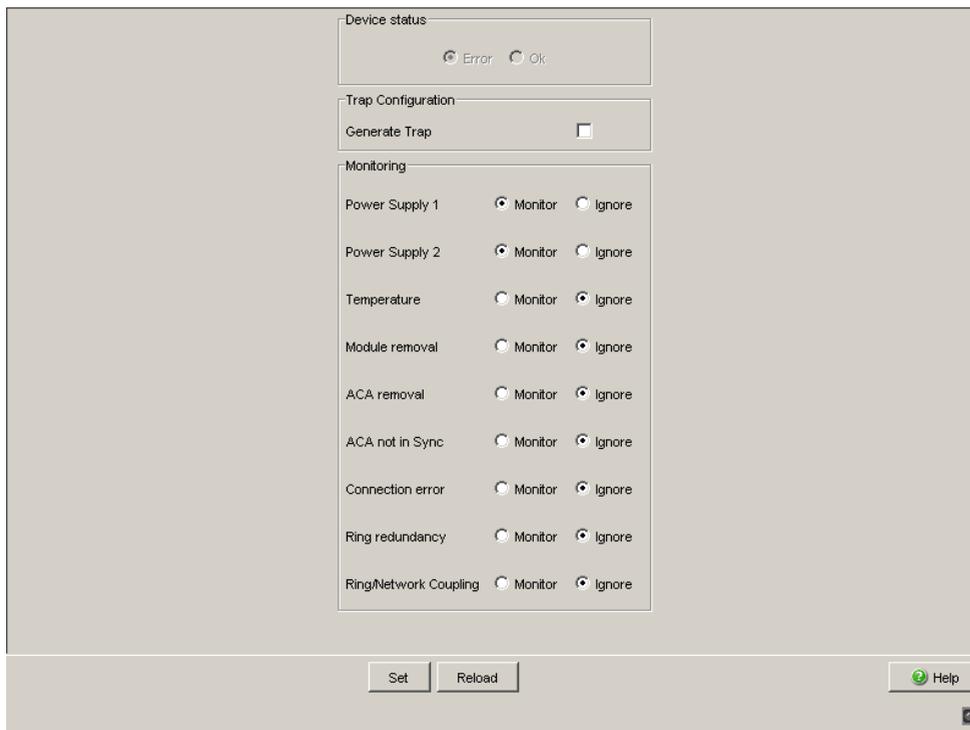


Figure 55: Device State dialog (for PowerMICE)

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

The events which can be selected are:

Name	Meaning
“Device Status” Frame	The device determines this status from the individual monitoring results. It can have the values “Error” or “OK”.
“Trap Configuration” Frame	-
Generate Trap	Activate this setting so the device sends a trap if it changes its device status.
“Monitoring” Frame	-
Power supply ...	Monitor/ignore supply voltage(s).
Temperature (°C)	Monitor/ignore temperature thresholds set (see on page 20 “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.
ACA not in sync	Monitor/ignore non-matching of the configuration on the device and on the ACA ^a .
Connection error	Monitor/ignore the link status (Ok or inoperable) of at least one port. The reporting of the link status can be masked for each port by the management (see on page 34 “Port Configuration”). Link status is not monitored in the state on delivery.
Ring Redundancy	Monitor/ignore ring redundancy (for HIPER-Ring only in Ring Manager mode). On delivery, ring redundancy is not monitored. If the device is a normal ring subscriber and not the ring manager, it reports the following: <ul style="list-style-type: none"> ▶ nothing (for the HIPER-Ring) ▶ detected errors in the local configuration (for Fast HIPER-Ring and for MRP)
Ring/Network coupling	Monitor/ignore the redundant coupling operation. On delivery, no monitoring of the redundant coupling is set. For two-Switch coupling with control line, the slave additionally reports the following conditions: <ul style="list-style-type: none"> – Incorrect link status of the control line – Partner device is also a slave (in standby mode).

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

Table 125: Device Status

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

Note: With a non-redundant voltage supply, the device reports the absence of a supply voltage. If you do not want this message to be displayed, feed the supply voltage over both inputs or switch off the monitoring ([see on page 205 “Signal contact”](#)).

■ Buttons

Button	Meaning
Set	Transfers the changes to the volatile memory (RAM) of the device. To permanently save the changes afterwards, you open the <code>Basic Settings:Load/Save</code> dialog and click "Save".
Reload	Updates the fields with the values that are saved in the volatile memory (RAM) of the device.
Help	Opens the online help.

Table 126: Buttons

7.7 Signal contact

The signal contacts are used for

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

7.7.1 Manual Setting

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

Application options:

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

7.7.2 Function monitoring

- Select the tab “Signal contact 1” or “Signal contact 2” (for devices with two signal contacts).
- In the “Mode Signal contact” box, you select the “Monitoring correct operation” mode. In this mode, the signal contacts monitor the functions of the device, thus enabling remote diagnosis.
A break in contact is reported via the potential-free signal contact (relay contact, closed circuit).
- ▶ Loss of the supply voltage 1/2 (either of the external voltage supply or of the internal voltage).¹ Select “Monitor” for the respective power supply if the signal contact shall report the loss of the power supply voltage, or of the internal voltage that is generated from the external power supply.
- ▶ One of the temperature thresholds has been exceeded (see on page 21 “System Data”). Select “Monitor” for the temperature if the signal contact should report an impermissible temperature.
- ▶ Removing a module. Select “Monitor” for removing modules if the signal contact is to report the removal of a module (for modular devices).
- ▶ The removal of the ACA. Select “Monitor” for ACA removal if the signal contact is to report the removal of an ACA (for devices which support the ACA).
- ▶ Non-matching of the configuration in the device and on the ACA². Select “Monitor” ACA not in sync if the signal contact is to report the non-matching of the configuration (for devices which support ACA).
- ▶ The connection error (non-functioning link status) of at least one port. The reporting of the link status can be masked via the management for each port in the device. On delivery, the link monitoring is inactive. You select “Monitor” for link errors if device is to use the signal contact to report a defective link status for at least one port.

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

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

- ▶ If the device is part of a redundant ring: the elimination of the reserve redundancy (i.e. the redundancy function did actually switch on), ([see on page 152 “Ring Redundancy”](#)).
 - Select “Monitor” for the ring redundancy if the signal contact is to report the elimination of the reserve redundancy in the redundant ring.
 - Select “Monitor” for the sub-ring redundancy if the signal contact is to report the elimination of the reserve redundancy in the redundant sub-ring.

Default setting: no monitoring.

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

- ▶ The elimination of the reserve redundancy for the ring/network coupling (i.e. the redundancy function did actually switch on). Select “Monitor” for the ring/network coupling if the signal contact is to report the elimination of the reserve redundancy for the ring/network coupling ([see on page 152 “Ring Redundancy”](#)).

Default setting: no monitoring.

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

7.7.3 Device status

- Select the tab page “Alarm 1” or “Alarm 2” (for devices with two signal contacts).
- In the “Mode Signal Contact” field, you select the “Device status” mode. In this mode, the signal contact monitors the device status ([see on page 20 “Device Status”](#)) and thereby offers remote diagnosis. The device status “Error detected” ([see on page 20 “Device Status”](#)) is reported by means of a break in the contact via the potential-free signal contact (relay contact, closed circuit).

7.7.4 Configuring Traps

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

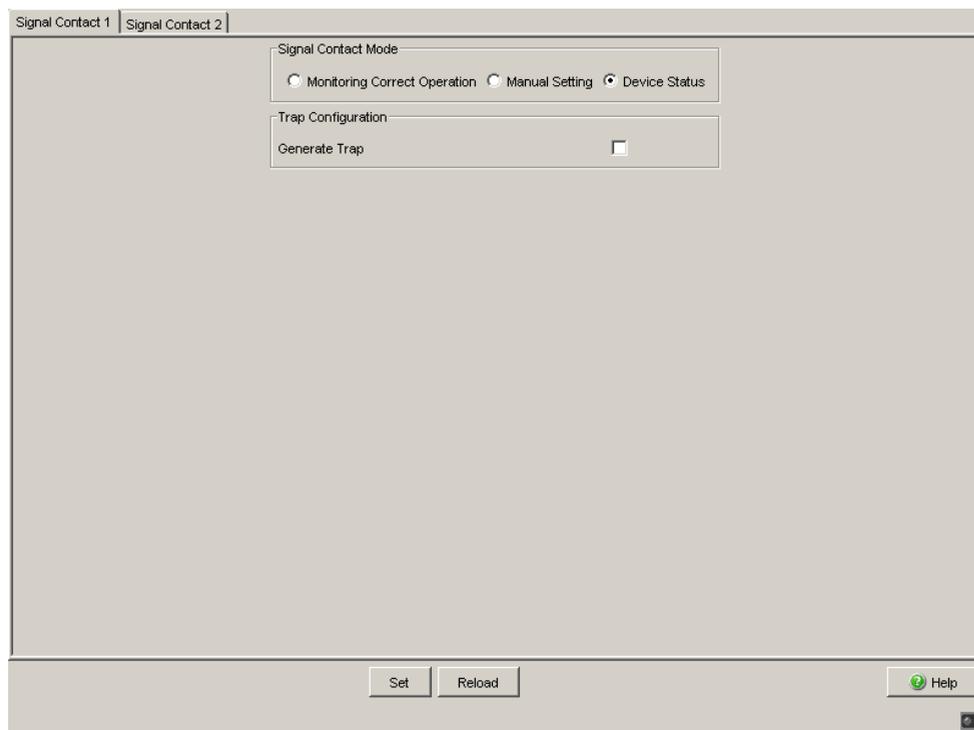


Figure 56: Signal Contact Dialog

The Signal Contact dialog contains 1 tab (“Signal contact 1”) if the device has 1 signal contact.

The Signal Contact dialog contains 2 tabs (“Signal contact 1” and “Signal contact 2”) if the device has 2 signal contacts.

■ Buttons

Button	Meaning
Set	Transfers the changes to the volatile memory (RAM) of the device. To permanently save the changes afterwards, you open the <code>Basic Settings:Load/Save</code> dialog and click "Save".

Table 127: Buttons

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

Table 127:Buttons (cont.)

7.8 Alarms (Traps)

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

The following device types support 10 trap destinations:

- ▶ RS20, RS30, RS40
- ▶ MS20, MS30
- In the "Configuration" frame, select the trap categories from which you want to send traps. Default setting: all trap categories are active.
- Click "Create".
- In the "IP Address" column, enter the IP address of the management station to which the traps should be sent.
- In the column "Password", enter the community name that the device uses to identify itself as the trap's source.
- In the "Enabled" column, you mark the entries that the device should take into account when it sends traps. Default setting: inactive.

The events which can be selected are:

Name	Meaning
Authentication	The device has rejected an unauthorized access attempt (see on page 61 "SNMPv1/v2 Access Settings").
Link Up/Down	At one port of the device, the link to another device has been established/interrupted.
Spanning Tree	The topology of the Rapid Spanning Tree has changed.

Table 128: Trap categories

Name	Meaning
Chassis	<p>Summarizes the following events:</p> <ul style="list-style-type: none"> ▶ The status of a supply voltage has changed (see the <code>System</code> dialog). ▶ The status of the signal contact has changed. To take this event into account, you activate “Create trap when status changes” in the <code>Diagnostics:Signal Contact 1/2</code> dialog. ▶ The AutoConfiguration Adapter (ACA) has been added or removed. <ul style="list-style-type: none"> – The configuration on the AutoConfiguration Adapter (ACA) differs from that in the device. ▶ The temperature thresholds have been exceeded/not reached. ▶ The receiver power status of a port with an SFP module has changed (see dialog <code>Diagnosis:Ports:SFP Modules</code>). ▶ The configuration has been successfully saved in the device and in the AutoConfiguration Adapter(ACA), if present. ▶ The configuration has been changed for the first time after being saved in the device.
Redundancy	The redundancy status of the ring redundancy (redundant line active/inactive) or (for devices that support redundant ring/network coupling) the redundant ring/network coupling (redundancy exists) has changed.
Port security	On one port a data packet has been received from an unauthorized terminal device (see the <code>Port Security</code> dialog).

Table 128: Trap categories

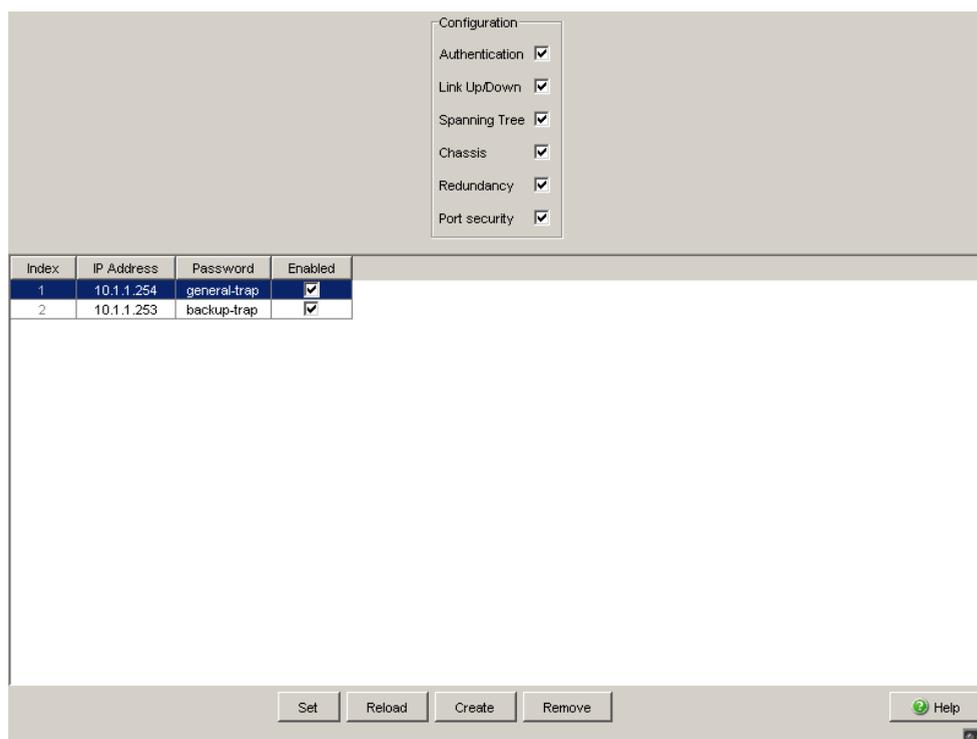


Figure 57: Alarms Dialog

■ Buttons

Button	Meaning
Set	Transfers the changes to the volatile memory (RAM) of the device. To permanently save the changes afterwards, you open the <code>Basic Settings:Load/Save</code> dialog and click "Save".
Reload	Updates the fields with the values that are saved in the volatile memory (RAM) of the device.
Create	Adds a new table entry.
Remove	Removes the selected table entry.
Help	Opens the online help.

Table 129: Buttons

7.9 Report

The following reports are available for the diagnostics:

- ▶ System Information ([see on page 215 “System Information”](#)).
The System Information is an HTML file with system-relevant data. The device displays the system information in its own dialog.
- ▶ Event Log ([see on page 216 “Event Log”](#)).
The Event Log is an HTML file in which the device writes important device-internal events. The device displays the event log in its own dialog.

Note: You have the option to also send the logged events to one or more syslog servers ([see on page 186 “Syslog”](#)).

The following buttons are available:

- ▶ Download Switch Dump.
This button allows you to download system information as files in a ZIP archive ([see table 130](#)).
 - Select the directory in which you want to save the switch dump.
 - Click “Save”.

The device creates the file name of the switch dumps automatically in the format <IP address>_<system name>.zip, e.g. for a device of the type PowerMICE: “10.0.1.112_PowerMICE-517A80.zip”.

- ▶ Download JAR-File.
This button allows you to download the applet of the Web-based interface as a JAR file. Afterwards you have the option to start the applet outside a browser.
This enables you to administer the device even when you have deactivated its Web server for security reasons.
 - Select the directory in which you want to save the applet.
 - Click “Save”.

The device creates the file name of the applet automatically in the format <device type><software variant><software version>_<software revision of applet>.jar, e.g. for a device of type PowerMICE with software variant L3P: “pmL3P06000_00.jar”.

File	Name	Format	Comments
Log file	event_log.html	HTML	
System information	systemInfo.html	HTML	
Trap log	traplog.txt	Text	
Internal memory extract for the manufacturer to improve the product	dump.hmd	Binary	
Exception log	exception_log.html	HTML	
Output of CLI commands ^a : – show running-config ^b – show port all – show sysinfo – show mac-address-table – show mac-filter-table igmpsnooping	clicommands.txt	Text	

Table 130: Files in switch dump archive

a: Prerequisite: a Telnet connection is available.

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

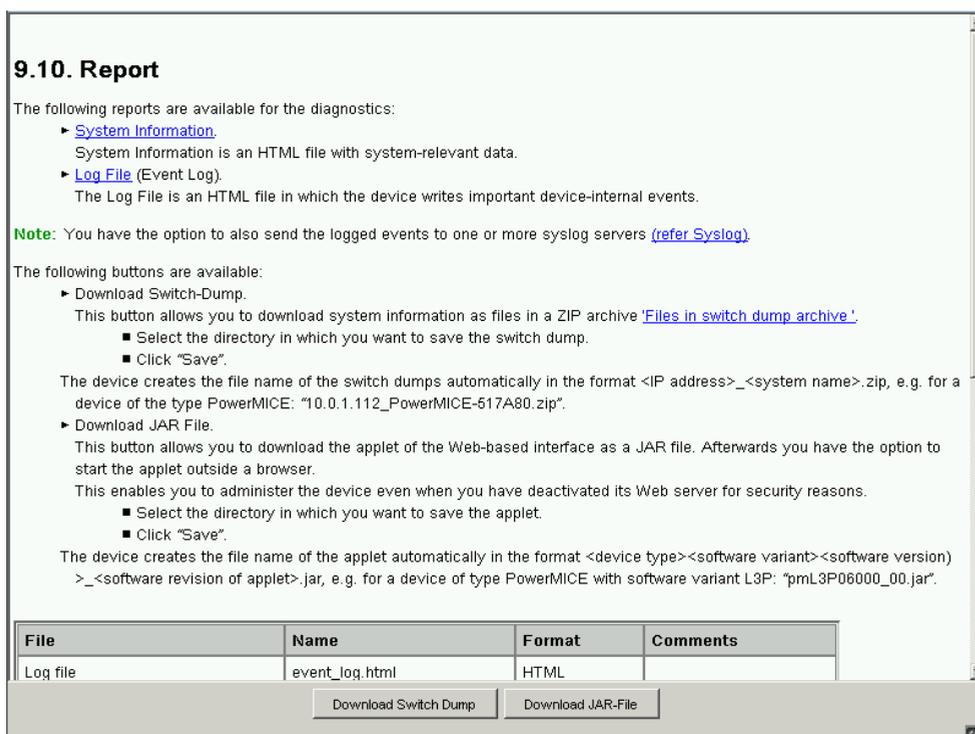


Figure 58: Report dialog

7.9.1 System Information

The System Information is an HTML file with system-relevant data.

■ Buttons

Button	Meaning
Reload	Updates the fields with the values that are saved in the volatile memory (RAM) of the device.
Search	Opens the "Search" dialog. The dialog allows you to search the log file for search terms or regular expressions.

Table 131: Buttons

Button	Meaning
Save	Opens the "Save" dialog. The dialog allows you to save the log file in HTML format on your PC.
Help	Opens the online help.

Table 131: Buttons (cont.)

7.9.2 Event Log

The Event Log is an HTML file in which the device writes important device-internal events.

■ Buttons

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

Table 132: Buttons

7.10 IP address conflict detection

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

- In “Status”, select the operating mode for the IP address conflict detection (see table 133). The default setting is `disable`.
- In the “Fault State” field, the device displays the current result of the IP address conflict detection.
Possible values:
 - ▶ `false`: the detection is disabled, or the device has not detected any problem; or
 - ▶ `true`: the device has detected a problem.

Mode	Meaning
Field „Status“	Defines the status for the IP address conflict detection. The value of the status field can be „enable“, „disable“, „activeDetectionOnly“ or „passiveDetectionOnly“.
<code>enable</code>	Enables active and passive detection.
<code>disable</code>	Disables the function
<code>activeDetectionOnly</code>	Enables active detection only. After connecting to a network or after the IP configuration has been changed, the device immediately checks whether its own 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. The device thus avoids participating in the network traffic with a duplicate IP address.
<code>passiveDetectionOnly</code>	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 is no conflict, it will connect back to the network.
Field „Fault State“	Displays, if the device has detected an IP address conflict. In this case the value of the field is „false“.

Table 133: Possible address conflict operating modes

- ▶ In the table, the device logs IP address conflicts with its IP address. The device logs the following data for each conflict:
 - ▶ the time („Timestamp“ column)
 - ▶ the conflicting IP address („IP Address“ column)
 - ▶ the MAC address of the device with which the IP address conflicted („MAC Address“ column).
 For each IP address, the device logs a line with the last conflict that occurred.
- During a restart, the device deletes the table.

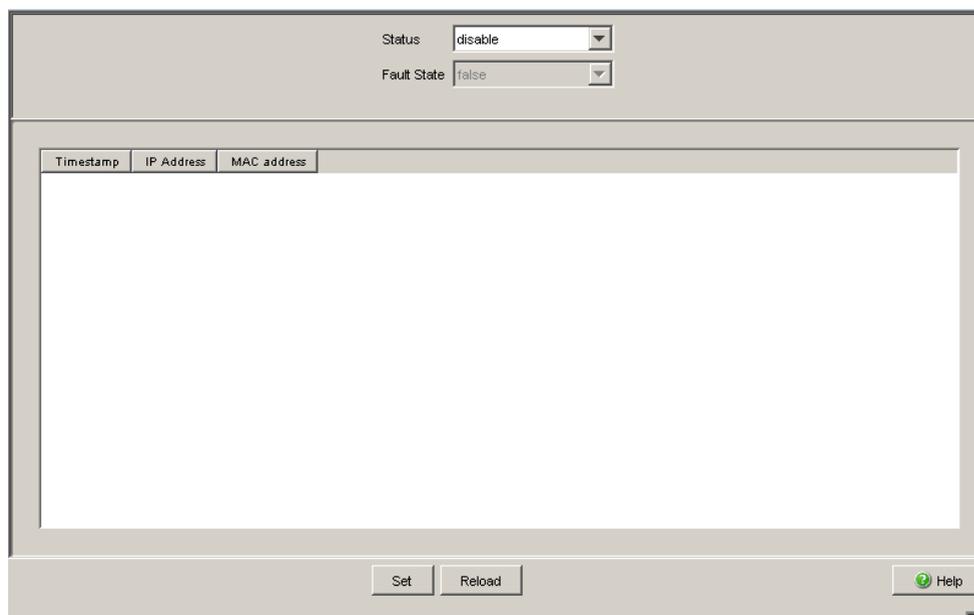


Figure 59: IP Address Conflict Detection dialog

■ Buttons

Button	Meaning
Set	Transfers the changes to the volatile memory (RAM) of the device. To permanently save the changes afterwards, you open the <i>Basic Settings:Load/Save</i> dialog and click "Save".
Reload	Updates the fields with the values that are saved in the volatile memory (RAM) of the device.
Help	Opens the online help.

Table 134: Buttons

7.11 MAC Notification

The device allows you to track changes in the network using the MAC address of the end devices. When on a port the MAC address of a connected device changes, the device sends an SNMP trap periodically.

This function is intended solely for ports on which you connect end devices and thus the MAC address changes infrequently.

7.11.1 Operation

Parameters	Meaning
Operation	<p>Activates/deactivates the MAC Notification function globally on the device.</p> <p>Possible values:</p> <ul style="list-style-type: none"> ▶ On The device sends traps for the active rows to the active management stations in <code>Diagnostics:Status Configuration:Alarms (Traps)</code>. ▶ Off (default setting)

Table 135: "Operation" frame in the `Diagnostics:Status Configuration:MAC Notification` dialog

7.11.2 Configuration

Parameters	Meaning
Intervals [s]	<p>Defines the interval, in seconds, between notifications. The device buffer contains up to 20 addresses. If the buffer is full before the interval expires, then the device sends a trap to the management station.</p> <p>Possible values:</p> <ul style="list-style-type: none"> ▶ 0..2147483647

Table 136: "Configuration" frame in the `Diagnostics:Status Configuration:MAC Notification` dialog

7.11.3 Table

Parameters	Meaning
Port	Shows the number of the device port to which the table entry relates.
Enable	<p>Activates/deactivates the MAC Notification function on this port.</p> <p>Possible values:</p> <ul style="list-style-type: none"> ▶ Selected When globally activated, the device sends traps for this row to the active management stations in <code>Diagnostics:Status Configuration:Alarms (Traps)</code>. ▶ Not selected (default setting)

Table 137: Table in the `Diagnostics:Status Configuration:MAC Notification` dialog

Parameters	Meaning
Mode	<p>Defines when the device sends a trap for MAC address events on a specific interface.</p> <p>Possible values:</p> <ul style="list-style-type: none"> ▶ add The device sends notifications for entries added to the FDB. ▶ remove The device sends notifications for entries removed from the FDB. ▶ add + remove (default setting) The device sends notifications for entries added to or removed from the FDB.
Last MAC Address	Shows the last MAC address added or removed from the address table for this interface.
Last MAC Status	<p>Displays the status of the last MAC address on this interface.</p> <p>Possible values:</p> <ul style="list-style-type: none"> ▶ other ▶ added ▶ removed

Table 137: Table in the `Diagnostics:Status Configuration:MAC Notification` dialog (cont.)

■ Buttons

Button	Meaning
Set	Transfers the changes to the volatile memory (RAM) of the device. To permanently save the changes afterwards, you open the <code>Basic Settings:Load/Save</code> dialog and click "Save".
Reload	Updates the fields with the values that are saved in the volatile memory (RAM) of the device.
Help	Opens the online help.

Table 138: Buttons

7.12 Self Test

With this dialog you can:

- ▶ activate/deactivate the RAM test for a cold start of the device.
Deactivating the RAM test shortens the booting time for a cold start of the device.
Default setting: activated.
- ▶ allow or prevent a restart due to an undefined software or hardware state.
Default setting: activated.
- ▶ to allow/prohibit a change to the system monitor during the system start.
Default setting: enabled, so that changing to the system monitor during the system start via a V.24 connection is possible.
This function works exclusively in combination with a boot code in version 09.0.00 or higher. To update the boot code, contact your sales partner.

Note: If changing to the system monitor is prohibited and you forget the password, you are permanently unable to access the device. To have the device unlocked again, contact your sales partner.

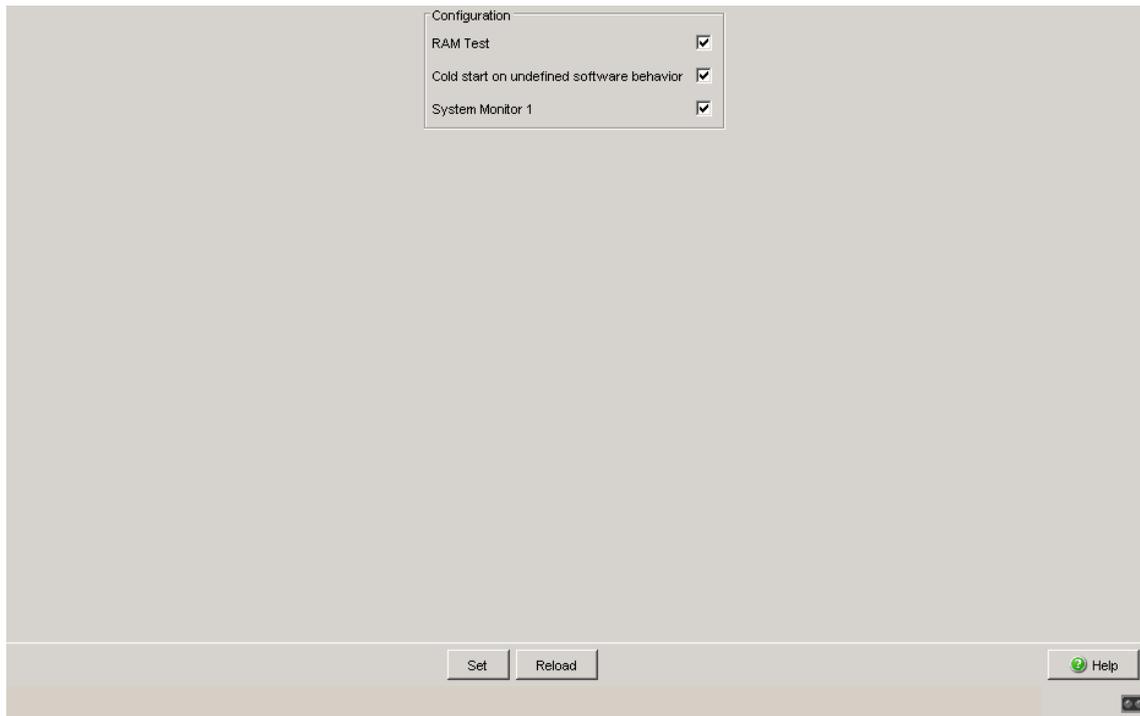


Figure 60: Self-test dialog

■ Buttons

Button	Meaning
Set	Transfers the changes to the volatile memory (RAM) of the device. To permanently save the changes afterwards, you open the <code>Basic Settings:Load/Save</code> dialog and click "Save".
Reload	Updates the fields with the values that are saved in the volatile memory (RAM) of the device.
Help	Opens the online help.

Table 139: Buttons

7.13 Service Mode

The following devices support the service mode:
RS20/RS30/RS40 and MS20/MS30.

The service mode enables you to divide the device into 2 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 specifies 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 prevents GVRP from dynamically changing the service mode port settings as a result.
- ▶ activates “Ingress Filtering” at all ports of this VLAN. As a consequence, the device only transmits packets when the input and output ports belong to this VLAN.

■ Buttons

Button	Meaning
Set	Transfers the changes to the volatile memory (RAM) of the device. To permanently save the changes afterwards, you open the <code>Basic Settings:Load/Save</code> dialog and click "Save".
Reload	Updates the fields with the values that are saved in the volatile memory (RAM) of the device.
Help	Opens the online help.

Table 140: Buttons

7.13.1 Activating the service mode

Prerequisites:

- HIPER-Ring ports are defined (HIPER-Ring or MRP-Ring).
- The supply voltage is redundant at P1 and P2.

Note: If there is no redundant voltage when activating the service mode (by clicking on “Set” - see below), the switch immediately creates the 2 switching areas. Depending on the settings already entered, this may interrupt your communication to the switch.

- Select the `Diagnostics:Service Mode` dialog.
- Activate “Mode”.
- Enter a number other than 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 “Set”. The device outputs the following system message:



- If you have verified that your communication with the Switch will not be interrupted, click “OK” to activate the service mode.

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

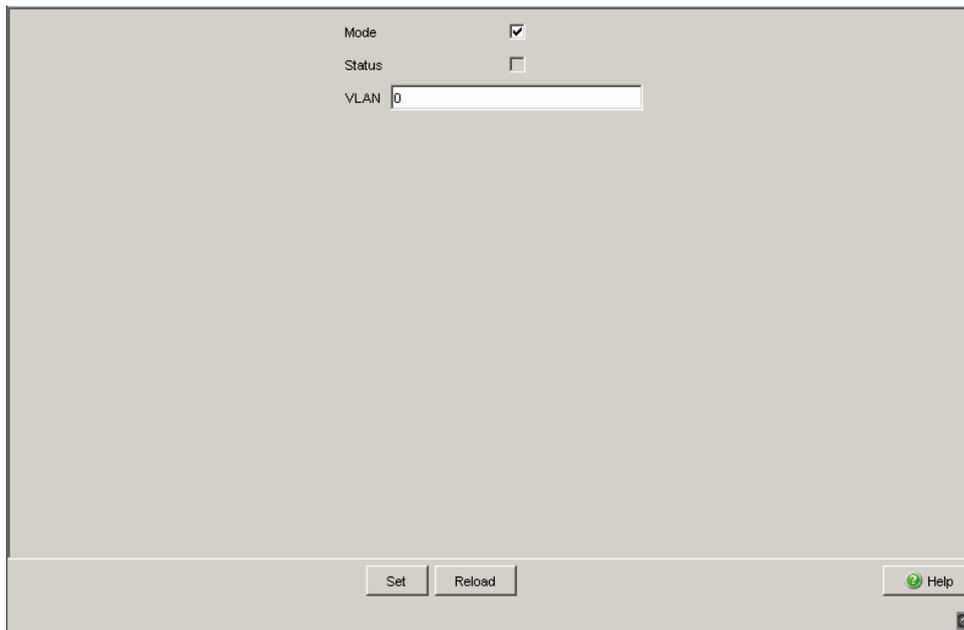


Figure 61: Service Mode dialog - mode activated

- Deactivate the redundant supply voltage.

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

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

7.13.2 Deactivating the service mode

- Reactivate the redundant voltage.

The service mode is now deactivated.

- Select the `Diagnostics:Service Mode` dialog.
- Deactivate “Mode”.
- Click “Set” to deactivate the service mode so that the device will no longer switch to the service mode if the redundant voltage supply is lost.

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

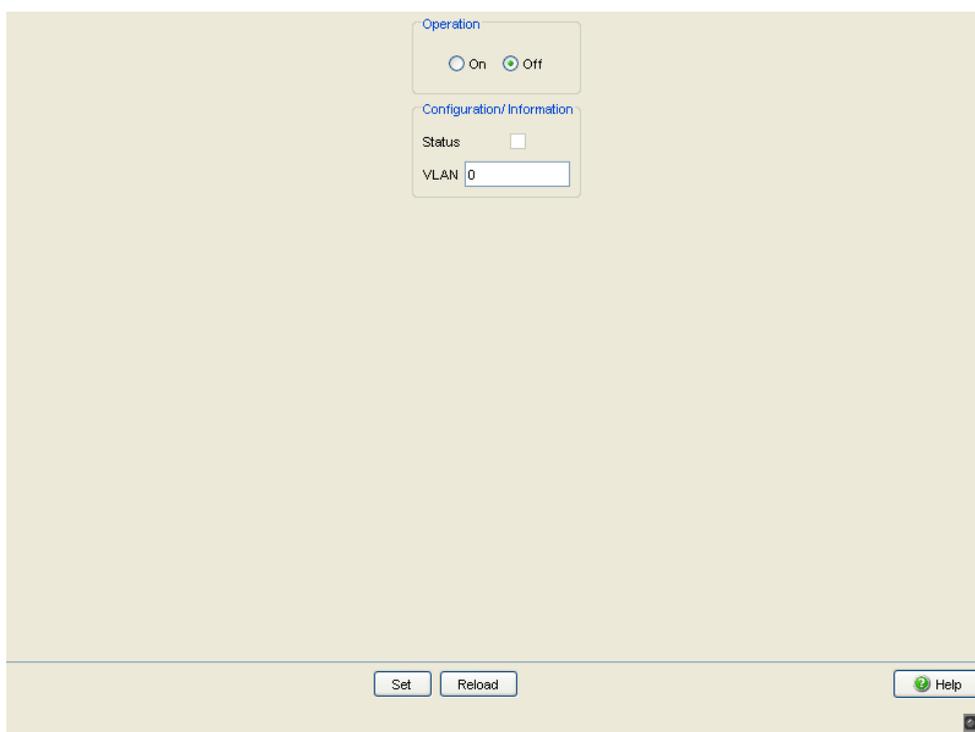


Figure 62: Service Mode dialog - mode deactivated

8 Advanced

The menu contains the dialogs, displays and tables for:

- ▶ DHCP Relay Agent
- ▶ Industry Protocols
- ▶ Command Line

8.1 DHCP Relay Agent

This menu allows you to configure the DHCP relay agent.

The DHCP relay agent forwards the DHCP requests of connected terminal devices to a DHCP server. The forwarding to a specific DHCP server is performed independently of the port or interface at which the device receives the DHCP request. You define the required settings for this in the

`Advanced:DHCP Relay Agent:Server` dialog. There you can define up to 16 DNCP servers.

8.1.1 Global

This dialog allows you to configure the DHCP relay agent.

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

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

The “[Network](#)” Chapter contains further information about VLAN 0.

Example of a configuration of your DHCP server:

Type: `mac`

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

Circuit ID: `B3 06 00 00 01 00 01 01`

This results in the entry for the "Hardware address" in the DHCP server:

B306000001000101000600806300061E

- The "DHCP-Relay on" activates the relay on the port. Clients connected to an activated port communicate directly with a DHCP Server.
- The "DHCP-Relay Operation" shows the operating state of the relay on the port.
- In the "Option 82 on" column in the table, you switch this function on/off for each port.
- In the "Hirschmann Device" column, you check the ports connected to a Hirschmann device.

Note: The DHCP relay function requires a minimum of 2 ports. Connect a port to the DHCP client and a port to the DHCP server. Enable the DHCP relay function globally and on the relay ports. The DHCP server function has priority over the DHCP relay function. Therefore, disable the DHCP server function on both the client and the server ports.

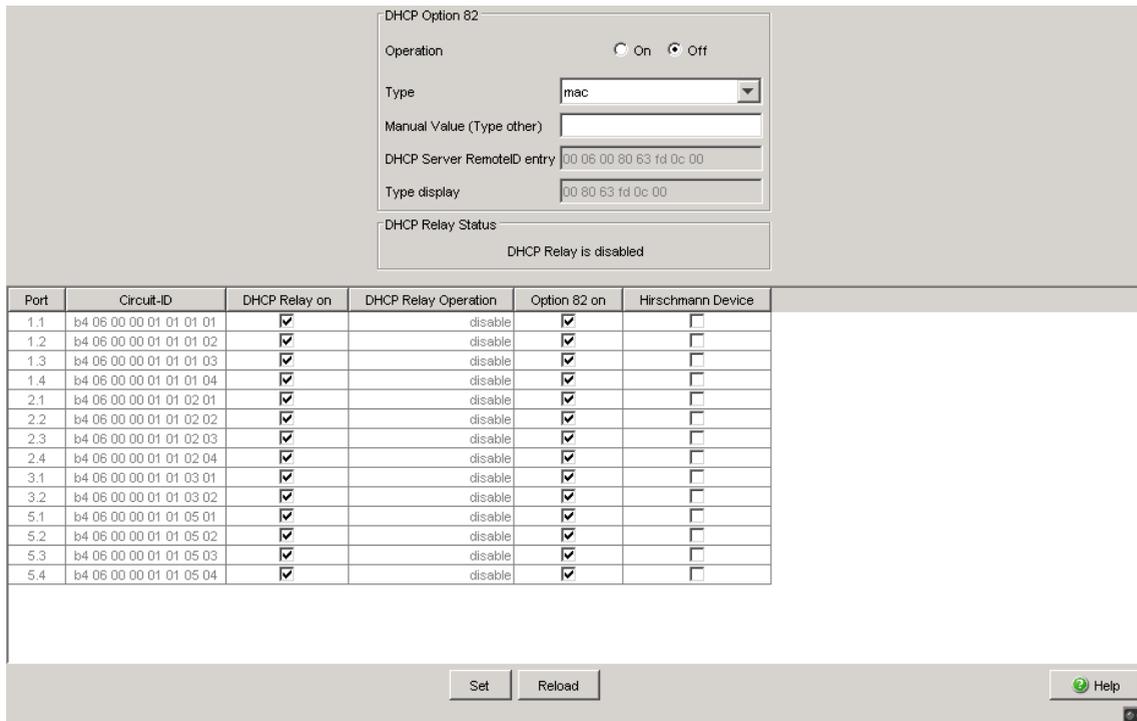


Figure 63: DHCP Relay Agent dialog

Buttons

Button	Meaning
Set	Transfers the changes to the volatile memory (RAM) of the device. To permanently save the changes, open the Basic Settings:Load/Save dialog, select the location to save the configuration, and click "Save".
Reload	Updates the fields with the values that are saved in the volatile memory (RAM) of the device.
Help	Opens the online help.

Table 141: Buttons

8.1.2 Server

With this dialog you can define up to 16 DHCP servers to which the DHCP relay agent sends the DHCP requests. The device forwards either every DHCP request to a server or only requests that it receives at a specific port or interface.

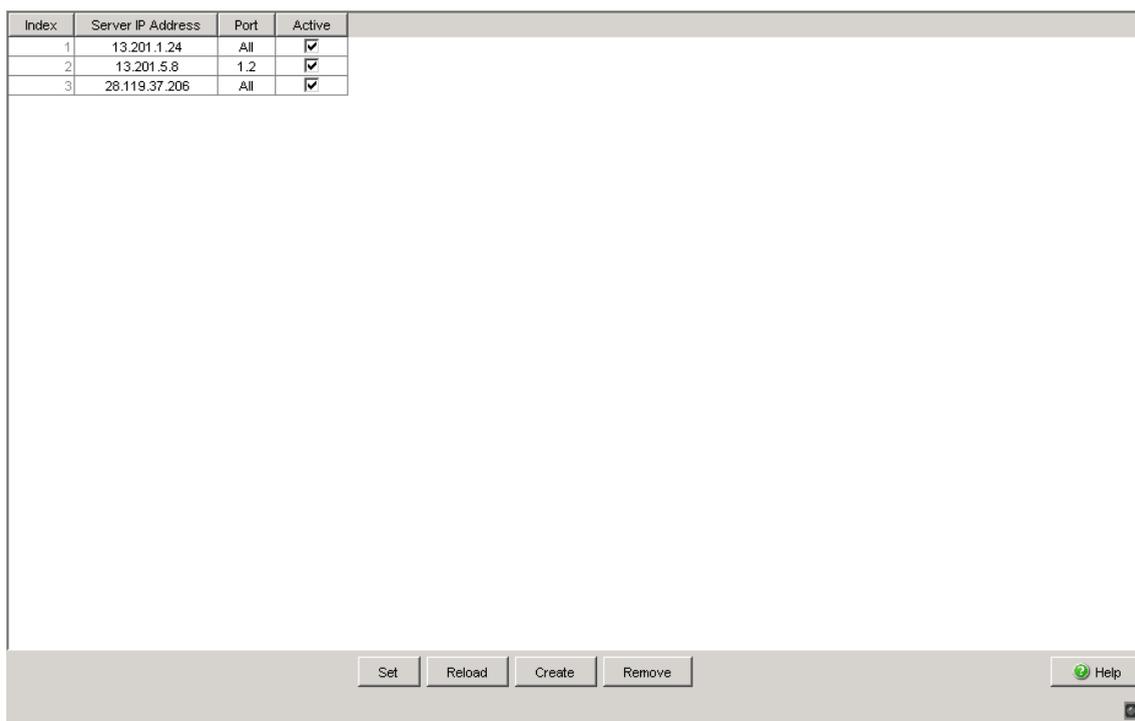


Figure 64: *Advanced:DHCP Relay Agent:Port dialog*

Parameter	Meaning	Value range	Default setting
Index	Shows a sequential number to which the table entry relates. The device automatically defines this number.	1..16	–
Server IP Address	Defines the IP address of the DHCP server.	Valid IPv4 address	0.0.0.0

Table 142: "DHCP-Server Mode" frame in the *Advanced:DHCP Server:Global dialog*

Parameter	Meaning	Value range	Default setting
Port	Defines whether the device forwards every DHCP request to the server or only requests that it receives at a port or interface.	All <Port number>	All
Active	Activates/deactivates the forwarding of DHCP requests to this DHCP server.	activated deactivated	deactivated

Table 142: "DHCP-Server Mode" frame in the *Advanced:DHCP Server:Global* dialog

■ Buttons

Button	Meaning
Set	Transfers the changes to the volatile memory (RAM) of the device. To permanently save the changes, open the <i>Basic Settings:Load/Save</i> dialog, select the location to save the configuration, and click "Save".
Reload	Updates the fields with the values that are saved in the volatile memory (RAM) of the device.
Create	Adds a new table entry.
Remove	Removes the selected table entry.
Help	Opens the online help.

Table 143: Buttons

8.2 Industrial Protocols

The “Industry Protocols” menu allows you to configure the following protocols

- ▶ the PROFINET protocol
- ▶ the EtherNet/IP protocol
- ▶ the IEC61850 MMS protocol

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

8.2.1 PROFINET

This dialog allows you to configure the PROFINET protocol. To integrate this in a control system, perform the following steps.

General settings:

- In the `Basic Settings:System` dialog, check if a valid system name for the device is specified in the “Name” field.
The system name can only contain alphanumeric characters, hyphens, and periods.
- In the `Basic Settings:Network` dialog, check whether `Local` is selected in the “Mode” frame ([see on page 27 “Network”](#)).
- In the `Switching:VLAN:Global` dialog, check whether “VLAN 0 Transparent Mode” is selected ([see on page 127 “VLAN Global”](#)).

Note: Preclude a combination of the VLAN 0 Transparent mode and the use of MSTP (Multiple Spanning Tree).

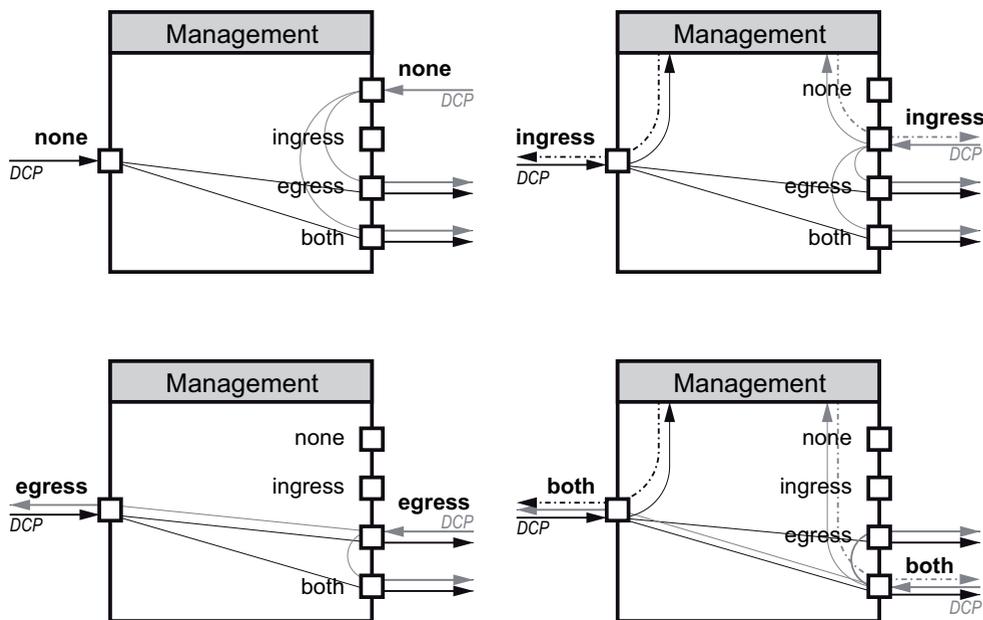
- Configure the alarm settings and the threshold values for the alarms you want to monitor ([see on page 202 “Device Status”](#)).

Global PROFINET settings:

- Activate PROFINET in the “Operation” frame.
- Click on “Download GSDML File” to load the GSDML file onto your PC.

PROFINET Port settings:

- Specify the desired settings for every port in the `DCP Mode` column. DCP frames are multicast, the responses from the management are unicast. Regardless of the settings, the device forwards the received DCP frames to other device ports whose setting is either `egress` or `both`.



- ▶ **none:**
The management does not respond to DCP frames received on this port.
The port does not forward DCP frames received on other ports.
- ▶ **ingress:**
The management responds to DCP frames received on this port.
The port does not forward DCP frames received on other ports.
- ▶ **egress:**
The management does not respond to DCP frames received on this port.
The port forwards DCP frames received on other ports.
- ▶ **both:**
The management responds to DCP frames received on this port.
The port forwards DCP frames received on other ports.

The default setting is `both`.

Note: If you connect 2 switches which are located in separate DCP domains, change the DCP mode of the corresponding ports to `none` or to `ingress` on **both** switches. This way neither of the switches receives or forwards DCP frames.

- Select the port for which you want to set its PHY module to the fast start mode, and select from the following in the column `Fast Start Up`:
 - ▶ `disable` to set the normal start mode,
 - ▶ `enable` to set the fast start mode.

Note: The setting `enable` only becomes effective if the automatic configuration of the port (Autoneg) is switched off (see on page 34 “Port Configuration”).

The default setting is `disable`. If a port does not support the fast start mode, the device will show `unsupported` in this column.

Settings for the PLC:

- Configure the PLC as described in the “Industry Protocols” user manual.

■ Buttons

Button	Meaning
Set	Transfers the changes to the volatile memory (RAM) of the device. To permanently save the changes, open the <code>Basic Settings:Load/Save</code> dialog, select the location to save the configuration, and click "Save".
Reload	Updates the fields with the values that are saved in the volatile memory (RAM) of the device.
Help	Opens the online help.

Table 144:Buttons

8.2.2 EtherNet/IP

This dialog allows you to activate the EtherNet/IP protocol. To integrate this in a control system, perform the following steps.

General settings:

- In the `Switching:Multicast:IGMP` dialog, check whether IGMP is activated (see on page 120 “IGMP (Internet Group Management Protocol)”).

EtherNet/IP settings:

- Activate EtherNet/IP in the “Operation” frame (default setting: Off).
- Click on “Download EDS File” to load the EDS file onto your PC.

Settings for the PLC:

- Configure the PLC as described in the “Industry Protocols” user manual.

■ Buttons

Button	Meaning
Set	Transfers the changes to the volatile memory (RAM) of the device. To permanently save the changes, open the <code>Basic Settings:Load/Save</code> dialog, select the location to save the configuration, and click "Save".
Reload	Updates the fields with the values that are saved in the volatile memory (RAM) of the device.
Help	Opens the online help.

Table 145: Buttons

8.2.3 IEC61850 MMS Protocol (RSR, MACH 1000)

The IEC61850 is a standardized industrial communication protocol from the International Electrotechnical Commission (IEC). For example, automatic switching equipment uses this protocol when communicating with power station equipment.

The packet orientated protocol defines a uniform communication language based on the transport protocol, TCP/IP. The protocol uses a Manufacturing Message Specification (MMS) server for client server communications. The protocol includes functions for SCADA, Intelligent Electronic Device (IED) and the network control systems.

This dialog allows you to configure the following MMS Server functions:

- ▶ Activate/deactivate the MMS server
- ▶ Activate/deactivate write access to the MMS server

Parameter	Meaning	Value range	Default setting
Operation	Activate/deactivate the MMS server.	On, Off	Off

Table 146: "Operation" frame in the *Advanced:Industrial Protocols:IEC61850* dialog

Parameter	Meaning	Value range	Default setting
Write Access	Activate/deactivate the MMS server.	select, not selected	not selected
Technical Key	Specifies the IED Name. Thus, the IED Name is eligible independently of the System Name.	a..z A..Z _0..9	KEY

Table 147: "Configuration" frame in the *Advanced:Industrial Protocols:IEC61850* dialog

Parameter	Meaning	Value range	Default setting
Download ICD File	This button copys the ICD file to your PC.	-	-

Table 148: "Download" frame in the *Advanced:Industrial Protocols:IEC61850* dialog

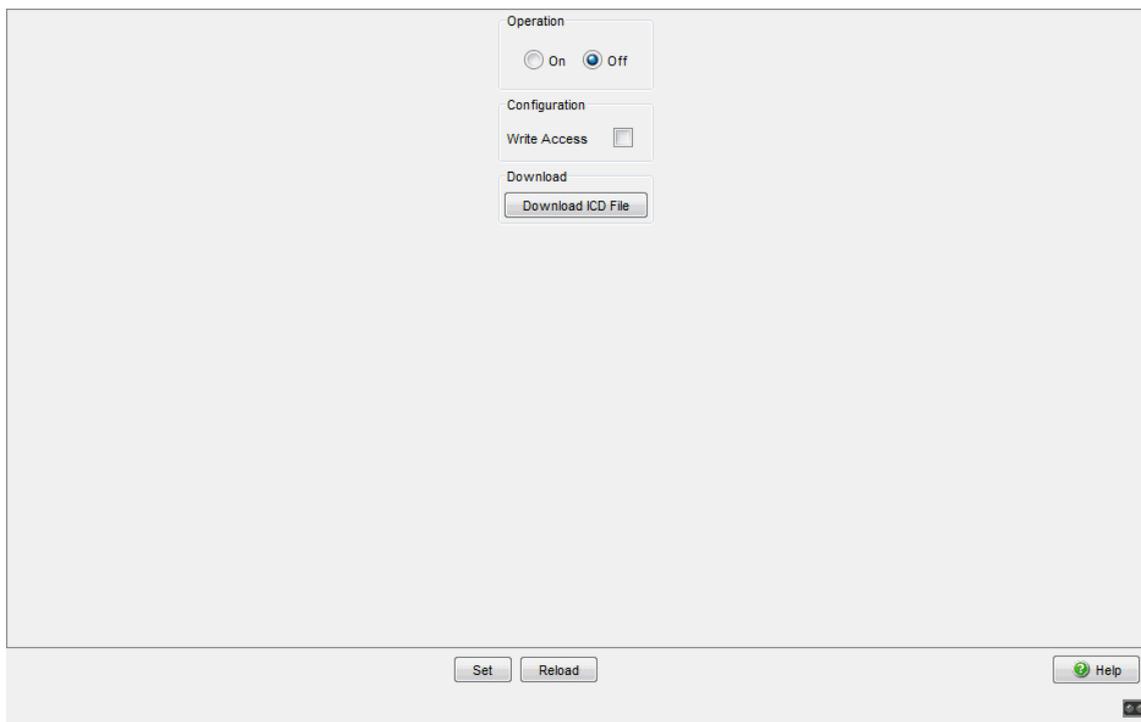


Figure 65: *Advanced:Industrial Protocols:IEC61850* dialog

■ Buttons

Button	Meaning
Set	Transfers the changes to the volatile memory (RAM) of the device. To permanently save the changes, open the <i>Basic Settings:Load/Save</i> dialog, select the location to save the configuration, and click "Save".
Reload	Updates the fields with the values that are saved in the volatile memory (RAM) of the device.
Help	Opens the online help.

Table 149: Buttons

8.3 Software DIP Switch overwrite (MICE, PowerMICE and RS)

This dialog allows you to display the settings of the DIP switches on the device. If required, you can deactivate the settings of the DIP switches or overwrite them using the setting from the software.

Parameter	Meaning	Value range	Default setting
Function	<p>Activates/deactivates the DIP switches on the device.</p> <p>On: The device uses the settings specified with the DIP switches. The prerequisite is that "DIP Switch On" is active.</p> <p>Off: The device ignores the settings of the DIP switches.</p>	On, Off	On

Table 150: "Operation" frame in the *Advanced:DIP-Switch* dialog

Parameter	Meaning	Value range	Default setting
Conflict with hardware settings	Displays the conflicts between the settings of the DIP switches on the device and the software settings. <i>Active</i> : Conflict between the settings of the DIP switches on the device and the software settings. <i>Inactive</i> : No conflict.	Active, inactive	-
DIP-Switch On (Mice)	Displays the setting of the DIP switch that activates/deactivates the setting of the other DIP switches on the device. <i>Active</i> : The DIP switch on the device is positioned in such a way that the device uses the DIP switch settings. The prerequisite is that in the "Function" frame the value <i>On</i> is selected. <i>Inactive</i> : The DIP switch on the device is positioned in such a way that the device uses the software settings.	Active, inactive	-
Ring Manager On (Mice, RS)	Displays the setting of the DIP switch for the Ring Manager function. <i>Active</i> : The DIP switch on the device is positioned in such a way that the Ring Manager function is activated on the device. The prerequisite is that in the "Function" frame the value <i>On</i> is selected and "DIP Switch On" is active. <i>Inactive</i> : The DIP switch on the device is positioned in such a way that the device uses the software settings for the Ring Manager function.	Active, inactive	-

Table 151: "DIP-Switch Status" frame in the *Advanced:DIP-Switch dialog*

Parameter	Meaning	Value range	Default setting
Standby On (Mice, RS)	<p>Displays the setting of the DIP switch for the STAND-BY switch. With the STAND-BY switch, you specify whether the device has the main coupling or the redundant coupling role within a Ring/Network coupling.</p> <p><i>Active:</i> The DIP switch on the device is positioned in such a way that the device has the main coupling role. The prerequisite is that in the "Function" frame the value <code>On</code> is selected and "DIP Switch On" is active.</p> <p><i>Inactive:</i> The DIP switch on the device is positioned in such a way that the device has the redundant coupling role. The prerequisite is that in the "Function" frame the value <code>On</code> is selected and "DIP Switch On" is active.</p>	Active, inactive	-
Ring Ports (Mice)	<p>Displays the setting of the DIP switch for the selection of the ring ports.</p> <p><i>1.1 & 1.2:</i> The DIP switch on the device is positioned in such a way that the device uses the ports 1.1 & 1.2 as ring ports. The prerequisite is that in the "Function" frame the value <code>On</code> is selected and "DIP Switch On" is active.</p> <p><i>2.1 & 2.2:</i> The DIP switch on the device is positioned in such a way that the device uses the ports 2.1 & 2.2 as ring ports. The prerequisite is that in the "Function" frame the value <code>On</code> is selected and "DIP Switch On" is active.</p>	1.1 & 1.2 2.1 & 2.2	-

Table 151: "DIP-Switch Status" frame in the `Advanced:DIP-Switch` dialog

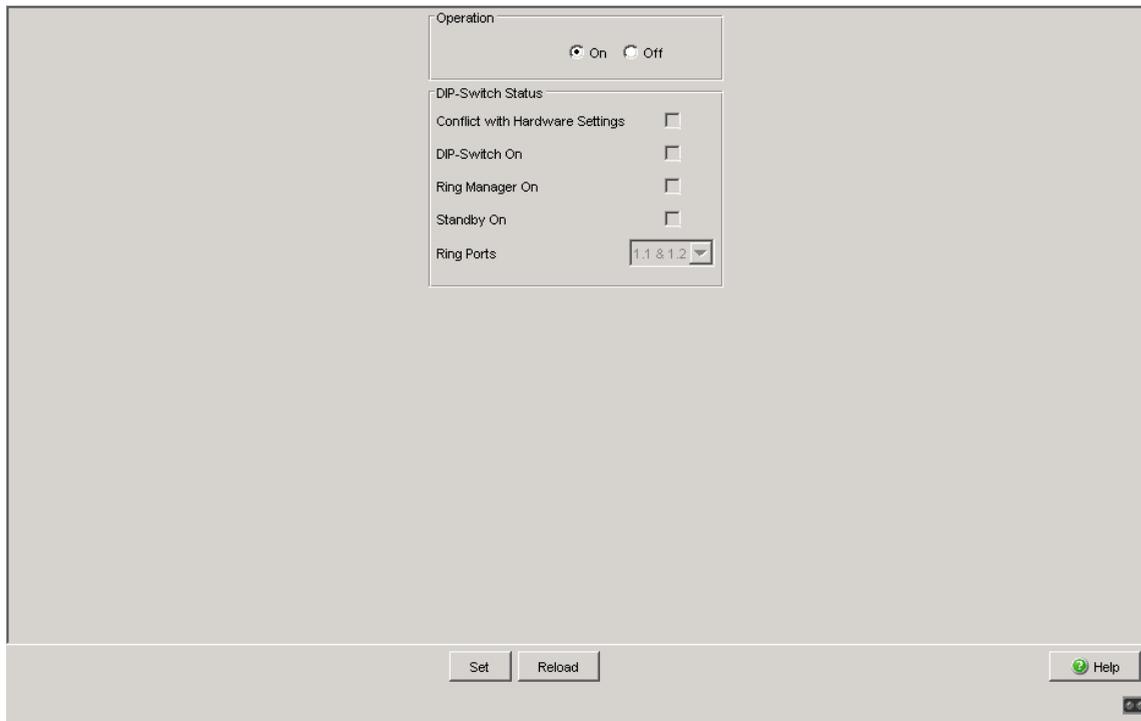


Figure 66: *Advanced:DIP-Switch dialog*

■ Buttons

Button	Meaning
Set	Transfers the changes to the volatile memory (RAM) of the device. To permanently save the changes afterwards, you open the <i>Basic Settings:Load/Save</i> dialog and click "Save".
Reload	Updates the fields with the values that are saved in the volatile memory (RAM) of the device.
Help	Opens the online help.

Table 152: *Buttons*

8.4 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.

■ Buttons

Button	Meaning
Help	Opens the online help.

Table 153: Buttons

A Appendix

A.1 Technical Data

Switching	
Size of MAC address table (incl. static filters)	8,000 (16,000 for PowerMICE and MACH 4000)
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	1,632 bytes

VLAN	
VLAN ID	1 to 4,042
Number of VLANs	max. 255 simultaneously per device max. 255 simultaneously per port
Number of VLANs in GMRP in VLAN 1	max. 255 simultaneously per device max. 255 simultaneously per port

A.2 List of RFCs

RFC 768	UDP
RFC 783	TFTP
RFC 791	IP
RFC 792	ICMP
RFC 793	TCP
RFC 826	ARP
RFC 951	BOOTP
RFC 1157	SNMPv1
RFC 1155	SMIv1
RFC 1212	Concise MIB Definitions
RFC 1213	MIB2
RFC 1493	Dot1d
RFC 1643	Ethernet-like -MIB
RFC 1757	RMON
RFC 1769	SNTP
RFC 1867	Form-Based File Upload in HTML
RFC 1901	Community based SNMP v2
RFC 1905	Protocol Operations for SNMP v2
RFC 1906	Transport Mappings for SNMP v2
RFC 1907	Management Information Base for SNMP v2
RFC 1908	Coexistence between SNMP v1 and SNMP v2
RFC 1945	HTTP/1.0
RFC 2068	HTTP/1.1 protocol as updated by draft-ietf-http-v11-spec-rev-03
RFC 2233	The Interfaces Group MIB using SMI v2
RFC 2246	The TLS Protocol, Version 1.0
RFC 2271	SNMP Framework MIB
RFC 2346	AES Ciphersuites for Transport Layer Security
RFC 2365	Administratively Scoped Boundaries
RFC 2474	Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers
RFC 2475	An Architecture for Differentiated Service
RFC 2570	Introduction to SNMP v3
RFC 2571	Architecture for Describing SNMP Management Frameworks
RFC 2572	Message Processing and Dispatching for SNMP
RFC 2573	SNMP v3 Applications
RFC 2574	User Based Security Model for SNMP v3
RFC 2575	View Based Access Control Model for SNMP
RFC 2576	Coexistence between SNMP v1, v2 & v3
RFC 2578	SMIv2

RFC 2579	Textual Conventions for SMI v2
RFC 2580	Conformance statements for SMI v2
RFC 2618	RADIUS Authentication Client MIB
RFC 2620	RADIUS Accounting MIB
RFC 2674	Dot1p/Q
RFC 2818	HTTP over TLS
RFC 2851	Internet Addresses MIB
RFC 2865	RADIUS Client
RFC 3164	The BSD Syslog Protocol

A.3 Underlying IEEE Standards

IEEE 802.1AB	Topology Discovery (LLDP)
IEEE 802.1af	Power over Ethernet
IEEE 802.1D-1998, IEEE 802.1D-2004	Media access control (MAC) bridges (includes IEEE 802.1p Priority and Dynamic Multicast Filtering, GARP, GMRP)
IEEE 802.1Q-2005	Spanning Tree (STP), Rapid Spanning Tree (RSTP), Multiple Spanning Tree (MSTP)
IEEE 802.3-2002	Ethernet
IEEE 802.3ac	VLAN Tagging
IEEE 802.3x	Flow Control

A.4 Underlying IEC Norms

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

A.5 Literature references

- ▶ “TCP/IP Illustrated”, Vol. 1
W.R. Stevens
Addison Wesley 1994
ISBN 0-201-63346-9
- ▶ Hirschmann “Installation” user manual
- ▶ Hirschmann “Basic Configuration” user manual
- ▶ Hirschmann “Redundancy Configuration” user manual
- ▶ Hirschmann “Routing Configuration” user manual
- ▶ Hirschmann “GUI Graphical User Interface” reference manual
- ▶ Hirschmann “Command Line Interface” reference manual

A.6 Copyright of Integrated Software

A.6.1 Bouncy Castle Crypto APIs (Java)

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

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

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

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

A.6.2 Broadcom Corporation

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

B Readers' Comments

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

Your assessment of this manual:

	Very good	Good	Satisfactory	Mediocre	Poor
Precise description	<input type="radio"/>				
Readability	<input type="radio"/>				
Understandability	<input type="radio"/>				
Examples	<input type="radio"/>				
Structure	<input type="radio"/>				
Completeness	<input type="radio"/>				
Graphics	<input type="radio"/>				
Drawings	<input type="radio"/>				
Tables	<input type="radio"/>				

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

Readers' Comments

Suggestions for improvement and additional information:

General comments:

Sender:

Company / Department:

Name / Telephone no.:

Street:

Zip code / City:

e-mail:

Date / Signature:

Dear User,

Please fill out and return this page

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

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

C Index

1

802.1D/p mapping 146

A

ACA (AutoConfiguration Adapter) 40, 211

Acceptable Frame Types 136

Address Conflict Detection (ACD) 217

Advanced 229

AF 149

Aging Time 110

Alarm 210

Assured Forwarding 149

AutoConfiguration Adapter (ACA) 211

B

Basic Settings 19

BPDU Guard 173

Broadcast Limiter 118

C

Cable crossing 35

CLI 245

Class Selector 148

Clock 87

Coldstart 55

Cold start (after software update) 32, 32

Command Line Interface 245

Current VLAN Dialog 131

D

DHCP Relay Agent 230

DIP switch 154

Diagnostics 185

DiffServ 139

DSCP 139

E

EF 148

EtherNet/IP 238

Event Log 216

Event log 190

Expedited Forwarding 148

F

FAQ 263

Filters for MAC addresses 114

Firmware update 30

Forward Delay 172, 174

G

Grandmaster 98

Graphical User Interface (GUI) 13

H

Hello Time 172, 174

HIPER-Ring 135, 154, 154

HIPER-Ring (source for alarms) 211

HiView 13

I

IGMP querier 121

IGMP settings 121

IGMP snooping 121

Independent VLAN 129

Industrial HiVision 10

Industry protocols 9, 235

Ingress Filtering 137

IP DSCP mapping 139, 148

IP DSCP value 140

J

Java Runtime Environment 19

L

Link State (Port) 34

LLDP 198

Login Banner 74, 75

Login window 15

M

Max Age 172, 174

Media module (for modular devices) 21

MRP-Ring 135, 158, 158

Multicasts 120

N

Network load 168, 194

Network management station 198

O

One-Switch coupling 164

Operating instructions (GUI) 16

P

Password 58, 59

Per-Hop-Behavior (PHB) 148

PHY Fast Startup per Port 237

Ports 192

Port configuration	34, 144	SFP Module	196
Port configuration (QoS/priority)	144	SFP Status Display	196
Port Mirroring	200	Shared VLAN	129
Port priority	144, 145	Signal contact	205
Port State (Link)	34	Signal contact (source for alarm)	211
Port security (IP-/MAC-based)	67	SNMPv1/v2 access settings	61
Port security (source for alarms)	69, 73	SNMP logging	186
Port statistics table	192	SNTP Broadcasts	84
Port VLAN ID	136	SNTP server	233
Power over ETHERNET	37	Software update	30
PROFINET IO	9, 235	Spanning Tree (STP)	168
Precedence	148	Starting the graphical user interface	13
Precision Time Protocol	87	Statistics table	192
Pre-login Banner	74	Status line via menu	16
Priority queue	141	Supply voltage	211
PTP	87	Switching	109
		Symbol	11
		Syslog	186
		System Information	215
		System requirements (GUI)	13
		System time	84
Q		T	
QoS/Priority	139	Technical Questions	263
R		Telnet Access	64
RAM test	222	Temperature (device)	21
Rapid Spanning Tree (RSTP)	168, 176	Temperature (SFPs)	196
Rate Limiter	117	Time	79, 80
Rate Limiter Settings	118	Time Management	87
Reboot	55	Time Stamp Unit	88
Receiver power status	211	Topology	198
Redundancy	9, 151, 168	ToS	139
Reference clock	98	Training Courses	263
Report	213	Trap	210
Request Interval (SNTP)	84	TrustDot1p (global trust mode)	141
Restart	55	TrustIpDscp	141
Restore default settings	40	Trust mode	141
Restore state on delivery	40	Two-switch coupling	164
RFC	249	TX Hold Count	172
Ring	152	Type of Service	139
Ring Manager	152	U	
Ring port	154	Untrusted (global trust mode)	141
Ring Redundancy	151	V	
Ring structure	152	VLAN	127
Ring/Network coupling	135, 151, 162, 203	VLAN 0	29
Ring/Network coupling (source for alarms)	211	VLAN and GOOSE Protocol	128
RMON probe	200	VLAN and redundancy rings	137
RM Function	152	VLAN Global dialog	127
Root bridge	169	VLAN ID (network parameter)	27
S		VLAN Mapping	139
Saving a configuration profile (GUI)	17		
Security	57		
Self-test	222		
Service Mode	224		

Index

VLAN Mode	129
VLAN Port dialog	136
VLAN priority	140
VLAN Static dialog	133
VLAN (HIPER-Ring)	156
W	
Web Access	64

D Further Support

■ Technical Questions

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

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

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

You can contact us

in the EMEA region at

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

in the America region at

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

in the Asia-Pacific region at

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

■ Hirschmann Competence Center

The Hirschmann Competence Center is ahead of its competitors:

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

The current technology and product training courses can be found at <http://www.hicomcenter.com>

- ▶ Support ranges from the first installation through the standby service to maintenance concepts.

With the Hirschmann Competence Center, you have decided against making any compromises. Our client-customized package leaves you free to choose the service components you want to use.

Internet:

<http://www.hicomcenter.com>



HIRSCHMANN

A **BELDEN** BRAND



HIRSCHMANN

A **BELDEN** BRAND

Reference Manual

**CLI Command Line Interface
Industrial ETHERNET (Gigabit) Switch
RS20/RS30/RS40, MS20/MS30**

L2E Rel. 9.0

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.

© 2015 Hirschmann Automation and Control GmbH

Manuals and software are protected by copyright. All rights reserved. The copying, reproduction, translation, conversion into any electronic medium or machine scannable form is not permitted, either in whole or in part. An exception is the preparation of a backup copy of the software for your own use. For devices with embedded software, the end-user license agreement on the enclosed CD/DVD applies.

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

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

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

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

Content

Content	3
About this Manual	15
Maintenance	17
Service Shell	19
Permanently disabling the Service Shell	19
1 Command Structure	21
1.1 Format	22
1.1.1 Command	23
1.1.2 Parameters	23
1.1.3 Values	23
1.1.4 Conventions	25
1.1.5 Annotations	26
1.1.6 Special keys	27
1.1.7 Secrets in scripts	29
2 Quick Start up	31
2.1 Quick Starting the Switch	32
2.2 System Info and System Setup	33
3 Mode-based CLI	39
3.1 Mode-based Topology	40
3.2 Mode-based Command Hierarchy	41
3.3 Flow of Operation	43
3.4 “No” Form of a Command	45
3.4.1 Support for “No” Form	45
3.4.2 Behavior of Command Help (“?”)	45
4 CLI Commands: Base	47
4.1 System Information and Statistics	48

4.1.1	show	48
4.1.2	show address-conflict	48
4.1.3	show arp switch	49
4.1.4	show bridge address-learning	49
4.1.5	show bridge address-relearn-detect	50
4.1.6	show bridge aging-time	50
4.1.7	show bridge duplex-mismatch-detect	51
4.1.8	show bridge framesize	51
4.1.9	show bridge vlan-learning	51
4.1.10	bridge framesize	52
4.1.11	show config-watchdog	52
4.1.12	show device-status	53
4.1.13	show authentication	54
4.1.14	show eventlog	54
4.1.15	show interface	55
4.1.16	show interface ethernet	57
4.1.17	show interface switchport	64
4.1.18	show interface utilization	65
4.1.19	show logging	66
4.1.20	show mac-address-conflict	67
4.1.21	show mac-addr-table	68
4.1.22	show signal-contact	69
4.1.23	show slot	71
4.1.24	show running-config	72
4.1.25	show sysinfo	73
4.1.26	show temperature	75
4.1.27	utilization alarm-threshold	76
4.2	Management VLAN Commands	77
4.2.1	network mgmt_vlan	77
4.3	Class of Service (CoS) Commands	78
4.3.1	classofservice dot1p-mapping	79
4.3.2	classofservice ip-dscp-mapping	80
4.3.3	classofservice trust	81
4.3.4	show classofservice dot1p-mapping	82
4.3.5	show classofservice ip-dscp-mapping	83
4.3.6	show classofservice trust	84
4.3.7	vlan port priority all	84
4.3.8	vlan priority	85
4.4	Management Commands	86

4.4.1	transport input telnet	86
4.4.2	bridge address-learning	87
4.4.3	bridge address-relearn detect operation	87
4.4.4	bridge address-relearn detect threshold	87
4.4.5	bridge aging-time	89
4.4.6	bridge fast-link-detection	90
4.4.7	bridge duplex-mismatch-detect operation	90
4.4.8	bridge vlan-learning	91
4.4.9	ethernet-ip	91
4.4.10	network mgmt-access add	92
4.4.11	network mgmt-access delete	92
4.4.12	network mgmt-access modify	93
4.4.13	network mgmt-access operation	94
4.4.14	network mgmt-access status	95
4.4.15	network parms	95
4.4.16	network protocol	96
4.4.17	network priority	97
4.4.18	profinetio	98
4.4.19	serial timeout	99
4.4.20	set prompt	99
4.4.21	show ethernet-ip	100
4.4.22	show network	100
4.4.23	show network mgmt-access	102
4.4.24	show profinetio	103
4.4.25	show serial	103
4.4.26	show snmp-access	104
4.4.27	show snmpcommunity	105
4.4.28	show snmp sync	106
4.4.29	show snmptrap	107
4.4.30	show telnet	108
4.4.31	show telnetcon	109
4.4.32	show trapflags	110
4.4.33	snmp-access global	111
4.4.34	snmp-access version	112
4.4.35	snmp-access version v3-encryption	113
4.4.36	snmp-server	114
4.4.37	snmp-server community	115
4.4.38	snmp-server contact	116
4.4.39	snmp-server community ipaddr	117
4.4.40	snmp-server community ipmask	118
4.4.41	snmp-server community mode	119

4.4.42	snmp-server community ro	120
4.4.43	snmp-server community rw	120
4.4.44	snmp-server location	120
4.4.45	snmp-server sysname	121
4.4.46	snmp-server enable traps	121
4.4.47	snmp-server enable traps chassis	122
4.4.48	snmp-server enable traps l2redundancy	123
4.4.49	snmp-server enable traps linkmode	124
4.4.50	snmp-server enable traps multiusers	125
4.4.51	snmp-server enable traps port-sec	126
4.4.52	snmp-server enable traps stpmode	127
4.4.53	snmptrap	128
4.4.54	snmptrap ipaddr	129
4.4.55	snmptrap mode	130
4.4.56	snmptrap snmpversion	131
4.4.57	telnetcon maxsessions	132
4.4.58	telnetcon timeout	133
4.5	Syslog Commands	134
4.5.1	logging buffered	134
4.5.2	logging buffered wrap	135
4.5.3	logging cli-command	136
4.5.4	logging console	137
4.5.5	logging host	138
4.5.6	logging host reconfigure	139
4.5.7	logging host remove	139
4.5.8	logging snmp-requests get operation	139
4.5.9	logging snmp-requests set operation	140
4.5.10	logging snmp-requests get severity	140
4.5.11	logging snmp-requests set severity	141
4.5.12	logging syslog	142
4.5.13	logging syslog port	142
4.6	Device Configuration Commands	143
4.6.1	auto-disable reason	143
4.6.2	auto-disable reset	145
4.6.3	auto-disable timer	145
4.6.4	auto-negotiate	146
4.6.5	auto-negotiate all	147
4.6.6	cable-crossing	148
4.6.7	media-module	149
4.6.8	dip-switch operation	150

4.6.9	macfilter	151
4.6.10	macfilter adddest	152
4.6.11	macfilter adddest all	153
4.6.12	monitor session	154
4.6.13	monitor session mode	156
4.6.14	monitor session <session-id> source/destination	157
4.6.15	set igmp	158
4.6.16	set igmp	159
4.6.17	set igmp aging-time-unknown	159
4.6.18	set igmp automatic-mode	160
4.6.19	set igmp forward-all	161
4.6.20	set igmp forward-unknown	162
4.6.21	set igmp static-query-port	163
4.6.22	set igmp groupmembershipinterval	164
4.6.23	set igmp interfacemode	165
4.6.24	set igmp lookup-interval-unknown	165
4.6.25	set igmp lookup-resp-time-unknown	166
4.6.26	set igmp maxresponse	167
4.6.27	set igmp querier max-response-time	168
4.6.28	set igmp querier protocol-version	168
4.6.29	set igmp querier status	169
4.6.30	set igmp querier tx-interval	169
4.6.31	set igmp query-ports-to-filter	170
4.6.32	selftest ramtest	170
4.6.33	selftest reboot-on-hdxerror	171
4.6.34	selftest reboot-on-error	172
4.6.35	serviceshell	173
4.6.36	update module-configuration	173
4.6.37	show auto-disable brief	174
4.6.38	show auto-disable reasons	175
4.6.39	show dip-switch	176
4.6.40	show igmpsnooping	177
4.6.41	show mac-filter-table igmpsnooping	178
4.6.42	show mac-filter-table multicast	179
4.6.43	show mac-filter-table static	180
4.6.44	show mac-filter-table staticfiltering	181
4.6.45	show mac-filter-table stats	182
4.6.46	show monitor session	183
4.6.47	show port	184
4.6.48	show rmon-alarm	185
4.6.49	show selftest	186

4.6.50	show serviceshell	186
4.6.51	show storm-control	187
4.6.52	show storm-control limiters port	187
4.6.53	show vlan	188
4.6.54	show vlan brief	190
4.6.55	show vlan port	191
4.6.56	shutdown	192
4.6.57	shutdown all	193
4.6.58	snmp sync community-to-v3	194
4.6.59	snmp sync v3-to-community	195
4.6.60	snmp trap link-status	195
4.6.61	snmp trap link-status all	196
4.6.62	spanning-tree bpdumigrationcheck	197
4.6.63	speed	198
4.6.64	storm-control broadcast	199
4.6.65	storm-control egress-limiting	199
4.6.66	storm-control ingress-limiting	200
4.6.67	storm-control ingress-mode	200
4.6.68	storm-control broadcast (port-related)	201
4.6.69	storm-control egress-limit	201
4.6.70	storm-control ingress-limit	202
4.6.71	storm-control ingress-mode	202
4.6.72	storm-control flowcontrol	203
4.6.73	storm-control flowcontrol per port	204
4.6.74	vlan	205
4.6.75	vlan0-transparent-mode	206
4.6.76	vlan acceptframe	207
4.6.77	vlan database	208
4.6.78	vlan ingressfilter	209
4.6.79	vlan name	210
4.6.80	vlan participation	211
4.6.81	vlan participation all	212
4.6.82	vlan port acceptframe all	213
4.6.83	vlan port ingressfilter all	214
4.6.84	vlan port pvid all	215
4.6.85	vlan port tagging all	216
4.6.86	vlan pvid	217
4.6.87	vlan tagging	218
4.7	User Account Management Commands	219
4.7.1	disconnect	219

4.7.2	show loginsession	220
4.7.3	show users	221
4.7.4	users defaultlogin	222
4.7.5	users login <user>	222
4.7.6	users access	223
4.7.7	users name	224
4.7.8	users passwd	225
4.7.9	users snmpv3 accessmode	226
4.7.10	users snmpv3 authentication	227
4.7.11	users snmpv3 encryption	228
4.8	System Utilities	229
4.8.1	address-conflict	229
4.8.2	boot skip-aca-on-boot	230
4.8.3	show boot skip-aca-on-boot	230
4.8.4	clear eventlog	231
4.8.5	traceroute	231
4.8.6	clear arp-table-switch	232
4.8.7	clear config	232
4.8.8	clear config factory	232
4.8.9	clear counters	233
4.8.10	clear hiper-ring	233
4.8.11	clear igmpsnooping	233
4.8.12	clear mac-addr-table	234
4.8.13	clear pass	234
4.8.14	clear signal-contact	235
4.8.15	clear traplog	235
4.8.16	clear ring-coupling	236
4.8.17	clear vlan	236
4.8.18	config-watchdog	237
4.8.19	copy	237
4.8.20	device-status connection-error	243
4.8.21	device-status monitor	244
4.8.22	logout	245
4.8.23	mac-address conflict operation	245
4.8.24	ping	246
4.8.25	signal-contact connection-error	246
4.8.26	signal-contact	247
4.8.27	temperature	248
4.8.28	reboot	249
4.8.29	show reboot	250

4.8.30	reload	251
4.8.31	show reload	252
4.8.32	set clibanner	253
4.8.33	set pre-login-banner	255
4.9	LLDP - Link Layer Discovery Protocol	257
4.9.1	show lldp	257
4.9.2	show lldp config	257
4.9.3	show lldp config chassis	258
4.9.4	show lldp config chassis admin-state	258
4.9.5	show lldp config chassis notification-interval	258
4.9.6	show lldp config chassis re-init-delay	259
4.9.7	show lldp config chassis tx-delay	259
4.9.8	show lldp config chassis tx-hold-mult	259
4.9.9	show lldp config chassis tx-interval	260
4.9.10	show lldp config port	261
4.9.11	show lldp config port tlv	262
4.9.12	show lldp remote-data	263
4.9.13	lldp	265
4.9.14	lldp config chassis admin-state	266
4.9.15	lldp config chassis notification-interval	266
4.9.16	lldp config chassis re-init-delay	267
4.9.17	lldp config chassis tx-delay	267
4.9.18	lldp config chassis tx-hold-mult	268
4.9.19	lldp chassis tx-interval	268
4.9.20	clear lldp config all	269
4.9.21	lldp admin-state	269
4.9.22	lldp fdb-mode	270
4.9.23	lldp hm-mode	270
4.9.24	lldp max-neighbors	271
4.9.25	lldp notification	271
4.9.26	lldp tlv link-aggregation	271
4.9.27	lldp tlv mac-phy-config-state	272
4.9.28	lldp tlv max-frame-size	272
4.9.29	lldp tlv mgmt-addr	272
4.9.30	lldp tlv pnio	273
4.9.31	lldp tlv pnio-alias	273
4.9.32	lldp tlv pnio-mrp	273
4.9.33	lldp tlv port-desc	274
4.9.34	lldp tlv port-vlan	274
4.9.35	lldp tlv gmrp	274

4.9.36	lldp tlv igmp	275
4.9.37	lldp tlv portsec	275
4.9.38	lldp tlv ptp	275
4.9.39	lldp tlv protocol	276
4.9.40	lldp tlv sys-cap	276
4.9.41	lldp tlv sys-desc	276
4.9.42	lldp tlv sys-name	277
4.9.43	lldp tlv vlan-name	277
4.9.44	name	278
4.10	SNTP - Simple Network Time Protocol	279
4.10.1	show sntp	279
4.10.2	show sntp anycast	281
4.10.3	show sntp client	281
4.10.4	show sntp operation	282
4.10.5	show sntp server	283
4.10.6	show sntp status	283
4.10.7	show sntp time	284
4.10.8	no sntp	284
4.10.9	sntp anycast address	285
4.10.10	sntp anycast transmit-interval	285
4.10.11	sntp anycast vlan	286
4.10.12	sntp client accept-broadcast	286
4.10.13	sntp client disable-after-sync	287
4.10.14	sntp client offset	287
4.10.15	sntp client request-interval	288
4.10.16	no sntp client server	288
4.10.17	sntp client server primary	289
4.10.18	sntp client server secondary	290
4.10.19	sntp client threshold	291
4.10.20	sntp operation	292
4.10.21	sntp server disable-if-local	293
4.10.22	sntp time system	293
4.11	PoE - Power over Ethernet	294
4.11.1	show inlinepower	294
4.11.2	show inlinepower port	295
4.11.3	inlinepower (Global Config)	298
4.11.4	inlinepower (Interface Config)	299
4.11.5	clear inlinepower	300

5	CLI Commands: Switching	301
5.1	Spanning Tree Commands	303
5.1.1	show spanning-tree	303
5.1.2	show spanning-tree interface	306
5.1.3	show spanning-tree mst detailed	307
5.1.4	show spanning-tree mst port detailed	308
5.1.5	show spanning-tree mst port summary	311
5.1.6	show spanning-tree mst summary	312
5.1.7	show spanning-tree summary	313
5.1.8	show spanning-tree vlan	314
5.1.9	spanning-tree	315
5.1.10	spanning-tree auto-edgeport	316
5.1.11	spanning-tree bpduguard	317
5.1.12	spanning-tree configuration name	318
5.1.13	spanning-tree configuration revision	319
5.1.14	spanning-tree edgeport	320
5.1.15	spanning-tree forceversion	321
5.1.16	spanning-tree forward-time	322
5.1.17	spanning-tree guard loop	323
5.1.18	spanning-tree guard none	324
5.1.19	spanning-tree guard root	325
5.1.20	spanning-tree hello-time	326
5.1.21	spanning-tree hold-count	326
5.1.22	spanning-tree max-age	327
5.1.23	spanning-tree max-hops	328
5.1.24	spanning-tree mst	329
5.1.25	spanning-tree mst priority	331
5.1.26	spanning-tree mst vlan	332
5.1.27	spanning-tree mst instance	333
5.1.28	spanning-tree port mode	334
5.1.29	spanning-tree port mode all	335
5.1.30	spanning-tree stp-mrp-mode	336
5.1.31	spanning-tree tcnguard	337
5.2	MRP	338
5.2.1	show mrp	338
5.2.2	show mrp current-domain	339
5.2.3	mrp current-domain	340
5.2.4	mrp delete-domain	342
5.2.5	mrp new-domain	342

5.3	HIPER-Ring	343
5.3.1	show hiper-ring	344
5.3.2	hiper-ring	345
5.3.3	hiper-ring mode	345
5.3.4	hiper-ring port primary	346
5.3.5	hiper-ring port secondary	346
5.3.6	hiper-ring recovery-delay	347
5.4	Fast-HIPER-Ring	348
5.4.1	fast-hiper-ring	351
5.5	Redundant Coupling	353
5.5.1	show ring-coupling	354
5.5.2	ring-coupling	356
5.5.3	ring-coupling config	357
5.5.4	ring-coupling net-coupling	358
5.5.5	ring-coupling operation	358
5.5.6	ring-coupling port	359
5.5.7	ring-coupling redundancy-mode	359
5.6	Port Security	360
5.6.1	show port-sec dynamic	360
5.6.2	show port-sec mode	361
5.6.3	show port-sec port	362
5.6.4	port-sec mode	362
5.6.5	port-sec action	363
5.6.6	port-sec allowed-ip	364
5.6.7	port-sec allowed-ip add	364
5.6.8	port-sec allowed-ip remove	365
5.6.9	port-sec allowed-mac	365
5.6.10	port-sec allowed-mac add	366
5.6.11	port-sec allowed-mac remove	366
5.6.12	port-sec dynamic	367
5.6.13	clear port-sec	367
5.7	DHCP Relay Commands	368
5.7.1	dhcp-relay	369
5.7.2	dhcp-relay	370
5.7.3	show dhcp-relay	371
6	CLI Commands: Security	373
6.1	Security Commands	375
6.1.1	users login	375

6.2	HTTP Commands	376
6.2.1	ip http server	376
6.2.2	show ip http	377
6.2.3	ip https server	378
6.2.4	ip https port	379
6.2.5	ip https certgen	379
6.2.6	show ip https	380
7	Appendix- VLAN Example	381
7.1	SOLUTION 1	383
7.2	SOLUTION 2	385
8	Index	387
9	Glossary	397
10	Further support	413

About this Manual

The "GUI" reference manual contains detailed information on using the graphical user interface (web-based interface) to operate the individual functions of the device.

The "Command Line Interface" reference manual contains detailed information on using the Command Line Interface to operate the individual functions of the device.

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

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

The "Redundancy Configuration" user manual contains the information you need to select a suitable redundancy procedure and configure that procedure.

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 or PROFINET IO.

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

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

Maintenance

Hirschmann are continually working on improving and developing their software. You should regularly check whether there is a new version of the software that provides you with additional benefits. You will find software information and downloads on the product pages of the Hirschmann website

Service Shell

A service technician uses the Service Shell function for maintenance of your functioning device. If you need service support, this function allows the service technician to access internal functions of your device from an external location.

Note: The Service Shell function is for service purposes exclusively. This function allows the access on internal functions of the device. In no case, execute internal functions without service technician instructions. Executing internal functions such as deleting the content of the NVM (non-volatile memory) possibly leads to inoperability of your device.

Permanently disabling the Service Shell

If you do not need the Service Shell, the device allows you to disable the function. In this case you still have the option to configure the device. Though, the service technician has no possibilities to access internal functions of your device to call up additional required information.

Note: Disabling the Service Shell function produces a permanent effect. This process is irreversible.

To reactivate the Service Shell function, send the device back to the manufacturer.

- To display the Service Shell function, enter `serviceshell` and a space, and then a question mark `?`
- To permanently deactivate the Shell Service function, enter `serviceshell deactivate` and a space, and press the enter key.

1 Command Structure

The Command Line Interface (CLI) syntax, conventions and terminology are described in this section. Each CLI command is illustrated using the structure outlined below.

1.1 Format

Commands are followed by values, parameters, or both.

■ Example 1

```
network parms <ipaddr> <netmask> [gateway]
```

- ▶ network parms
is the command name.
- ▶ <ipaddr> <netmask>
are the required values for the command.
- ▶ [gateway]
is the optional value for the command.

■ Example 2

```
snmp-server location <loc>
```

- ▶ snmp-server location
is the command name.
- ▶ <loc>
is the required parameter for the command.

■ Example 3

```
clear vlan
```

- ▶ clear vlan
is the command name.

1.1.1 Command

The text in courier font is to be typed exactly as shown.

1.1.2 Parameters

Parameters are order dependent.

Parameters may be mandatory values, optional values, choices, or a combination.

- ▶ `<parameter>`. The `<>` angle brackets indicate that a mandatory parameter is to be entered in place of the brackets and text inside them.
- ▶ `[parameter]`. The `[]` square brackets indicate that an optional parameter may be entered in place of the brackets and text inside them.
- ▶ `choice1 | choice2`. The `|` indicates that only one of the parameters should be entered.
- ▶ The `{}` curly braces indicate that a parameter must be chosen from the list of choices.

1.1.3 Values

macaddr

The MAC address format is six hexadecimal numbers separated by colons, for example 00:06:29:32:81:40.

areaid

Area IDs may be entered in dotted-decimal notation (for example, 0.0.0.1). An area ID of 0.0.0.0 is reserved for the backbone. Area IDs have the same form as IP addresses, but are distinct from IP addresses. The IP network address of the

sub-netted network may be used for the area ID.

slot/port

Valid slot and port number separated by forward slashes. For example, 1/1 represents slot number 1 and port number 1.

logical slot/port

Logical slot and port number. This is applicable in the case of a link-aggregation (LAG) and vlan router interfaces (9/x). The operator can use the logical slot/port to configure the link-aggregation.

1.1.4 Conventions

Network addresses are used to define a link to a remote host, workstation or network. Network addresses are shown using the following syntax:

Address Type	Format	Range
ipaddr	192.168.11.110	0.0.0.0 to 255.255.255.255 (decimal)
macaddr	A7:C9:89:DD:A9:B3	hexadecimal digit pairs

Table 1: Network Address Syntax

Double quotation marks such as "System Name with Spaces" set off user defined strings. If the operator wishes to use spaces as part of a name parameter then it must be enclosed in double quotation marks.

Empty strings ("") are not valid user defined strings.

Command completion finishes spelling the command when enough letters of a command are typed to uniquely identify the command word. The command may be executed by typing <enter> (command abbreviation) or the command word may be completed by typing the <tab> or <space bar> (command completion).

The value 'Err' designates that the requested value was not internally accessible.

The value of '-----' designates that the value is unknown.

1.1.5 Annotations

The CLI allows the user to type single-line annotations at the command prompt for use when writing test or configuration scripts and for better readability. The exclamation point (!) character flags the beginning of a comment. The comment flag character can begin a word anywhere on the command line and all input following this character is ignored. Any command line that begins with the character ! is recognized as a comment line and ignored by the parser.

Some examples are provided below:

```
! Script file for setting the CLI prompt
set prompt example-switch
! End of the script file
```

1.1.6 Special keys

The following list of special keys may be helpful to enter command lines.

BS	delete previous character
Ctrl-A	go to beginning of line
Ctrl-E	go to end of line
Ctrl-F	go forward one character
Ctrl-B	go backward one character
Ctrl-D	delete current character
Ctrl-H	display command history or retrieve a command
Ctrl-U, X	delete to beginning of line
Ctrl-K	delete to end of line
Ctrl-W	delete previous word
Ctrl-T	transpose previous character
Ctrl-P	go to previous line in history buffer
Ctrl-R	rewrites or pastes the line
Ctrl-N	go to next line in history buffer
Ctrl-Y	print last deleted character
Ctrl-Q	enables serial flow
Ctrl-S	disables serial flow
Ctrl-Z	return to root command prompt
Tab, <SPACE>	command-line completion
Exit	go to next lower command prompt
?	list choices

The commands with strings that may contain these special characters are listed below.

Note: Not every string is allowed to contain special characters. The string that is output with the escape characters (if necessary) is shown as "...".

Command	Note
!System Description "..."	"At the beginning of the script
!System Version "..."	"At the beginning of the script

Tab. 2: Commands in Privileged Exec mode

Command	Note
snmp-server location "..."	
snmp-server contact "..."	
snmp-server community "..."	
snmp-server community ipaddr <ip> "..."	
snmp-server community ipmask <ip> "..."	
snmp-server community ro "..."	
snmp-server community rw "..."	
no snmp-server community mode "..."	
no snmp-server community "..."	
spanning-tree configuration name "..."	
ptp subdomain-name "..."	

Tab. 3: Commands in Global Config mode

Command	Note
name "..."	

Tab. 4: Commands in Interface Config mode

Command	Note
vlan name <n> "..."	

Tab. 5: Commands in VLAN Database mode

When a device creates a script, a human-readable header is included that lists the special characters and the escape characters:

```
!Parameter string escape handling \, 1
!Characters to be preceded with escape char (\): \, !, ", ', ?
```

1.1.7 Secrets in scripts

A configuration may include secrets (e. g., passwords). When creating a script, these secrets are written to it in a scrambled form, not in clear text. These secrets may be up to 31 characters long. The format for a scrambled secret is: ":v1:<scrambled secret>:" (without the quotes (")), they were added for readability). v1 denotes the scrambling method (v1 in this case), the value of the scrambled secret is a 64-digit hex string.

The following commands produce scrambled secrets (if necessary):

Command	Note
radius server key acct <ip> <password>	
radius server key auth <ip> <password>	
users passwd <username> <password>	
users snmpv3 encryption <username> des <password>	

Tab. 6: Commands in Global Config mode

Applying or validating a script requires the following conditions for a scrambled secret, else it will be considered invalid (usually only relevant if a script is edited manually):

- ▶ string must not be longer than 64 hex digits
- ▶ string must only contain the digits 0-9 and the characters A-F (or a-f)
- ▶ string length must be even

2 Quick Start up

The CLI Quick Start up details procedures to quickly become acquainted with the software.

2.1 Quick Starting the Switch

- ▶ Read the device Installation Guide for the connectivity procedure. In-band connectivity allows access to the software locally or from a remote workstation. The device must be configured with IP information (IP address, subnet mask, and default gateway).
- ▶ Turn the Power on.
- ▶ Allow the device to load the software until the login prompt appears. The device's initial state is called the default mode.
- ▶ When the prompt asks for operator login, execute the following steps:
 - ▶ Type the word `admin` in the login area. Since a number of the Quick Setup commands require administrator account rights, we recommend logging into an administrator account. Press the enter key.
 - ▶ Enter the state on delivery password `private`.
 - ▶ Press the enter key
 - ▶ The CLI User EXEC prompt will be displayed.
User EXEC prompt:
`(Hirschmann Product) >`
 - ▶ Use “enable” to switch to the Privileged EXEC mode from User EXEC.
Privileged EXEC prompt:
`(Hirschmann Product) #`
 - ▶ Use “configure” to switch to the Global Config mode from Privileged EXEC.
Global Config prompt:
`(Hirschmann Product) (Config) #`
 - ▶ Use “exit” to return to the previous mode.

2.2 System Info and System Setup

This chapter informs you about:

- ▶ Quick Start up Software Version Information
- ▶ Quick Start up Physical Port Data
- ▶ Quick Start up User Account Management
- ▶ Quick Start up IP Address
- ▶ Quick Start up Uploading from Switch to Out-of-Band PC (Only XMODEM)
- ▶ Quick Start up Downloading from Out-of-Band PC to Switch (Only XMODEM)
- ▶ Quick Start up Downloading from TFTP Server
- ▶ Quick Start up Factory Defaults

■ Quick Start up Physical Port Data

Command	Details
show port all (in Privileged EXEC)	Displays the Ports slot/port Type - Indicates if the port is a special type of port Admin Mode - Selects the Port Control Administration State Physical Mode - Selects the desired port speed and duplex mode Physical Status - Indicates the port speed and duplex mode Link Status - Indicates whether the link is up or down Link Trap - Determines whether or not to send a trap when link status changes LACP Mode - Displays whether LACP is enabled or disabled on this port.

Table 7: Quick Start up Physical Port Data

■ Quick Start up User Account Management

Command	Details
show users (in Privileged EXEC)	Displays all of the users that are allowed to access the switch Access Mode - Shows whether the user is able to change parameters on the switch(Read/Write) or is only able to view them (Read Only). As a factory default, the 'admin' user has Read/Write access and the 'user' user has Read Only access. There can only be one Read/Write user and up to five Read Only users.
show login session (in User EXEC)	Displays all of the login session information

Table 8: Quick Start up User Account Management

Command	Details
<pre>users passwd <user- name></pre> (in Global Config)	<p>Allows the user to set passwords or change passwords needed to login</p> <p>A prompt will appear after the command is entered requesting the users old password. In the absence of an old password leave the area blank. The operator must press enter to execute the command.</p> <p>The system then prompts the user for a new password then a prompt to confirm the new password. If the new password and the confirmed password match a message will be displayed.</p> <p>User password should not be more than eight characters in length.</p> <p>Make sure, that the passwords of the users differ from each other. If two or more users try to choose the same password, the CLI will display an error message.</p>
<pre>copy system:running- config nvram:startup-config</pre> (in Privileged EXEC)	<p>This will save passwords and all other changes to the device.</p> <p>If you do not save the configuration by doing this command, all configurations will be lost when a power cycle is performed on the switch or when the switch is reset.</p>
<pre>logout</pre> (in User EXEC and Privileged EXEC)	<p>Logs the user out of the switch</p>

Table 8: Quick Start up User Account Management

■ Quick Start up IP Address

To view the network parameters the operator can access the device by the following three methods.

- ▶ Simple Network Management Protocol - SNMP
- ▶ Telnet
- ▶ Web Browser

Note: After configuring the network parameters it is advisable to execute the command 'copy system:running-config nvram:startup-config' to ensure that the configurations are not lost.

Command	Details
show network (in User EXEC)	<p>Displays the Network Configurations</p> <p>IP Address - IP Address of the switch Default IP is 0.0.0.0</p> <p>Subnet Mask - IP Subnet Mask for the switch Default is 0.0.0.0</p> <p>Default Gateway - The default Gateway for this switch Default value is 0.0.0.0</p> <p>Burned in MAC Address - The Burned in MAC Address used for in-band connectivity</p> <p>Network Configurations Protocol (BOOTP/DHCP) - Indicates which network protocol is being used Default is DHCP</p> <p>Network Configurations Protocol HiDiscovery - Indicates the status of the HiDiscovery protocol. Default is read-write</p> <p>Management VLAN Id - Specifies VLAN id</p> <p>Web Mode - Indicates whether HTTP/Web is enabled.</p> <p>JavaScript Mode - Indicates whether java mode is enabled. When the user accesses the switch's graphical user interface (web interface) and JavaScript Mode is enabled, the switch's web server will deliver a HTML page that contains JavaScript. Some browsers do not support JavaScript. In this case, a HTML page without JavaScript is necessary. In this case, set JavaScript Mode to disabled. Default: enabled.</p>
network parms <ipaddr> <net-mask> [gateway] (in Privileged EXEC)	<p>Sets the IP Address, subnet mask and gateway of the router. The IP Address and the gateway must be on the same subnet.</p> <p>IP Address range from 0.0.0.0 to 255.255.255.255</p>

Table 9: Quick Start up IP Address

Command	Details
	Subnet Mask range from 0.0.0.0 to 255.255.255.255
	Gateway Address range from 0.0.0.0 to 255.255.255.255

Table 9: Quick Start up IP Address

■ Quick Start up Downloading from TFTP Server

Before starting a TFTP server download, the operator must complete the Quick Start up for the IP Address.

Command	Details
<code>copy <url> {nvram:startup-config system:image}</code>	Sets the destination (download) datatype to be an image (system:image) or a configuration file (nvram:startup-config). The URL must be specified as: ftp://ipAddr/filepath/fileName. The nvram:startup-config option downloads the configuration file using tftp and system:image option downloads the code file.

Table 10: Quick Start up Downloading from TFTP Server

■ Quick Start up Factory Defaults

Command	Details
<code>clear config</code> (in Privileged EXEC Mode)	Enter yes when the prompt pops up to clear all the configurations made to the switch.
<code>copy system:running-config nvram:startup-config</code>	Enter yes when the prompt pops up that asks if you want to save the configurations made to the switch.
<code>reboot</code> (or cold boot the switch) (in Privileged EXEC Mode)	Enter yes when the prompt pops up that asks if you want to reset the system. This is the users choice either reset the switch or cold boot the switch, both work effectively.

Table 11: Quick Start up Factory Defaults

3 Mode-based CLI

The CLI groups all the commands in appropriate modes according to the nature of the command. A sample of the CLI command modes are described below. Each of the command modes support specific software commands.

- ▶ User Exec Mode
- ▶ Privileged Exec Mode
- ▶ Global Config Mode
- ▶ Vlan Mode
- ▶ Interface Config Mode
- ▶ Line Config Mode

The Command Mode table captures the command modes, the prompts visible in that mode and the exit method from that mode.

Command Mode	Access Method	Prompt	Exit or Access Next Mode
User Exec Mode	This is the first level of access. Perform basic tasks and list system information	(Hirschmann Product) >	Enter Logout command
Privileged Exec Mode	From the User Exec Mode, enter the enable command	(Hirschmann Product) #	To exit to the User Exec mode, enter exit or press Ctrl-Z.
VLAN Mode	From the Privileged User Exec mode, enter the vlan database command	(Hirschmann Product) (Vlan) #	To exit to the Privileged Exec mode, enter the exit command, or press Ctrl-Z to switch to User Exec mode.
Global Config Mode	From the Privileged Exec mode, enter the configure command	(Hirschmann Product) (Config) #	To exit to the Privileged Exec mode, enter the exit command, or press Ctrl-Z to switch to user exec mode.
Interface Config Mode	From the Global Configuration mode, enter the interface <slot/port> command	(Hirschmann Product) (Interface- "if number") #	To exit to the Global Config mode enter exit. To return to user EXEC mode enter ctrl-Z.
Line Config Mode	From the Global Configuration mode, enter the lineconfig command	(Hirschmann Product) (line) #	To exit to the Global Config mode enter exit. To return to User Exec mode enter ctrl-Z.

Table 12: Command Mode

3.1 Mode-based Topology

The CLI tree is built on a mode concept where the commands are available according to the interface. Some of the modes are depicted in the following figure.

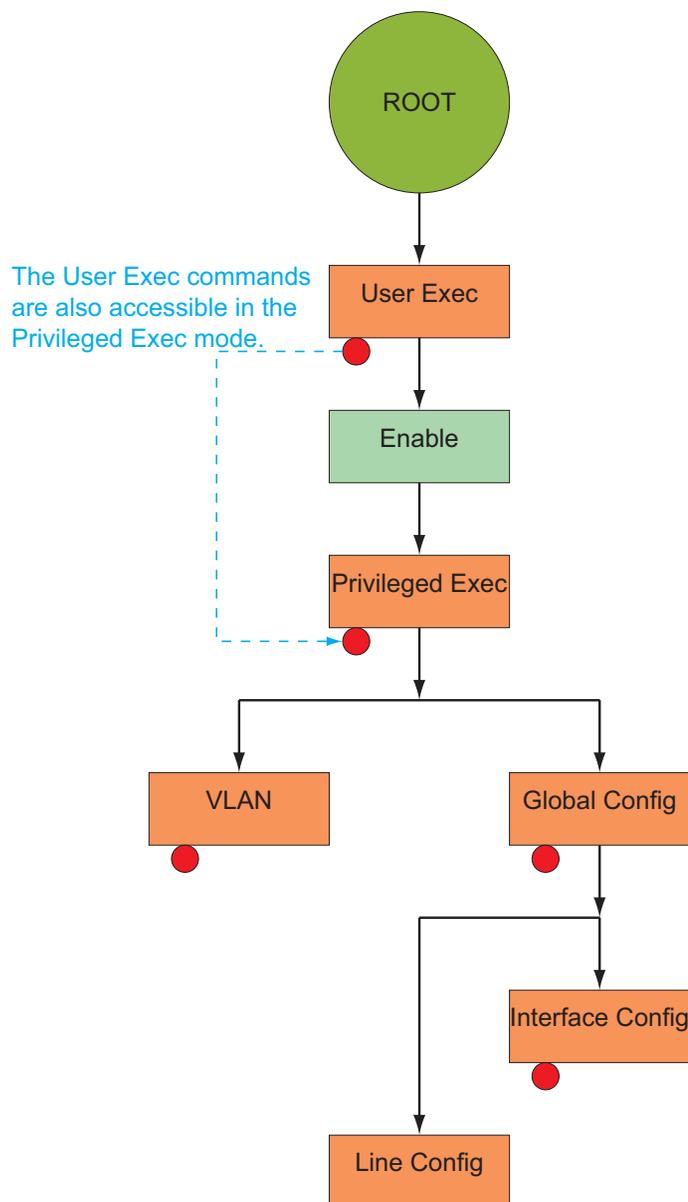


Fig. 1: Mode-based CLI

3.2 Mode-based Command Hierarchy

The CLI is divided into various modes. The Commands in one mode are not available until the operator switches to that particular mode, with the exception of the User Exec mode commands. The User Exec mode commands may also be executed in the Privileged Exec mode.

The commands available to the operator at any point in time depend upon the mode. Entering a question mark (?) at the CLI prompt, displays a list of the available commands and descriptions of the commands.

The CLI provides the following modes:

User Exec Mode

When the operator logs into the CLI, the User Exec mode is the initial mode. The User Exec mode contains a limited set of commands. The command prompt shown at this level is:

```
Command Prompt: (Hirschmann Product)>
```

Privileged Exec Mode

To have access to the full suite of commands, the operator must enter the Privileged Exec mode. Privileged users authenticated by login are able to enter the Privileged EXEC mode. From Privileged Exec mode, the operator can issue any Exec command, enter the VLAN mode or enter the Global Configuration mode . The command prompt shown at this level is:

```
Command Prompt: (Hirschmann Product)#
```

VLAN Mode

This mode groups all the commands pertaining to VLANs. The command prompt shown at this level is:

```
Command Prompt: (Hirschmann Product) (VLAN) #
```

Global Config Mode

This mode permits the operator to make modifications to the running configuration. General setup commands are grouped in this mode. From the Global Configuration mode, the operator can enter the System Configuration mode, the Physical Port Configuration mode, the

Interface Configuration mode, or the Protocol Specific modes specified below. The command prompt at this level is:

```
Command Prompt: (Hirschmann Product) (Config) #
```

From the Global Config mode, the operator may enter the following configuration modes:

Interface Config Mode

Many features are enabled for a particular interface. The Interface commands enable or modify the operation of an interface.

In this mode, a physical port is set up for a specific logical connection operation. The Interface Config mode provides access to the router interface configuration commands. The command prompt at this level is:

```
Command Prompt: (Hirschmann Product) (Interface  
<slot/port>) #
```

The resulting prompt for the interface configuration command entered in the Global Configuration mode is shown below:

```
(Hirschmann Product) (Config) # interface 2/1  
(Hirschmann Product) (Interface 2/1) #
```

Line Config Mode

This mode allows the operator to configure the console interface. The operator may configure the interface from the directly connected console or the virtual terminal used with Telnet. The command prompt at this level is:

```
Command Prompt: (Hirschmann Product) (Line) #
```

MAC Access-List Config Mode

Use the MAC Access-List Config mode to create a MAC Access-List and to enter the mode containing Mac Access-List configuration commands.

```
(Hirschmann Product) (Config) # mac-access-list  
extended <name>
```

```
Command Prompt: (Hirschmann Product) (Config mac-  
access-list) #
```

3.3 Flow of Operation

This section captures the flow of operation for the CLI:

- ▶ The operator logs into the CLI session and enters the User Exec mode. In the User Exec mode the (Hirschmann Product) (exec)> prompt is displayed on the screen.

The parsing process is initiated whenever the operator types a command and presses <ENTER>. The command tree is searched for the command of interest. If the command is not found, the output message indicates where the offending entry begins. For instance, command node A has the command "show spanning-tree" but the operator attempts to execute the command "show arpp brief" then the output message would be (Hirschmann Product) (exec)> show sspanning-tree^. (Hirschmann Product)%Invalid input detected at '^' marker. If the operator has given an invalid input parameter in the command, then the message conveys to the operator an invalid input was detected. The layout of the output is depicted below:

```
(Hirschmann Product) (exec) #show sspanning-tree
                               ^
(Hirschmann Product) Invalid input detected at '^' marker.
```

Fig. 2: Syntax Error Message

After all the mandatory parameters are entered, any additional parameters entered are treated as optional parameters. If any of the parameters are not recognized a syntax error message will be displayed.

- ▶ After the command is successfully parsed and validated, the control of execution goes to the corresponding CLI callback function.

- ▶ For mandatory parameters, the command tree extends till the mandatory parameters make the leaf of the branch. The callback function is only invoked when all the mandatory parameters are provided. For optional parameters, the command tree extends till the mandatory parameters and the optional parameters make the leaf of the branch. However, the call back function is associated with the node where the mandatory parameters are fetched. The call back function then takes care of the optional parameters.
- ▶ Once the control has reached the callback function, the callback function has complete information about the parameters entered by the operator.

3.4 “No” Form of a Command

“No” is a specific form of an existing command and does not represent a new or distinct command. Only the configuration commands are available in the “no” form. The behavior and the support details of the “no” form is captured as part of the mapping sheets.

3.4.1 Support for “No” Form

Almost every configuration command has a “no” form. In general, use the no form to reverse the action of a command or reset a value back to the default. For example, the `no shutdown interface` configuration command reverses the shutdown of an interface. Use the command without the keyword “no” to re-enable a disabled feature or to enable a feature that is disabled by default.

3.4.2 Behavior of Command Help (“?”)

The “no” form is treated as a specific form of an existing command and does not represent a new or distinct command. However, the behavior of the “?” and help text differ for the “no” form (the help message shows only options that apply to the “no” form).

- ▶ The help message is the same for all forms of the command. The help string may be augmented with details about the “no” form behavior.
- ▶ For the `(no interface?)` and `(no inte?)` cases of the “?”, the options displayed are identical to the case when the “no” token is not specified as in `(interface)` and `(inte?)`.

4 CLI Commands: Base

This chapter provides detailed explanation of the Switching commands. The commands are divided into five functional groups:

- ▶ Show commands display switch settings, statistics, and other information.
- ▶ Configuration commands configure features and options of the switch. For every configuration command, there is a show command that displays the configuration setting.
- ▶ Copy commands transfer or save configuration and informational files to and from the switch.
- ▶ Clear commands clear
 - some
(e.g. the "clear arp-table-switch" command which clears the agent's ARP table) or
 - all
(e.g. the "clear config" command which resets the whole configuration to the factory defaults)

This chapter includes the following configuration types:

- ▶ System information and statistics commands
- ▶ Management commands
- ▶ Device configuration commands
- ▶ User account management commands
- ▶ Security commands
- ▶ System utilities
- ▶ Link Layer Discovery Protocol Commands
- ▶ Simple Network Time Protocol Commands
- ▶ Precision Time Protocol Commands
- ▶ Power over Ethernet Commands

4.1 System Information and Statistics

4.1.1 show

This command displays the interface's configuration.

Format

```
show [all]
```

Mode

```
Interface Config
```

all

Show all the running configuration parameters on this interface. The configuration parameters will be displayed even if their value is the default value.

4.1.2 show address-conflict

This command displays address-conflict settings.

Format

```
show address-conflict
```

Mode

```
Privileged EXEC and User EXEC
```

4.1.3 show arp switch

This command displays the Address Resolution Protocol cache of the switch.

Format

```
show arp switch
```

Mode

Privileged EXEC and User EXEC

4.1.4 show bridge address-learning

This command displays the address-learning setting. The setting can be enable or disable.

Format

```
show bridge address-learning
```

Mode

Privileged EXEC and User EXEC

4.1.5 show bridge address-relearn-detect

This command displays the Bridge Address Relearn Detection setting and the Bridge Address Relearn Threshold.

Format

```
show bridge address-relearn-detect
```

Mode

Privileged EXEC and User EXEC

Bridge Address Relearn Detection

Setting can be enable or disable.

Bridge Address Relearn Threshold

The threshold can be 1 to 1024.

4.1.6 show bridge aging-time

This command displays the timeout for address aging.

Format

```
show bridge aging-time
```

Mode

Privileged EXEC and User EXEC

4.1.7 show bridge duplex-mismatch-detect

This command displays the Bridge Duplex Mismatch Detection setting (Enabled or Disabled).

Format

```
show bridge duplex-mismatch-detect
```

Mode

Privileged EXEC and User EXEC

4.1.8 show bridge framesize

This command displays the maximum size of frame (packet size) setting.

Format

```
show bridge framesize
```

Mode

Privileged EXEC and User EXEC

4.1.9 show bridge vlan-learning

This command displays the bridge vlan-learning mode.

Format

```
show bridge vlan-learning
```

Mode

Privileged EXEC and User EXEC

4.1.10 bridge framesize

Activation of long frames. Configure 1522 or 1632¹⁾ as maximum size of frame (packet size).

Default

1522

Format

```
bridge framesize { 1522 | 16321) | 90222) }
```

Mode

Global Config

bridge framesize 1522

Configure 1522 as maximum size of frame (packet size).

bridge framesize 1632 ¹⁾

Configure 1632 ¹⁾ as maximum size of frame (packet size).

¹⁾ On MACH4000, MACH100, MACH1000 and PowerMICE: 1552

4.1.11 show config-watchdog

Activating the watchdog enables you to return automatically to the last configuration after a set time period has elapsed. This gives you back your access to the Switch.

Format

```
show config-watchdog
```

Mode

Privileged EXEC and User EXEC

4.1.12 show device-status

The signal device status is for displaying

- ▶ the monitoring functions of the switch,
- ▶ the device status trap setting.

Format

```
show device-status  
[monitor|state|trap]
```

Mode

Privileged EXEC and User EXEC

Device status monitor

Displays the possible monitored events and which of them are monitored:

- the detected failure of at least one of the supply voltages.
- the removal of the ACA
- the removal of a media module
- the temperature limits
- the defective link status of at least one port. With the switch, the indication of link status can be masked by the management for each port. Link status is not monitored in the delivery condition.
- the loss of Redundancy guarantee.

Ring/network coupling:

- The following conditions are reported in Stand-by mode:
 - interrupted control line
 - partner device running in Stand-by mode.

HIPER-Ring:

- The following condition is reported in RM mode additionally:
 - Ring redundancy guaranteed. Ring redundancy is not monitored in the delivery condition.

Device status state

`Error` The current device status is error.

`No Error` The current device status is no error.

Device status trap

`enabled` A trap is sent if the device status changes.

`disabled` No trap is sent if the device status changes.

4.1.13 show authentication

This command displays users assigned to authentication login lists.

Format

```
show authentication [users <listname>]
```

Mode

Privileged EXEC and User EXEC

4.1.14 show eventlog

This command displays the event log, which contains error messages from the system. The event log is not cleared on a system reset.

Format

```
show eventlog
```

Mode

Privileged EXEC and User EXEC

File

The file in which the event originated.

Line

The line number of the event

Task Id

The task ID of the event.

Code

The event code.

Time

The time this event occurred.

Note: Event log information is retained across a switch reset.

4.1.15 show interface

This command displays a summary of statistics for a specific port or a count of all CPU traffic based upon the argument.

Format

```
show interface {<slot/port> |  
                ethernet {<slot/port> | switchport} |  
                switchport}
```

Mode

Privileged EXEC and User EXEC

The display parameters, when the argument is '<slot/port>', is as follows :

Packets Received Without Error

The total number of packets (including broadcast packets and multi-cast packets) received by the processor.

Packets Received With Error

The number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol.

Broadcast Packets Received

The total number of packets received that were directed to the broadcast address. Note that this does not include multicast packets.

Packets Transmitted Without Error

The total number of packets transmitted out of the interface.

Transmit Packets Errors

The number of outbound packets that could not be transmitted because of errors.

Collisions Frames

The best estimate of the total number of collisions on this Ethernet segment.

Time Since Counters Last Cleared

The elapsed time, in days, hours, minutes, and seconds since the statistics for this port were last cleared.

The display parameters, when the argument is 'switchport', is as follows :

Packets Received Without Error

The total number of packets (including broadcast packets and multi-cast packets) received by the processor.

Broadcast Packets Received

The total number of packets received that were directed to the broadcast address. Note that this does not include multicast packets.

Packets Received With Error

The number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol.

Packets Transmitted Without Error

The total number of packets transmitted out of the interface.

Broadcast Packets Transmitted

The total number of packets that higher-level protocols requested to be transmitted to the Broadcast address, including those that were discarded or not sent.

Transmit Packet Errors

The number of outbound packets that could not be transmitted because of errors.

Address Entries Currently In Use

The total number of Forwarding Database Address Table entries now active on the switch, including learned and static entries.

VLAN Entries Currently In Use

The number of VLAN entries presently occupying the VLAN table.

Time Since Counters Last Cleared

The elapsed time, in days, hours, minutes, and seconds since the statistics for this switch were last cleared.

4.1.16 show interface ethernet

This command displays detailed statistics for a specific port or for all CPU traffic based upon the argument.

Format

```
show interface ethernet {<slot/port> | switchport}
```

Mode

Privileged EXEC and User EXEC

The display parameters, when the argument is '<slot/port>', are as follows :

Packets Received

Octets Received - The total number of octets of data (including those in bad packets) received on the network (excluding framing bits but including Frame Check Sequence (FCS) octets). This object can be used as a reasonable estimate of ethernet utilization. If greater precision is desired, the etherStatsPkts and etherStatsOctets objects should be sampled before and after a common interval. ----- The result of this equation is the value Utilization which is the percent utilization of the ethernet segment on a scale of 0 to 100 percent.

Packets Received < 64 Octets - The total number of packets (including bad packets) received that were < 64 octets in length (excluding framing bits but including FCS octets).

Packets Received 64 Octets - The total number of packets (including bad packets) received that were 64 octets in length (excluding framing bits but including FCS octets).

Packets Received 65-127 Octets - The total number of packets (including bad packets) received that were between 65 and 127 octets in length inclusive (excluding framing bits but including FCS octets).

Packets Received 128-255 Octets - The total number of packets (including bad packets) received that were between 128 and 255 octets in length inclusive (excluding framing bits but including FCS octets).

Packets Received 256-511 Octets - The total number of packets (including bad packets) received that were between 256 and 511 octets in length inclusive (excluding framing bits but including FCS octets).

Packets Received 512-1023 Octets - The total number of packets (including bad packets) received that were between 512 and 1023

octets in length inclusive (excluding framing bits but including FCS octets).

Packets Received 1024-1518 Octets - The total number of packets (including bad packets) received that were between 1024 and 1518 octets in length inclusive (excluding framing bits but including FCS octets).

Packets Received 1519-1522 Octets - The total number of packets (including bad packets) received that were between 1519 and 1522 octets in length inclusive (excluding framing bits but including FCS octets).

Packets Received > 1522 Octets - The total number of packets received that were longer than 1522 octets (excluding framing bits, but including FCS octets) and were otherwise well formed.

Packets Received Successfully

Total - The total number of packets received that were without errors.

Unicast Packets Received - The number of subnetwork-unicast packets delivered to a higher-layer protocol.

Multicast Packets Received - The total number of good packets received that were directed to a multicast address. Note that this number does not include packets directed to the broadcast address.

Broadcast Packets Received - The total number of good packets received that were directed to the broadcast address. Note that this does not include multicast packets.

Packets Received with MAC Errors

Total - The total number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol.

Jabbers Received - The total number of packets received that were longer than 1518 octets (excluding framing bits, but including FCS octets), and had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error). Note that this definition of jabber is different than the definition in IEEE-802.3 section 8.2.1.5 (10BASE5) and section 10.3.1.4 (10BASE2). These documents define jabber as the condition where any packet exceeds 20 ms. The allowed range to detect jabber is between 20 ms and 150 ms.

Fragments/Undersize Received - The total number of packets received that were less than 64 octets in length (excluding framing bits but including FCS octets).

Alignment Errors - The total number of packets received that had a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets, inclusive, but had a bad Frame Check Sequence (FCS) with a non-integral number of octets.

Rx FCS Errors - The total number of packets received that had a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets, inclusive, but had a bad Frame Check Sequence (FCS) with an integral number of octets

Overruns - The total number of frames discarded as this port was overloaded with incoming packets, and could not keep up with the inflow.

Received Packets not forwarded

Total - A count of valid frames received which were discarded (i.e. filtered) by the forwarding process.

Local Traffic Frames - The total number of frames dropped in the forwarding process because the destination address was located off of this port.

802.3x Pause Frames Received - A count of MAC Control frames received on this interface with an opcode indicating the PAUSE operation. This counter does not increment when the interface is operating in half-duplex mode.

Unacceptable Frame Type - The number of frames discarded from this port due to being an unacceptable frame type.

VLAN Membership Mismatch - The number of frames discarded on this port due to ingress filtering.

VLAN Viable Discards - The number of frames discarded on this port when a lookup on a particular VLAN occurs while that entry in the VLAN table is being modified, or if the VLAN has not been configured.

Multicast Tree Viable Discards - The number of frames discarded when a lookup in the multicast tree for a VLAN occurs while that tree is being modified.

Reserved Address Discards - The number of frames discarded that are destined to an IEEE 802.1 reserved address and are not supported by the system.

Broadcast Storm Recovery - The number of frames discarded that are destined for FF:FF:FF:FF:FF:FF when Broadcast Storm Recovery is enabled.

CFI Discards - The number of frames discarded that have CFI bit set and the addresses in RIF are in non-canonical format.

Upstream Threshold - The number of frames discarded due to lack of cell descriptors available for that packet's priority level.

Packets Transmitted Octets

Total Bytes - The total number of octets of data (including those in bad packets) transmitted into the network (excluding framing bits but including FCS octets). This object can be used as a reasonable estimate of ethernet utilization. If greater precision is desired, the etherStatsPkts and etherStatsOctets objects should be sampled before and after a common interval. -----

Packets Transmitted 64 Octets - The total number of packets (including bad packets) transmitted that were 64 octets in length (excluding framing bits but including FCS octets).

Packets Transmitted 65-127 Octets - The total number of packets (including bad packets) transmitted that were between 65 and 127 octets in length inclusive (excluding framing bits but including FCS octets).

Packets Transmitted 128-255 Octets - The total number of packets (including bad packets) transmitted that were between 128 and 255 octets in length inclusive (excluding framing bits but including FCS octets).

Packets Transmitted 256-511 Octets - The total number of packets (including bad packets) transmitted that were between 256 and 511 octets in length inclusive (excluding framing bits but including FCS octets).

Packets Transmitted 512-1023 Octets - The total number of packets (including bad packets) transmitted that were between 512 and 1023 octets in length inclusive (excluding framing bits but including FCS octets).

Packets Transmitted 1024-1518 Octets - The total number of packets (including bad packets) transmitted that were between 1024 and 1518 octets in length inclusive (excluding framing bits but including FCS octets).

Packets Transmitted 1519-1522 Octets - The total number of packets (including bad packets) transmitted that were between 1519 and 1522 octets in length inclusive (excluding framing bits but including FCS octets).

Max Info - The maximum size of the Info (non-MAC) field that this port will receive or transmit.

Packets Transmitted Successfully

Total - The number of frames that have been transmitted by this port to its segment.

Unicast Packets Transmitted - The total number of packets that higher-level protocols requested be transmitted to a subnetwork-unicast address, including those that were discarded or not sent.

Multicast Packets Transmitted - The total number of packets that higher-level protocols requested be transmitted to a Multicast address, including those that were discarded or not sent.

Broadcast Packets Transmitted - The total number of packets that higher-level protocols requested be transmitted to the Broadcast address, including those that were discarded or not sent.

Transmit Errors

Total Errors - The sum of Single, Multiple, and Excessive Collisions.

Tx FCS Errors - The total number of packets transmitted that had a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets, inclusive, but had a bad Frame Check Sequence (FCS) with an integral number of octets

Oversized - The total number of frames that exceeded the max permitted frame size. This counter has a max increment rate of 815 counts per sec. at 10 Mb/s.

Underrun Errors - The total number of frames discarded because the transmit FIFO buffer became empty during frame transmission.

Transmit Discards

Total Discards - The sum of single collision frames discarded, multiple collision frames discarded, and excessive frames discarded.

Single Collision Frames - A count of the number of successfully transmitted frames on a particular interface for which transmission is inhibited by exactly one collision.

Multiple Collision Frames - A count of the number of successfully transmitted frames on a particular interface for which transmission is inhibited by more than one collision.

Excessive Collisions - A count of frames for which transmission on a particular interface is discontinued due to excessive collisions.

Port Membership - The number of frames discarded on egress for this port due to egress filtering being enabled.

VLAN Viable Discards - The number of frames discarded on this port when a lookup on a particular VLAN occurs while that entry in the VLAN table is being modified, or if the VLAN has not been configured.

Protocol Statistics

BPDUs received - The count of BPDUs (Bridge Protocol Data Units) received in the spanning tree layer.

BPDUs Transmitted - The count of BPDUs (Bridge Protocol Data Units) transmitted from the spanning tree layer.

802.3x Pause Frames Received - A count of MAC Control frames received on this interface with an opcode indicating the PAUSE operation. This counter does not increment when the interface is operating in half-duplex mode.

GVRP PDU's Received - The count of GVRP PDU's received in the GARP layer.

STP BPDUs Transmitted - Spanning Tree Protocol Bridge Protocol Data Units sent

STP BPDUs Received - Spanning Tree Protocol Bridge Protocol Data Units received

RST BPDUs Transmitted - Rapid Spanning Tree Protocol Bridge Protocol Data Units sent

RSTP BPDUs Received - Rapid Spanning Tree Protocol Bridge Protocol Data Units received

MSTP BPDUs Transmitted - Multiple Spanning Tree Protocol Bridge Protocol Data Units sent

MSTP BPDUs Received - Multiple Spanning Tree Protocol Bridge Protocol Data Units received

Time Since Counters Last Cleared

The elapsed time, in days, hours, minutes, and seconds since the statistics for this port were last cleared.

The display parameters, when the argument is 'switchport, are as follows :

Octets Received - The total number of octets of data received by the processor (excluding framing bits but including FCS octets).

Total Packets Received Without Error- The total number of packets (including broadcast packets and multicast packets) received by the processor.

Unicast Packets Received - The number of subnetwork-unicast packets delivered to a higher-layer protocol.

Multicast Packets Received - The total number of packets received that were directed to a multicast address. Note that this number does not include packets directed to the broadcast address.

Broadcast Packets Received - The total number of packets received that were directed to the broadcast address. Note that this does not include multicast packets.

Receive Packets Discarded - The number of inbound packets which were chosen to be discarded even though no errors had been detected to prevent their being deliverable to a higher-layer protocol. A possible reason for discarding a packet could be to free up buffer space.

Octets Transmitted - The total number of octets transmitted out of the interface, including framing characters.

Packets Transmitted without Errors - The total number of packets transmitted out of the interface.

Unicast Packets Transmitted - The total number of packets that higher-level protocols requested be transmitted to a subnetwork-unicast address, including those that were discarded or not sent.

Multicast Packets Transmitted - The total number of packets that higher-level protocols requested be transmitted to a Multicast address, including those that were discarded or not sent.

Broadcast Packets Transmitted - The total number of packets that higher-level protocols requested be transmitted to the Broadcast address, including those that were discarded or not sent.

Transmit Packets Discarded - The number of outbound packets which were chosen to be discarded even though no errors had been detected to prevent their being deliverable to a higher-layer protocol. A possible reason for discarding a packet could be to free up buffer space.

Most Address Entries Ever Used - The highest number of Forwarding Database Address Table entries that have been learned by this switch since the most recent reboot.

Address Entries in Use - The number of Learned and static entries in the Forwarding Database Address Table for this switch.

Maximum VLAN Entries - The maximum number of Virtual LANs (VLANs) allowed on this switch.

Most VLAN Entries Ever Used - The largest number of VLANs that have been active on this switch since the last reboot.

Static VLAN Entries - The number of presently active VLAN entries on this switch that have been created statically.

Dynamic VLAN Entries - The number of presently active VLAN entries on this switch that have been created by GVRP registration.

VLAN Deletes - The number of VLANs on this switch that have been created and then deleted since the last reboot.

Time Since Counters Last Cleared

The elapsed time, in days, hours, minutes, and seconds, since the statistics for this switch were last cleared.

4.1.17 show interface switchport

This command displays data concerning the internal port to the management agent.

Format

```
show interface switchport
```

Mode

Privileged EXEC and User EXEC

4.1.18 show interface utilization

This command displays the utilization statistics for the entire device.

Format

```
show interface utilization
```

Mode

```
Global Config
```

Interface

Display port number in <slot/port> notation.

Utilization

Display the utilization on this port.

Possible values: 0..100.00%

Lower threshold

Display the lower threshold setting for the utilization statistics on this port.

Possible values: 0..100.00%

Upper threshold

Display the upper threshold setting for the utilization statistics on this port.

Possible values: 0..100.00%

Alarm condition

Display the alarm condition setting for the utilization statistics on this port.

Possible values: true, false

4.1.19 show logging

This command displays the trap log maintained by the switch. The trap log contains a maximum of 256 entries that wrap.

Format

```
show logging [buffered | hosts | traplogs |  
snmp-requests]
```

Mode

Privileged EXEC and User EXEC

buffered

Display buffered (in-memory) log entries.

hosts

Display logging hosts.

traplogs

Display trap records.

snmp-requests

Display logging SNMP requests and severity level.

4.1.20 show mac-address-conflict

This command displays the mac-address-conflict configuration.

Format

```
show mac-address-conflict
```

Mode

Privileged EXEC and User EXEC

MAC Address Conflict Detection

The status of the mac-address-conflict configuration.

MAC Address Conflict Detection Operation

Possible values: `enabled`, `disabled`

Default value: `enabled`

The meanings of the values are:

enabled MAC Address Conflict Detection enabled.

The device sends a trap if it detects a packet with its own MAC address in the network.

disabled MAC Address Conflict Detection disabled.

The device disclaims sending a trap if it detects a packet with its own MAC address in the network.

4.1.21 show mac-addr-table

This command displays the forwarding database entries. If the command is entered with no parameter, the entire table is displayed. This is the same as entering the optional *all* parameter. Alternatively, the administrator can enter a MAC Address to display the table entry for the requested MAC address and all entries following the requested MAC address.

Note: This command displays only learned unicast addresses. For other addresses use the command `show mac-filter-table`.

See [“show mac-filter-table stats” on page 182](#).

Format

```
show mac-addr-table [<macaddr> <1-4042> | all]
```

Mode

Privileged EXEC and User EXEC

Mac Address

A unicast MAC address for which the switch has forwarding and or filtering information. The format is 6 or 8 two-digit hexadecimal numbers that are separated by colons, for example 01:23:45:67:89:AB.

Slot/Port

The port which this address was learned.

if Index

This object indicates the ifIndex of the interface table entry associated with this port.

Status

The status of this entry. The meanings of the values are:

Learned The value of the corresponding instance was learned by observing the source MAC addresses of incoming traffic, and is currently in use.

Management The value of the corresponding instance (system MAC address) is also the value of an existing instance of `dot1dStaticAddress`.

4.1.22 show signal-contact

The signal contact is for displaying

- ▶ the manual setting and the current state of the signal contact,
- ▶ the monitoring functions of the switch,
- ▶ the signal-contacts trap setting.

Format

```
show signal-contact  
    [1|2|all [mode|monitor|state|trap]]
```

Mode

Privileged EXEC and User EXEC

Signal contact mode

Auto The signal contact monitors the functions of the switch which makes it possible to perform remote diagnostics.

A break in contact is reported via the zero-potential signal contact (relay contact, closed circuit).

Device Status The signal contact monitors the device-status.

Manual This command gives you the option of remote switching the signal contact.

Signal contact monitor

Displays the possible monitored events and which of them are monitored:

- the detected failure of at least one of the supply voltages.
- the removal of the ACA
- the removal of a media module
- the temperature limits
- the defective link status of at least one port. With the switch, the indication of link status can be masked by the management for each port. Link status is not monitored in the delivery condition.
- the loss of Redundancy guarantee.

Ring/network coupling:

- The following conditions are reported in Stand-by mode:
- interrupted control line
- partner device running in Stand-by mode.

HIPER-Ring:

- The following condition is reported in RM mode additionally:
- Ring redundancy guaranteed. Ring redundancy is not monitored in the delivery condition.

Signal contact manual setting

`closed` The signal contact's manual setting is closed.

`open` The signal contact's manual setting is open.

Signal contact operating state

`closed` The signal contact is currently closed.

`open` The signal contact is currently open.

Signal contact trap

`enabled` A trap is sent if the signal contact state changes.

`disabled` No trap is sent if the signal contact state changes.

Note: To show the signal contact's port related settings, use the command `show port {<slot/port> | all}` (see ["show port" on page 184](#)).

4.1.23 show slot

This command is used to display information about slot(s).
For [slot] enter the slot ID.

Format

```
show slot [slot]
```

Mode

Privileged EXEC, Global Config

Slot

Display the number of the media module slot.

Status

`Full` The media module slot is equipped with a module.

`Empty` The media module slot is not equipped.

Admin State

Note: This feature is available for MS20/MS30, PowerMICE, MACH102 and MACH4000 devices.

`Enable` The media module slot is logically enabled.

`Disable` The media module slot is logically disabled.

Configured Card Model ID

Display the type of the media module.

Card Description

Display the type of the media module.

Product Code

Display the type of the media module.

Pluggable

`Yes` The module is pluggable.

`No` The module is not pluggable.

4.1.24 show running-config

This command is used to display the current setting of different protocol packages supported on the switch. This command displays only those parameters, the values of which differ from default value.

Format

```
show running-config [all]
```

Mode

Privileged EXEC

all

Show all the running configuration on the switch. All configuration parameters will be output even if their value is the default value.

4.1.25 show sysinfo

Use this command to display system information for the device, including system-up time.

Format

```
show sysinfo
```

Mode

Privileged EXEC and User EXEC

Device Status

Displays the latest status for this device.

Alarms

Displays the latest present Alarm for a signal contact.

System Description

Text used to identify this switch.

System Name

Name used to identify the switch.

System Location

Text used to identify the location of the switch. May be up to 31 alpha-numeric characters. The factory default is blank.

System Contact

Text used to identify a contact person for this switch. May be up to 31 alpha-numeric characters. The factory default is blank.

System UpTime

The time in days, hours and minutes since the last switch reboot.

System Date and Time

The system clock's date and time in local time zone.

System IP Address

The system's IP address.

Boot Software Release

The boot code's version number.

Boot Software Build Date

The boot code's build date.

Operating system Software Release

The operating system's software version number.

Operating system Software Build Date

The operating system's software build date.

Backplane Hardware Revision

The hardware's revision number.

Backplane Hardware Description

The hardware's device description.

Serial Number (Backplane)

The hardware's serial number.

Base MAC Address (Backplane)

The hardware's base MAC address.

Number of MAC Addresses (Backplane)

The number of hardware MAC addresses.

Configuration state

The state of the actual configuration.

Configuration signature

The signature (watermark) of the stored configuration. The signature changes each time the configuration is saved.

Auto Config Adapter, State

The Auto Configuration Adapter's state.

Auto Config Adapter, Serial Number

The Auto Configuration Adapter's serial number (if present and operative).

Factory Hardware Description

The product code (factory hardware description) of the device, e.g.
MAR1020-99TTTTMMMMTTTTTTTTTTTTTTTTTTTUC9HPHH

Power Supply Information

The status of the power supplies.

Media Module Information

The description of each media module

- Description: media module type,
 - Serial Number of the media modul (if available),
- SFP Information:
- SFP Part ID: SFP type (if available),
 - SFP Serial No. of the SFP module (if available),
 - SFP Supported: yes/no,

- SFP Temperature (°C, F),
- SFP Tx Pwr, SFP transmit power (dBm / mW),
- SFP Rx Pwr, SFP receive power (dBm / mW)

CPU Utilization

The utilization of the central processing unit.

Average CPU Utilization

The average utilization of the central processing unit.

Flashdisk

Free memory on flashdisk (in Kbytes).

4.1.26 show temperature

Note: The command is available for RS20/RS30/RS40, MS20/MS30, RSR20/RSR30, MACH100, MACH1000, PowerMICE, MACH4000 and OCTOPUS devices.

This command displays the lower and upper temperature limit for sending a trap.

Format

```
show temperature
```

Mode

```
Privileged EXEC and User EXEC
```

4.1.27 utilization alarm-threshold

Use this command to add the alarm threshold value for monitoring bandwidth utilization of the interface.

Format

```
utilization alarm-threshold  
    {lower <0..10000> | upper <0..10000>}
```

Mode

Interface Config

lower

Enter lower utilization alarm threshold in the range of 0 . . 10000 where 10000 represents 100%.

upper

Enter upper utilization alarm threshold in the range of 0 . . 10000 where 10000 represents 100%.

4.2 Management VLAN Commands

4.2.1 network mgmt_vlan

This command configures the Management VLAN ID. If you enter the VLAN ID "0", the agent can be accessed by all VLANs.

Default

1

Format

```
network mgmt_vlan <0-4042>
```

Mode

Privileged EXEC

4.3 Class of Service (CoS) Commands

This chapter provides a detailed explanation of the QoS CoS commands. The following commands are available.

The commands are divided into these different groups:

- ▶ Configuration Commands are used to configure features and options of the switch. For every configuration command there is a show command that will display the configuration setting.
- ▶ Show commands are used to display device settings, statistics and other information.

Note: The 'Interface Config' mode only affects a single interface, whereas the 'Global Config' mode is applied to all interfaces.

4.3.1 classofservice dot1p-mapping

This command maps an 802.1p priority to an internal traffic class for a device when in 'Global Config' mode. The number of available traffic classes may vary with the platform. Userpriority and trafficclass can both be the range from 0-7. The command is only available on platforms that support priority to traffic class mapping on a 'per-port' basis, and the number of available traffic classes may vary with the platform.

Format

```
classofservice dot1p-mapping
    <userpriority> <trafficclass>
```

Mode

Global Config or Interface Config

userpriority

Enter the 802.1p priority (0-7).

trafficclass

Enter the traffic class to map the 802.1p priority (0-3).

■ no classofservice dot1p-mapping

This command restores the default mapping of the 802.1p priority to an internal traffic class.

Format

```
no classofservice dot1p-mapping
```

Modes

Global Config or Interface Config

4.3.2 classofservice ip-dscp-mapping

This command maps an IP DSCP value to an internal traffic class. The <ipdscp> value is specified as either an integer from 0 to 63, or symbolically through one of the following keywords: af11, af12, af13, af21, af22, af23, af31, af32, af33, af41, af42, af43, be, cs0, cs1, cs2, cs3, cs4, cs5, cs6, cs7, ef.

Format

```
classofservice ip-dscp-mapping
                        <ipdscp> <trafficclass>
```

Mode

Global Config

ipdscp

Enter the IP DSCP value in the range of 0 to 63 or an IP DSCP keyword (af11, af12, af13, af21, af22, af23, af31, af32, af33, af41, af42, af43, be, cs0, cs1, cs2, cs3, cs4, cs5, cs6, cs7, ef).

trafficclass

Enter the traffic class to map the 802.1p priority (0-3).

■ no classofservice ip-dscp-mapping

This command restores the default mapping of the IP DSCP value to an internal traffic class.

Format

```
no classofservice dot1p-mapping
```

Modes

Global Config

4.3.3 classofservice trust

This command sets the class of service trust mode of an interface. The mode can be set to trust one of the Dot1p (802.1p) or IP DSCP packet markings.

Note: In `trust ip-dscp` mode the switch modifies the vlan priority for outgoing frames according to

– the fix mapping table

(see Reference Manual „GUI Graphical User Interface“ (Web-based Interface) for further details).

Format

```
classofservice trust dot1p | ip-dscp
```

Mode

```
Global Config
```

■ no classofservice trust

This command sets the interface mode to untrusted, i.e. the packet priority marking is ignored and the default port priority is used instead.

Format

```
no classofservice trust
```

Modes

```
Global Config
```

4.3.4 show classofservice dot1p-mapping

This command displays the current 802.1p priority mapping to internal traffic classes for a specific interface. The slot/port parameter is required on platforms that support priority to traffic class mapping on a 'per-port' basis.

Platforms that support priority to traffic class mapping on a per-port basis:

Format

```
show classofservice dot1p-mapping
```

Platforms that do not support priority to traffic class mapping on a per-port basis:

Format

```
Show classofservice dot1p-mapping
```

Mode

```
Privileged EXEC and User EXEC
```

4.3.5 show classofservice ip-dscp-mapping

This command displays the current IP DSCP mapping to internal traffic classes for the global configuration settings.

Format

```
show classofservice ip-dscp-mapping [<slot/port>]
```

Mode

Privileged EXEC

The following information is repeated for each user priority.

IP DSCP

The IP DSCP value.

Traffic Class

The traffic class internal queue identifier to which the IP DSCP value is mapped.

slot/port

Valid slot and port number separated by forward slashes.

4.3.6 show classofservice trust

This command displays the current trust mode for the specified interface. The slot/port parameter is optional. If specified, the trust mode of the interface is displayed. If omitted, the most recent global configuration settings are displayed.

Format

```
show classofservice trust [slot/port]
```

Mode

Privileged EXEC

Class of Service Trust Mode

The current trust mode: Dot1p, IP DSCP, or Untrusted.

Untrusted Traffic Class

The traffic class used for all untrusted traffic. This is only displayed when the COS trust mode is set to 'untrusted'.

slot/port

Valid slot and port number separated by forward slashes.

4.3.7 vlan port priority all

This command configures the port priority assigned for untagged packets for all ports presently plugged into the device. The range for the *priority* is 0..7. Any subsequent per port configuration will override this configuration setting.

Format

```
vlan port priority all <priority>
```

Mode

Global Config

4.3.8 vlan priority

This command configures the default 802.1p port priority assigned for untagged packets for a specific interface. The range for the *priority* is 0..7.

Default

0

Format

```
vlan priority <priority>
```

Mode

Interface Config

4.4 Management Commands

These commands manage the switch and show current management settings.

4.4.1 transport input telnet

This command regulates new telnet sessions. If sessions are enabled, new telnet sessions can be established until there are no more sessions available. If sessions are disabled, no new telnet sessions are established. An established session remains active until the session is ended or an abnormal network error ends the session.

Default

enabled

Format

```
transport input telnet
```

Mode

Line Config

■ no transport input telnet

This command disables telnet sessions. If sessions are disabled, no new telnet sessions are established.

Format

```
no transport input telnet
```

Mode

Line Config

4.4.2 bridge address-learning

To enable you to observe the data at all the ports, the Switch allows you to disable the learning of addresses. When the learning of addresses is disabled, the Switch transfers all the data from all ports to all ports. The default value is `enable`.

Format

```
bridge address-learning {disable|enable}
```

Mode

```
Global Config
```

4.4.3 bridge address-relearn detect operation

This command enables or disables Bridge Address Relearn Detection. The default value is `disable`.

Default

```
Disabled
```

Format

```
bridge address-relearn detect operation  
{disable|enable}
```

Mode

```
Global Config
```

4.4.4 bridge address-relearn detect threshold

This command defines the value of relearned addresses to signal address relearn threshold exceeded.

The default relearn threshold is 1. Possible values to configure threshold count are 1 to 1024.

Default

1

Format

```
bridge address-relearn-detect threshold <value>
```

Mode

Global Config

value

1 to 1024

4.4.5 bridge aging-time

This command configures the forwarding database address aging timeout in seconds.

Default

30

Format

```
bridge aging-time <10-630>
```

Mode

Global Config

Seconds

The <seconds> parameter must be within the range of 10 to 630 seconds.

■ no bridge aging-time

This command sets the forwarding database address aging timeout to 30 seconds.

Format

```
no bridge aging-time
```

Mode

Global Config

4.4.6 bridge fast-link-detection

This command enables or disables the Bridge Fast Link Detection.

Default

Enabled

Format

```
bridge fast-link-detection {disable|enable}
```

Mode

Global Config

4.4.7 bridge duplex-mismatch-detect operation

This command enables or disables Bridge Duplex Mismatch Detection.

Reasons for Duplex Mismatch can be:

- A local port is configured to fix full-duplex.
- A port is configured to auto-negotiation and has negotiated HalfDuplex-Mode.

Duplex Mismatch can be excluded, when the local port is configured to auto-negotiation and duplex mode is negotiated to full-duplex.

Note: If counters and configuration settings indicate a Duplex Mismatch, the reason can also be a bad cable and/or EMI.

Default

Enabled

Format

```
bridge duplex-mismatch-detect operation  
{disable|enable}
```

Mode

Global Config

4.4.8 bridge vlan-learning

With "independent" you set the Shared VLAN Learning mode to Independent. The switch will treat equal MAC source addresses from different VLANs as separate addresses.

With "shared" you set the Shared VLAN Learning mode to Shared. The switch will treat equal MAC source addresses from different VLANs as the same address.

Format

```
bridge vlan-learning {independent | shared}
```

Mode

```
Global Config
```

4.4.9

ethernet-ip

This command controls the EtherNet/IP function on the switch. Detailed information you can find in the User Manual Industrial Protocols.

Default

depends on the order code (standard = disable)

Format

```
ethernet-ip admin-state {enable | disable}
```

Mode

```
Global Config
```

Admin-state

`disable`: Disables the EtherNet/IP function on this device.

Note: The relevant MIB objects are still accessible.

`enable`: Enables the EtherNet/IP function on this device.

4.4.10 network mgmt-access add

This command is used to configure the restricted management access feature (RMA).

It creates a new empty entry at the <index> (if you enter the command with parameter <index>) or at the next free index (if you enter the command without parameter <index>).

Format

```
network mgmt-access add [index]
```

Mode

```
Global Config
```

[index]

Index of the entry in the range 1..16.

4.4.11 network mgmt-access delete

This command is used to configure the restricted management access feature (RMA).

It deletes an existing entry with <index>.

Format

```
network mgmt-access delete <index>
```

Mode

```
Global Config
```

<index>

Index of the entry in the range 1..16.

4.4.12 network mgmt-access modify

This command is used to configure the restricted management access feature (RMA).

The command modifies an existing rule with <index> to change IP address, net mask and allowed services.

Format

```
network mgmt-access modify <index>
                                { ip <address> |
                                  mask <netmask> |
                                  http {enable | disable} |
                                  https {enable | disable} |
                                  snmp {enable | disable} |
                                  telnet {enable | disable} |
                                  ssh {enable |disable } }
```

Mode

Global Config

<index>

Index of the entry in the range 1..16.

<ip>

Configure IP address which should have access to management

<mask>

Configure network mask to allow a subnet for management access.

<http>

Configure if HTTP is allowed to have management access.

<https>

Configure if HTTPS is allowed to have management access.

<snmp>

Configure if SNMP is allowed to have management access.

<telnet>

Configure if TELNET is allowed to have management access.

<ssh>

Configure if SSH is allowed to have management access.

enable

Allow the service to have management access.

disable

Do not allow the service to have management access.

4.4.13 network mgmt-access operation

This command is used to configure the restricted management access feature (RMA).

It enables or disables the service to have management access. The default value is `disable`.

Format

```
network mgmt-access operation {disable|enable}
```

Mode

Global Config

enable

Enable the restricted management access function globally.

disable

Disable the restricted management access function globally.

4.4.14 network mgmt-access status

This command is used to configure the restricted management access feature (RMA).

It activates/deactivates an existing rule with <index>.

Format

```
network mgmt-access status <index>
                                     {enable | disable}
```

Mode

Global Config

<index>

Index of the entry in the range 1..16.

enable

Allow the service to have management access.

disable

Do not allow the service to have management access.

4.4.15 network parms

This command sets the IP Address, subnet mask and gateway of the router. The IP Address and the gateway must be on the same subnet.

Format

```
network parms <ipaddr> <netmask> [gateway]
```

Mode

Privileged EXEC

4.4.16 network protocol

This command specifies the network configuration protocol to be used. If you modify this value, change is effective immediately after you saved your changes.

The parameter `bootp` indicates that the switch periodically sends requests to a Bootstrap Protocol (BootP) server or a DHCP server until a response is received.

`none` indicates that the switch should be manually configured with IP information.

Independently of the BootP and DHCP settings, HiDiscovery can be configured as an additional protocol.

Default

DHCP

Format

```
network protocol {none | bootp | dhcp | hidiscovery  
                {off | read-only | read-write}}
```

Mode

Privileged EXEC

4.4.17 network priority

This command configures the VLAN priority or the IP DSCP value for outgoing management packets. The <ipdscp> is specified as either an integer from 0-63, or symbolically through one of the following keywords:

af11,af12,af13,af21,af22,af23,af31,af32,af33,af41,af42,af43,be,cs0, cs1, cs2,cs3,cs4,cs5,cs6,cs7,ef.

Default

0 for both values

Format

```
network priority {dot1p-vlan <0-7> |  
ip-dscp <ipdscp> }
```

Mode

Privileged EXEC

■ no network priority

This command sets the VLAN priority or the IP DSCP value for outgoing management packets to default which means VLAN priority 0 or IP DSCP value 0 (Best effort).

Format

```
no network priority {dot1p-vlan | ip-dscp }
```

Mode

Privileged EXEC

4.4.18 profinetio

This command controls the PROFINET IO function on the switch. Detailed information you can find in the User Manual Industrial Protocols.

Default

depends on the order code (standard = disable)

Format

```
profinetio admin-state {enable | disable}
```

Mode

Global Config

Admin-state

`disable` Disables the PROFINET IO function on this device.

Note: The relevant MIB objects are still accessible.

`enable` Enables the PROFINET IO function on this device.

4.4.19 serial timeout

This command specifies the maximum connect time (in minutes) without console activity. A value of 0 indicates that a console can be connected indefinitely. The time range is 0 to 160.

Default

5

Format

```
serial timeout <0-160>
```

Mode

Line Config

■ no serial timeout

This command sets the maximum connect time without console activity (in minutes) back to the default value.

Format

```
no serial timeout
```

Mode

Line Config

4.4.20 set prompt

This command changes the name of the prompt. The length of name may be up to 64 alphanumeric characters.

Format

```
set prompt <prompt string>
```

Mode

Privileged EXEC

4.4.21 show ethernet-ip

This command displays the admin state of the EtherNet/IP function.

Format

```
show ethernet-ip
```

Mode

Privileged EXEC and User EXEC

4.4.22 show network

This command displays configuration settings associated with the switch's network interface. The network interface is the logical interface used for in-band connectivity with the switch via any of the switch's front panel ports. The configuration parameters associated with the switch's network interface do not affect the configuration of the front panel ports through which traffic is switched or routed.

Format

```
show network
```

Mode

Privileged EXEC and User EXEC

System IP Address

The IP address of the interface. The factory default value is 0.0.0.0

Subnet Mask

The IP subnet mask for this interface. The factory default value is
0.0.0.0

Default Gateway

The default gateway for this IP interface. The factory default value is
0.0.0.0

Burned In MAC Address

The burned in MAC address used for in-band connectivity.

Network Configuration Protocol (BootP/DHCP)

Indicates which network protocol is being used. Possible values:
bootp | dhcp | none.

DHCP Client ID (same as SNMP System Name)

Displays the DHCP Client ID.

Network Configuration Protocol HiDiscovery

Indicates in which way the HiDiscovery protocol is being used. Possible values: off | read-only | read-write.

HiDiscovery Version

Indicates the supported HiDiscovery protocol version.
Possible values: v1 | v2.

Management VLAN ID

Specifies the management VLAN ID.

Management VLAN Priority

Specifies the management VLAN Priority.

Management VLAN IP-DSCP Value

Specifies the management VLAN IP-DSCP value.

Web Mode

Specifies if the switch will use Java Script to start the Management Applet. The factory default is `Enable`.

4.4.23 show network mgmt-access

This command displays the operating status and entries for restricted management access (RMA).

Format

```
show network mgmt-access
```

Mode

Privileged EXEC and User EXEC

Operation

Indicates whether the operation for RMA is enabled or not.

Possible values: Enabled | Disabled.

ID

Index of the entry for restricted management access (1 to max. 16).

IP address

The IP address which should have access to management.

The factory default value is 0.0.0.0.

Netmask

The network mask to allow a subnet for management access.

The factory default value is 0.0.0.0.

HTTP

Indicates whether HTTP is allowed to have management access or not. Possible values: Yes | No.

HTTPS

Indicates whether HTTPS is allowed to have management access or not. Possible values: Yes | No.

SNMP

Indicates whether SNMP is allowed to have management access or not. Possible values: Yes | No.

TELNET

Indicates whether TELNET is allowed to have management access or not. Possible values: Yes | No.

SSH

Indicates whether SSH is allowed to have management access or not. Possible values: Yes | No.

Active

Indicates whether the feature is active or not.

Possible values: [x] | [].

4.4.24 show profinetio

This command displays the admin state of the PROFINET IO function.

Format

```
show profinetio
```

Mode

Privileged EXEC and User EXEC

4.4.25 show serial

This command displays serial communication settings for the switch.

Format

```
show serial
```

Mode

Privileged EXEC and User EXEC

Serial Port Login Timeout (minutes)

Specifies the time, in minutes, of inactivity on a Serial port connection, after which the Switch will close the connection. Any numeric value between 0 and 160 is allowed, the factory default is 5. A value of 0 disables the timeout.

4.4.26 show snmp-access

This command displays SNMP access information related to global and SNMP version settings. SNMPv3 is always enabled.

Format

```
show snmp-access
```

Mode

```
Privileged EXEC
```

4.4.27 show snmpcommunity

This command displays SNMP community information. Six communities are supported. You can add, change, or delete communities. The switch does not have to be reset for changes to take effect.

The SNMP agent of the switch complies with SNMP Version 1 (for more about the SNMP specification, see the SNMP RFCs). The SNMP agent sends traps through TCP/IP to an external SNMP manager based on the SNMP configuration (the trap receiver and other SNMP community parameters).

Format

```
show snmpcommunity
```

Mode

Privileged EXEC

SNMP Community Name

The community string to which this entry grants access. A valid entry is a case-sensitive alphanumeric string of up to 32 characters. Each row of this table must contain a unique community name.

Client IP Address -

An IP address (or portion thereof) from which this device will accept SNMP packets with the associated community. The requesting entity's IP address is ANDed with the Subnet Mask before being compared to the IP Address. Note that if the Subnet Mask is set to 0.0.0.0, an IP Address of 0.0.0.0 matches all IP addresses. The default value is 0.0.0.0

Client IP Mask -

A mask to be ANDed with the requesting entity's IP address before comparison with IP Address. If the result matches with IP Address then the address is an authenticated IP address. For example, if the IP Address = 9.47.128.0 and the corresponding Subnet Mask = 255.255.255.0 a range of incoming IP addresses would match, i.e. the incoming IP Address could equal 9.47.128.0 - 9.47.128.255. The default value is 0.0.0.0

Access Mode

The access level for this community string.

Status

The status of this community access entry.

4.4.28 show snmp sync

This command displays the status of the synchronization between the SNMPv1/v2 community table and the SNMPv3 password table and reverse.

Format

```
show snmp sync
```

Mode

```
Privileged EXEC
```

V1/V2 community to V3 password

Display the status of the synchronization between the SNMPv1/v2 community table and the SNMPv3 password table.

Enabled - Synchronization enabled.

Disabled - Synchronization disabled.

V3 password to V1/V2 community

Display the status of the synchronization between the SNMPv3 password table and the SNMPv1/v2 community table.

Enabled - Synchronization enabled.

Disabled - Synchronization disabled.

4.4.29 show snmptrap

This command displays SNMP trap receivers. Trap messages are sent across a network to an SNMP Network Manager. These messages alert the manager to events occurring within the switch or on the network. Six trap receivers are simultaneously supported.

Format

```
show snmptrap
```

Mode

```
Privileged EXEC
```

SNMP Trap Name

The community string of the SNMP trap packet sent to the trap manager. This may be up to 32 alphanumeric characters. This string is case sensitive.

IP Address

The IP address to receive SNMP traps from this device. Enter four numbers between 0 and 255 separated by periods.

Status

A pull down menu that indicates the receiver's status (enabled or disabled) and allows the administrator/user to perform actions on this user entry:

Enable - send traps to the receiver

Disable - do not send traps to the receiver.

Delete - remove the table entry.

4.4.30 show telnet

This command displays outbound telnet settings.

Format

```
show telnet
```

Mode

Privileged EXEC and User EXEC

Outbound Telnet Connection Login Timeout (minutes)

This object indicates the number of minutes a remote connection session is allowed to remain inactive before being logged off. May be specified as a number from 1 to 160. The factory default is 5.

Maximum Number of Outbound Telnet Sessions

This object indicates the number of simultaneous outbound connection sessions allowed. The factory default is 5.

Allow New Outbound Telnet Sessions

Indicates that new outbound telnet sessions will not be allowed when set to no. The factory default value is *yes*.

4.4.31 show telnetcon

This command displays inbound telnet settings.

Format

```
show telnetcon
```

Mode

Privileged EXEC and User EXEC

Telnet Connection Login Timeout (minutes)

This object indicates the number of minutes a remote connection session is allowed to remain inactive before being logged off. May be specified as a number from 1 to 160. The factory default is 4.

Maximum Number of Remote Telnet Sessions

This object indicates the number of simultaneous remote connection sessions allowed. The factory default is 2 .

Allow New Telnet Sessions

Indicates that new telnet sessions will not be allowed when set to no. The factory default value is `yes`.

4.4.32 show trapflags

This command displays trap conditions. Configure which traps the switch should generate by enabling or disabling the trap condition. If a trap condition is enabled and the condition is detected, the switch's SNMP agent sends the trap to all enabled trap receivers. The switch does not have to be reset to implement the changes. Cold and warm start traps are always generated and cannot be disabled.

Format

```
show trapflags
```

Mode

Privileged EXEC and User EXEC

Authentication Flag

May be enabled or disabled. The factory default is enabled. Indicates whether authentication failure traps will be sent.

Chassis

Indicates whether traps that are related to the chassis functionality of the switch will be sent. These functions include the signal contacts, the ACA, temperature limits exceeded, changes in the module map, addition or removal of SFP modules, status of power supply has changed and the LLDP and Sntp features. May be enabled or disabled.

Default value: enabled.

Layer 2 Redundancy

Indicates whether traps that are related to the layer 2 redundancy features of the switch will be sent. The HiPER-Ring and the Redundant Coupling will tell you with these traps when the main line has become inoperative or returned. May be enabled or disabled.

Default value: enabled.

Link Up/Down Flag

May be enabled or disabled. The factory default is enabled. Indicates whether link status traps will be sent.

Multiple Users Flag

May be enabled or disabled. The factory default is enabled. Indicates whether a trap will be sent when the same user ID is logged into the switch more than once at the same time (either via telnet or serial port).

Port Security (MAC, IP)

Enable/disable sending port security event traps (for MAC/IP port security).

Spanning Tree Flag

May be enabled or disabled. The factory default is enabled. Indicates whether spanning tree traps will be sent.

4.4.33 snmp-access global

This command configures the global SNMP access setting (for all SNMP versions).

Format

```
snmp-access global {disable|enable|read-only}
```

Mode

```
Global Config
```

disable

Disable SNMP access to this switch, regardless of the SNMP version used.

enable

Enable SNMP read and write access to this switch, regardless of the SNMP version used.

read-only

Enable SNMP read-only access to this switch (disable write access), regardless of the SNMP version used.

4.4.34 snmp-access version

This command configures the SNMP version specific access mode for SNMPv1 and SNMPv2.

Format

```
snmp-access version {all|v1|v2} {disable|enable}
```

Mode

Global Config

all

Enable or disable SNMP access by all protocol versions (v1 and v2).

v1

Enable or disable SNMP access by v1.

v2

Enable or disable SNMP access by v2.

4.4.35 snmp-access version v3-encryption

Use this command to activate/deactivate SNMPv3 data encryption.

Format

```
snmp-access version v3-encryption  
                {readonly | readwrite} {enable | disable}
```

Mode

Global Config

disable

Disable SNMP access to this switch by SNMPv3 protocol version.

enable

Enable SNMP read and write access to this switch by SNMPv3 protocol version.

readonly

Enable SNMP read-only access to this switch (disable write access) by SNMPv3 protocol version.

readwrite

Enable SNMP read-write access to this switch (enable write access) by SNMPv3 protocol version.

4.4.36 snmp-server

This command sets the name and the physical location of the switch, and the organization responsible for the network. The range for *name*, *location* and *contact* is from 0 to 64 alphanumeric characters.

Default

None

Format

```
snmp-server
{community <name> |
 ipaddr <ipaddr> <name> |
 ipmask <ipmask> <name> |
 mode <name> |
 ro <name> |
 rw <name> |
 contact <con> |
 enable traps { chassis | l2redundancy |
 linkmode | multiusers | port-sec | stpmode }
 location <loc> |
 sysname <name> }
```

Mode

Global Config

4.4.37 snmp-server community

This command adds a new SNMP community name. A community name is a name associated with the switch and with a set of SNMP managers that manage it with a specified privileged level. The length of name can be up to 32 case-sensitive characters.

Note: Community names in the SNMP community table must be unique. When making multiple entries using the same community name, the first entry is kept and processed and all duplicate entries are ignored.

Default

Two default community names: Public and Private. You can replace these default community names with unique identifiers for each community. The default values for the remaining four community names are blank.

Format

```
snmp-server community <name>
```

Mode

```
Global Config
```

■ no snmp-server community

This command removes this community name from the table. The name is the community name to be deleted.

Format

```
no snmp-server community <name>
```

Mode

```
Global Config
```

4.4.38 snmp-server contact

This command adds a new SNMP server contact.

Format

```
snmp-server contact <con>
```

Mode

Global Config

con

Enter system contact up to 63 characters in length.

If the name contains spaces, enclose it in quotation marks (").

■ no snmp-server contact

This command removes this SNMP server contact from the table.

<con> is the SNMP server contact to be deleted.

Format

```
no snmp-server contact <con>
```

Mode

Global Config

4.4.39 snmp-server community ipaddr

This command sets a client IP address for an SNMP community. The address is the associated community SNMP packet sending address and is used along with the client IP mask value to denote a range of IP addresses from which SNMP clients may use that community to access the device. A value of 0.0.0.0 allows access from any IP address. Otherwise, this value is ANDed with the mask to determine the range of allowed client IP addresses. The name is the applicable community name.

Default

0.0.0.0

Format

```
snmp-server community ipaddr <ipaddr> <name>
```

Mode

Global Config

■ no snmp-server community ipaddr

This command sets a client IP address for an SNMP community to 0.0.0.0. The name is the applicable community name.

Format

```
no snmp-server community ipaddr <name>
```

Mode

Global Config

4.4.40 snmp-server community ipmask

This command sets a client IP mask for an SNMP community. The address is the associated community SNMP packet sending address and is used along with the client IP address value to denote a range of IP addresses from which SNMP clients may use that community to access the device. A value of 255.255.255.255 will allow access from only one station, and will use that machine's IP address for the client IP Address. A value of 0.0.0.0 will allow access from any IP address. The name is the applicable community name.

Default

0.0.0.0

Format

```
snmp-server community ipmask <ipmask> <name>
```

Mode

Global Config

■ no snmp-server community ipmask

This command sets a client IP mask for an SNMP community to 0.0.0.0. The name is the applicable community name. The community name may be up to 32 alphanumeric characters.

Format

```
no snmp-server community ipmask <name>
```

Mode

Global Config

4.4.41 snmp-server community mode

This command activates an SNMP community. If a community is enabled, an SNMP manager associated with this community manages the switch according to its access right. If the community is disabled, no SNMP requests using this community are accepted. In this case the SNMP manager associated with this community cannot manage the switch until the Status is changed back to Enable.

Default

The default private and public communities are enabled by default.
The four undefined communities are disabled by default.

Format

```
snmp-server community mode <name>
```

Mode

```
Global Config
```

■ no snmp-server community mode

This command deactivates an SNMP community. If the community is disabled, no SNMP requests using this community are accepted. In this case the SNMP manager associated with this community cannot manage the switch until the Status is changed back to Enable.

Format

```
no snmp-server community mode <name>
```

Mode

```
Global Config
```

4.4.42 snmp-server community ro

This command restricts access to switch information. The access mode is read-only (also called public).

Format

```
snmp-server community ro <name>
```

Mode

```
Global Config
```

4.4.43 snmp-server community rw

This command restricts access to switch information. The access mode is read/write (also called private).

Format

```
snmp-server community rw <name>
```

Mode

```
Global Config
```

4.4.44 snmp-server location

This command configures the system location.

Format

```
snmp-server location <system location>
```

Mode

```
Global Config
```

4.4.45 snmp-server sysname

This command configures the system name.

Format

```
snmp-server sysname <system name>
```

Mode

```
Global Config
```

4.4.46 snmp-server enable traps

This command enables the Authentication Trap Flag.

Default

```
enabled
```

Format

```
snmp-server enable traps
```

Mode

```
Global Config
```

■ no snmp-server enable traps

This command disables the Authentication Trap Flag.

Format

```
no snmp-server enable traps
```

Mode

```
Global Config
```

4.4.47 snmp-server enable traps chassis

Configures whether traps that are related to the chassis functionality of the switch will be sent. These functions include the signal contacts, the ACA, temperature limits exceeded, changes in the module map, addition or removal of SFP modules, status of power supply has changed and the LLDP and SNMP features. May be enabled or disabled.

Default value: enabled.

Default

enabled

Format

```
snmp-server enable traps chassis
```

Mode

Global Config

■ no snmp-server enable traps chassis

This command disables chassis traps for the entire switch.

Format

```
no snmp-server enable traps chassis
```

Mode

Global Config

4.4.48 snmp-server enable traps l2redundancy

Indicates whether traps that are related to the layer 2 redundancy features of the switch will be sent. The HiPER-Ring and the Redundant Coupling will tell you with these traps when the main line has become inoperative or returned. May be enabled or disabled.

Default value: enabled.

Default

enabled

Format

```
snmp-server enable traps l2redundancy
```

Mode

Global Config

■ no snmp-server enable traps l2redundancy

This command disables layer 2 redundancy traps for the entire switch.

Format

```
no snmp-server enable traps l2redundancy
```

Mode

Global Config

4.4.49 snmp-server enable traps linkmode

This command enables Link Up/Down traps for the entire switch. When enabled, link traps are sent only if the Link Trap flag setting associated with the port is enabled (see 'snmp trap link-status' command).

Default

enabled

Format

```
snmp-server enable traps linkmode
```

Mode

Global Config

■ no snmp-server enable traps linkmode

This command disables Link Up/Down traps for the entire switch.

Format

```
no snmp-server enable traps linkmode
```

Mode

Global Config

4.4.50 snmp-server enable traps multiusers

This command enables Multiple User traps. When the traps are enabled, a Multiple User Trap is sent when a user logs in to the terminal interface (EIA 232 (serial port) or telnet) and there is an existing terminal interface session.

Default

enabled

Format

```
snmp-server enable traps multiusers
```

Mode

Global Config

■ no snmp-server enable traps multiusers

This command disables Multiple User traps.

Format

```
no snmp-server enable traps multiusers
```

Mode

Global Config

4.4.51 snmp-server enable traps port-sec

This command enables port security traps. When the traps are enabled, a Port Security Trap is sent if a port security event occurs (applies to MAC/IP Port Security).

Default

enabled

Format

```
snmp-server enable traps port-sec
```

Mode

Global Config

■ no snmp-server enable traps port-sec

This command disables Port Security traps.

Format

```
no snmp-server enable traps port-sec
```

Mode

Global Config

4.4.52 snmp-server enable traps stpmode

This command enables the sending of new root traps and topology change notification traps.

Default

enabled

Format

```
snmp-server enable traps stpmode
```

Mode

Global Config

■ no snmp-server enable traps stpmode

This command disables the sending of new root traps and topology change notification traps.

Format

```
no snmp-server enable traps stpmode
```

Mode

Global Config

4.4.53 snmptrap

This command adds an SNMP trap name. The maximum length of name is 32 case-sensitive alphanumeric characters.

Default

The default name for the six undefined community names is Delete.

Format

```
snmptrap <name> <ipaddr> [snmpversion snmpv1]
```

Mode

Global Config

■ no snmptrap

This command deletes trap receivers for a community.

Format

```
no snmptrap <name> <ipaddr>
```

Mode

Global Config

4.4.54 snmptrap ipaddr

This command assigns an IP address to a specified community name. The maximum length of name is 32 case-sensitive alphanumeric characters.

Note: IP addresses in the SNMP trap receiver table must be unique. If you make multiple entries using the same IP address, the first entry is retained and processed. All duplicate entries are ignored.

Format

```
snmptrap ipaddr <name> <ipaddr> <ipaddrnew>
```

Mode

Global Config

ipaddr

Enter the old IP Address.

ipaddrnew

Enter the new IP Address.

4.4.55 snmptrap mode

This command activates or deactivates an SNMP trap. Enabled trap receivers are active (able to receive traps). Disabled trap receivers are inactive (not able to receive traps).

Format

```
snmptrap mode <name> <ipaddr>
```

Mode

```
Global Config
```

■ no snmptrap mode

This command deactivates an SNMP trap. Disabled trap receivers are inactive (not able to receive traps).

Format

```
no snmptrap mode <name> <ipaddr>
```

Mode

```
Global Config
```

4.4.56 snmptrap snmpversion

This command configures SNMP trap version for a specified community.

Format

```
snmptrap snmpversion <name> <ipAddr>
      {snmpv1 | snmpv2}
```

Mode

Global Config

name

Enter the community name.

ipAddr

Enter the IP Address.

snmpv1

Use SNMP v1 to send traps.

snmpv2

Use SNMP v2 to send traps.

4.4.57 telnetcon maxsessions

Configure the number of remote telnet connections allowed.

Default

5

Format

```
telnetcon maxsessions <0-5>
```

Mode

Privileged EXEC

■ no telnetcon maxsessions

This command sets the maximum number of telnet connection sessions that can be established to the default value.

Format

```
no telnetcon maxsessions
```

Mode

Privileged EXEC

4.4.58 telnetcon timeout

This command sets the telnet connection session timeout value, in minutes. A session is active as long as the session has not been idle for the value set. The time is a decimal value from 1 to 160.

Default

5

Format

```
telnetcon timeout <1-160>
```

Mode

Privileged EXEC

■ no telnetcon timeout

This command sets the telnet connection session timeout value to the default.

Changing the timeout value for active sessions does not become effective until the session is reaccessed. Also, any keystroke activates the new timeout duration.

Format

```
no telnetcon timeout
```

Mode

Privileged EXEC

4.5 Syslog Commands

This section provides a detailed explanation of the Syslog commands. The commands are divided into two functional groups:

- ▶ Show commands display spanning tree settings, statistics, and other information.
- ▶ Configuration Commands configure features and options of the device. For every configuration command there is a show command that displays the configuration setting.

4.5.1 logging buffered

This command enables logging to an in-memory log where up to 128 logs are kept.

Default

enabled

Format

logging buffered

Mode

Global Config

■ no logging buffered

This command disables logging to in-memory log.

Format

no logging buffered

4.5.2 logging buffered wrap

This command enables wrapping of in-memory logging when full capacity reached. Otherwise when full capacity is reached, logging stops.

Default

```
wrap
```

Format

```
logging buffered wrap
```

Mode

```
Privileged EXEC
```

■ no logging buffered wrap

This command disables wrapping of in-memory logging and configures logging to stop when capacity is full.

Format

```
no logging buffered wrap
```

4.5.3 logging cli-command

This command enables the CLI command Logging feature. The Command Logging component enables the switch software to log all Command Line Interface (CLI) commands issued on the system.

Default

disabled

Format

logging cli-command

Mode

Global Config

■ no logging cli-command

This command disables the CLI command Logging feature.

Format

no logging cli-command

4.5.4 logging console

This command enables logging to the console. The <severitylevel> value is specified as either an integer from 0 to 7 or symbolically through one of the following keywords: emergency (0), alert (1), critical (2), error (3), warning (4), notice (5), informational (6), debug (7).

Default

```
disabled; alert
```

Format

```
logging console [severitylevel] | <[0-7]>
```

Mode

```
Global Config
```

severitylevel | [0-7]

Enter Logging Severity Level (emergency|0, alert|1, critical|2, error|3, warning|4, notice|5, info|6, debug|7).

Note: Selecting a lower severity level (larger number) will include all messages from higher severity levels (smaller numbers).

Possible severity levels: see Table 13

■ no logging console

This command disables logging to the console.

Format

```
no logging console
```

4.5.5 logging host

This command enables logging to a host where up to eight hosts can be configured.

Default

```
Port - 514; Level - Critical;
```

Format

```
logging host <hostaddress>
  [<port> [<severitylevel>]]
```

Mode

```
Global Config
```

Severity number	Severity name	Meaning
0	emergency	Minimum severity to be logged is 0. This is the highest level and will result in all other messages of lower levels not being logged.
1	alert	Minimum severity to be logged is 1.
2	critical	Minimum severity to be logged is 2.
3	error	Minimum severity to be logged is 3.
4	warning	Minimum severity to be logged is 4.
5	notice	Minimum severity to be logged is 5.
6	info	Minimum severity to be logged is 6.
7	debug	Minimum severity to be logged is 7. This is the lowest level and will result in messages of all levels being logged.

Tab. 13: Possible severity levels

4.5.6 logging host reconfigure

The Logging Host Index for which to change the IP Address.

Format

```
logging host reconfigure <hostindex> <hostaddress>
```

Mode

```
Global Config
```

4.5.7 logging host remove

The Logging Host Index to be removed.

Format

```
logging host remove <hostindex>
```

Mode

```
Global Config
```

4.5.8 logging snmp-requests get operation

This command enables or disables the logging of SNMP GET requests.

Default

```
Disabled
```

Format

```
logging snmp-requests get operation  
{ enable | disable }
```

Mode

```
Global Config
```

4.5.9 logging snmp-requests set operation

This command enables or disables the logging of SNMP SET requests.

Default

Disabled

Format

```
logging snmp-requests set operation  
{ enable | disable }
```

Mode

Global Config

4.5.10 logging snmp-requests get severity

With this command you can define the severity level of logging SNMP GET requests.

Default

Disabled

Format

```
logging snmp-requests get severity <level|[0-7]>
```

Mode

Global Config

level | [0-7]

Enter Logging Severity Level (emergency|0, alert|1, critical|2, error|3, warning|4, notice|5, info|6, debug|7).

Note: Selecting a lower severity level (larger number) will include all messages from higher severity levels (smaller numbers).

4.5.11 logging snmp-requests set severity

With this command you can define the severity level of logging SNMP SET requests.

Default

Disabled

Format

```
logging snmp-requests set severity <level|[0-7]>
```

Mode

Global Config

level | [0-7]

Enter Logging Severity Level (emergency|0, alert|1, critical|2, error|3, warning|4, notice|5, info|6, debug|7).

Note: Selecting a lower severity level (larger number) will include all messages from higher severity levels (smaller numbers).

4.5.12 logging syslog

This command enables syslog logging.

Default

disabled

Format

logging syslog

Mode

Global Config

■ no logging syslog

This command disables syslog logging.

Format

no logging syslog

4.5.13 logging syslog port

Enter the port number of the syslog server.

Default

514

Format

logging syslog port <portid>

Mode

Global Config

4.6 Device Configuration Commands

4.6.1 auto-disable reason

This command enables the port disabling on this device by reason.

Default

Disabled

Format

```
auto-disable reason {link-flap | crc-error |  
overload-detection | speed-duplex | port-security}
```

Mode

Global Config

link-flap

Enable the port disabling on this device by link flap.

crc-error

Enable the port disabling on this device by CRC error.

overload-detection

Enable the port disabling on this device by overload detection.

speed-duplex

Enable the port disabling on this device by speed-duplex.

port-security

Enable the port disabling on this device by port-security.

■ no auto-disable reason

This command disables the port disabling on this device by reason.

Default

Disabled

Format

```
no auto-disable reason {link-flap | crc-error |  
                        overload-detection | speed-duplex}
```

Mode

Global Config

link-flap

Disable the port disabling on this device by link flap.

crc-error

Disable the port disabling on this device by CRC error.

overload-detection

Disable the port disabling on this device by overload detection.

port-security

Disable the port disabling on this device by port-security.

speed-duplex

Disable the port disabling on this device by speed-duplex.

4.6.2 auto-disable reset

Use this command to reset the specific interface and reactivate the port.

Format

```
auto-disable reset
```

Mode

```
Interface Config
```

4.6.3 auto-disable timer

This command defines the time after which a deactivated port is activated again.

Default

```
0
```

Format

```
auto-disable timer {0 | 30..2147483}
```

Mode

```
Interface Config
```

{0 | 30..2147483}

Timer value in seconds after a deactivated port is activated again.

Possible values:

0 The value 0 disables the timer.

30..2147483.

4.6.4 auto-negotiate

This command enables automatic negotiation on a port. The default value is enable.

Format

```
auto-negotiate
```

Mode

```
Interface Config
```

■ no auto-negotiate

This command disables automatic negotiation on a port.

Format

```
no auto-negotiate
```

Mode

```
Interface Config
```

4.6.5 auto-negotiate all

This command enables automatic negotiation on all ports.
The default value is `enable`.

Format

```
auto-negotiate all
```

Mode

```
Global Config
```

■ no auto-negotiate all

This command disables automatic negotiation on all ports.

Format

```
no auto-negotiate all
```

Mode

```
Global Config
```

4.6.6 cable-crossing

Note: This function is available for the RS20/RS30/RS40, MS20/MS30, RSR20/RSR30, MACH1000, PowerMICE and OCTOPUS devices.

Use this command to enable or disable the cable crossing function.

Note: The `cable-crossing` settings become effective for a certain port, if `auto-negotiate` is disabled for this port.

The `cable-crossing` settings are irrelevant for a certain port, if `auto-negotiate` is enabled for this port.

Format

```
cable-crossing {enable|disable}
```

Mode

```
Interface Config
```

cable-crossing enable

The device swaps the port output and port input of the TP port.

cable-crossing disable

The device does not swap the port output and port input of the TP port.

4.6.7 media-module

Use this command to logically configure media modules.

Default

```
media-module enable all
```

Format

```
media-module { remove <1-7> |  
                enable { <1-7> | all } |  
                disable { <1-7> | all } }
```

Mode

```
Global Config
```

remove

Logically remove a media-module that has already been physically removed.

<1-7>

Enter the number of a media module that has already been physically removed but is logically still present in the configuration.

enable

Enable a media-module slot.

<1-7>

Enter the number of the media module to be enabled.

all

Enable all media modules on the device.

disable

Disable a media-module slot.

<1-7>

Enter the number of the media module to be disabled.

all

Disable all media modules on the device.

4.6.8 dip-switch operation

Note: This command is available for the MICE, PowerMICE and RS20/RS30/RS40 devices.

Use this command to enable/disable the DIP switch configuration.

Default

disabled

Format

```
dip-switch operation { enable | disable }
```

Mode

Global Config

enable

Enable the DIP switch configuration.

disable

Disable the DIP switch configuration.
The device ignores DIP switch settings.

4.6.9 macfilter

This command adds a static MAC filter entry for the MAC address <macaddr> on the VLAN <vlanid>. The <macaddr> parameter must be specified as a 6-byte hexadecimal number in the format of b1:b2:b3:b4:b5:b6.

The restricted MAC Addresses are: 00:00:00:00:00:00, 01:80:C2:00:00:00 to 01:80:C2:00:00:0F, 01:80:C2:00:00:20 to 01:80:C2:00:00:21, and FF:FF:FF:FF:FF:FF.

The <vlanid> parameter must identify a valid VLAN (1 to 4042).

Up to 100 static MAC filters may be created.

Format

```
macfilter <macaddr> <vlanid>
```

Mode

```
Global Config
```

■ no macfilter

This command removes all filtering restrictions and the static MAC filter entry for the MAC address <macaddr> on the VLAN <vlanid>. The <macaddr> parameter must be specified as a 6-byte hexadecimal number in the format of b1:b2:b3:b4:b5:b6.

The <vlanid> parameter must identify a valid VLAN (1 to 4042).

Format

```
no macfilter <macaddr> <vlanid>
```

Mode

```
Global Config
```

4.6.10 macfilter adddest

This command adds the interface to the destination filter set for the MAC filter with the given <macaddr> and VLAN of <vlanid>. The <macaddr> parameter must be specified as a 6-byte hexadecimal number in the format of b1:b2:b3:b4:b5:b6.

The <vlanid> parameter must identify a valid VLAN (1-4042).

Format

```
macfilter adddest <macaddr> <vlanid>
```

Mode

Interface Config

■ no macfilter adddest

This command removes a port from the destination filter set for the MAC filter with the given <macaddr> and VLAN of <vlanid>. The <macaddr> parameter must be specified as a 6-byte hexadecimal number in the format of b1:b2:b3:b4:b5:b6.

The <vlanid> parameter must identify a valid VLAN (1-4042).

Format

```
no macfilter adddest <macaddr> <vlanid>
```

Mode

Interface Config

4.6.11 macfilter adddest all

This command adds all interfaces to the destination filter set for the MAC filter with the given <macaddr> and VLAN of <vlanid>. The <macaddr> parameter must be specified as a 6-byte hexadecimal number in the format of b1:b2:b3:b4:b5:b6.

The <vlanid> parameter must identify a valid VLAN (1 to 4042).

Format

```
macfilter adddest {all | <macaddr> <vlanid>}
```

Mode

Global Config

■ no macfilter adddest all

This command removes all ports from the destination filter set for the MAC filter with the given <macaddr> and VLAN of <vlanid>. The <macaddr> parameter must be specified as a 6-byte hexadecimal number in the format of b1:b2:b3:b4:b5:b6.

The <vlanid> parameter must identify a valid VLAN (1 to 4042).

Format

```
no macfilter adddest [all | <macaddr> <vlanid>]
```

Mode

Global Config

4.6.12 monitor session

This command configures a probe port and a monitored port for monitor session (port monitoring). The first slot/port is the source monitored port and the second slot/port is the destination probe port. If this command is executed while port monitoring is enabled, it will have the effect of changing the probe and monitored port values.

Format

```
monitor session
  [ mode |
    source interface <slot/port>
      [direction { rx | tx | tx/rx } ] |
    destination interface <slot/port> ]
```

Mode

Global Config

session-id

Session number (currently, session number 1 is supported).

mode

Enable/Disable port mirroring session.

Note: does not affect the source or destination interfaces.

source interface <slot/port>

Configure the source interface (in `slot/port` notation).

direction

Configure the direction of the interface.

rx

Configure the direction of the interface as rx (receive).

tx

Configure the direction of the interface as tx (transmit).

rx/tx

Configure the direction of the interface as rx/tx (receive and transmit).

destination interface <slot/port>

Configure the probe interface (in `slot/port` notation).

■ **no monitor session**

This command removes the monitor session (port monitoring) designation from both the source probe port and the destination monitored port and removes the probe port from all VLANs. The port must be manually re-added to any desired VLANs.

Format

```
no monitor session
```

Mode

```
Global Config
```

session-id

Session number (currently, session number 1 is supported).

4.6.13 monitor session mode

This command configures the monitor session (port monitoring) mode to enable. The probe and monitored ports must be configured before monitor session (port monitoring) can be enabled. If enabled, the probe port will monitor all traffic received and transmitted on the physical monitored port. It is not necessary to disable port monitoring before modifying the probe and monitored ports.

Default

disabled

Format

```
monitor session mode
```

Mode

Global Config

session-id

Session number (currently, session number 1 is supported).

■ no monitor session mode

This command sets the monitor session (port monitoring) mode to disable.

Format

```
no monitor session mode
```

Mode

Global Config

session-id

Session number (currently, session number 1 is supported).

4.6.14 monitor session <session-id> source/destination

This command allows you to configure and activate the port mirroring function of the switch. Port mirroring is when the data traffic of a source port is copied to a specified destination port. The data traffic at the source port is not influenced by port mirroring. A management tool connected at the specified port, e.g., an RMON probe, can thus monitor the data traffic of the source port.

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

Default

none

Format

```
monitor session {source | destination} interface
<slot/port>
```

Mode

Global Config

session-id

Session number (currently, session number 1 is supported).

■ no monitor session <session-id> source/destination

This command resets the monitor session (port monitoring) source/destination. The port will be removed from port mirroring

Format

```
no monitor session <session-id> {source | destina-
tion} interface
```

Mode

Global Config

session-id

Session number (currently, session number 1 is supported).

4.6.15 set igmp

This command enables IGMP Snooping on the system. The default value is `disable`.

Note: The IGMP snooping application supports the following:

- ▶ Global configuration or per interface configuration.
- ▶ Validation of the IP header checksum (as well as the IGMP header checksum) and discarding of the frame upon checksum error.
- ▶ Maintenance of the forwarding table entries based on the MAC address versus the IP address.
- ▶ Flooding of unregistered multicast data packets to all ports in the VLAN.

Format

```
set igmp
```

Mode

```
Global Config
```

■ no set igmp

This command disables IGMP Snooping on the system.

Format

```
no set igmp
```

Mode

```
Global Config
```

4.6.16 set igmp

This command enables IGMP Snooping on a selected interface.

Default

enabled

Format

```
set igmp
```

Mode

Interface Config

■ no set igmp

This command disables IGMP Snooping on a selected interface.

Format

```
no set igmp
```

Mode

Interface Config

4.6.17 set igmp aging-time-unknown

This command configures the IGMP Snooping aging time for unknown multicast frames (unit: seconds, min.: 3, max.: 3600, Default value: 260).

Format

```
set igmp aging-time-unknown <3-3600>
```

Mode

Global Config

4.6.18 set igmp automatic-mode

If enabled, this port is allowed to be set as static query port automatically, if the LLDP protocol has found a switch or router connected to this port. Use the command's normal form to enable the feature, the 'no' form to disable it.

Default

disabled

Format

set igmp automatic-mode

Mode

Interface Config

4.6.19 set igmp forward-all

This command activates the forwarding of multicast frames to this interface even if the given interface has not received any reports by hosts. N. B.: this applies only to frames that have been learned via IGMP Snooping. The purpose is that an interface (e. g. a HIPER Ring's ring port) may need to forward all such frames even if no reports have been received on it. This enables faster recovery from ring interruptions for multicast frames.

Default

disabled

Format

```
set igmp forward-all
```

Mode

Interface Config

■ no set igmp forward-all

This command disables the forwarding of all multicast frames learned via IGMP Snooping on a selected interface.

Format

```
no set igmp forward-all
```

Mode

Interface Config

4.6.20 set igmp forward-unknown

Note: This command is available for MS20/MS30.

This command defines how to handle unknown multicast frames.

Format

```
set igmp forward-unknown
    { discard | flood | query-ports}
```

Mode

Global Config

discard

Unknown multicast frames will be discarded.

flood

Unknown multicast frames will be flooded.

query-ports

Unknown multicast frames will be forwarded only to query ports.

4.6.21 set igmp static-query-port

This command activates the forwarding of IGMP membership report frames to this interface even if the given interface has not received any queries. The purpose is that a port may need to forward such frames even if no queries have been received on it (e. g., if a router is connected to the interface that sends no queries).

Default

disabled

Format

```
set igmp static-query-port
```

Mode

Interface Config

■ no set igmp

This command disables the unconditional forwarding of IGMP membership report frames to this interface.

Format

```
no set igmp static-query-port
```

Mode

Interface Config

4.6.22 set igmp groupmembershipinterval

This command sets the IGMP Group Membership Interval time on the system. The Group Membership Interval time is the amount of time in seconds that a switch will wait for a report from a particular group on a particular interface before deleting the interface from the entry. This value must be greater than the IGMP Maximum Response time value. The range is 3 to 3,600 seconds.

Default

260

Format

```
set igmp groupmembershipinterval <3-3600>
```

Mode

Global Config

■ no set igmp groupmembershipinterval

This command sets the IGMP Group Membership Interval time on the system to 260 seconds.

Format

```
no set igmp groupmembershipinterval
```

Mode

Global Config

4.6.23 set igmp interfacemode

This command enables IGMP Snooping on all interfaces.

Format

```
set igmp interfacemode
```

Mode

```
Global Config
```

■ no set igmp interfacemode

This command disables IGMP Snooping on all interfaces.

Format

```
no set igmp interfacemode
```

Mode

```
Global Config
```

4.6.24 set igmp lookup-interval-unknown

This command configures the IGMP Snooping lookup response time for unknown multicast frames (unit: seconds, min.: 2, max.: 3599, Default value: 125).

Format

```
set igmp lookup-interval-unknown <2-3599>
```

Mode

```
Global Config
```

<2-3599>

Enter the IGMP Snooping lookup response time for unknown multicast frames (unit: seconds, min.: 2, max.: 3599, Default value: 125).

4.6.25 set igmp lookup-resp-time-unknown

This command configures the IGMP Snooping lookup interval for unknown multicast frames (unit: seconds, min.: 1, max.: 3,598, Default value: 10).

Format

```
set igmp lookup-resp-time-unknown <1-3598>
```

Mode

Global Config

<2-3598>

Enter the IGMP Snooping lookup interval for unknown multicast frames (unit: seconds, min.: 1, max.: 3598, Default value: 10).

4.6.26 set igmp maxresponse

This command sets the IGMP Maximum Response time on the system. The Maximum Response time is the amount of time in seconds that a switch will wait after sending a query in response to a received leave message, before deleting the multicast group received in the leave message. If the switch receives a report in response to the query within the maxresponse time, then the multicast group is not deleted. This value must be less than the IGMP Query Interval time value. The range is 1 to 3,598 seconds.

Default

10

Format

```
set igmp maxresponse <1-3598>
```

Mode

Global Config

Note: the IGMP Querier's max. response time was also set. It is always the same value as the IGMP Snooping max. response time.

■ no set igmp maxresponse

This command sets the IGMP Maximum Response time on the system to 10 seconds.

Format

```
no set igmp maxresponse
```

Mode

Global Config

4.6.27 set igmp querier max-response-time

Configure the IGMP Snooping Querier's maximum response time. The range is 1 to 3,598 seconds. The default value is 10 seconds.

Default

10

Format

```
set igmp querier max-response-time <1-3598>
```

Mode

Global Config

Note: The IGMP Snooping max. response time was also set. It is always the same value as the IGMP Querier's max. response time.

4.6.28 set igmp querier protocol-version

Configure the IGMP Snooping Querier's protocol version (1, 2 or 3).

Default

2

Format

```
set igmp querier protocol-version {1 | 2 | 3}
```

Mode

Global Config

4.6.29 set igmp querier status

Configure the IGMP Snooping Querier's administrative status (enable or disable).

Default

disable

Format

```
set igmp querier status {enable | disable}
```

Mode

Global Config

4.6.30 set igmp querier tx-interval

Configure the IGMP Snooping Querier's transmit interval. The range is 2 to 3,599 seconds.

Default

125

Format

```
set igmp querier tx-interval <2-3599>
```

Mode

Global Config

4.6.31 set igmp query-ports-to-filter

This command enables or disables the addition of query ports to multicast filter portmasks. The setting can be enable or disable.

Default

Disable

Format

```
set igmp query-ports-to-filter {enable | disable}
```

Mode

Global Config

enable

Addition of query ports to multicast filter portmasks.

disable

No addition of query ports to multicast filter portmasks.

4.6.32 selftest ramtest

Enable or disable the RAM test for a cold start of the device. Deactivating the RAM test reduces the booting time for a cold start of the device.

Default value: enabled.

Format

```
selftest ramtest {disable|enable}
```

Mode

Global Config

selftest ramtest disable

Disable the ramtest.

selftest ramtest enable

Enable the ramtest. This is the default.

4.6.33 selftest reboot-on-hdxerror

Enable or disable a restart when the device detects a half duplex mismatch error. Default value: `enabled`.

Format

```
selftest reboot-on-hdxerror {disable | enable}
```

Mode

```
Global Config
```

selftest reboot-on-hdxerror disable

Disable the reboot-on-hdxerror function.

selftest reboot-on-hdxerror enable

Enable the reboot-on-hdxerror function. This is the default.

4.6.34 selftest reboot-on-error

Enable or disable a restart due to an undefined software or hardware state.
Default value: disabled.

Format

```
selftest reboot-on-error  
                {disable | enable | seriousOnly}
```

Mode

Global Config

selftest reboot-on-error disable

Disable the reboot-on-error function. This is the default.

selftest reboot-on-error enable

Enable the reboot-on-error function.

selftest reboot-on-error seriousOnly

The device will only reboot on errors considered to be critical.

Note: Duplex mismatch errors are considered to be non-critical. In case of a detected duplex mismatch error, the device will not reboot. Reset the device to restore ports to an usable state.

4.6.35 serviceshell

Use this command to execute a service shell command.

Format

```
serviceshell [deactivate]
```

Mode

Privileged EXEC

deactivate

Disable the service shell access permanently (**Cannot be undone**).

Note: If you execute this command the system asks for confirmation: When you disable the service shell function it is permanently disabled. Please see the Basic Configuration Manual for details.

4.6.36 update module-configuration

Note: This command is available for the MACH1020 and MACH1030 devices.

Use this command to update the product code of the device.

Format

```
update module-configuration
```

Mode

Global Config

Note: Update the product code specifically after you replaced or added a module to the device.

4.6.37 show auto-disable brief

Use this command to display the Auto Disable summary.

Format

```
show auto-disable brief
```

Mode

Global Config

Intf

Display the number of the interface in slot/port format.

Error reason

Display the error reason for auto-disable.

Possible values: no error | link-flap | crc-error |
overload-detection | port-security | speed-duplex.

Component name

Display the name of the component for auto-disable.

Possible values: PORTSEC | PORTMON.

Remaining time (sec.)

Display the remaining time in seconds for auto-disable.

Possible values: 0 | 30..2147483.

Auto-Disable time (sec.)

Display the time for auto-disable in seconds.

Possible values: 0 | 30..2147483.

Auto-Disable oper state

Display the operational state of the auto-disable function.

Possible values: active | inactive.

4.6.38 show auto-disable reasons

Use this command to display the reasons for port auto-disable on this device.

Format

```
show auto-disable reasons
```

Mode

```
Global Config
```

Error reason

Display the error reasons of the port auto-disable function

Possible values: link-flap | crc-error | overload-detection | port-security | speed-duplex.

State

Display the state of the port auto-disable function.

Possible values: enabled | disabled.

4.6.39 show dip-switch

This command displays the DIP switch operation configuration.

Format

```
show dip-switch
```

Mode

```
Global Config
```

DIP Switch operation

This field displays the DIP Switch operation status.

Possible values: Enabled, Disabled

DIP Switch conflict

This field displays the DIP Switch conflict status.

Possible values: True, False

DIP Switch Red. Manager

This field displays the DIP Switch Redundancy Manager status.

Possible values: Enabled, Disabled

DIP Switch Standby

This field displays the DIP Switch Standby status.

Possible values: Enabled, Disabled

DIP Switch RingPort

Note: This command is available for the MICE devices.

This field displays the DIP Switch RingPort numbers.

Possible values: Interface number in slot/port notation.

DIP Switch SW config

Note: This command is available for the MICE devices.

This field displays the DIP Switch SW config status.

Possible values: Enabled, Disabled

4.6.40 show igmpsnooping

This command displays IGMP Snooping information. Configured information is displayed whether or not IGMP Snooping is enabled. Status information is only displayed when IGMP Snooping is enabled.

Format

```
show igmpsnooping
```

Mode

Privileged EXEC and User EXEC

Admin Mode

This indicates whether or not IGMP Snooping is globally enabled on the switch.

Forwarding of Unknown Frames

This displays if and how unknown multicasts are forwarded. The setting can be Discard, Flood or Query Ports. The default is Query Ports.

Group Membership Interval

This displays the IGMP Group Membership Interval. This is the amount of time a switch will wait for a report for a particular group on a particular interface before it sends a query on that interface. This value may be configured.

Multicast Control Frame Count

This displays the number of multicast control frames that are processed by the CPU.

Interfaces Enabled for IGMP Snooping

This is the list of interfaces on which IGMP Snooping is enabled. Additionally, if a port has a special function, it will be shown to the right of its slot/port number. There are 3 special functions: Forward All, Static Query Port and Learned Query Port.

Querier Status (the administrative state).

This displays the IGMP Snooping Querier's administrative status.

Querier Mode (the actual state, read only)

This displays the IGMP Snooping Querier's operating status.

Querier Transmit Interval

This displays the IGMP Snooping Querier's transmit interval in seconds.

Querier Max. Response Time

This displays the IGMP Snooping Querier's maximum response time in seconds.

Querier Protocol Version

This displays the IGMP Snooping Querier's protocol version number.

4.6.41 show mac-filter-table igmpsnooping

This command displays the IGMP Snooping entries in the Multicast Forwarding Database (MFDB) table.

Format

```
show mac-filter-table igmpsnooping
```

Mode

Privileged EXEC and User EXEC

Mac Address

A multicast MAC address for which the switch has forwarding and or filtering information. The format is two-digit hexadecimal numbers that are separated by colons, for example 01:23:45:67:89:AB.

Type

This displays the type of the entry. Static entries are those that are configured by the end user. Dynamic entries are added to the table as a result of a learning process or protocol.

Description

The text description of this multicast table entry.

Interfaces

The list of interfaces that are designated for forwarding (Fwd:) and filtering (Flt:).

4.6.42 show mac-filter-table multicast

This command displays the Multicast Forwarding Database (MFDB) information. If the command is entered with no parameter, the entire table is displayed. This is the same as entering the optional `all` parameter. The user can display the table entry for one MAC Address by specifying the MAC address as an optional parameter.

Format

```
show mac-filter-table multicast
        [<macaddr> <1-4042>]
```

Mode

Privileged EXEC and User EXEC

Mac Address

A multicast MAC address for which the switch has forwarding and or filtering information. The format is two-digit hexadecimal numbers that are separated by colons, for example 01:23:45:67:89:AB.

Type

This displays the type of the entry. Static entries are those that are configured by the end user. Dynamic entries are added to the table as a result of a learning process or protocol.

Component

The component that is responsible for this entry in the Multicast Forwarding Database. Possible values are `IGMP Snooping` and `Static Filtering`.

Description

The text description of this multicast table entry.

Interfaces

The list of interfaces that are designated for forwarding (Fwd:) and filtering (Flt:).

Forwarding Interfaces

The resultant forwarding list is derived from combining all the component's forwarding interfaces and removing the interfaces that are listed as the static filtering interfaces.

4.6.43 show mac-filter-table static

This command displays the Static MAC Filtering information for all Static MAC Filters. If `all` is selected, all the Static MAC Filters in the system are displayed. If a `macaddr` is entered, a `vlan` must also be entered and the Static MAC Filter information will be displayed only for that MAC address and VLAN.

Format

```
show mac-filter-table static {<macaddr> <vlanid> |  
all}
```

Mode

Privileged EXEC and User EXEC

MAC Address

Is the MAC Address of the static MAC filter entry.

VLAN ID

Is the VLAN ID of the static MAC filter entry.

Source Port(s)

Indicates the source port filter set's slot and port(s).

Destination Port(s)

Indicates the destination port filter set's slot and port(s).

4.6.44 show mac-filter-table staticfiltering

This command displays the Static Filtering entries in the Multicast Forwarding Database (MFDB) table.

Format

```
show mac-filter-table staticfiltering
```

Mode

Privileged EXEC and User EXEC

Mac Address

A unicast MAC address for which the switch has forwarding and or filtering information. The format is 6 or 8 two-digit hexadecimal numbers that are separated by colons, for example 01:23:45:67:89:AB.

Type

This displays the type of the entry. Static entries are those that are configured by the end user. Dynamic entries are added to the table as a result of a learning process or protocol.

Description

The text description of this multicast table entry.

Interfaces

The list of interfaces that are designated for forwarding (Fwd:) and filtering (Flt:).

4.6.45 show mac-filter-table stats

This command displays the Multicast Forwarding Database (MFDB) statistics.

Format

```
show mac-filter-table stats
```

Mode

Privileged EXEC and User EXEC

Total Entries

This displays the total number of entries that can possibly be in the Multicast Forwarding Database table.

Most MFDB Entries Ever Used

This displays the largest number of entries that have been present in the Multicast Forwarding Database table. This value is also known as the MFDB high-water mark.

Current Entries

This displays the current number of entries in the Multicast Forwarding Database table.

4.6.46 show monitor session

This command displays the port monitoring information for the system.

Format

```
show monitor session <Session Number>
```

Mode

Global Config, Privileged EXEC, User EXEC

Session

Display port monitor session settings.

Session Number

Session number. Enter 1 for the session number.

Session ID

Displays the session number of the port monitor session.

Possible values: 1.

Admin Mode

Displays the status of the port monitoring feature.

Possible values: Enable, Disable.

Probe Port

Displays the interface configured as the probe port (in slot/port notation). If this value has not been configured, 'Not Configured' will be displayed.

Mirrored Port

Displays the interface configured as the mirrored port (in slot/port notation). If this value has not been configured, 'Not Configured' will be displayed.

Direction

Displays the direction which has been configured for the port.

Possible values: rx (receive), tx (transmit), rx/tx (receive and transmit)

If this value has not been configured, 'Not Configured' will be displayed.

4.6.47 show port

This command displays port information.

Format

```
show port {<slot/port> | all} [name]
```

Mode

Privileged EXEC and User EXEC

Slot/Port

Valid slot and port number separated by forward slashes.

Name

When the optional command parameter `name` was specified, the output is different. It specifically includes the Interface Name as the second column, followed by other basic settings that are also shown by the normal command without the command parameter `name`.

Type

If not blank, this field indicates that this port is a special type of port. The possible values are:

`Mon` – this port is a monitoring port. Look at the Port Monitoring screens to find out more information.

`LA Mbr` – this port is a member of a Link Aggregation (LAG).

`Probe` – this port is a probe port.

Admin Mode

Indicates the Port control administration state. The port must be enabled in order for it to be allowed into the network. - May be enabled or disabled. The factory default is enabled.

Physical Mode

Indicates the desired port speed and duplex mode. If auto-negotiation support is selected, then the duplex mode and speed will be set from the auto-negotiation process. Note that the port's maximum capability (full duplex -100M) will be advertised. Otherwise, this object will determine the port's duplex mode and transmission rate. The factory default is Auto.

Physical Status

Indicates the port speed and duplex mode.

Link Status

Indicates whether the Link is up or down.

Link Trap

This object determines whether or not to send a trap when link status changes. The factory default is enabled.

Flow

Indicates if enable flow control is enabled on this port.

Device Status

Indicates whether or not the given port's link status is monitored by the device status.

VLAN Prio

This object displays the port VLAN priority.

4.6.48 show rmon-alarm

This command displays switch configuration information.

Format

```
show rmon-alarm
```

Mode

Privileged EXEC and User EXEC

4.6.49 show selftest

This command displays switch configuration information.

Format

```
show selftest
```

Mode

Privileged EXEC and User EXEC

Ramtest state

May be enabled or disabled. The factory default is enabled.

Reboot on error

May be enabled, disabled or seriousOnly. The factory default is enabled.

4.6.50 show serviceshell

This command displays the admin state of the service shell access.

Format

```
show serviceshell
```

Mode

Privileged EXEC and User EXEC

Admin state of service shell

Display the admin state of the service shell access
Possible values: Disabled, Enabled.

4.6.51 show storm-control

This command displays switch configuration information.

Format

```
show storm-control
```

Mode

Privileged EXEC and User EXEC

Ingress Limiting

May be enabled or disabled. The factory default is disabled.

Ingress Limiter Mode

Note: This command is available for the MACH4000 and PowerMICE devices.

Sets the global mode for the ingress limiter. The factory default is: Broadcasts only.

Egress Broadcast Limiting

May be enabled or disabled. The factory default is disabled.

Egress Limiting (all traffic)

May be enabled or disabled. The factory default is disabled.

802.3x Flow Control Mode

May be enabled or disabled. The factory default is disabled.

4.6.52 show storm-control limiters port

This command displays the limiter settings per port. "0" means that the respective limiter is disabled.

Format

```
show storm-control limiters port {<slot/port>|all}
```

Mode

Privileged EXEC and User EXEC

Ingress Mode

Note: This command is available for the devices RS20/RS30/RS40, MS20/MS30 and OCTOPUS.

Shows the mode for the ingress limiter. The factory default is: Broadcasts only.

Ingress Limit

Shows the ingress rate limit. The factory default is: 0.

Egress Broadcast Limit

Shows the egress broadcast rate limit. The factory default is: 0.

Egress Limit (all traffic)

Note: This command is available for the devices RS20/RS30/RS40, MS20/MS30 and OCTOPUS.

Shows the egress rate limit for all frame types.

The factory default is: 0.

4.6.53 show vlan

This command displays detailed information, including interface information, for a specific VLAN. The ID is a valid VLAN identification number

Format

```
show vlan <vlanid>
```

Mode

Privileged EXEC and User EXEC

VLAN ID

There is a VLAN Identifier (VID) associated with each VLAN. The range of the VLAN ID is 1 to 4042.

VLAN Name

A string associated with this VLAN as a convenience. It can be up to 32 alphanumeric characters long, including blanks. The default is blank. VLAN ID 1 always has a name of `Default`. This field is optional.

VLAN Type

Type of VLAN, which can be Default, (VLAN ID = 1), a static (one that is configured and permanently defined), or Dynamic (one that is created by GVRP registration).

VLAN Creation Time

Time since VLAN has been created:
d days, hh:mm:ss (System Uptime).

Interface

Valid slot and port number separated by forward slashes. It is possible to set the parameters for all ports by using the selectors on the top line.

Current

Determines the degree of participation of this port in this VLAN. The permissible values are:

`Include` – This port is always a member of this VLAN. This is equivalent to registration fixed in the IEEE 802.1Q standard.

`Exclude` – This port is never a member of this VLAN. This is equivalent to registration forbidden in the IEEE 802.1Q standard.

`Autodetect` – Specifies to allow the port to be dynamically registered in this VLAN via GVRP. The port will not participate in this VLAN unless a join request is received on this port. This is equivalent to registration normal in the IEEE 802.1Q standard.

Configured

Determines the configured degree of participation of this port in this VLAN. The permissible values are:

`Include` – This port is always a member of this VLAN. This is equivalent to registration fixed in the IEEE 802.1Q standard.

`Exclude` – This port is never a member of this VLAN. This is equivalent to registration forbidden in the IEEE 802.1Q standard.

`Autodetect` – Specifies to allow the port to be dynamically registered in this VLAN via GVRP. The port will not participate in this VLAN unless a join request is received on this port. This is equivalent to registration normal in the IEEE 802.1Q standard.

Tagging

Select the tagging behavior for this port in this VLAN.

`Tagged` – specifies to transmit traffic for this VLAN as tagged frames.

`Untagged` – specifies to transmit traffic for this VLAN as untagged frames.

4.6.54 show vlan brief

This command displays a list of all configured VLANs.

Format

```
show vlan brief
```

Mode

Privileged EXEC and User EXEC

VLAN ID

There is a VLAN Identifier (vlanid) associated with each VLAN. The range of the VLAN ID is 1 to 4042.

VLAN Name

A string associated with this VLAN as a convenience. It can be up to 32 alphanumeric characters long, including blanks. The default is blank. VLAN ID 1 always has a name of `Default`. This field is optional.

VLAN Type

Type of VLAN, which can be Default, (VLAN ID = 1), a static (one that is configured and permanently defined), or a Dynamic (one that is created by GVRP registration).

VLAN Creation Time

Displays the time (as the system time up time) when the VLAN was created.

4.6.55 show vlan port

This command displays VLAN port information.

Format

```
show vlan port {<slot/port> | all}
```

Mode

Privileged EXEC and User EXEC

Slot/Port

Valid slot and port number separated by forward slashes. It is possible to set the parameters for all ports by using the selectors on the top line.

Port VLAN ID

The VLAN ID that this port will assign to untagged frames or priority tagged frames received on this port. The value must be for an existing VLAN. The factory default is 1.

Acceptable Frame Types

Specifies the types of frames that may be received on this port. The options are 'VLAN only' and 'Admit All'. When set to 'VLAN only', untagged frames or priority tagged frames received on this port are discarded. When set to 'Admit All', untagged frames or priority tagged frames received on this port are accepted and assigned the value of the Port VLAN ID for this port. With either option, VLAN tagged frames are forwarded in accordance to the 802.1Q VLAN specification.

Ingress Filtering

May be enabled or disabled. When enabled, the frame is discarded if this port is not a member of the VLAN with which this frame is associated. In a tagged frame, the VLAN is identified by the VLAN ID in the tag. In an untagged frame, the VLAN is the Port VLAN ID specified for the port that received this frame. When disabled, all frames are forwarded in accordance with the 802.1Q VLAN bridge specification. The factory default is disabled.

GVRP

The protocol for VLAN administration, GVRP (GARP VLAN Registration Protocol) is particularly used for the adjustment of terminal devices and VLAN switches. In realtime, it traces users log-in and log-off and provides updated configuration data to the network management system. In order to be able to use this protocol, GVRP has

to be supported by every switch.

GVRP may be enabled or disabled. The factory default is disabled.

Default Priority

The 802.1p priority assigned to tagged packets arriving on the port.

4.6.56 shutdown

This command disables a port.

Default

enabled

Format

shutdown

Mode

Interface Config

■ no shutdown

This command enables a port.

Format

no shutdown

Mode

Interface Config

4.6.57 **shutdown all**

This command disables all ports.

Default

enabled

Format

shutdown all

Mode

Global Config

■ no shutdown all

This command enables all ports.

Format

no shutdown *all*

Mode

Global Config

4.6.58 snmp sync community-to-v3

This command enables the synchronization between the SNMPv1/v2 community table and the SNMPv3 password table.

Format

```
snmp sync community-to-v3
```

Mode

```
Global Config
```

■ no snmp sync community-to-v3

This command disables the synchronization between the SNMPv1/v2 community table and the SNMPv3 password table.

Format

```
no snmp sync community-to-v3
```

Mode

```
Global Config
```

4.6.59 snmp sync v3-to-community

This command enables the synchronization between the SNMPv3 password table and the SNMPv1/v2 community table.

Format

```
snmp sync v3-to-community
```

Mode

```
Global Config
```

■ no snmp sync v3-to-community

This command disables the synchronization between the SNMPv3 password table and the SNMPv1/v2 community table.

Format

```
no snmp sync v3-to-community
```

Mode

```
Global Config
```

4.6.60 snmp trap link-status

This command enables link status traps by interface.

Note: This command is valid only when the Link Up/Down Flag is enabled. See 'snmp-server enable traps linkmode' command.

Format

```
snmp trap link-status
```

Mode

```
Interface Config
```

■ no snmp trap link-status

This command disables link status traps by interface.

Note: This command is valid only when the Link Up/Down Flag is enabled. See 'snmp-server enable traps linkmode' command).

Format

```
no snmp trap link-status
```

Mode

Interface Config

4.6.61 snmp trap link-status all

This command enables link status traps for all interfaces.

Note: This command is valid only when the Link Up/Down Flag is enabled (see "snmp-server enable traps linkmode").

Format

```
snmp trap link-status all
```

Mode

Global Config

■ no snmp trap link-status all

This command disables link status traps for all interfaces.

Note: This command is valid only when the Link Up/Down Flag is enabled (see "snmp-server enable traps linkmode").

Format

```
no snmp trap link-status all
```

Mode

Global Config

4.6.62 **spanning-tree bpdumigrationcheck**

This command enables BPDU migration check on a given interface. This will force the specified port to transmit RST or MST BPDUs. The **all** option enables BPDU migration check on all interfaces.

Format

```
spanning-tree bpdumigrationcheck {<slot/port>|all}
```

Mode

Global Config

■ **no spanning-tree bpdumigrationcheck**

This command disables BPDU migration check on a given interface. The **all** option disables BPDU migration check on all interfaces.

Format

```
no spanning-tree bpdumigrationcheck {<slot/  
port>|all}
```

Mode

Global Config

4.6.63 speed

This command sets the speed and duplex setting for the interface.

Format

```
speed {<100 | 10> <half-duplex | full-duplex> |  
      1000 full-duplex}
```

Mode

```
Interface Config
```

Acceptable values are:

1000 full-duplex

Set speed for the interface to 1000 Mbps.

Set duplex mode for the interface to full duplex.

100 full-duplex

Set speed for the interface to 100 Mbps.

Set duplex mode for the interface to full duplex.

100 half-duplex

Set speed for the interface to 100 Mbps.

Set duplex mode for the interface to half duplex.

10 full-duplex

Set speed for the interface to 10 Mbps.

Set duplex mode for the interface to full duplex.

10 half-duplex

Set speed for the interface to 10 Mbps.

Set duplex mode for the interface to half duplex.

4.6.64 storm-control broadcast

This command enables the egress broadcast limiter globally.

Format

```
storm-control broadcast
```

Mode

```
Global Config
```

■ no storm-control broadcast

This command disables the egress broadcast limiter globally.

Format

```
no storm-control broadcast
```

Mode

```
Global Config
```

4.6.65 storm-control egress-limiting

This command enables or disables the egress limiter globally for all frame types.

Format

```
storm-control egress-limiting {disable | enable}
```

Mode

```
Global Config
```

4.6.66 storm-control ingress-limiting

This command enables or disables the ingress limiter globally.

Format

```
storm-control ingress-limiting {disable | enable}
```

Mode

```
Global Config
```

4.6.67 storm-control ingress-mode

Note: This command is available for the MACH4000 and PowerMICE devices.

This command sets the frame type for the ingress limiter globally to: BC or BC+MC.

Format

```
storm-control ingress-mode {bc | mc+bc}
```

Mode

```
Global Config
```

4.6.68 storm-control broadcast (port-related)

This command enables the broadcast limiter per port.
Enter the maximum number of broadcasts that the given port is allowed to send (unit: frames per second, min.: 0 (no limit), Default value: 0 (no limit)).

Format

```
storm-control broadcast <max. broadcast rate>
```

Mode

```
Interface Config
```

4.6.69 storm-control egress-limit

Note: This command is available for the RS20/RS30/RS40, MS20/MS30 and OCTOPUS devices.

Sets the egress rate limit in kbit/s. "0" means: no limit.

Format

```
storm-control egress-limit <max. egress rate>
```

Mode

```
Interface Config
```

4.6.70 storm-control ingress-limit

Sets the ingress rate limit in kbit/s. "0" means: no limit.

Format

```
storm-control ingress-limit <max. ingress rate>
```

Mode

```
Interface Config
```

4.6.71 storm-control ingress-mode

Note: This command is available for the RS20/RS30/RS40, MS20/MS30, OCTOPUS devices.

This command sets the frame type for the ingress limiter to:
All, BC, BC+MC, BC+MC+uUC.

Format

```
storm-control ingress-mode {all | bc | mc+bc |  
uuc+mc+bc}
```

Mode

```
Interface Config
```

4.6.72 storm-control flow control

This command enables 802.3x flow control for the switch.

Note: This command only applies to full-duplex mode ports.

Default

disabled

Format

```
storm-control flowcontrol
```

Mode

Interface Config
Global Config

■ no storm-control flow control

This command disables 802.3x flow control for the switch.

Note: This command only applies to full-duplex mode ports.

Format

```
no storm-control flowcontrol
```

Mode

Interface Config
Global Config

4.6.73 storm-control flowcontrol per port

This command enables 802.3x flow control for the port.

Note: This command only applies to full-duplex mode ports.

Default

enabled

Format

```
storm-control flowcontrol
```

Mode

Interface Config

■ no storm-control flowcontrol per port

This command disables 802.3x flow control for the port.

Note: This command only applies to full-duplex mode ports.

Format

```
no storm-control flowcontrol
```

Mode

Interface Config

4.6.74 vlan

This command creates a new VLAN and assigns it an ID. The ID is a valid VLAN identification number (ID 1 is reserved for the default VLAN). VLAN range is 1-4042.

Format

```
vlan <1-4042>
```

Mode

```
VLAN database
```

■ no vlan

This command deletes an existing VLAN. The ID is a valid VLAN identification number (ID 1 is reserved for the default VLAN). VLAN range is 1-4042.

Format

```
no vlan <1-4042>
```

Mode

```
VLAN database
```

4.6.75 vlan0-transparent-mode

Activate the “Transparent Mode“ to be able to switch priority tagged frames without a VLAN affiliation thus with VLAN-ID “0”.

In this mode the VLAN-ID “0” persists in the frame, irrespective of the Port VLAN ID setting in the “VLAN Port“ dialog.

Note: For PowerMICE, MACH100, MACH1000 and MACH4000:

In transparency mode devices ignore received vlan tags. Set the vlan membership of the ports to untagged for all vlans.

Note: For RS20/RS30/RS40, MS20/MS30 and OCTOPUS:

In transparency mode devices ignore the configured port vlan id. Set the vlan membership of the ports from vlan 1 to untagged or member.

Format

```
vlan0-transparent-mode {disable|enable}
```

Mode

```
VLAN database
```

4.6.76 vlan acceptframe

This command sets the frame acceptance mode per interface. For VLAN Only mode, untagged frames or priority frames received on this interface are discarded. For Admit All mode, untagged frames or priority frames received on this interface are accepted and assigned the value of the interface VLAN ID for this port. With either option, VLAN tagged frames are forwarded in accordance with the IEEE 802.1Q VLAN Specification.

Default

```
Admit All
```

Format

```
vlan acceptframe <vlanonly | all | untaggedonly>
```

Mode

```
Interface Config
```

all

Untagged frames or priority frames received on this interface are accepted and assigned the value of the interface VLAN ID for this port.

vlanonly

Only frames received with a VLAN tag will be forwarded. Other frames will be dropped.

untaggedonly

Only frames received without a VLAN tag will be forwarded. Other frames will be dropped.

Note: This command is available for devices of the RS20/RS30/RS40, MS20/MS30, MACH102, RSR20/RSR30, MACH1020/MACH1030 and OCTOPUS family.

■ no vlan acceptframe

This command sets the frame acceptance mode per interface to `Admit All`. For `Admit All` mode, untagged frames or priority frames received on this interface are accepted and assigned the value of the interface VLAN ID for this port. With either option, VLAN tagged frames are forwarded in accordance with the IEEE 802.1Q VLAN Specification.

Format

```
no vlan acceptframe
```

Mode

```
Interface Config
```

4.6.77 vlan database

This command switches into the global VLAN mode.

Default

```
Admit All
```

Format

```
vlan database
```

Mode

```
Privileged EXEC
```

4.6.78 vlan ingressfilter

This command enables ingress filtering. If ingress filtering is disabled, frames received with VLAN IDs that do not match the VLAN membership of the receiving interface are admitted and forwarded to ports that are members of that VLAN.

Default

disabled

Format

vlan ingressfilter

Mode

Interface Config

■ no vlan ingressfilter

This command disables ingress filtering. If ingress filtering is disabled, frames received with VLAN IDs that do not match the VLAN membership of the receiving interface are admitted and forwarded to ports that are members of that VLAN.

Format

no vlan ingressfilter

Mode

Interface Config

4.6.79 vlan name

This command changes the name of a VLAN. The name is an alphanumeric string of up to 32 characters, and the ID is a valid VLAN identification number. ID range is 1-4042.

Default

The name for VLAN ID 1 is always Default. The name for other VLANs is defaulted to a blank string.

Format

```
vlan name <1-4042> <newname>
```

Mode

VLAN database

■ no vlan name

This command sets the name of a VLAN to a blank string. The VLAN ID is a valid VLAN identification number. ID range is 1-4042.

Format

```
no vlan name <1-4042>
```

Mode

VLAN database

4.6.80 vlan participation

This command configures the degree of participation for a specific interface in a VLAN. The ID is a valid VLAN identification number, and the interface is a valid interface number.

Format

```
vlan participation  
    <exclude | include | auto> <1-4042>
```

Mode

```
Interface Config
```

Participation options are:

include

The interface is always a member of this VLAN. This is equivalent to registration fixed.

exclude

The interface is never a member of this VLAN. This is equivalent to registration forbidden.

auto

The interface is dynamically registered in this VLAN by GVRP. The interface will not participate in this VLAN unless a join request is received on this interface. This is equivalent to registration normal.

4.6.81 vlan participation all

This command configures the degree of participation for all interfaces in a VLAN. The ID is a valid VLAN identification number.

Format

```
vlan participation all <exclude | include | auto>  
<1-4042>
```

Mode

Global Config

Participation options are:

include

The interface is always a member of this VLAN. This is equivalent to registration fixed.

exclude

The interface is never a member of this VLAN. This is equivalent to registration forbidden.

auto

The interface is dynamically registered in this VLAN by GVRP. The interface will not participate in this VLAN unless a join request is received on this interface. This is equivalent to registration normal.

4.6.82 vlan port acceptframe all

This command sets the frame acceptance mode for all interfaces. For VLAN Only mode, untagged frames or priority frames received on this interface are discarded. For Admit All mode, untagged frames or priority frames received on this interface are accepted and assigned the value of the interface VLAN ID for this port. With either option, VLAN tagged frames are forwarded in accordance with the IEEE 802.1Q VLAN Specification.

Default

```
Admit All
```

Format

```
vlan port acceptframe all <vlanonly | all>
```

Mode

```
Global Config
```

■ no vlan port acceptframe all

This command sets the frame acceptance mode for all interfaces to `Admit All`. For Admit All mode, untagged frames or priority frames received on this interface are accepted and assigned the value of the interface VLAN ID for this port. With either option, VLAN tagged frames are forwarded in accordance with the IEEE 802.1Q VLAN Specification.

Format

```
no vlan port acceptframe all
```

Mode

```
Global Config
```

4.6.83 **vlan port ingressfilter all**

This command enables ingress filtering for all ports. If ingress filtering is disabled, frames received with VLAN IDs that do not match the VLAN membership of the receiving interface are admitted and forwarded to ports that are members of that VLAN.

Default

disabled

Format

```
vlan port ingressfilter all
```

Mode

Global Config

■ **no vlan port ingressfilter all**

This command disables ingress filtering for all ports. If ingress filtering is disabled, frames received with VLAN IDs that do not match the VLAN membership of the receiving interface are admitted and forwarded to ports that are members of that VLAN.

Format

```
no vlan port ingressfilter all
```

Mode

Global Config

4.6.84 **vlan port pvid all**

This command changes the VLAN ID for all interface.

Default

1

Format

```
vlan port pvid all <1-4042>
```

Mode

Global Config

■ no vlan port pvid all

This command sets the VLAN ID for all interfaces to 1.

Format

```
no vlan port pvid all <1-4042>
```

Mode

Global Config

4.6.85 vlan port tagging all

This command configures the tagging behavior for all interfaces in a VLAN to enabled. If tagging is enabled, traffic is transmitted as tagged frames. If tagging is disabled, traffic is transmitted as untagged frames. The ID is a valid VLAN identification number.

Format

```
vlan port tagging all <1-4042>
```

Mode

```
Global Config
```

■ no vlan port tagging all

This command configures the tagging behavior for all interfaces in a VLAN to disabled. If tagging is disabled, traffic is transmitted as untagged frames. The ID is a valid VLAN identification number.

Format

```
no vlan port tagging all <1-4042>
```

Mode

```
Global Config
```

4.6.86 vlan pvid

This command changes the VLAN ID per interface.

Default

1

Format

```
vlan pvid <1-4042>
```

Mode

Interface Config

■ no vlan pvid

This command sets the VLAN ID per interface to 1.

Format

```
no vlan pvid <1-4042>
```

Mode

Interface Config

4.6.87 vlan tagging

This command configures the tagging behavior for a specific interface in a VLAN to enabled. If tagging is enabled, traffic is transmitted as tagged frames. If tagging is disabled, traffic is transmitted as untagged frames. The ID is a valid VLAN identification number.

Format

```
vlan tagging <1-4042>
```

Mode

```
Interface Config
```

■ no vlan tagging

This command configures the tagging behavior for a specific interface in a VLAN to disabled. If tagging is disabled, traffic is transmitted as untagged frames. The ID is a valid VLAN identification number.

Format

```
no vlan tagging <1-4042>
```

Mode

```
Interface Config
```

4.7 User Account Management Commands

These commands manage user accounts.

4.7.1 disconnect

This command closes a telnet session.

Format

```
disconnect {<sessionID> | all}
```

Mode

```
Privileged EXEC
```

Session ID

Enter the session ID (1-11).

4.7.2 show loginsession

This command displays current telnet and serial port connections to the switch.

Format

```
show loginsession
```

Mode

Privileged EXEC and User EXEC

ID

Login Session ID

User Name

The name the user will use to login using the serial port or Telnet. A new user may be added to the switch by entering a name in a blank entry. The user name may be up to 8 characters, and is not case sensitive. Two users are included as the factory default, 'admin' and 'user'.

Connection From

IP address of the telnet client machine or EIA-232 for the serial port connection.

Idle Time

Time this session has been idle.

Session Time

Total time this session has been connected.

4.7.3 show users

This command displays the configured user names and their settings. This command is only available for users with readwrite privileges. The SNMPv3 fields will only be displayed if SNMP is available on the system.

Format

```
show users
```

Mode

Privileged EXEC

User Name

The name the user will use to login using the serial port, Telnet or Web. A new user may be added to the switch by entering a name in a blank entry. The user name may be up to eight characters, and is not case sensitive. Two users are included as the factory default, 'admin' and 'user'

Access Mode

Shows whether the operator is able to change parameters on the switch (Read/Write) or is only able to view them (Read Only). As a factory default, the 'admin' user has Read/Write access and the 'user' has Read Only access. There can only be one Read/Write user and up to five Read Only users.

SNMPv3 AccessMode

This field displays the SNMPv3 Access Mode. If the value is set to ReadWrite, the SNMPv3 user will be able to set and retrieve parameters on the system. If the value is set to ReadOnly, the SNMPv3 user will only be able to retrieve parameter information. The SNMPv3 access mode may be different than the CLI and Web access mode.

SNMPv3 Authentication

This field displays the authentication protocol to be used for the specified login user.

SNMPv3 Encryption

This field displays the encryption protocol to be used for the specified login user.

4.7.4 users defaultlogin

This command assigns the authentication login list to use for non-configured users when attempting to log in to the system. This setting is overridden by the authentication login list assigned to a specific user if the user is configured locally. If this value is not configured, users will be authenticated using local authentication only.

Format

```
users defaultlogin <listname>
```

Mode

```
Global Config
```

listname

Enter an alphanumeric string of not more than 15 characters.

4.7.5 users login <user>

Enter user name.

Format

```
users login <user> <listname>
```

Mode

```
Global Config
```

■ no users login <user>

This command removes an operator.

Format

```
no users login <user> <listname>
```

Mode

```
Global Config
```

Note:

The 'admin' user account cannot be deleted.

4.7.6 users access

This command sets access for a user: readonly/readwrite.

Format

```
users access <username> {readonly | readwrite}
```

Mode

Global Config

<username>

Enter a name up to 32 alphanumeric characters in length.

readonly

Enter the access mode as readonly.

readwrite

Enter the access mode as readwrite.

■ no users access

This command deletes access for a user.

Format

```
no users access <username>
```

Mode

Global Config

4.7.7 users name

This command adds a new user (account) if space permits. The account <username> can be up to eight characters in length. The name may be comprised of alphanumeric characters as well as the dash ('-') and underscore ('_'). The <username> is not case-sensitive. Six user names can be defined.

Format

```
users name <username>
```

Mode

```
Global Config
```

■ no users name

This command removes an operator.

Format

```
no users name <username>
```

Mode

```
Global Config
```

Note:

The 'admin' user account cannot be deleted.

4.7.8 users passwd

This command is used to change a password. The password should not be more than eight alphanumeric characters in length. If a user is authorized for authentication or encryption is enabled, the password must be at least eight alphanumeric characters in length. The username and password are case-sensitive. When a password is changed, a prompt will ask for the former password. If none, press enter.

Note: Make sure, that the passwords of the users differ from each other. If two or more users try to choose the same password, the CLI will display an error message.

Default

No Password

Format

```
users passwd <username> {<password>}
```

Mode

Global Config

■ no users passwd

This command sets the password of an existing operator to blank. When a password is changed, a prompt will ask for the operator's former password. If none, press enter.

Format

```
no users passwd <username> {<password>}
```

Mode

Global Config

4.7.9 users snmpv3 accessmode

This command specifies the snmpv3 access privileges for the specified login user. The valid accessmode values are `readonly` or `readwrite`. The `<username>` is the login user name for which the specified access mode applies. The default is `readwrite` for 'admin' user; `readonly` for all other users

Default

```
admin -- readwrite; other -- readonly
```

Format

```
users snmpv3 accessmode <username> <readonly |  
readwrite>
```

Mode

```
Global Config
```

■ no users snmpv3 accessmode

This command sets the snmpv3 access privileges for the specified login user as `readwrite` for the 'admin' user; `readonly` for all other users. The `<username>` is the login user name for which the specified access mode will apply.

Format

```
no users snmpv3 accessmode <username>
```

Mode

```
Global Config
```

4.7.10 users snmpv3 authentication

This command specifies the authentication protocol to be used for the specified login user. The valid authentication protocols are `none`, `md5` or `sha`. If `md5` or `sha` are specified, the user login password is also used as the snmpv3 authentication password and therefore must be at least eight characters in length. The `<username>` is the login user name associated with the authentication protocol.

Default

```
no authentication
```

Format

```
users snmpv3 authentication <username> <none | md5  
| sha>
```

Mode

```
Global Config
```

■ no users snmpv3 authentication

This command sets the authentication protocol to be used for the specified login user to `none`. The `<username>` is the login user name for which the specified authentication protocol will be used.

Format

```
users snmpv3 authentication <username>
```

Mode

```
Global Config
```

4.7.11 users snmpv3 encryption

This command specifies the encryption protocol to be used for the specified login user. The valid encryption protocols are `des` or `none`.

If `des` is specified, the required key may be specified on the command line. The `key` may be up to 16 characters long. If the `des` protocol is specified but a key is not provided, the user will be prompted for the key. When using the `des` protocol, the user login password is also used as the `snmpv3` encryption password and therefore must be at least eight characters in length.

If `none` is specified, a key must not be provided. The `<username>` is the login user name associated with the specified encryption.

Default

```
no encryption
```

Format

```
users snmpv3 encryption <username> <none |  
des[key]>
```

Mode

```
Global Config
```

■ no users snmpv3 encryption

This command sets the encryption protocol to `none`. The `<username>` is the login user name for which the specified encryption protocol will be used.

Format

```
no users snmpv3 encryption <username>
```

Mode

```
Global Config
```

4.8 System Utilities

This section describes system utilities.

4.8.1 address-conflict

This command configures the setting for detection possible address conflicts of the agent's IP address with other devices' IP addresses in the network.

Format

```
address-conflict
  {detection-mode { active-only | disable |
    enable | passive-only}|
  ongoing-detection { disable | enable } }
```

Mode

Global Config

detection mode

Configure the device's address conflict detection mode (active-only, disable, enable or passive-only). Default value: `enable`.

ongoing detection

Disable or enable the ongoing address conflict detection. Default value: `enable`.

4.8.2 boot skip-aca-on-boot

Use this command to skip external memory (AutoConfiguration Adapter ACA21) during boot phase to shorten startup duration. The ACA21 functionality will be available after the boot phase.

Format

```
boot skip-aca-on-boot {disable | enable}
```

Mode

Global Config

Default

disabled

enable

Enable ACA21 skip during boot phase.

disable

Disable ACA21 skip during boot phase.

4.8.3 show boot skip-aca-on-boot

Use this command display the status of the option of skipping external memory (AutoConfiguration Adapter ACA21) during boot phase.

Format

```
show boot skip-aca-on-boot
```

Mode

Global Config

Default

disabled

Enabled

ACA21 skip during boot phase is enabled.

Disabled

ACA21 skip during boot phase is disabled.

4.8.4 clear eventlog

Clear the event log. The CLI will ask for confirmation.

Answer `y` (yes) or `n` (no).

The CLI displays the end of this operation.

Format

```
clear eventlog
```

Mode

Privileged EXEC

4.8.5 traceroute

This command is used to discover the routes that packets actually take when traveling to their destination through the network on a hop-by-hop basis.

`<ipaddr>` should be a valid IP address.

The optional port parameter is the UDP port used as the destination of packets sent as part of the traceroute. This port should be an unused port on the destination system. `[port]` should be a valid decimal integer in the range of 0 (zero) to 65,535. The default value is 33434.

Format

```
traceroute <ipaddr> [port]
```

Mode

Privileged EXEC

4.8.6 clear arp-table-switch

This command clears the agent's ARP table (cache).

Format

```
clear arp-table-switch
```

Mode

Privileged EXEC

4.8.7 clear config

This command resets the configuration in RAM to the factory defaults without powering off the switch.

Format

```
clear config
```

Mode

Privileged EXEC

4.8.8 clear config factory

This command resets the whole configuration to the factory defaults. Configuration data and scripts stored in nonvolatile memory will also be deleted.

Format

```
clear config factory
```

Mode

Privileged EXEC

4.8.9 clear counters

This command clears the stats for a specified <slot/port> or for all the ports or for the entire switch based upon the argument.

Format

```
clear counters {<slot/port> | all}
```

Mode

Privileged EXEC

4.8.10 clear hiper-ring

This command clears the HIPER Ring configuration (deletes it).

Format

```
clear hiper-ring
```

Mode

Privileged EXEC

4.8.11 clear igmpsnooping

This command clears the tables managed by the IGMP Snooping function and will attempt to delete these entries from the Multicast Forwarding Database.

Format

```
clear igmpsnooping
```

Mode

Privileged EXEC

4.8.12 clear mac-addr-table

This command clears the switch's MAC address table (the forwarding database that contains the learned MAC addresses).

Note: this command does not affect the MAC filtering table.

Format

```
clear mac-addr-table
```

Mode

Privileged EXEC

4.8.13 clear pass

This command resets all user passwords to the factory defaults without powering off the switch. You are prompted to confirm that the password reset should proceed.

Format

```
clear pass
```

Mode

Privileged EXEC

4.8.14 clear signal-contact

This command clears the signal-contact output configuration.

Switches the signal contact 1's mode to `auto` and its manual setting to `open`.

Switches the signal contact 2's mode to `manual` and its manual setting to `closed`.

Enables the monitoring of the power supplies for signal contact 1 only.

Disables the sending of signal contact traps.

Format

```
clear signal-contact
```

Mode

```
Privileged EXEC
```

4.8.15 clear traplog

This command clears the trap log.

Format

```
clear traplog
```

Mode

```
Privileged EXEC
```

4.8.16 clear ring-coupling

This command clears the ring-coupling configuration.

Format

```
clear ring-coupling
```

Mode

Privileged EXEC

4.8.17 clear vlan

This command resets VLAN configuration parameters to the factory defaults.

Format

```
clear vlan
```

Mode

Privileged EXEC

4.8.18 config-watchdog

If the function is enabled and the connection to the switch is interrupted for longer than the time specified in “timeout [s]”, the switch then loads the last configuration saved.

Format

```
config-watchdog {admin-state {disable|enable}|  
timeout <10..600>}
```

Mode

Global Config

admin-state

Enable or disable the Auto Configuration Undo feature
Default value: disabled.

timeout

Configure the Auto Configuration Undo timeout (unit: seconds).

4.8.19 copy

This command uploads and downloads to/from the switch. Remote URLs can be specified using tftp.

`copy` (without parameters) displays a brief explanation of the most important `copy` commands. A list of valid commands is provided below.

The command can be used to save the running configuration to nvram by specifying the source as `system:running-config` and the destination as `nvram:startup-config`.

Default

none

Format

```
copy  
copy nvram:clibanner <url>  
copy nvram:capture aca:capture  
copy nvram:capture <url>  
copy nvram:capturefilter <sourcefilename>
```

```
aca:capturefilter <targetfilename>
copy nvram:capturefilter <sourcefilename>
copy nvram:errorlog <url>
copy nvram:startup-config <url>
copy nvram:startup-config system:running-config
copy nvram:traplog <url>
copy system:running-config nvram:startup-config
<url>
copy system:running-config <url>
copy tftp://<server_ip>/<path_to_pem>
    nvram:httpscert
copy <url> nvram:clibanner
copy <url> nvram:capturefilter <destfilename>
copy aca:capturefilter <sourcefilename>
    nvram:capturefilter <destfilename>
copy <url> nvram:startup-config
copy <url> system:image
copy <url> system:running-config
copy <url> system:bootcode
```

Mode

Privileged EXEC

■ **copy tftp://<server_ip>/<path_to_pem> nvram:httpscert**

Use this command for uploading a PEM certificate for HTTPS over TFTP

Note: Reboot the device or re-enable the HTTPS server after uploading a PEM certificate.

■ **copy nvram:clibanner <url>**

Downloads the CLI banner file via TFTP using <tftp://ip/filepath/fileName>.

■ copy nvram:capture aca:capture

Save the internal packet capture file to the Auto Configuration Adapter ACA21 (file name: "capture.cap").

■ copy nvram:capture <url>

Save the internal packet capture file to a tftp URL using <tftp://ip/filepath/fileName>.

**■ copy nvram:capturefilter <sourcefilename>
aca:capturefilter <targetfilename>**

Save a capture filter file from the flash memory to the Auto Configuration Adapter.

– sourcefilename: Filename of source capture filter expressions file.

– targetfilename: Filename of target capture filter expressions file.

■ copy nvram:capturefilter <sourcefilename> <url>

Save the internal packet capture filter file from the flash memory to a tftp URL using <tftp://ip/filepath/fileName>.

– sourcefilename: Filename of source capture filter expressions file.

■ copy nvram:errorlog <url>

Uploads Errorlog file.

– <url>: Uploads Error log file using <tftp://ip/filepath/fileName>.

■ copy nvram:startup-config <url>

Uploads config file using <tftp://ip/filepath/fileName>.

- **copy nvram:startup-config system:running-config**
Uploads/Copies config file. The target is the currently running configuration.

- **copy nvram:traplog <url>**
Uploads Trap log file. Uploads Trap log file using <tftp://ip/filepath/fileName>.

- **copy system:running-config nvram:startup-config**
Copies system config file. Save the running configuration to NVRAM.

- **copy system:running-config <url>**
Copies system config file. Uploads system running-config via tftp using <tftp://ip/filepath/fileName>.

■ `copy <url> nvram:clibanner`

This feature provides a privileged user the capability to change the CLI default banner:

```
-----
Copyright (c) 2004-2015 <Company Name>
```

```
    All rights reserved
```

```
    <Product Name> Release L3P-09.0.00
```

```
    (Build date 2015-02-02 02:02)
```

```
    System Name:    <Product Name>
```

```
    Mgmt-IP       :    a.b.c.d
```

```
    1.Router-IP   :    0.0.0.0
```

```
    Base-MAC      :    aa:bb:cc:dd:ee:ff
```

```
    System Time:  2015-02-02 15:15:15
-----
```

The command uploads the CLI banner file by tftp using `<tftp://ip/filepath/fileName>`.

After the upload you logout from CLI and the new CLI banner file will be displayed at the next login.

– `url`: Upload CLI banner file using `<tftp://ip/filepath/fileName>`.

If no cli banner file is defined, the default cli banner is displayed (see above).

Note: Note that the CLI banner file you created has the following properties:

- Use ASCII format (character codes 0x20 .. 0x7F, \n and \t as C-like sequences)
- Do not use regular expressions
- Do not exceed the limit of 2048 byte
- Do not exceed the limit of 20 lines
- Do not exceed the limit of 80 characters per line
- A device can only have one banner file at the moment
- Save the CLI banner file as *.bnr.

Note: Alternatively, use the following command to define the text for the CLI login banner. This banner replaces the banner before login.

```
set clibanner text <Max. 2048 characters>
```

See “set clibanner” on page 253

■ **no clibanner**

This command deletes an existing CLI banner file.

■ **copy <url> nvram:capturefilter <destfilename>**

Load a Capture Filter file from a tftp URL into the flash memory using <tftp://ip/filepath/fileName>.

– **destfilename:** Destination filename of capture filter expressions file.

■ **copy aca:capturefilter <sourcefilename> nvram:capturefilter <targetfilename>**

Load a capture filter file from AutoConfiguration Adapter ACA21 into the flash memory.

– **sourcefilename:** Filename of source capture filter expressions file.

– **targetfilename:** Specify the file name on the switch's NVRAM.

■ **copy <url> nvram:startup-config**

Downloads Config file by tftp using <tftp://ip/filepath/fileName>.

■ **copy <url> system:image**

Downloads code file by tftp using <tftp://ip/filepath/fileName>.

■ copy <url> system:running-config

Downloads Code/Config file using <tftp://ip/filepath/fileName>. The target is the currently running configuration.

■ copy <url> system:bootcode

Use the "copy <url> system:bootcode" command to load the bootcode file via tftp into the device. For <url> enter the path of the tftp server using the following notation: "<tftp://ip/filepath/fileName>", e.g. "tftp://10.1.112.214/switch/switch01.cfg".

4.8.20 device-status connection-error

This command configures the device status link error monitoring for this port.

Default

ignore

Format

device-status connection-error {ignore|propagate}

Mode

Interface Config

4.8.21 device-status monitor

This command configures the device-status.

Format

```
device-status monitor
  {aca-removal | all | connection-error |
  hiper-ring |
  module-removal | power-supply-1 |
  power-supply-2 | power-supply-3-1 |
  power-supply-3-2 | power-supply-4-1 |
  power-supply-4-2 | ring-coupling | temperature }
  {error|ignore}
device-status trap {disable|enable}
```

Mode

Global Config

monitor

Determines the monitoring of the selected event or all events.

- `error` If the given event signals an error, the device state will also signal `error`,
- `ignore` Ignore the given event - even if it signals an error, the device state will not signal 'error' because of that.

trap

Configure if a trap is sent when the device status changes its state.

- `enable` enables sending traps,
- `disable` disables sending traps.

4.8.22 logout

This command closes the current telnet connection or resets the current serial connection.

Note: Save configuration changes before logging out.

Format

```
logout
```

Mode

```
Privileged EXEC
```

4.8.23 mac-address conflict operation

Use this command to enable sending a trap if the device detects a packet with its own MAC address in the network.

Possible values: `enabled`, `disabled`

Default value: `enabled`

Format

```
mac-address-conflict operation
```

Mode

```
Privileged EXEC
```

■ no mac-address conflict operation

Use this command to disable sending a trap if the device detects a packet with its own MAC address in the network.

Format

```
no mac-address conflict operation
```

Mode

```
Privileged EXEC
```

4.8.24 ping

This command checks if another computer is on the network and listens for connections. To use this command, configure the switch for network (in-band) connection. The source and target devices must have the ping utility enabled and running on top of TCP/IP. The switch can be pinged from any IP workstation with which the switch is connected through the default VLAN (VLAN 1), as long as there is a physical path between the switch and the workstation. The terminal interface sends, three pings to the target station.

Format

```
ping <ipaddr>
```

Mode

Privileged EXEC and User EXEC

4.8.25 signal-contact connection-error

This command configures the signal contact link error monitoring for this port.

Format

```
signal-contact connection-error {disable|enable}
```

Mode

Interface Config

disable

A link down event on this port will be not monitored by a signal contact (default).

enable

A link down event on this port will be monitored by a signal contact.

4.8.26 signal-contact

This command configures the signal contacts.

Format

```
signal-contact {1|2|all}
  {mode {auto|device-status|manual}
  |monitor {aca-removal|
    all|
    connection-error|hiper-ring|module-removal
    |power-supply-1| power-supply-2
    |power-supply-3-1|power-supply-3-2
    |power-supply-4-1|power-supply-4-2
    |ring-coupling|temperature} {disable|enable}
  |state {closed|open}
  |trap {disable|enable} }
```

Mode

Global Config

Contact No.

Selection of the signal contact:

- 1 signal contact 1,
- 2 signal contact 2,
- all signal contact 1 and signal contact 2.

mode

Selection of the operational mode:

- auto function monitoring,
- device-status the device-status determines the signal contact's status.
- manual manually setting the signal contact.

monitor

Enables or disables the monitoring of the selected event or all events.

- enable monitoring,
- disable no monitoring.

state

Set the manual setting of the signal contact:

- closed,
- open.

Only takes immediate effect in manual mode.

trap

Configures the sending of traps concerning the signal contact.

- `enable` enables sending traps,
- `disable` disables sending traps.

4.8.27 temperature

Note: The command is available for RS20/RS30/RS40, MS20/MS30, RSR20/RSR30, MACH100, MACH1000, PowerMICE, MACH4000 and OCTOPUS devices.

This command configures the lower and upper temperature limit for the device. If these limits are exceeded, a trap is sent. The unit for the temperature limit is °C (Celsius), the minimum value is -99, the maximum value is 99. The default for the lower limit is 0, for the upper limit, it is 70.

Note: To give the temperature in Fahrenheit, use the suffix `f`.

Format

```
temperature {lower-limit|upper-limit} <temperature value> [c|f]
```

Mode

Global Config

lower-limit

Configure the lower temperature limit.

upper-limit

Configure the upper temperature limit.

4.8.28 reboot

This command resets the switch (cold start) after a given time delay, for warm start. See [“reload” on page 251](#). Reset means that all network connections are terminated and the boot code executes. The switch uses the stored configuration to initialize the switch. You are prompted to confirm that the reset should proceed. A successful reset is indicated by the LEDs on the switch.

Format

```
reboot {delay <seconds>}
```

Mode

Privileged EXEC

<seconds>

The number of seconds after which the switch will reboot.

Value range: None (no reboot scheduled), 0 . . 2147483 sec
(= 596 h + 31 min + 23 sec).

■ clear reboot

This command cancels a scheduled reboot.

4.8.29 show reboot

This command displays if a reboot is scheduled for the device. If scheduled, the command displays the number of seconds after which the switch will reboot.

Format

```
show reboot
```

Modes

Privileged EXEC

User Exec

<seconds>

The number of seconds after which the switch will reboot.

Value range: None (no reboot scheduled), 0 . . 2147483 sec
(= 596 h + 31 min + 23 sec).

4.8.30 reload

This command enables you to reset the switch (warm start) after a given time delay, for cold start [See “reboot” on page 249](#).

Note: First, the device is checking the software in the flash memory and then it resets. If a warm start is not possible, the device automatically executes a cold start.

Reset means that all network connections are terminated and the boot code executes. The switch uses the stored configuration to initialize the switch. You are prompted to confirm that the reset should proceed. A successful reset is indicated by the LEDs on the switch.

Format

```
reload {delay <seconds>}
```

Mode

```
Privileged EXEC
```

<seconds>

The number of seconds after which the switch will reload.

Value range: 0..2147483 sec.

■ clear reload

This command cancels a scheduled reload.

4.8.31 show reload

This command displays if a reload is scheduled for the device. If scheduled, the command displays the number of seconds after which the switch will reload.

Format

```
show reload
```

Modes

```
Privileged EXEC
```

```
User Exec
```

<seconds>

The number of seconds after which the switch will reload.

Possible values: None (no reload scheduled), 0 . . 2147483 sec.

4.8.32 set clibanner

Use this command to set the preferences for the CLI login banner. Enable or disable the CLI login banner and define the text for the login banner. This banner replaces the CLI banner before login.

Format

```
set clibanner {operation |
                text <Max. 2048 characters>}
```

Modes

Privileged EXEC

operation

Enable the CLI login banner.

text

Define the text for the CLI login banner.

Possible values: Max. 2048 characters in the range ASCII code 0x20 (space character, " ") to ASCII code 0x7E (tilde, "~"), except ASCII code 0x25 (percent sign, "%").

Use `\\n`: for new line and `\\t` for horizontal tabulator.

Enter the text with quotes, e.g.

```
"This is a login banner text."
```

Example:

```
*****
*
*   Site:          <Name of the location>
*   Equipment:    <Device name>
*
*   Unauthorized access will be prosecuted.
*
*****
```

■ **no set clibanner operation**

Use this command to disable the CLI login banner.

Format

```
no set clibanner operation
```

Mode

Privileged EXEC

4.8.33 set pre-login-banner

Use this command to set the preferences for the CLI pre-login banner. Enable or disable the CLI pre-login banner and define the text for the pre-login banner.

The device displays this banner additionally before login in CLI and Graphical User Interface.

Format

```
set pre-login-banner { operation |
                        text <max. 255 characters> }
```

Modes

Privileged EXEC

operation

Enable the CLI login banner.

text

Define the text for the CLI pre-login banner.

Default: Empty string

Possible values: Max. 255 characters in the range ASCII code 0x20 (space character, " ") to ASCII code 0x7E (tilde, "~"), except ASCII code 0x25 (percent sign, "%").

Use `\\n`: for new line and `\\t` for horizontal tabulator.

Enter the text within quotes, e.g.

```
"This is a pre-login banner text."
```

Example:

```
*****
*
*      Site:      Name of the location      *
*      Equipment: Device name              *
*
*      Unauthorized access will be prosecuted. *
*
*****
```

■ **no set pre-login-banner operation**

Use this command to disable the CLI pre-login banner.

Format

```
no set pre-login-banner operation
```

Mode

Privileged EXEC

4.9 LLDP - Link Layer Discovery Protocol

These commands show and configure the LLDP parameters in compliance with IEEE 802.1 AB.

4.9.1 show lldp

This command shows all LLDP settings.

Format

```
show lldp
```

Mode

```
Privileged EXEC and User EXEC
```

4.9.2 show lldp config

This command shows all LLDP configuration settings.

Format

```
show lldp config
```

Mode

```
Privileged EXEC and User EXEC
```

4.9.3 show lldp config chassis

This command shows all LLDP configuration settings concerning the entire device.

Format

```
show lldp config chassis
```

Mode

Privileged EXEC and User EXEC

4.9.4 show lldp config chassis admin-state

Display the LLDP/IEEE802.1AB functionality on this device. If disabled, the LLDP protocol is inactive but the LLDP MIBs can still be accessed.

Format

```
show lldp config chassis admin-state
```

Mode

Privileged EXEC and User EXEC

4.9.5 show lldp config chassis notification-interval

Display the LLDP minimum notification trap interval (unit: seconds).

Format

```
show lldp config chassis notification-interval
```

Mode

Privileged EXEC and User EXEC

4.9.6 **show lldp config chassis re-init-delay**

Display the LLDP configuration's chassis re-initialization delay (unit: seconds).

Format

```
show lldp config chassis re-init-delay
```

Mode

```
Privileged EXEC and User EXEC
```

4.9.7 **show lldp config chassis tx-delay**

Display the LLDP transmit delay (unit: seconds). It indicates the delay between successive LLDP frame transmissions.

Format

```
show lldp config chassis tx-delay
```

Mode

```
Privileged EXEC and User EXEC
```

4.9.8 **show lldp config chassis tx-hold-mult**

Display the LLDP transmit hold multiplier, a time-to-live value expressed as a multiple of the LLDP Message Tx Interval (tx-interval).

Format

```
show lldp config chassis tx-hold-mult
```

Mode

```
Privileged EXEC and User EXEC
```

4.9.9 show lldp config chassis tx-interval

Display the interval (unit: seconds) at which LLDP frames are transmitted on behalf of this LLDP agent.

Format

```
show lldp config chassis tx-interval
```

Mode

Privileged EXEC and User EXEC

4.9.10 show lldp config port

This command shows all LLDP configuration settings and states concerning one or all ports.

Format

```
show lldp config port <{slot/port|all}>  
  admin-state | fdb-mode | hm-mode |  
  max-neighbors | notification | tlv
```

Mode

Privileged EXEC and User EXEC

admin-state

Display the port's LLDP admin state (if LLDP/IEEE802.1AB frames will be transmitted and/or received).

fdb-mode

Display the port's LLDP FDB mode.

hm-mode

Display the port's LLDP Hirschmann mode.

.max-neighbors

Display the port's max. no. of LLDP neighbors.

notification

Display the port's LLDP notification (trap) setting.

tlv

Display the port's LLDP TLV settings (they determine which information is included in the LLDP frames that are sent). The command is a group command and will output several lines of data.

4.9.11 show lldp config port tlv

This command shows all LLDP TLV configuration settings (if the given information is included in the sent LLDP frames or not) concerning one or all ports.

Format

```
show lldp config port <{slot/port|all}> tlv
```

Mode

Privileged EXEC and User EXEC

link-aggregation

Display the port's LLDP TLV inclusion of Link Aggregation.

mac-phy-config-state

Display the port's LLDP TLV inclusion of MAC Phy. Cfg. State.

max-frame-size

Display the port's LLDP TLV inclusion of Max. Frame Size.

PROFINET IO Status

Display the port's LLDP TLV inclusion of PROFINET IO Status.

PROFINET IO Alias

Display the port's LLDP TLV inclusion of PROFINET IO Alias.

PROFINET IO MRP

Display the port's LLDP TLV inclusion of PROFINET IO MRP.

mgmt-addr

Display the port's LLDP TLV inclusion of Management Address.

port-desc

Display the port's LLDP TLV inclusion of Port Description.

port-vlan

Display the port's LLDP TLV inclusion of Port VLAN.

protocol

Display the port's LLDP TLV inclusion of Protocol.

sys-cap

Display the port's LLDP TLV inclusion of System Capabilities.

sys-desc

Display the port's LLDP TLV inclusion of System Description.

sys-name

Display the port's LLDP TLV inclusion of System Name.

vlan-name

Display the port's LLDP TLV inclusion of VLAN Name.

4.9.12 show lldp remote-data

This command shows all LLDP remote-data settings and states concerning one or all ports.

Format

```
show lldp remote-data <{slot/port|all}>
  chassis-id | detailed | ether-port-info |
  inlinpower | link-aggregation-info |
  mgmt-addr | profinetio-port-info |
  port-desc | port-id | summary | sys-desc |
  sys-name | vlan-info
```

Mode

Privileged EXEC and User EXEC

chassis-id

Display the remote data's chassis ID only.

detailed

Display remote data in detailed format (i. e., all available data).

Note: most important data is output first (not in alphabetic order of command names). This is the default command if no specific command is given.

ether-port-info

Display the remote data's port Ethernet properties only (group command, outputs: Port Autoneg. Supported, Port Autoneg. Enabled,

Port Autoneg. Advertized Capabilities and Port Operational MAU Type).

inlinepower

Displays the remote port's Power over Ethernet capabilities (PoE, IEEE 802.3af). Included are if the remote device is a PSE (Power Source Device) or a PD (Powered Device), if PoE is supported and if the power pairs are selectable.

link-aggregation-info

Display the remote data's link aggregation information only (group command, outputs: Link Agg. Status and Link Agg. Port ID).

mgmt-addr

Display the remote data's management address only.

profinetio-port-info

Display the remote data's Port ProfinetIO properties only.

port-desc

Display the port's LLDP TLV inclusion of Port Description.

port-id

Display the remote data's port ID only.

summary

Display remote data in summary format (table with most important data only, strings will be truncated if necessary, indicated by an appended '>' character).

sys-desc

Display the remote data's system description only.

sys-name

Display the remote data's system name only.

vlan-info

Display the remote data's VLAN information only (group command, outputs: Port VLAN ID, Membership VLAN IDs and their respective names).

4.9.13 lldp

Enable/disable the LLDP/IEEE802.1AB functionality on this device. If disabled, the LLDP protocol will become inactive, but the LLDP MIBs can still be accessed. This command is a shorthand notation for `lldp config chassis admin-state {off|on}` (see [“lldp config chassis admin-state” on page 266](#)).

The default setting is `on`.

Format

```
lldp
```

Mode

```
Global Config
```

■ no lldp

Disable the LLDP/IEEE802.1AB functionality on this device.

Format

```
no lldp
```

Mode

```
Global Config
```

4.9.14 lldp config chassis admin-state

Configure the LLDP/IEEE802.1AB functionality on this device. If disabled, the LLDP protocol will become inactive, but the LLDP MIBs can still be accessed.

- ▶ `off`: Disable the LLDP/IEEE802.1AB functionality.
- ▶ `on`: Enable the LLDP/IEEE802.1AB functionality.

The default setting is `on`.

Format

```
lldp config chassis admin-state {off|on}
```

Mode

Global Config

4.9.15 lldp config chassis notification-interval

Configure the LLDP minimum notification interval (the minimum time after a notification trap has been sent until a new trap can be sent, unit: seconds, min.: 5 sec., max.: 3600 sec., Default value: 5 sec.).

Format

```
lldp config chassis notification-interval  
<notification interval>
```

Mode

Global Config

Notification interval

Configure the LLDP minimum notification interval (the minimum time after a notification trap has been sent until a new trap can be sent, unit: seconds, min.: 5 sec., max.: 3600 sec., Default value: 5 sec.).

4.9.16 lldp config chassis re-init-delay

Configure the LLDP re-initialization delay (unit: seconds, min.: 1 sec., max.: 10 sec., Default value: 2 sec.).

Format

```
lldp config chassis re-init-delay <re-init delay>
```

Mode

```
Global Config
```

Re-init-delay

Configure the LLDP re-initialization delay (unit: seconds, min.: 1 sec., max.: 10 sec., Default value: 2 sec.).

4.9.17 lldp config chassis tx-delay

Configure the LLDP transmit delay, the delay between successive LLDP frame transmissions (unit: seconds, min.: 1 sec., max.: 8192 sec., Default value: 2 sec.).

Format

```
lldp config chassis tx-delay <tx delay>
```

Mode

```
Global Config
```

Tx-delay

Configure the LLDP transmit delay, the delay between successive LLDP frame transmissions (unit: seconds, min.: 1 sec., max.: 8192 sec., Default value: 2 sec.).

4.9.18 **lldp config chassis tx-hold-mult**

Configure the LLDP transmit hold multiplier, a time-to-live value expressed as a multiple of the LLDP Message Tx Interval (tx-interval), min.: 2, max.: 10, Default value: 4.

Format

```
lldp config chassis tx-hold-mult  
                                <tx hold multiplier>
```

Mode

Global Config

Tx-hold-mult

Configure the LLDP transmit hold multiplier, a time-to-live value expressed as a multiple of the LLDP Message Tx Interval (tx-interval), min.: 2, max.: 10, Default value: 4.

4.9.19 **lldp chassis tx-interval**

Configure the interval at which LLDP frames are transmitted on behalf of this LLDP agent (unit: seconds, min.: 5 sec., max.: 32768 sec., Default value: 30 sec.)

Format

```
lldp chassis tx-interval <tx interval>
```

Mode

Global Config

Tx-interval

Configure the interval at which LLDP frames are transmitted on behalf of this LLDP agent (unit: seconds, min.: 5 sec., max.: 32768 sec., Default value: 30 sec.).

4.9.20 clear lldp config all

Clear the LLDP configuration, i. e., set all configurable parameters to default values (all chassis- as well as port-specific parameters at once).

Note: LLDP Remote data remains unaffected.

Format

```
clear lldp config all
```

Mode

Privileged EXEC

4.9.21 lldp admin-state

Configure the port's LLDP admin state (if LLDP/IEEE802.1AB frames will be transmitted to and/or received from the standard IEEE multicast address 01:80:c2:00:00:0e).

The default setting is tx-and-rx.

Format

```
lldp admin-state <{tx-only|rx-only|tx-and-rx|off}>
```

Mode

Interface Config

4.9.22 `lldp fdb-mode`

Configure the port's LLDP FDB mode.

The default setting is `autodetect`.

Format

```
lldp fdb-mode <{lldp-only|mac-only|lldp-and-  
mac|autodetect}>
```

Mode

Interface Config

4.9.23 `lldp hm-mode`

Configure the port's LLDP Hirschmann mode (if LLDP/IEEE802.1AB frames will be transmitted to and/or received from the Hirschmann-specific multicast address `01:80:63:2f:ff:0b`).

The default setting is `tx-and-rx`.

Format

```
lldp hm-mode <{tx-only|rx-only|tx-and-rx|off}>
```

Mode

Interface Config

4.9.24 Ildp max-neighbors

Configure the port's LLDP max. no. of neighbors (min.: 1, max.: 50, Default value: 10).

Format

```
lldp max-neighbors <1..50>
```

Mode

```
Interface Config
```

4.9.25 Ildp notification

Configure the port's LLDP notification setting (on or off, Default value: off).

Format

```
lldp notification <{off|on}>
```

Mode

```
Interface Config
```

4.9.26 Ildp tlv link-aggregation

Configure the port's LLDP TLV inclusion of Link Aggregation (on or off, default: on).

Format

```
lldp tlv link-aggregation <{off|on}>
```

Mode

```
Interface Config
```

4.9.27 **lldp tlv mac-phy-config-state**

Configure the port's LLDP TLV inclusion of MAC Phy. Cfg. State (on or off, default: on).

Format

```
lldp tlv mac-phy-config-state <{off|on}>
```

Mode

```
Interface Config
```

4.9.28 **lldp tlv max-frame-size**

Configure the port's LLDP TLV inclusion of Max. Frame Size (on or off, default: on).

Format

```
lldp tlv max-frame-size <{off|on}>
```

Mode

```
Interface Config
```

4.9.29 **lldp tlv mgmt-addr**

Configure the port's LLDP TLV inclusion of Management Address (on or off, default: on).

Format

```
lldp tlv mgmt-addr <{off|on}>
```

Mode

```
Interface Config
```

4.9.30 `lldp tlv pnio`

Configure the port's LLDP TLV inclusion of PROFINET IO Status (on or off, default: on).

Format

```
lldp tlv pnio <{off|on}>
```

Mode

```
Interface Config
```

4.9.31 `lldp tlv pnio-alias`

Configure the port's LLDP TLV inclusion of PROFINET IO Alias (on or off, default: on).

Format

```
lldp tlv pnio-alias <{off|on}>
```

Mode

```
Interface Config
```

4.9.32 `lldp tlv pnio-mrp`

Configure the port's LLDP TLV inclusion of PROFINET IO MRP (on or off, default: on).

Format

```
lldp tlv pnio-mrp <{off|on}>
```

Mode

```
Interface Config
```

4.9.33 `lldp tlv port-desc`

Configure the port's LLDP TLV inclusion of Port Description (on or off, default: on).

Format

```
lldp tlv port-desc <{off|on}>
```

Mode

Interface Config

4.9.34 `lldp tlv port-vlan`

Configure the port's LLDP TLV inclusion of Port VLAN (on or off, default: on).

Format

```
lldp tlv port-vlan <{off|on}>
```

Mode

Interface Config

4.9.35 `lldp tlv gmrp`

Configure the port's LLDP TLV inclusion of GMRP (on or off, default: on).

Format

```
lldp tlv gmrp <{off|on (on)}>
```

Mode

Interface Config

4.9.36 `lldp tlv igmp`

Configure the port's LLDP TLV inclusion of IGMP (on or off, default: on).

Format

```
lldp tlv igmp <{off|on (on)}>
```

Mode

```
Interface Config
```

4.9.37 `lldp tlv portsec`

Configure the port's LLDP TLV inclusion of PortSec (on or off, default: on).

Format

```
lldp tlv portsec <{off|on (on)}>
```

Mode

```
Interface Config
```

4.9.38 `lldp tlv ptp`

Configure the port's LLDP TLV inclusion of PTP (on or off, default: on).

Format

```
lldp tlv ptp <{off|on (on)}>
```

Mode

```
Interface Config
```

4.9.39 lldp tlv protocol

Configure the port's LLDP TLV inclusion of Protocol (on or off, default: on).

Format

```
lldp tlv protocol <{off|on (on)}>
```

Mode

```
Interface Config
```

4.9.40 lldp tlv sys-cap

Configure the port's LLDP TLV inclusion of System Capabilities (on or off, default: on).

Format

```
lldp tlv sys-cap <{off|on}>
```

Mode

```
Interface Config
```

4.9.41 lldp tlv sys-desc

Configure the port's LLDP TLV inclusion of System Description (on or off, default: on).

Format

```
lldp tlv sys-desc <{off|on}>
```

Mode

```
Interface Config
```

4.9.42 lldp tlv sys-name

Configure the port's LLDP TLV inclusion of System Name (on or off, default: on).

Format

```
lldp tlv sys-name <{off|on}>
```

Mode

```
Interface Config
```

4.9.43 lldp tlv vlan-name

Configure the port's LLDP TLV inclusion of VLAN Name.

Format

```
lldp tlv vlan-name <{off|on}>
```

Mode

```
Interface Config
```

4.9.44 name

Set or remove a descriptive name for the current interface (physical ports only).

Format

```
name <descriptive name>
```

Mode

```
Interface Config
```

<descriptive name>

Enter a descriptive name for the current interface (physical ports only). Max. length is 20 characters.

Note: If it contains blanks or exclamation marks (!), enclose it in quotation marks ("). The description itself must not contain any quotation marks (' or "), question marks (?) or backslashes (\).

■ no name

Delete the descriptive name for the current interface (physical ports only).

Format

```
no name
```

Mode

```
Interface Config
```

4.10 SNTP - Simple Network Time Protocol

These commands show and configure the SNTP parameters.

4.10.1 show sntp

This command shows all SNTP settings.

Format

```
show sntp
```

Mode

```
Privileged EXEC and User EXEC
```

SNTP Server Anycast Address

Show SNTP Server Anycast Address (a.b.c.d).

SNTP Server Anycast Transmit Interval

Show SNTP Anycast Transmit Interval (in seconds).

SNTP Server Anycast VLAN

Show SNTP Server Anycast VLAN.

SNTP Server Disable if Timesource is local

Show SNTP Server Disable if Timesource is local (Yes/No).

SNTP Client Accepts Broadcasts

Show SNTP Client Accepts Broadcasts (Yes/No).

SNTP Client Disable after Synchronization

Show SNTP Client Disable after Synchronization (Yes/No).

SNTP Client Request Interval

Show SNTP Client Request Interval (in seconds).

SNTP Client Local Time Offset

Show SNTP Client Local Time Offset (in minutes).

SNTP Client Primary Server IP Address

Show SNTP Client Primary Server IP Address (a.b.c.d).

SNTP Client Secondary Server IP Address

Show SNTP Client Secondary Server IP Address (a.b.c.d).

SNTP Client Threshold to Server Time

Show SNTP Client Threshold to Server Time (in milliseconds).

SNTP Operation Global

Show SNTP Operation Global (Disabled or Enabled).

SNTP Operation Server

Show SNTP Operation Server (Disabled or Enabled).

SNTP Operation Client

Show SNTP Operation Client (Disabled or Enabled).

SNTP Status

Show SNTP Status

SNTP Time

Show SNTP Time (yyyy-mm-dd hh:mm:ss).

SNTP System Time

Show SNTP system Time (yyyy-mm-dd hh:mm:ss).

4.10.2 show sntp anycast

This command shows all SNTP anycast configuration settings.

Format

```
show sntp anycast [address|transmit-interval|vlan]
```

Mode

Privileged EXEC and User EXEC

address

Show the SNTP server's anycast destination IP Address.

transmit-interval

Show the SNTP Server's interval for sending Anycast messages (unit: seconds).

vlan

Show the SNTP server's Anycast VLAN ID (used for sending Anycast messages).

4.10.3 show sntp client

This command shows all SNTP anycast configuration settings.

Format

```
show sntp client [accept-broadcast |  
                 disable-after-sync |  
                 offset |  
                 request-interval |  
                 server<primary|secondary> |  
                 threshold]
```

Mode

Privileged EXEC and User EXEC

accept-broadcast

Show if the SNTP Client accepts SNTP broadcasts.

disable-after-sync

Show if the SNTP client will be disabled once it is synchronized to the time server.

offset

Show the local time's offset (in minutes) with respect to UTC (positive values for locations east of Greenwich).

request-interval

Show the SNTP Client's request interval (unit: seconds).

server

Show the SNTP Client's server IP addresses.

server primary

Show the SNTP Client's primary server IP addresses.

server secondary

Show the SNTP Client's redundant server IP addresses.

server threshold

Show the SNTP Client's threshold in milliseconds.

4.10.4 show sntp operation

This command shows if the SNTP function is enabled or disabled.

Format

```
show sntp operation
```

Mode

Privileged EXEC and User EXEC

4.10.5 show sntp server

This command shows the SNTP Server's configuration parameters.

Format

```
show sntp server [disable-if-local]
```

Mode

Privileged EXEC and User EXEC

disable-if-local

Show if the server will be disabled if the time is running from the local clock and not synchronized to an external time source.

4.10.6 show sntp status

This command shows the SNTP state, synchronization and error messages.

Format

```
show sntp status
```

Mode

Privileged EXEC and User EXEC

4.10.7 show sntp time

This command shows time and date.

Format

```
show sntp time [sntp|system]
```

Mode

Privileged EXEC and User EXEC

sntp

Show the current SNTP date and UTC time.

system

Show the local system's current date and time.

4.10.8 no sntp

This command disables sntp.

Format

```
no sntp
```

Mode

Global Config

4.10.9 sntp anycast address

Set the SNTP server's anycast destination IP Address, default: 0.0.0.0 (none).

Format

```
sntp anycast address <IPAddress>
```

Mode

```
Global Config
```

■ no sntp anycast address

Set the SNTP server's anycast destination IP Address to 0.0.0.0.

Format

```
no sntp anycast address
```

Mode

```
Global Config
```

4.10.10 sntp anycast transmit-interval

The transmit interval in seconds, default: 120.

Format

```
sntp anycast transmit-interval <1-3600>
```

Mode

```
Global Config
```

4.10.11 sntp anycast vlan

Set the SNTP server's Anycast VLAN ID used for sending Anycast messages, default: 1.

Format

```
sntp anycast vlan <1-4042>
```

Mode

```
Global Config
```

4.10.12 sntp client accept-broadcast

Enable/Disable that the SNTP Client accepts SNTP broadcasts.

Format

```
sntp client accept-broadcast <on | off>
```

Mode

```
Global Config
```

■ no sntp accept-broadcast

Disable the SNTP Client accepts SNTP broadcasts.

Format

```
no sntp client accept-broadcast
```

Mode

```
Global Config
```

4.10.13 sntp client disable-after-sync

If this option is activated, the SNTP client disables itself once it is synchronized to a server.

Format

```
sntp client disable-after-sync <on | off>
```

Mode

Global Config

off

Do not disable SNTP client when it is synchronized to a time server.

on

Disable SNTP client as soon as it is synchronized to a time server.

4.10.14 sntp client offset

The offset between UTC and local time in minutes, default: 60.

Format

```
sntp client offset <-1000 to 1000>
```

Mode

Global Config

4.10.15 sntp client request-interval

The synchronization interval in seconds, default: 30.

Format

```
sntp client request-interval <1-3600>
```

Mode

```
Global Config
```

4.10.16 no sntp client server

Disable the SNTP client servers.

Format

```
no sntp client server
```

Mode

```
Global Config
```

4.10.17 sntp client server primary

Set the SNTP Client's primary server IP Address, default: 0.0.0.0 (none).

Format

```
sntp client server primary <IP-Address>
```

Mode

```
Global Config
```

■ no sntp client server primary

Disable the primary SNTP client server.

Format

```
no sntp client server primary
```

Mode

```
Global Config
```

4.10.18 sntp client server secondary

Set the SNTP Client's secondary server IP Address, default: 0.0.0.0 (none).

Format

```
sntp client server secondary <IP-Address>
```

Mode

Global Config

■ no sntp client server secondary

Disable the secondary SNTP client server.

Format

```
no sntp client server secondary
```

Mode

Global Config

4.10.19 sntp client threshold

With this option you can reduce the frequency of time alterations. Enter this threshold as a positive integer value in milliseconds. The switch obtains the server timer as soon as the deviation to the server time is above this threshold.

Format

```
sntp client threshold <milliseconds>
```

Mode

```
Global Config
```

Milliseconds

```
Enter the allowed deviation to the server time as a  
positive integer value in milliseconds.
```

■ no sntp client threshold

Disable the sntp client threshold.

Format

```
no sntp client threshold
```

Mode

```
Global Config
```

4.10.20 sntp operation

Enable/Disable the SNTP function.

Format

```
sntp operation <on | off> |  
                client { on | off } |  
                server { on | off }
```

Mode

Global Config

client

Enable or disable SNTP Client.

server

Enable or disable SNTP Server.

■ no sntp operation

Disable the SNTP Client and Server.

Format

```
no sntp operation
```

Mode

Global Config

4.10.21 sntp server disable-if-local

With this option enabled, the switch disables the SNTP Server Function if it is not synchronized to a time server itself.

Format

```
sntp server disable-if-local <on | off>
```

Mode

Global Config

off

Enable the SNTP Server even if it is not synchronized to a time server itself.

on

Disable the SNTP Server if it is not synchronized to a time server itself.

4.10.22 sntp time system

Set the current sntp time.

Format

```
sntp time system <YYYY-MM-DD HH:MM:SS>
```

Mode

Global Config

4.11 PoE - Power over Ethernet

These commands show and configure the Power over Ethernet (IEEE 802.3af) parameters.

4.11.1 show inlinepower

This command shows global PoE inline power settings.

Format

```
show inlinepower
```

Mode

```
Privileged EXEC and User EXEC
```

4.11.2 show inlinepower port

This command shows the configuration settings and states per port.

Format

```
show inlinepower port [<slot/port> | all]
```

Mode

Privileged EXEC and User EXEC

<slot/port>

Enter the interface (in <slot/port> notation).

Admin Mode

Display the PoE inline power administrative settings on the specific interface.

- Possible values: Enabled, Disabled
- Default value: Enabled

Status

Display the PoE inline power status on the specific interface.

- Possible values: Delivering Power, Disabled

Class

Display the PoE class of the specific interface.

- Value range: 0..4
- Default value: 0

Current Power

Display the PoE power in Watts on the specific interface being currently delivered by the device.

Max Observed

Display the maximum PoE power in Watts on the specific interface which has been observed by the device.

Power Limit

Display the maximum PoE power that can be reserved on the specific interface. The power limit is ignored if the maximum observed power consumption exceeds this limit.

- Possible values: 0 . . 300001 (in Milliwatts)
- Default value: 0. (disable the limitation of PoE inline power)

Interface Name

Display the name of the specific interface.

- Possible values: <None>, ...
- Default value: <None>

all

Display the global PoE inline power configuration settings and states for the interfaces of the device.

Intf

Display the interface (in <slot/port> notation).

Admin Mode

Display the PoE inline power administrative settings for each interface of the device.

- Possible values: Enabled, Disabled
- Default value: Enabled

Operating Status

Display the PoE inline power status for each interface of the device.

- Possible values: Delivering Power, Disabled

Priority

Display the PoE inline power priority for each interface of the device. In case of power scarcity, inline power on ports configured with the lowest priority is dropped first.

- Possible values: Critical, High, Low.
- Default value: Low

The highest priority is *critical*.

Note: This parameter is available for MACH1000, MACH4000 and devices which support Power over Ethernet Plus (MACH104-16TX-PoEP devices and MACH102 devices with media module M1-8TP-RJ45 PoE).

Class

Display the PoE class for each interface of the device.

- Value range: 0 . . 4
- Default value: 0

Curr. Power

Display the PoE power in Watts being currently delivered by the device for each interface.

Max. Observed

Display the maximum PoE power in Watts for each interface which has been observed by the device.

Power Limit

Display the maximum PoE power that can be reserved for each interface of the device. The power limit is ignored if the maximum observed power consumption exceeds this limit.

- Possible values: 0 . . 300001 (in Milliwatts)
- Default value: 0. (disable the limitation of PoE inline power)

4.11.3 inlinepower (Global Config)

Configure the global inline power parameters.

Format

```
inlinepower {admin-mode {disable|enable} |  
trap {disable|enable} | threshold <1-99> |  
fast-startup {enable|disable} }
```

Mode

Global Config

admin-mode

Configure the global inline power administrative setting.

- Possible values: `enable` or `disable`.
- Default value: `enable`.

trap

Configure the inline power notification (trap) setting.

- Possible values: `enable` or `disable`.
- Default value: `disable`.

threshold

Configure the inline power notification (trap) threshold (unit: percent of maximum rated power).

- Value range: 1 . . 99.
- Default value: 90 .

fast-startup

Configure the inline power to be enabled at the beginning of the start phase.

- Possible values: `enable` or `disable`.
- Default value: `disable`.

4.11.4 inlinepower (Interface Config)

Configure the port related inline power parameters.

Note: The interface name you enter in the `name`-command.

Format

```
inlinepower {admin-mode {disable|enable} |  
            power-limit <milliwatts> |  
            priority {critical|high|low} }|
```

Mode

Interface Config

admin-mode

Configure the port-related inline power administrative setting

- Possible values: `enable` or `disable`.
- Default value: `enable`.

power-limit

Configure the maximum power that can be reserved on the port. If set to 0 then the limitation is disabled. The power limit is ignored if the maximum observed power consumption exceeds this limit.

- Possible values: 0...300001 (in milliwatts)
- Default value: 0. (disable the limitation of inline power)

priority

Configure the inline power priority for this port. In case of power scarcity, inline power on ports configured with the lowest priority is dropped first.

- Possible values: `critical`, `high` or `low`.
The highest priority is `critical`.
- Default value: `low`.

Note: This parameter is available for MACH1000, MACH4000 and devices which support Power over Ethernet Plus (MACH104-16TX-PoEP devices and MACH102 devices with media module M1-8TP-RJ45 PoE).

4.11.5 clear inlinepower

Reset the inline power parameters to default settings.

Format

```
clear inlinepower
```

Mode

```
Privileged EXEC
```

5 CLI Commands: Switching

This section provides detailed explanation of the Switching commands. The commands are divided into two functional groups:

- ▶ Show commands display spanning tree settings, statistics, and other information.
- ▶ Configuration Commands configure features and options of the switch. For every configuration command there is a show command that displays the configuration setting.

5.1 Spanning Tree Commands

5.1.1 show spanning-tree

This command displays spanning tree settings for the common and internal spanning tree, when the optional parameter “brief” is not included in the command. The following details are displayed.

Format

```
show spanning-tree [brief]
```

Mode

Privileged EXEC and User EXEC

Spanning Tree Adminmode

Enabled or Disabled

Bridge Priority

Configured value.

Bridge Identifier

The bridge identifier for the CST (CST = Classical Spanning Tree IEEE 802.1d). It is made up using the bridge priority and the base MAC address of the bridge.

Time Since Topology Change

in seconds

Topology Change Count

Number of times changed.

Topology Change

Boolean value of the Topology Change parameter for the switch indicating if a topology change is in progress on any port assigned to the common and internal spanning tree.

Designated Root

The bridge identifier of the root bridge. It is made up from the bridge priority and the base MAC address of the bridge.

Root Path Cost

Value of the Root Path Cost parameter for the common and internal spanning tree.

Root Port Identifier

Identifier of the port to access the Designated Root for the CST.

Root Port Max Age

Derived value

Root Port Bridge Forward Delay

Derived value

Hello Time

Configured value

Bridge Hold Time

Minimum time between transmission of Configuration Bridge Protocol Data Units (BPDUs)

CST Regional Root

Bridge Identifier of the CST Regional Root. It is made up using the bridge priority and the base MAC address of the bridge.

Regional Root Path Cost

Path Cost to the CST Regional Root.

Associated FIDs

List of forwarding database identifiers currently associated with this instance.

Associated VLANs

List of VLAN IDs currently associated with this instance.

■ show spanning-tree brief

When the “brief” optional parameter is included, this command displays a brief overview of the spanning tree settings for the bridge. In this case, the following details are displayed.

Bridge Priority

Configured value.

Bridge Identifier

The bridge identifier for the selected MST instance. It is made up using the bridge priority and the base MAC address of the bridge.

Bridge Max Age

Configured value.

Bridge Hello Time

Configured value.

Bridge Forward Delay

Configured value.

Bridge Hold Time

Minimum time between transmission of Configuration Bridge Protocol Data Units (BPDUs)

Rstp Mrp Mode

Rapid spanning tree mrp (Media Redundancy Protocol) mode (Enabled/Disabled)

Rstp Mrp configuration error

Configuration error in Rapid spanning tree mrp (Media Redundancy Protocol) (No/Yes)

5.1.2 show spanning-tree interface

This command displays the settings and parameters for a specific switch port within the common and internal spanning tree. The <slot/port> is the desired switch port. The following details are displayed on execution of the command.

Format

```
show spanning-tree interface <slot/port>
```

Mode

Privileged EXEC and User EXEC

Port mode

Enabled or disabled.

Port Up Time Since Counters Last Cleared

Time since port was reset, displayed in days, hours, minutes, and seconds.

STP BPDUs Transmitted

Spanning Tree Protocol Bridge Protocol Data Units sent

STP BPDUs Received

Spanning Tree Protocol Bridge Protocol Data Units received.

RST BPDUs Transmitted

Rapid Spanning Tree Protocol Bridge Protocol Data Units sent

RST BPDUs Received

Rapid Spanning Tree Protocol Bridge Protocol Data Units received.

MSTP BPDUs Transmitted

Multiple Spanning Tree Protocol Bridge Protocol Data Units sent

MSTP BPDUs Received

Multiple Spanning Tree Protocol Bridge Protocol Data Units received.

5.1.3 show spanning-tree mst detailed

This command displays settings and parameters for the specified multiple spanning tree instance. The instance <mstid> is a number that corresponds to the desired existing multiple spanning tree instance ID. The following details are displayed.

Format

```
show spanning-tree mst detailed <mstid>
```

Mode

Privileged EXEC and User EXEC

mstid

Enter a multiple spanning tree instance identifier.
Valid values: 0 - 4094.

MST Instance ID

Valid value: 0

MST Bridge Priority

Valid values: 0-61440 in increments of 4096.

Time Since Topology Change

in seconds

Topology Change Count

Number of times the topology has changed for this multiple spanning tree instance.

Topology Change in Progress

Value of the Topology Change parameter for the multiple spanning tree instance.

Designated Root

Identifier of the Regional Root for this multiple spanning tree instance.

Root Path Cost

Path Cost to the Designated Root for this multiple spanning tree instance

Root Port Identifier

Port to access the Designated Root for this multiple spanning tree instance

Associated FIDs

List of forwarding database identifiers associated with this instance.

Associated VLANs

List of VLAN IDs associated with this instance.

5.1.4 show spanning-tree mst port detailed

This command displays the detailed settings and parameters for a specific switch port within a particular multiple spanning tree instance. The instance <mstid> is a number that corresponds to the desired existing multiple spanning tree instance. The <slot/port> is the desired switch port.

Format

```
show spanning-tree mst port detailed <mstid> <slot/  
port>
```

Mode

Privileged EXEC and User EXEC

MST Instance ID

Valid value: 0

Port Identifier

Port priority as a two digit hex number followed by the port number as a two digit hex number.

Port Priority

Decimal number.

Port Forwarding State

Current spanning tree state of this port

Port Role

The port's current RSTP port role.

Port Path Cost

Configured value of the Internal Port Path Cost parameter

Designated Root

The Identifier of the designated root for this port.

Designated Port Cost

Path Cost offered to the LAN by the Designated Port

Designated Bridge

Bridge Identifier of the bridge with the Designated Port.

Designated Port Identifier

Port on the Designated Bridge that offers the lowest cost to the LAN
If 0 (defined as the default CIST ID) is passed as the <mstid>, then this command displays the settings and parameters for a specific switch port within the common and internal spanning tree. The <slot/port> is the desired switch port. In this case, the following are displayed.

Port Identifier

The port identifier for this port within the CST.

Port Priority

The priority of the port within the CST.

Port Forwarding State

The forwarding state of the port within the CST.

Port Role

The role of the specified interface within the CST.

Port Path Cost

The configured path cost for the specified interface.

Designated Root

Identifier of the designated root for this port within the CST.

Designated Port Cost

Path Cost offered to the LAN by the Designated Port.

Designated Bridge

The bridge containing the designated port

Designated Port Identifier

Port on the Designated Bridge that offers the lowest cost to the LAN

Topology Change Acknowledgement

Value of flag in next Configuration Bridge Protocol Data Unit (BPDU) transmission indicating if a topology change is in progress for this port.

Hello Time

The hello time in use for this port.

Edge Port

The configured value indicating if this port is an edge port.

Edge Port Status

The derived value of the edge port status. True if operating as an edge port; false otherwise.

Point To Point MAC Status

Derived value indicating if this port is part of a point to point link.

CST Regional Root

The regional root identifier in use for this port.

CST Port Cost

The configured path cost for this port.

5.1.5 show spanning-tree mst port summary

This command displays the settings of one or all ports within the specified multiple spanning tree instance. The parameter <mstid> indicates a particular MST instance. The parameter {<slot/port> | all} indicates the desired switch port or all ports.

If 0 (defined as the default CIST ID) is passed as the <mstid>, then the status summary is displayed for one or all ports within the common and internal spanning tree.

Format

```
show spanning-tree mst port summary <mstid> {<slot/  
port> | all}
```

Mode

Privileged EXEC and User EXEC

MST Instance ID

The MST instance associated with this port. Valid value: 0.

Interface

Valid slot and port number separated by forward slashes.

STP Mode

Current STP mode of this port in the specified spanning tree instance.

Type

Currently not used.

Port Forwarding State

The forwarding state of the port in the specified spanning tree instance

Port Role

The role of the specified port within the spanning tree.

5.1.6 show spanning-tree mst summary

This command displays settings and parameters for the specified multiple spanning tree instance. The following details are displayed.

Format

```
show spanning-tree mst summary
```

Mode

Privileged EXEC and User EXEC

MST Instance ID

Valid value: 0

Associated FIDs

List of forwarding database identifiers associated with this instance.

Associated VLANs

List of VLAN IDs associated with this instance.

5.1.7 show spanning-tree summary

This command displays spanning tree settings and parameters for the switch. The following details are displayed on execution of the command.

Format

```
show spanning-tree summary
```

Mode

Privileged EXEC and User EXEC

Spanning Tree Adminmode

Enabled or disabled.

Spanning Tree Version

Version of 802.1 currently supported (IEEE 802.1Q-2005, IEEE 802.1D-2004) based upon the Force Protocol Version parameter

Configuration Name

Configured name.

Configuration Revision Level

Configured value.

Configuration Digest Key

Calculated value.

Configuration Format Selector

Configured value.

MST Instances

List of all multiple spanning tree instances configured on the switch

5.1.8 show spanning-tree vlan

This command displays the association between a VLAN and a multiple spanning tree instance. The <vlanid> corresponds to an existing VLAN ID (1-4042).

Format

```
show spanning-tree vlan <vlanid>
```

Mode

Privileged EXEC and User EXEC

vlanid

Enter a VLAN identifier (1 - 4042).

VLAN Identifier

The VLANs associated with the selected MST instance.

Associated Instance

Identifier for the associated multiple spanning tree instance or "CST" if associated with the common and internal spanning tree

5.1.9 spanning-tree

This command sets the spanning-tree operational mode to enabled.

Default

```
disabled
```

Format

```
spanning-tree
```

Mode

```
Global Config
```

■ no spanning-tree

This command sets the spanning-tree operational mode to disabled. While disabled, the spanning-tree configuration is retained and can be changed, but is not activated.

Format

```
no spanning-tree
```

Mode

```
Global Config
```

5.1.10 spanning-tree auto-edgeport

This command specifies that this port is an Edge Port within the common and internal spanning tree. This will allow this port to transition to Forwarding State without delay.

Format

```
spanning-tree auto-edgeport
```

Mode

```
Interface Config
```

■ no spanning-tree auto-edgeport

This command specifies that this port is not an Edge Port within the common and internal spanning tree.

Format

```
no spanning-tree auto-edgeport
```

Mode

```
Interface Config
```

5.1.11 spanning-tree bpduguard

This command sets the BPDU (Bridge Protocol Data Units) Guard on the switch to enabled.

Default

disabled

Format

spanning-tree bpduguard

Mode

Global Config

■ no spanning-tree bpduguard

This command sets the BPDU (Bridge Protocol Data Units) Guard to disabled.

Format

no spanning-tree bpduguard

Mode

Global Config

5.1.12 spanning-tree configuration name

This command sets the Configuration Identifier Name for use in identifying the configuration that this switch is currently using. The <name> is a string of at most 32 characters.

Default

The base MAC address displayed using hexadecimal notation as specified in IEEE 802 standard.

Format

```
spanning-tree configuration name <name>
```

Mode

```
Global Config
```

■ no spanning-tree configuration name

This command resets the Configuration Identifier Name to its default.

Format

```
no spanning-tree configuration name
```

Mode

```
Global Config
```

5.1.13 spanning-tree configuration revision

This command sets the Configuration Identifier Revision Level for use in identifying the configuration that this switch is currently using. The Configuration Identifier Revision Level is a number in the range of 0 to 65535.

Default

0

Format

```
spanning-tree configuration revision <0-65535>
```

Mode

Global Config

■ no spanning-tree configuration revision

This command sets the Configuration Identifier Revision Level for use in identifying the configuration that this switch is currently using to the default value, i.e. 0.

Format

```
no spanning-tree configuration revision
```

Mode

Global Config

5.1.14 spanning-tree edgeport

This command specifies that this port is an Edge Port within the common and internal spanning tree. This will allow this port to transition to Forwarding State without delay.

Format

```
spanning-tree edgeport
```

Mode

```
Interface Config
```

■ no spanning-tree edgeport

This command specifies that this port is not an Edge Port within the common and internal spanning tree.

Format

```
no spanning-tree edgeport
```

Mode

```
Interface Config
```

5.1.15 spanning-tree forceversion

This command sets the Force Protocol Version parameter to a new value. The Force Protocol Version can be one of the following:

- ▶ 802.1d - ST BPDUs are transmitted (802.1Q-2005 functionality supported)
- ▶ 802.1s - ST BPDUs are transmitted (802.1Q-2005 functionality supported)
- ▶ 802.1w - RST BPDUs are transmitted (802.1Q-2005 functionality supported)

Default

802.1w

Format

```
spanning-tree forceversion  
                        <802.1d | 802.1s | 802.1w>
```

Mode

Global Config

■ no spanning-tree forceversion

This command sets the Force Protocol Version parameter to the default value, i.e. 802.1w.

Format

```
no spanning-tree forceversion
```

Mode

Global Config

5.1.16 spanning-tree forward-time

This command sets the Bridge Forward Delay parameter to a new value for the common and internal spanning tree. The forward-time value is in seconds within a range of 4 to 30, with the value being greater than or equal to $(\text{Bridge Max Age} / 2) + 1$.

Default

15

Format

```
spanning-tree forward-time <4-30>
```

Mode

Global Config

■ no spanning-tree forward-time

This command sets the Bridge Forward Delay parameter for the common and internal spanning tree to the default value, i.e. 15.

Format

```
no spanning-tree forward-time
```

Mode

Global Config

5.1.17 spanning-tree guard loop

This command enables loop guard and disables root guard on an interface.

Default

disabled

Format

spanning-tree guard loop

Mode

Interface Config

■ no spanning-tree guard

This command disables the guard for this port.

Format

no spanning-tree guard

Mode

Interface Config

5.1.18 spanning-tree guard none

This command disables root guard and disables loop guard on an interface.

Default

disabled

Format

```
spanning-tree guard none
```

Mode

Interface Config

■ no spanning-tree guard

This command disables the guard for this port.

Format

```
no spanning-tree guard
```

Mode

Interface Config

5.1.19 spanning-tree guard root

This command enables root guard and disables loop guard on an interface.

Default

disabled

Format

spanning-tree guard root

Mode

Interface Config

■ no spanning-tree guard

This command disables the guard for this port.

Format

no spanning-tree guard

Mode

Interface Config

5.1.20 spanning-tree hello-time

This command sets the Hello Time parameter to a new value for the common and internal spanning tree. The hellotime <value> is in whole seconds within a range of 1 to 2 with the value being less than or equal to "(Bridge Max Age / 2) - 1".

Default

2

Format

```
spanning-tree hello-time <1-2>
```

Mode

Interface Config
Global Config

■ no spanning-tree hello-time

This command sets the Hello Time parameter for the common and internal spanning tree to the default value, i.e. 2.

Format

```
no spanning-tree hello-time
```

Mode

Interface Config
Global Config

5.1.21 spanning-tree hold-count

This command sets the bridge hold count parameter.

Default

disabled

Format

```
spanning-tree hold-count <1-40>
```

Mode

Global Config

<1-40>

Enter the bridge parameter for hold count as an integer in the range 1 - 40.

■ no spanning-tree hold-count

This command sets bridge hold count to disabled.

Format

no spanning-tree hold-count

Mode

Global Config

5.1.22 spanning-tree max-age

This command sets the Bridge Max Age parameter to a new value for the common and internal spanning tree. The max-age value is in seconds within a range of 6 to 40, with the value being less than or equal to "2 times (Bridge Forward Delay - 1)".

Default

20

Format

spanning-tree max-age <6-40>

Mode

Global Config

■ no spanning-tree max-age

This command sets the Bridge Max Age parameter for the common and internal spanning tree to the default value, i.e. 20.

Format

```
no spanning-tree max-age
```

Mode

```
Global Config
```

5.1.23 spanning-tree max-hops

This command sets the Bridge Max Hops parameter to a new value for the common and internal spanning tree. The max-hops value is an integer within a range of 1 to 127.

Format

```
spanning-tree max-hops <1-127>
```

Mode

```
Global Config
```

■ no spanning-tree max-hops

This command sets the Bridge Max Hops parameter for the common and internal spanning tree to the default value, i.e. 20.

Format

```
no spanning-tree max-age
```

Mode

```
Global Config
```

5.1.24 spanning-tree mst

This command sets the Path Cost or Port Priority for this port within the multiple spanning tree instance or in the common and internal spanning tree. If the <mstid> parameter corresponds to an existing multiple spanning tree instance, then the configurations are done for that multiple spanning tree instance. If however 0 (defined as the default CIST ID) is passed as the <mstid>, then the configurations are performed for the common and internal spanning tree instance.

This command accepts the value 0 for the mstid, meaning the common and internal spanning tree.

If the 'cost' token is specified, this command sets the path cost for this port within a multiple spanning tree instance or the common and internal spanning tree instance, depending on the <mstid> parameter. The pathcost can be specified as a number in the range of 1 to 200000000 or auto. If "auto" is specified, the pathcost value will be set based on Link Speed.

If the 'port-priority' token is specified, this command sets the priority for this port within a specific multiple spanning tree instance or the common and internal spanning tree instance, depending on the <mstid> parameter. The port-priority value is a number in the range of 0 to 240 in increments of 16.

Default

```
cost : auto; external-cost : auto;
port-priority : 128
```

Format

```
spanning-tree mst <mstid>
    {{cost <1-200000000> | auto } |
     {external-cost <1-200000000> | auto } |
     port-priority <0-240>}
```

Mode

```
Interface Config
```

■ no spanning-tree mst

This command sets the Path Cost or Port Priority for this port within the multiple spanning tree instance or in the common and internal spanning tree to the respective default values. If the <mstid> parameter corresponds to an existing multiple spanning tree instance, then the configurations are done for that multiple spanning tree instance. If however 0 (defined as the default CIST ID) is passed as the <mstid>, then the configurations are performed for the common and internal spanning tree instance.

This command accepts the value 0 for the mstid, meaning the common and internal spanning tree.

If the 'cost' token is specified, this command sets the path cost for this port within a multiple spanning tree instance or the common and internal spanning tree instance, depending on the <mstid> parameter, to the default value, i.e. a pathcost value based on the Link Speed.

If the 'port-priority' token is specified, this command sets the priority for this port within a specific multiple spanning tree instance or the common and internal spanning tree instance, depending on the <mstid> parameter, to the default value, i.e. 128.

Format

```
no spanning-tree mst <mstid> <cost | port-priority>
```

Mode

```
Interface Config
```

5.1.25 spanning-tree mst priority

This command sets the bridge priority for a specific multiple spanning tree instance. The instance <mstid> is a number that corresponds to the desired existing multiple spanning tree instance. The priority value is a number within a range of 0 to 61440 in increments of 4096.

This command accepts the value 0 for the mstid.

If 0 (defined as the default CIST ID) is passed as the <mstid>, then this command sets the Bridge Priority parameter to a new value for the common and internal spanning tree. The bridge priority value again is a number within a range of 0 to 61440. The twelve least significant bits will be masked according to the 802.1s specification. This will cause the priority to be rounded down to the next lower valid priority.

Default

32768

Format

```
spanning-tree mst priority <mstid> <0-61440>
```

Mode

Global Config

■ no spanning-tree mst priority

This command sets the bridge priority for a specific multiple spanning tree instance to the default value, i.e. 32768. The instance <mstid> is a number that corresponds to the desired existing multiple spanning tree instance.

This command accepts the value 0 for the mstid.

If 0 (defined as the default CIST ID) is passed as the <mstid>, then this command sets the Bridge Priority parameter for the common and internal spanning tree to the default value, i.e. 32768.

Format

```
spanning-tree mst priority <mstid>
```

Mode

Global Config

5.1.26 spanning-tree mst vlan

This command adds an association between a multiple spanning tree instance and a VLAN. The VLAN will no longer be associated with the common and internal spanning tree. The instance <mstid> is a number that corresponds to the desired existing multiple spanning tree instance. The <vlanid> corresponds to an existing VLAN ID (1-4042). This command accepts the value 0 for the mstid.

Format

```
spanning-tree mst vlan <mstid> <vlanid>
```

Mode

```
Global Config
```

■ no spanning-tree mst vlan

This command removes an association between a multiple spanning tree instance and a VLAN. The VLAN will again be associated with the common and internal spanning tree. The instance <mstid> is a number that corresponds to the desired existing multiple spanning tree instance. The <vlanid> corresponds to an existing VLAN ID. This command accepts the value 0 for the mstid.

Format

```
no spanning-tree mst vlan <mstid> <vlanid>
```

Mode

```
Global Config
```

5.1.27 spanning-tree mst instance

This command creates a MST instance.

Format

```
spanning-tree mst instance <1-4094>
```

Mode

```
Global Config
```

<1-4094>

Enter a multiple spanning tree instance identifier.

■ no spanning-tree mst instance

This command removes a MST instance.

Format

```
no spanning-tree mst instance <1-4094>
```

Mode

```
Global Config
```

<1-4094>

Enter a multiple spanning tree instance identifier.

5.1.28 spanning-tree port mode

This command sets the Administrative Switch Port State for this port to enabled.

Default

disabled

Format

```
spanning-tree port mode
```

Mode

Interface Config

■ no spanning-tree port mode

This command sets the Administrative Switch Port State for this port to disabled.

Format

```
no spanning-tree port mode
```

Mode

Interface Config

5.1.29 spanning-tree port mode all

This command sets the Administrative Switch Port State for all ports to enabled.

Default

disabled

Format

```
spanning-tree port mode all
```

Mode

Global Config

■ no spanning-tree port mode all

This command sets the Administrative Switch Port State for all ports to disabled.

Format

```
no spanning-tree port mode all
```

Mode

Global Config

5.1.30 spanning-tree stp-mrp-mode

This command sets the spanning tree mrp (Media Redundancy Protocol) mode to enabled.

Default

disabled

Format

```
spanning-tree stp-mrp-mode
```

Mode

Global Config

■ no spanning-tree stp-mrp-mode

This command sets the spanning tree mrp (Medium Redundancy Protocol) mode to disabled.

Format

```
no spanning-tree stp-mrp-mode
```

Mode

Global Config

5.1.31 spanning-tree tcnguard

This command enables tcn guard on an interface.

Default

disabled

Format

spanning-tree guard tcnguard

Mode

Interface Config

■ no spanning-tree tcnguard

This command disables tcn guard for this port.

Format

no spanning-tree tcnguard

Mode

Interface Config

5.2 MRP

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

The two ends of a backbone in a line-type configuration can be closed to form a redundant ring - the MRP-Ring - by using the RM function (Redundancy Manager) of the Switch.

It is possible to mix the devices that support this function in any combination within the MRP ring.

If a line section becomes inoperable, the ring structure of up to 50 switches typically transforms back to a line-type configuration within 150 ms (maximum 500 ms).

5.2.1 show mrp

This command displays the settings and states of the MRP-Ring. The following details are displayed on execution of the command.

Format

```
show mrp [current-domain]
```

Mode

Privileged EXEC and User EXEC

current-domain

Specify the optional keyword "current-domain" to show the current MRP domain's settings. If you omit the keyword "current-domain", the show command will display the settings of all existing MRP domains.

Note: Currently, it is only possible to configure one MRP domain, so the keyword keyword "current-domain" can be omitted (it exists for future compatibility reasons).

5.2.2 show mrp current-domain

This command displays the settings and states of the MRP-Ring's current domain. The following details are displayed on execution of the command. If you omit the optional keywords (e. g., advanced-mode), all settings will be displayed.

Format

```
show mrp current-domain [advanced-mode |  
  domain-id | info | manager-priority | mode |  
  name | recovery-delay | operation |  
  port [primary | secondary] | summary | vlan]
```

Mode

Privileged EXEC and User EXEC

advanced mode

Show the switch's advanced mode setting for the given MRP domain.

domain-id

Show the given MRP domain's ID.

info

Show status information for the given MRP domain.

Note: The information displayed depends on the switch's mode (Client or Manager) because only a subset of them are useful for each mode.

manager-priority

Show the switch's manager priority for the given MRP domain.

mode

Show the switch's mode for the given MRP domain.

name

Show the given MRP domain's name.

recovery-delay

Show the given MRP domain's recovery delay.

operation

Show the switch's administrative setting for the given MRP domain (enabled or disabled).

port

Show the ports for the given MRP domain

port primary

Show the primary port for the given MRP domain.

port secondary

Show the secondary port for the given MRP domain.

summary

Show a summary for the given MRP domain.

vlan

Show the VLAN ID for the given MRP domain.

5.2.3 mrp current-domain

Specify that you want to configure the current MRP domain's settings.

Default

none

Format

```
mrp current-domain {advanced-mode {disable|enable}  
| manager-priority <0-65535>  
| mode {client|manager} | name <domain-name>  
| recovery-delay {500ms|200ms}  
| operation {disable|enable}  
| port {primary|secondary} <slot/port>  
| vlan <0-4042>}
```

Mode

Global Config

advanced-mode

Enable or disable the switch's advanced mode for the given MRP domain.

manager-priority

Configure the given MRP domain's manager priority (0-65535).

mode

Configure the switch's MRP mode for the given domain (client or manager).

`client`: Switch is client for the given MRP domain.

`manager`: Switch is manager for the given MRP domain.

name

Set a name for the given MRP domain.

recovery-delay

Configure the MRP recovery delay for the given domain.

`500ms`: Recovery delay is 500 ms for the given MRP domain.

`200ms`: Recovery delay is 200 ms for the given MRP domain.

operation

Enable or disable the switch for the given MRP domain.

port

Specify the switch's ports for the given MRP domain (in slot/port notation).

`primary`: Specify the switch's primary port for the given MRP domain.

`secondary`: Specify the switch's secondary port for the given MRP domain.

vlan

Enter the VLAN for the given MRP domain

Possible values: 0 . . 4042

Default Value: 0

5.2.4 mrp delete-domain

Delete current MRP domain.

Format

```
mrp delete-domain current-domain
```

Mode

```
Global Config
```

5.2.5 mrp new-domain

Create a new MRP domain. The configuration will consist of default parameters and its operation will be disabled.

Default

```
n/a not set
```

Format

```
mrp new-domain (<domain-id> | default-domain)
```

Mode

```
Global Config
```

domain-id

Enter a new MRP domain id. Format: 16 bytes in decimal notation, example: 1.2.3.4.5.6.7.8.9.10.11.12.13.14.15.16

The MRP domain id 0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0 is invalid.

default-domain

Create a default MRP domain (ID: 255.255.255.255.255.255.255.255.255.255.255.255.255.255.255.255).

5.3 HIPER-Ring

The concept of the HIPER-Ring enables the construction of high-availability, ring-shaped network structures. Within such a ring topology, network components supporting the HIPER-Ring are connected with each other via their ring ports. Exactly one redundancy manager assumes control of the ring. These commands are for configuring the Hirschmann High Performance Redundancy Ring.

Further information concerning this function you will find in the User Manual "Redundancy Configuration".

5.3.1 show hiper-ring

This command displays the settings and states of the HIPER-Ring. The following details are displayed on execution of the command.

Format

```
show hiper-ring
  {info | mode | port [primary | secondary] |
  redundancy-state | rm-state | recovery-delay}
```

Mode

Privileged EXEC and User EXEC

info

Display the information about the HIPER-Ring configuration (cabling).

mode

Display the HIPER-Ring mode settings.

port

Display the HIPER-Ring's primary and secondary port properties.

port primary

Display the HIPER Ring's primary port properties.

port secondary

Display the HIPER Ring's secondary port properties.

redundancy-state

Display the actual state of the HIPER-Ring redundancy.

rm-state

Display the state of the HIPER Ring redundancy manager.

recovery-delay

Display the value of the recovery delay.

5.3.2 hiper-ring

Configure the HIPER-Ring.

Press Enter for a list of valid commands and their recommended order.

Format

```
hiper-ring
```

Mode

```
Global Config
```

■ no hiper-ring

Clear the HIPER Ring configuration (delete it).

Format

```
no hiper-ring
```

Mode

```
Global Config
```

5.3.3 hiper-ring mode

This command sets the HIPER-Ring mode. Possible values are:

- ▶ `ring-manager` Set the switch's HIPER Ring mode to Ring Manager.
- ▶ `rm` Abbreviation of Ring Manager.
- ▶ `ring-switch` Set the switch's HIPER Ring mode to Ring Switch.
- ▶ `rs` Abbreviation of Ring Switch.

Default

```
none
```

Format

```
hiper-ring mode <{ring-manager|ring-switch|rm|rs}>
```

Mode

```
Global Config
```

5.3.4 hiper-ring port primary

Enter the switch's primary HIPER Ring port.

Default

n/a (not set)

Format

```
hiper-ring port primary <primary ring port>
```

Mode

Global Config

primary ring port

Enter the switch's primary HIPER Ring port (<slot/port>).

5.3.5 hiper-ring port secondary

Enter the switch's secondary HIPER Ring port.

Default

n/a not set

Format

```
hiper-ring port secondary <secondary ring port>
```

Mode

Global Config

secondary ring port

Enter the switch's secondary HIPER Ring port (<slot/port>).

5.3.6 hiper-ring recovery-delay

Defines the maximum recovery delay of ring recovery in the HIPER Ring (500 or 300 ms).

Default

n/a not set

Format

hiper-ring recovery-delay (<500/300>)

Mode

Global Config

5.4 Fast-HIPER-Ring

The concept of the Fast-HIPER-Ring enables the construction of high-availability, ring-shaped network structures. Within such a ring topology, network components supporting the Fast-HIPER-Ring are connected with each other via their ring ports. Exactly one redundancy manager assumes control of the ring.

These commands are for configuring the Hirschmann Fast High Performance Redundancy Ring.

Further information concerning this function you will find in the User Manual "Redundancy Configuration".

This command displays the settings and states of the HIPER-Ring. The following details are displayed on execution of the command.

Format

```
show fast-hiper-ring
```

Mode

Privileged EXEC and User EXEC

Ring ID

Display the Ring ID.

Mode of Switch (administrative setting)

Display the HIPER-Ring mode administrative settings.

Mode of Switch (real operating state)

Display the HIPER-Ring operation mode.

Ring Name

Display the Fast-HIPER-Ring's name.

Number of nodes in the ring

Display the number of nodes in the ring.

Port Number, Primary

Display the HIPER-Ring's primary port number and its properties.

Port Number, Secondary

Display the HIPER-Ring's secondary port number and its properties.

Operation

Display the admin state of the HIPER-Ring configuration.

General Operating States

Display general information concerning the fast-hiper-ring state.

Specify that you want to show the current Fast HIPER-Ring ID's settings.

Format

```
show fast-hiper-ring current-id
  {id | info | mode | operation | port |
  port [primary |secondary] | summary |
  ring-name | nodes | vlan}
```

Mode

Privileged EXEC and User EXEC

id

Display the given Fast HIPER-Ring's ID.

info

Display status information for the given Fast HIPER-Ring ID.

mode

Display the switch's mode for the given Fast HIPER-Ring ID.

operation

Display the switch's operative setting for the given Fast HIPER-Ring ID.

Note: In case of configuration problems, this value may differ from the administrative setting (may become 'Disabled').

port

Display the ports for the given Fast HIPER-Ring ID.

port primary

Display the primary port for the given Fast HIPER-Ring ID.

port secondary

Display the secondary port for the given Fast HIPER-Ring ID.

summary

Display a summary for the given Fast HIPER-Ring ID.

ring-name

Display the ring name for the given Fast HIPER-Ring ID.

nodes

Display the number of nodes in the ring for the given Fast HIPER-Ring ID.

vlan

Display the VLAN ID for the given Fast HIPER-Ring ID.

5.4.1 fast-hiper-ring

Configure the Fast-HIPER-Ring.

Format

```
fast-hiper-ring {current-id
  {mode {ring-manager|ring-switch|rm|rs} |
  operation {disable|enable} |
  port {primary|secondary} <slot/port> |
  ring-name <ring-name> |
  nodes <1-n> |
  vlan <0-4042>} |
delete-id current-id |
new-id {<id>|default-id}}
```

Mode

Global Config

current-id

Specify that you want to configure the current Fast-HIPER-Ring ID's settings.

mode

Configure the switch's Fast HIPER-Ring mode for the given ID (ring-manager or ring-switch).

rm: Abbreviation for 'ring-manager'.

rs: Abbreviation for 'ring-switch'.

mode ring-manager

Switch is ring-manager for the given Fast HIPER-Ring ID.

mode ring-switch

Switch is ring-switch for the given Fast HIPER-Ring ID.

mode rm

Abbreviation for 'ring-manager'.

mode rs

Abbreviation for 'ring-switch'.

operation

Enable or disable the switch for the given Fast-HIPER-Ring ID.

port

Specify the switch's ports for the given Fast-HIPER-Ring ID.

ring-name

Set a ring name for the given Fast HIPER-Ring ID.

nodes

Specify the number of nodes in the ring for the given Fast HIPER-Ring ID.

vlan

Specify the VLAN for the given Fast HIPER-Ring ID.

delete-id

Delete the given Fast HIPER-Ring ID.

new-id

Create a new Fast HIPER-Ring ID. The configuration will consist of default parameters and its operation will be disabled.

<id>

Enter a new Fast HIPER-Ring ID. Format: a number in the range 1-2147483647 ($2^{31} - 1$). An ID of 0 is invalid.

default-id

Create a default Fast HIPER-Ring ID (1).

5.5 Redundant Coupling

The control intelligence built into the switch allows the redundant coupling of HiPER-Rings and network segments. Two network segments can be connected via two separate paths with one of the following switches:

- ▶ RS2-16M
- ▶ RS20/RS30/RS40
- ▶ RSR20/RSR30
- ▶ MICE (Rel. 3.0 or higher)
- ▶ MS20/MS30
- ▶ PowerMICE
- ▶ MACH1000
- ▶ MACH3000 (Rel. 3.3 or higher)
- ▶ MACH4000

The switch in the redundant line and the switch in the main line inform each other about their operating states by using control frames via the ethernet or via the control line.

Note: For redundancy security reasons, the Rapid Spanning Tree protocol and redundant network/ring coupling may not be enabled simultaneously.

Note: The network that connects the master and the slave must always be a HiPER-Ring. The coupling switch in single mode also must have a HiPER-Ring Configured.

Further information concerning this function you will find in the User Manual "Redundancy Configuration".

These commands allow you to configure the redundant coupling of network segments.

5.5.1 show ring-coupling

This command displays the settings and states of the network coupling / ring coupling.

To set up a new Ring Coupling configuration when no configuration is currently present (e. g., after a clear command), always set the local port first. Please refer to: ring-coupling port local <slot/port>.

The following details are displayed on execution of the command.

Format

```
show ring-coupling <config | info |  
net-coupling | operation | partner-ip |  
port [ all | control | local | partner] |  
redundancy-mode>
```

Mode

Privileged EXEC and User EXEC

config

Display the Ring Coupling's configuration

- single
- dual-master-inband
- dual-master-outband
- dual-slave-inband
- dual-slave-outband.

info

Display information about the Ring Coupling's states:

- configuration failure,
- Extended diagnosis,
- redundancy guaranteed.

net-coupling

Display the Ring Coupling's ring/network coupling setting (network/ring-only).

operation

Display the Ring Coupling's operation setting

- on
- off

partner IP

Display the switch's Ring Coupling partner IP address (only valid for remote configurations).

port

Display the switch's Ring Coupling ports

- all
- local
- partner (only takes effect in dual configurations)
- control (only takes effect in outband configurations).

redundancy-mode

Display the Ring Coupling's redundancy mode

- normal
- extended.

Ring/Network Coupling Mode

Display the Ring/Network Coupling mode

- ring-only if you wish to couple a HIPER-Ring.
- network if you wish to couple a line-type configuration.

5.5.2 ring-coupling

Configure the redundant coupling of HIPER-Rings / network segments. This command, if called without arguments, lists the available subcommands, their recommended order and tips how to set up a new configuration.

Format

```
ring-coupling
```

Mode

```
Global Config
```

■ no ring-coupling

Clear the ring-coupling configuration (delete it).

Format

```
no ring-coupling
```

Mode

```
Global Config
```

5.5.3 ring-coupling config

This command sets the Ring Coupling configuration.

Possible values are:

- ▶ `single` Configure the Ring Coupling's basic setting to single (both coupling ports are local to the switch, switch performs master and slave functions).
- ▶ `dual-master-inband` Configure the Ring Coupling's basic setting to dual-master-inband (2nd coupling port is on a remote switch, local switch is master, communication over network).
- ▶ `dual-master-outband` Configure the Ring Coupling's basic setting to dual-master-outband (2nd coupling port is on a remote switch, local switch is master, communication over dedicated control port).
- ▶ `dual-slave-inband` Configure the Ring Coupling's basic setting to dual-slave-inband (2nd coupling port is on a remote switch, local switch is slave, communication over network).
- ▶ `dual-slave-outband` Configure the Ring Coupling's basic setting to dual-slave-outband (2nd coupling port is on a remote switch, local switch is slave, communication over dedicated control port).
- ▶ `dmi` Abbreviation for `dual-master-inband`.
- ▶ `dmo` Abbreviation for `dual-master-outband`.
- ▶ `dsi` Abbreviation for `dual-slave-inband`.
- ▶ `dso` Abbreviation for `dual-slave-outband`.

Default

`none`

Format

```
ring-coupling config <{ single |  
dual-master-inband | dual-master-outband |  
dual-slave-inband | dual-slave-outband |  
dmi | dmo | dsi | dso }>
```

Mode

Global Config

5.5.4 ring-coupling net-coupling

Coupling mode refers to the type of coupled network.

Possible values are:

- ▶ `network` ,if you wish to couple a line-type configuration.
- ▶ `ring-only` ,if you wish to couple a HIPER-Ring.

Default

`none`

Format

`ring-coupling net-coupling <{network|ring-only}>`

Mode

Global Config

5.5.5 ring-coupling operation

Configure the Ring Coupling's operation setting. Possible values are:

- ▶ `on` Enable the current Ring Coupling configuration.
- ▶ `off` Disable the current Ring Coupling configuration.

Default

`off`

Format

`ring-coupling operation <{off|on}>`

Mode

Global Config

5.5.6 ring-coupling port

Configure the Ring Coupling's ports. Possible values are:

- ▶ `control` Enter the Ring Coupling's control coupling port in outband configurations.
- ▶ `local` Enter the Ring Coupling's local coupling port.
- ▶ `partner` Enter the Ring Coupling's partner coupling port in single mode configuration.

Default

`none`

Format

```
ring-coupling port <{control|local|partner}> <slot/  
port>
```

Mode

Global Config

5.5.7 ring-coupling redundancy-mode

Configure the Ring Coupling's redundancy mode. Possible values are:

- ▶ `extended` Slave responds to a failure in the remote ring or network.
- ▶ `normal` Slave does not respond to a failure in the remote ring or network.

Default

`extended`

Format

```
ring-coupling redundancy-mode <{extended|normal}>
```

Mode

Global Config

5.6 Port Security

With the Port Security function you can specify for each port from which terminal devices data can be received and sent to other ports. This function helps to protect the network from unauthorized access.

5.6.1 show port-sec dynamic

Use this command to display the dynamic MAC limit port-related settings (dynamic limit, current MAC count, current action and current port state).

Format

```
show port-sec dynamic {all | <slot/port>}
```

Mode

Global Config

all

Display information for each port.

<slot|port>

Display information for one specific port.

Port

Display the number of the port (slot/port).

Possible values: 1/1, 1/2, ...

State

Display state of dynamic MAC limit port-related settings.

Possible values: Disabled, Enabled

Default value: Enabled

Limit

Display the currently configured dynamic limit of MAC addresses allowed to be learned on the interface.

Possible values: 0..50

Default value: 0

Current

Display current number of MAC addresses learned on the interface.

Possible values: 0..50

Default value: 0

Action

Display the currently configured action to be taken if port security is violated at this port.

Possible values: None, Auto Disable, Port Disable, Trap Only

Default value: Auto Disable

5.6.2 show port-sec mode

Display the MAC/IP Based Port Security global setting for all ports.

Format

```
show port-sec mode
```

Mode

Privileged EXEC and User EXEC

5.6.3 show port-sec port

Display the MAC/IP Based Port Security port-related settings (allowed MAC address, current MAC address, allowed IP address, current action and current port state).

Format

```
show port-sec port <{all|<slot/port>}>
```

Mode

Privileged EXEC and User EXEC

5.6.4 port-sec mode

Configure the global MAC/IP Based Port Security mode:

- ▶ ip-based Port security is based on a given, allowed source IP address.
- ▶ mac-based Port security is based on a given, allowed source MAC address.

Format

```
port-sec mode <{ip-based|mac-based}>
```

Mode

Global Config

5.6.5 port-sec action

Configure the action to be taken if port security is violated at this port.

- ▶ `none`
No action is taken if port security is violated at this port.
- ▶ `auto-disable`
The port is auto-disabled for traffic if port security is violated
- ▶ `port-disable`
The port is disabled for traffic if port security is violated.
- ▶ `trap-only`
A trap is sent if port security is violated at this port (this port remains open for traffic).

Configure the allowed IP source address for this port.

Configure the allowed MAC source address for this port.

Format

```
port-sec {action {none | auto-disable |
                 port-disable | trap-only}
         |allowed-ip <IP1> [IP2 [IP3 [IP4 [IP5
                           [IP6 [IP7 [IP8 [IP9 [IP10]]]]]]]]
         |allowed-mac <MAC1> [MAC2 [MAC3 [MAC4
                              [MAC5 [MAC6 [MAC7 [MAC8 [MAC9
                              [MAC10]]]]]]]] } }
```

Mode

Interface Config

■ no port-sec

No action is taken if port security is violated at this port.

Format

```
no port-sec
```

Mode

Interface Config

5.6.6 port-sec allowed-ip

Enter the allowed IP source address for this port, format: nnn.nnn.nnn.nnn (nnn: decimal number 0..255) (up to 10).

Format

```
port-sec allowed-ip <IP Address 1> <IP Address 2>
... <IP Address 10>
```

Mode

Interface Config

5.6.7 port-sec allowed-ip add

Enter the allowed IP source address for this port, format: nnn.nnn.nnn.nnn (nnn: decimal number 0..255) (up to 50).

Format

```
port-sec allowed-ip add <IP Address 1>
                        <IP Address 2> ... <IP Address 50>
```

Mode

Interface Config

5.6.8 port-sec allowed-ip remove

Enter the allowed IP source address for this port, format: nnn.nnn.nnn.nnn (nnn: decimal number 0..255) (up to 50).

Format

```
port-sec allowed-ip remove <IP Address 1>  
                               <IP Address 2> ... <IP Address 50>
```

Mode

Interface Config

5.6.9 port-sec allowed-mac

Enter the allowed MAC source address for this port, format: nn:nn:nn:nn:nn:nn (n: hexadecimal digit) or format: nn:nn:nn:nn:nn/m (n: hexadecimal digit) (m: decimal digit (1..48)) (up to 10).

Format

```
port-sec allowed-mac <MAC Address 1>  
                     <MAC Address 2> ... <MAC Address 10>
```

Mode

Interface Config

5.6.10 port-sec allowed-mac add

Enter the allowed MAC source address for this port,
format: nn:nn:nn:nn:nn:nn (n: hexadecimal digit) or
format: nn:nn:nn:nn:nn:nn/m
n: hexadecimal digit, m: decimal digit (1..48)
(up to 50).

Format

```
port-sec allowed-mac add <MAC Address 1>  
                        <MAC Address 2> ... <MAC Address 50>
```

Mode

Interface Config

5.6.11 port-sec allowed-mac remove

Enter the allowed MAC source address for this port,
format: nn:nn:nn:nn:nn:nn (n: hexadecimal digit) or
format: nn:nn:nn:nn:nn:nn/m
n: hexadecimal digit, m: decimal digit (1..48)
(up to 50).

Format

```
port-sec allowed-mac remove <MAC Address 1>  
                            <MAC Address 2> ... <MAC Address 50>
```

Mode

Interface Config

5.6.12 port-sec dynamic

Use this command to configure the dynamic limit of MAC addresses allowed to be learned on the interface. A value of 0 disables the dynamic limit.

Format

```
port-sec dynamic <max-count>
```

Mode

```
Interface Config
```

<max-count>

Enter the maximum number of dynamically learned allowed MAC addresses

- Possible values: 0 . . 50
- Default: 0
- A value of 0 disables the dynamic limit.

5.6.13 clear port-sec

Clear the MAC/IP Based Port Security by setting each port's security action (applied when port security is violated) to None. Additionally, the global mode is set to MAC Based.

Format

```
clear port-sec
```

Mode

```
User EXEC and Global Config
```

5.7 DHCP Relay Commands

These commands configure the DHCP Relay parameters. The commands are divided by functionality into these different groups:

- ▶ Configuration Commands are used to configure features and options of the switch. For every configuration command there is a show command that will display the configuration setting.
- ▶ Show commands are used to display switch settings, statistics and other information.
- ▶ Commands that start with the keyword 'no' (so-called 'no commands') are used to clear some or all of the settings to factory defaults.

5.7.1 dhcp-relay

Set different options for BOOTP/DHCP relay and option 82 inclusion.

Format

```
dhcp-relay
  {opt82
    {operation {disable|enable}|
    man-id <Manual Remote ID>|
    remote-id-type {client-id|ip|mac|other}}|
  server-address <Server-ID (1..16)>
    <Server IP Address> [<slot/port> | all] }
```

Mode

Global Config

dhcp-relay opt82 operation {disable|enable}

Enable/Disable option 82 globally. Default: enable.

dhcp-relay opt82 man-id <Manual Remote ID>

Configure the DHCP Relay's Option 82 Manual Value for the Remote ID Type (only effective, if Remote ID is set to "other"). Default: no ID.

dhcp-relay opt82 remote-id-type {client-id|ip|mac|other}

Configure the DHCP Relay's Option 82 Remote ID Type.
Default: mac

dhcp-relay server-address

<Server ID (1..16)> <Server IP Address> [<slot/port> | all]

Set the server IP address for one of the 16 possible server IDs.

Default: 0.0.0.0.

Optionally, configure this entry to a specific interface. If an interface is set, only DHCP packets from this interface are relayed to the server.

■ **no dhcp-relay**

Clear the DHCP Relay configuration (set all server addresses to 0.0.0.0).

Format

```
no dhcp-relay
```

Mode

Global Config

5.7.2 dhcp-relay

Set different port specific options for option 82 inclusion.

Format

```
dhcp-relay {admin-state {disable|enable} |  
            operation {disable|enable} |  
            hirschmann-device {disable|enable} |  
            hirschmann-agent {disable|enable}}
```

Mode

Interface Config

dhcp-relay admin-state {disable|enable}

Enable or disable the DHCP Relay's Admin State on this port.

Default: enable.

Note: Make sure that "Active Protocol" is "Relay" for both ports involved in DHCP Relaying (the one connected to DHCP client and the one connected to DHCP server).

dhcp-relay operation {disable|enable}

Enable or disable the DHCP Relay's Option 82 on this port. Default: enable.

dhcp-relay hirschmann-device {disable|enable}

Enable this parameter if a Hirschmann DHCP client is connected to this port.

- It disables the forwarding of DHCP multicast requests that are received on this port.
- It will send its own DHCP multicast requests to be relayed by the DHCP relay; this will reduce the load in your network.

Disable this parameter if a Non-Hirschmann DHCP client is connected to this port (these devices send normal broadcast DHCP requests; this enables the relaying of DHCP broadcast requests that are received on this port).

dhcp-relay hirschmann-agent {disable|enable}

Enable or disable the forwarding of DHCP requests that are received on this port. Enable this parameter if a Hirschmann DHCP client is connected to this port. Default: disable.

Disable this parameter if a Non-Hirschmann DHCP client is connected to this port (these devices send normal broadcast DHCP requests; this enables the relaying of DHCP broadcast requests that

are received on this port)

Enable this parameter if a Hirschmann DHCP client is connected to this port (it will send its own DHCP multicast requests to be relayed by the DHCP relay; this will reduce the load in your network).

5.7.3 show dhcp-relay

Display the settings of the BOOTP/DHCP relay.

Format

```
show dhcp-relay [opt82 | port {<slot/port>|all} |  
server-address]
```

Mode

Privileged EXEC and User EXEC

opt82

Show the DHCP Relay's Option 82 settings exclusively.

port

Display the DHCP Relay's port-related settings for the specified port exclusively.

<slot/port>

Show the DHCP Relay's port-related settings for the specified port exclusively.

all

Show the DHCP Relay's port-related settings for all ports.

server-address

Display the DHCP Relay's server address settings exclusively.

ID: The ID of the DHCP server (1..16).

Server IP: The DHCP server's IP address (a.b.c.d).

Interface: The number of the interface (<slot/port> or all).

Operation: The operational status (Enabled, Disabled).

Port

Display the port number in <slot/port> notation.

Admin State

Display the DHCP Relay's admin state settings.

Possible values: Disabled, Enabled

Active Protocol

Display the DHCP Relay's active protocol settings.

Possible values: Relay, Disabled, Server, Inaccessible

Option 82

Display the DHCP Relay's option 82 settings.

Possible values: Disabled, Enabled

Hirschmann Device

Display the DHCP Relay's Hirschmann device settings.

Possible values: Disabled, Enabled

6 CLI Commands: Security

This chapter provides a detailed explanation of the Security commands. The following Security CLI commands are available in the software Switching Package. Use the security commands to configure security settings for login users and port users.

The commands are divided into these different groups:

- ▶ Show commands are used to display device settings, statistics and other information.
- ▶ Configuration Commands are used to configure features and options of the switch. For every configuration command there is a show command that will display the configuration setting.

6.1 Security Commands

6.1.1 users login

This command assigns the specified authentication login list to the specified user for system login. The `<user>` must be a configured `<user>` and the `<listname>` must be a configured login list.

If the user is assigned a login list that requires remote authentication, all access to the interface from all CLI, web, and telnet sessions will be blocked until the authentication is complete.

Note: Note that the login list associated with the 'admin' user can not be changed to prevent accidental lockout from the switch.

Format

```
users login <user> <listname>
```

Mode

```
Global Config
```

user

Enter user name.

listname

Enter an alphanumeric string of not more than 15 characters.

Note: When assigning a list to the 'admin' account, include an authentication method that allows administrative access even when remote authentication is unavailable (use 'authentication login `<listname>` [method1 [method2 [method3]]]').

6.2 HTTP Commands

6.2.1 ip http server

This command enables access to the switch's graphical user interface (web-based interface) via a web browser. When access is enabled, the user can login to the switch from the web-based interface. When access is disabled, the user cannot login to the switch's web server.

Disabling the web-based interface takes effect immediately. All interfaces are effected.

Default

enabled

Format

```
ip http server
```

Mode

Privileged EXEC

■ no ip http server

This command disables access to the switch's graphical user interface (web-based interface) via a web browser. When access is disabled, the user cannot login to the switch's web server.

Format

```
no ip http server
```

Mode

Privileged EXEC

6.2.2 show ip http

This command displays the http settings for the switch.

Format

```
show ip http
```

Mode

```
Privileged EXEC and User EXEC
```

HTTP Mode (Unsecure)

This field indicates whether the HTTP mode is enabled or disabled.

6.2.3 ip https server

This command is used to turn on the HTTPS server 3.

This command enables access to the switch's graphical user interface (web-based interface) via a web browser. When access is enabled, the user can login to the switch from the web interface. When access is disabled, the user cannot login to the switch's web server.

Default

disabled

Format

```
ip https server
```

Mode

Privileged EXEC

■ no ip https server

This command is used to turn off the HTTPS server 3.

This command disables access to the switch's graphical user interface (web-based interface) via a web browser. When access is disabled, the user cannot login to the switch's web server.

Format

```
no ip https server
```

Mode

Privileged EXEC

6.2.4 ip https port

This command is used to set the HTTPS listening port. The acceptable range is 1-65535. The default is 443

Note: After this setting, re-enable the HTTPS server. See “ip http server” on page 376.

Default

443

Format

```
ip https port <port_no>
```

Mode

Privileged EXEC

■ no ip https port

This command is used to reset the https port to the default value.

Format

```
no ip https port
```

Mode

Privileged EXEC

6.2.5 ip https certgen

Use this command to generate an X509/PEM certificate in-place.

Format

```
ip https certgen
```

Mode

Privileged EXEC

6.2.6 show ip https

This command displays the status of the HTTPS server (status of the server and port number).

Format

```
show ip https
```

Mode

Privileged EXEC and User EXEC

HTTPS Mode

Displays the status of the HTTPS server (enabled, disabled).

HTTPS Port

Displays the port number of the HTTPS server (default: 443).

7 Appendix- VLAN Example

LAN switches can segment networks into logically defined virtual workgroups. This logical segmentation is commonly referred to as a virtual LAN (VLAN). This logical segmentation of devices provides better LAN administration, security, and management of broadcast activity over the network. Virtual LANs have become an integral feature of switched LAN solutions.

The VLAN example below demonstrates a simple VLAN configuration.

If a single port is a member of VLANs 2, 3 and 4, the port expects to see traffic tagged with either VLAN 2,3 or 4.

The PVID (Port Virtual Identification) could be something entirely different, for example '12' and things would still work fine, just so incoming traffic was tagged.

Example:

Project A = (VLAN2, ports 1,2)

Project B = (VLAN3, ports 3,4)

Project C = (VLAN4, ports 5,6)

Project P = (VLAN 9, port 7)

VLAN	Command
create VLAN 2	<pre>vlan database vlan 2 exit config interface 1/1 vlan participation include 2 exit interface 1/2 vlan participation include 2 exit</pre>

Table 14: Creating VLANs

VLAN	Command
create VLAN 3	<pre> vlan database vlan 3 exit config interface 0/3 vlan participation include 3 exit interface 0/4 vlan participation include 3 exit </pre>
create VLAN 4	<pre> vlan database vlan 4 exit config interface 0/5 vlan participation include 4 exit interface 0/6 vlan participation include 4 exit </pre>
create VLAN 9	<pre> vlan database vlan 9 exit config interface 0/1 vlan participation include 9 exit interface 0/2 vlan participation include 9 exit interface 0/3 vlan participation include 9 exit interface 0/4 vlan participation include 9 exit interface 0/5 vlan participation include 9 exit interface 0/6 vlan participation include 9 exit interface 0/7 vlan participation include 9 exit </pre>

Table 14: Creating VLANs

7.1 SOLUTION 1

All traffic entering the ports is tagged traffic. Since the traffic is tagged, the PVID configuration for each port is not a concern.

- ▶ The network card configuration for devices on Project A must be set to tag all traffic with 'VLAN 2'
- ▶ The network card configuration for devices on Project B must be set to tag all traffic with 'VLAN 3'
- ▶ The network card configuration for devices on Project C must be set to tag all traffic with 'VLAN 4'
- ▶ The network card configuration for devices on Project P must be set to tag all traffic with 'VLAN 9'

7.2 SOLUTION 2

The network card configuration for devices on Project A, B and C should be set to NOT tag traffic.

To take care of these untagged frames configure the following:

- ▶ vlan pvid 2 (in interface 0/1)
- ▶ vlan pvid 2 (in interface 0/2)
- ▶ vlan pvid 3 (in interface 0/3)
- ▶ vlan pvid 3 (in interface 0/4)
- ▶ vlan pvid 4 (in interface 0/5)
- ▶ vlan pvid 4 (in interface 0/6)

8 Index

A

address-conflict 229
 areaid 23
 auto-disable reason 143
 auto-disable reset 145
 auto-disable timer 145
 auto-negotiate 146
 auto-negotiate all 147

B

boot skip-aca-on-boot 230, 230
 bridge address-learning 87
 bridge address-relearn detect operation 87
 bridge address-relearn detect threshold 87
 bridge aging-time 89
 bridge duplex-mismatch-detect operation 90
 bridge fast-link-detection 90
 bridge framesize 52
 bridge vlan-learning 91
 broadcasts
 broadcast storm recovery mode 199, 200, 202

C

cable-crossing 148
 classofservice dot1pmapping 79
 classofservice ip-dscp-mapping 80
 classofservice trus 81
 clear arp-table-switch 232
 clear commands
 clear arp-table-switch 232
 clear config 232
 clear pass 234
 clear traplog 235, 236
 clear vlan 236
 clear config 232
 clear config factory 232
 clear counters 233
 clear eventlog 231
 clear hiper-ring 233
 clear igmpsnooping 233
 clear inlinepower 300
 clear lldp config all 269
 clear mac-addr-table 234
 clear pass 234
 clear port-sec 367
 clear ring-coupling 236
 clear signal-contact 235
 clear traplog 235

clear vlan 236
 Competence Center 413
 config commands
 config loginsession 219
 config port admin-mode 192, 193
 config port linktrap 194, 195, 196
 config port physical-mode 198
 config switchconfig broadcast 199, 200, 202
 config switchconfig flowcontrol 203, 204
 config users add 223, 224
 config users delete 222, 223, 224
 config users passwd 225
 config vlan add 205
 config vlan delete 205
 config vlan interface acceptframe 207, 208, 213
 config vlan name 210
 config vlan participation 211, 212
 config vlan ports ingressfilter 209, 214
 config vlan ports pvid 215, 217
 config vlan ports tagging 216, 218
 config switchconfig flowcontrol 203, 204
 config users delete 222, 223, 224, 225
 config users passwd 222, 223, 224, 225
 config vlan delete 205
 config vlan ports acceptframe 217
 config vlan ports ingressfilter 208, 213, 214, 215
 configuration reset 232
 config-watchdog 237
 copy 237
 copy nvram clibanner 241
 copy nvram startup-config 242
 copy system bootcode 243
 copy system image 242
 copy system running-config 243
 copy nvram capture 239
 copy nvram capture aca capture 239
 copy nvram clibanner 238
 copy nvram errorlog 239
 copy nvram traplog 240
 copy system running-config 240
 copy tftp/// nvram httpscert 238

D

device configuration commands 201

device-status connection-error	243	lldp max-neighbors	271
device-status monitor	244	lldp notification	271
dhcp-relay	369, 370	lldp tlv gmrp	274
dip-switch operation	150	lldp tlv igmp	275
disconnect	219	lldp tlv link-aggregation	271
duplex settings	198	lldp tlv mac-phy-config-state	272
		lldp tlv max-frame-size	272
		lldp tlv mgmt-addr	272
E		lldp tlv pnio	273
ethernet-ip	91	lldp tlv pnio-alias	273
		lldp tlv pnio-mrp	273
F		lldp tlv port-desc	274
fast-hiper-ring	351	lldp tlv portsec	275
flow control	203, 204	lldp tlv port-vlan	274
frame acceptance mode	207, 208, 213	lldp tlv protocol	276
		lldp tlv ptp	275
G		lldp tlv sys-cap	276
Global Config Mode	41	lldp tlv sys-desc	276
		lldp tlv sys-name	277
H		lldp tlv vlan-name	277
hiper-ring	345	logging buffered	134
hiper-ring mode	345	logging buffered wrap	135
hiper-ring port primary	346	logging cli-command	136
hiper-ring port secondary	346	logging console	137
hiper-ring recovery-delay	347	logging host	138
		logging host reconfigure	139
I		logging host remove	139
IEEE 802.1Q	207, 208, 213	logging snmp-requests get operation	139
ingress filtering	209, 214	logging snmp-requests get severity	140
inlinepower (Global Config)	298	logging snmp-requests set operation	140
inlinepower (Interface Config)	299	logging snmp-requests set severity	141
Interface Config Mode	42	logging syslog	142
inventory	176, 177, 178, 179, 181, 182	logging syslog port	142
ip http secure-port	376	logical slot/port	24
ip http secure-protocol	376	logout	245
ip http server	376	logout command	245
ip https certgen	379		
ip https port	379	M	
ip https server	378	macaddr	23
		mac-address conflict	245
L		macfilter	151
Line Config Mode	42	macfilter adddest	152
link traps		macfilter adddest all	153
interface	194, 195, 196	media-module	149
lldp	265	media-module remove	149
LLDP - Link Layer Discovery Protocol	257	monitor session	154
lldp admin-state	269	monitor session mode	156
lldp chassis tx-interval	268	monitor session source/destination	157
lldp config chassis admin-state	266	mrp current-domain	340
lldp config chassis notification-interval	266	mrp delete-domain	342
lldp config chassis re-init-delay	267	mrp new-domain	342
lldp config chassis tx-delay	267		
lldp config chassis tx-hold-mult	268	N	
lldp fdb-mode	270	name	278
lldp hm-mode	270		

Index

network javascriptmode	92	ring-coupling net-coupling	358
network mgmt_vlan	77	ring-coupling operation	358
network mgmt-access add	92	ring-coupling port	359
network mgmt-access delete	92	ring-coupling redundancy-mode	359
network mgmt-access modify	93		
network mgmt-access operation	94	S	
network mgmt-access status	95	Schulungsangebot	413
network parms	95	selftest ramtest	170
network priority	97	selftest reboot-on-error	172
network protocol	96	selftest reboot-on-hdxerror	171
no dhcp-relay	369	serial timeout	99
no lldp	265	serviceshell	173
no snmp	284	sessions	
no snmp anycast address	285, 286, 292	closing	219, 245
no snmp client server	288	displaying	220
no snmp client server primary	289, 290, 291	set cli banner	253
no storm-control broadcast	199	set igmp	158, 159
		set igmp aging-time-unknown	159
		set igmp automatic-mode	160
		set igmp forward-all	161
		set igmp forward-unknown	162
		set igmp groupmembershipinterval	164
		set igmp interfacemode	165
		set igmp lookup-interval-unknown	165
		set igmp lookup-resp-time-unknown	166
		set igmp maxresponse	167
		set igmp querier max-response-time	168
		set igmp querier protocol-version	168
		set igmp querier status	169
		set igmp querier tx-interval	169
		set igmp query-ports-to-filter	170
		set igmp static-query-port	163
		set pre-login-banner text	170
		set pro-login-banner banner	255
		set prompt	99
		show	48
		show address-conflict	48
		show arp switch	49, 54
		show authentication	54
		show auto-disable brief	174
		show auto-disable reasons	175
		show boot skip-aca-on-boot	230, 230
		show bridge address-learning	49
		show bridge address-relearn-detect	50
		show bridge aging-time	50
		show bridge duplex-mismatch-detect	51
		show bridge framesize	51
		show bridge vlan-learning	51
		show classofservice dot1pmapping	82
		show classofservice ip-dscp-mapping	83
		show classofservice trust	84
		show commands	
		show inventory	176, 177, 178, 179, 181, 182
P			
passwords			
changing user	225		
resetting all	234		
ping	246		
ping command	243, 244, 246		
PoE - Power over Ethernet	294		
ports			
administrative mode	192, 193		
frame acceptance mode	207, 208, 213		
information	184		
ingress filtering	209, 214		
link traps	194, 195, 196		
physical mode	198		
tagging	216, 218		
VLAN IDs	215, 217		
VLAN information	191		
port-sec action	363		
port-sec allowed-ip	364		
port-sec allowed-ip add	364		
port-sec allowed-ip remove	365		
port-sec allowed-mac	365		
port-sec allowed-mac add	366		
port-sec allowed-mac remove	366		
port-sec dynamic	367		
port-sec mode	362		
Privileged Exec Mode	41		
profinetio	98		
R			
reboot	249		
reload	251		
reset system command	249, 251		
ring-coupling	356		
ring-coupling config	357		

show loginsession	220	show network mgmt-access	102
show port	184	show port	184, 203, 204
show stats switch detailed	55, 57, 62	show port-sec dynamic	360
show switchconfig	185, 186, 187	show port-sec mode	361
show users	221	show port-sec port	362
show vlan detailed	188	show reboot	250
show vlan interface	191	show reload	252
show vlan summary	190	show ring-coupling	354
show config-watchdog	52	show rmon-alarm	185
show device-status	53	show running-config	72
show dhcp-relay	369, 371	show selftest	186
show dip-switch	176	show serial	103
show ethernet-ip	100, 103	show serviceshell	186
show eventlog	54	show signal-contact	69
show fast-hiper-ring	349	show slot	71
show hiper-ring	344	show snmp sync	106
show hiper-ring info	345	show snmp-access	104
show igmpsnooping	177	show snmpcommunity	105
show inlinepower	294	show snmptrap	107
show inlinepower port	295	show snmp	279
show interface	55	show snmp anycast	281
show interface ethernet	57	show snmp client	281
show interface switchport	64	show snmp operation	282
show interface utilization	65	show snmp server	283
show inventory	209	show snmp status	283
show ip http	377	show snmp time	284
show ip https	380	show spanning-tree	303
show lldp	257	show spanning-tree brief	304
show lldp chassis tx-interval	260	show spanning-tree interface	306
show lldp config	257	show spanning-tree mst detailed	307
show lldp config chassis	258	show spanning-tree mst port detailed	308
show lldp config chassis admin-state	258	show spanning-tree mst port summary	311
show lldp config chassis notification-interval	258	show spanning-tree mst summary	312
show lldp config chassis re-init-delay	259	show spanning-tree summary	313
show lldp config chassis tx-delay	259	show spanning-tree vlan	314
show lldp config chassis tx-hold-mult	259	show storm-control	187
show lldp config port	261	show storm-control limiters port	187
show lldp config port tlv	262	show switchconfig	89
show lldp remote-data	263	show sysinfo	73, 84, 85
show logging	66	show telnet	108
show loginsession	220, 226	show telnetcon	109
show mac-address-conflict	67	show temperature	75
show mac-addr-table	68	show trapflags	110
show mac-filter-table igmpsnooping	178	show users	221
show mac-filter-table multicast	179	show vlan	188
show mac-filter-table static	180	show vlan brief	190
show mac-filter-table staticfiltering	181	show vlan port	191
show mac-filter-table stats	182	shutdown	192
show monitor session	183	shutdown all	193
show mrp	338	signal-contact	247
show mrp current domain	339	signal-contact connection-error	246
show network	89, 100	slot/port	24
		snmp sync community-to-v3	194
		snmp trap link-status	195

snmp trap link-status all	196	spanning-tree mst priority	331
snmp-access global	111, 112	spanning-tree mst vlan	332
snmp-access version v3-encryption	112	spanning-tree port mode	334
snmp-server	77, 114	spanning-tree port mode all	335
snmp-server community	115	spanning-tree stp-mrp-mode	336
snmp-server community ipaddr	117	spanning-tree tcnguard	337
snmp-server community ipmask	118	speed	198
snmp-server community mode	119	speeds	198
snmp-server community ro	120	statistics	
snmp-server community rw	120	switch, related commands	55, 57, 62
snmp-server contact	116	storm-control broadcast	199
snmp-server enable traps	121	storm-control broadcast (port-related)	201
snmp-server enable traps linkmode	124	storm-control egress-limit	201
snmp-server enable traps multiusers	125	storm-control egress-limiting	199
snmp-server enable traps port-sec	126	storm-control flowcontrol	203
snmp-server enable traps stpmode	127	storm-control flowcontrol per port	204
snmp-server location	120	storm-control ingress-limit	202
snmp-server sysname	121	storm-control ingress-limiting	200
snmptrap	128	storm-control ingress-mode	200, 202
snmptrap ipaddr	129	switch	
snmptrap mode	130	information, related commands	185, 186, 187
snmptrap snmpversion	131	inventory	176, 177, 178, 179, 181, 182
SNTP - Simple Network Time Protocol	279	resetting	249, 251
sntp anycast address	285	statistics, related commands	55, 57, 62
sntp anycast transmit-interval	285	System Information and Statistics Commands	77
sntp anycast vlan	286	System Utilities	229, 375
sntp client accept-broadcast	286	system utilities	229–246
sntp client disable-after-sync	287		
sntp client offset	287	T	
sntp client request-interval	288	tagging	216, 218
sntp client server primary	289	telnet	
sntp client server secondary	290	sessions, closing	219, 245
sntp client threshold	291	sessions, displaying	220
sntp operation	292	telnetcon maxsessions	132
sntp server disable-if-local	293	telnetcon timeout	133
sntp time system	293	temperature	248
spanning-tree	315	traceroute	231
spanning-tree auto-edgeport	316	transport input telnet	86
spanning-tree bpduguard	317	trap log	
spanning-tree bpdumigrationcheck	197	clearing	235, 236
spanning-tree configuration name	318		
spanning-tree configuration revision	319	U	
spanning-tree edgeport	320	update module-configuration	173
spanning-tree forceversion	321	User Account Management Commands	219
spanning-tree forward-time	322, 324	user account management commands	
spanning-tree guard loop	323	commands	219
spanning-tree guard none	324	User Exec Mode	41
spanning-tree guard root	325	users	
spanning-tree hello-time	326	adding	223, 224
spanning-tree hold-count	326	deleting	222, 223, 224
spanning-tree max-age	327	displaying	221
spanning-tree max-hops	328		
spanning-tree mst	329		
spanning-tree mst instance	333		

Index

passwords	225, 234
users access	223
users defaultlogin	222
users login	222, 375
users name	224
users passwd	225
users snmpv3 accessmode	226
users snmpv3 authentication	227
users snmpv3 encryption	228
utilization alarm-threshold	76

V

vlan	205
vlan acceptframe	207, 208
vlan ingressfilter	209
VLAN Mode	41
vlan name	210
vlan participation	211
vlan participation all	212
vlan port acceptframe all	213
vlan port ingressfilter all	214
vlan port priority all	84
vlan port pvid all	215
vlan port tagging all	216
vlan priority	85
vlan pvid	217
vlan tagging	218
vlan0-transparent-mode	206
VLANs	
adding	205
changing the name of	210
deleting	205
details	188
frame acceptance mode	207, 208, 213
IDs	215, 217
ingress filtering	209, 214
participation in	211, 212
port information	191
resetting parameters	236
summary information	190
tagging	216, 218

W

Web connections, displaying	220
-----------------------------	-----

9 Glossary

Numerics

802.1D. The IEEE designator for Spanning Tree Protocol (STP). STP, a link management protocol, is part of the 802.1D standard for media access control bridges. Using the spanning tree algorithm, STP provides path redundancy while preventing endless loops in a network. An endless loop is created by multiple active paths between stations where there are alternate routes between hosts. To establish path redundancy, STP creates a logical tree that spans all of the switches in an extended network, forcing redundant paths into a standby, or blocked, state. STP allows only one active path at a time between any two network devices (this prevents the loops) but establishes the redundant links as a backup if the initial link should fail. If STP costs change, or if one network segment in the STP becomes unreachable, the spanning tree algorithm reconfigures the spanning tree topology and reestablishes the link by activating the standby path. Without spanning tree in place, it is possible that both connections may be simultaneously live, which could result in an endless loop of traffic on the LAN.

802.1P. The IEEE protocol designator for Local Area Network

(LAN). This Layer 2 network standard improves support of time critical traffic, and limits the extent of high bandwidth multicast traffic within a bridged LAN. To do this, 802.1P defines a methodology for introducing traffic class priorities. The 802.1P standard allows priority to be defined in all 802 MAC protocols (Ethernet, Token Bus, Token Ring), as well as in FDDI. For protocols (such as Ethernet) that do not contain a priority field, 802.1P specifies a method for indicating frame priority based on the new fields defined in the 802.1Q (VLAN) standard.

802.1Q VLAN. The IEEE protocol designator for Virtual Local Area Network (VLAN). This standard provides VLAN identification and quality of service (QoS) levels. Four bytes are added to an Ethernet frame to allow eight priority levels (QoS) and to identify up to 4096 VLANs. See “VLAN” on page 410 for more information.

A

Address Resolution Protocol. An Internet Protocol that dynamically maps Internet addresses to physical (hardware) addresses on a LAN.

Advanced Network Device Layer/Software. Hirschmann term for the Device Driver level.

Aging. When an entry for a node is added to the lookup table of a switch, it is given a timestamp. Each time a packet is received from a node, the timestamp is updated. The switch has a user-configurable timer that erases the entry after a certain length of time with no activity from that node.

Application Programming Interface. An API is an interface used by a programmer to interface with functions provided by an application.

AVL tree. Binary tree having the property that for any node in the tree, the difference in height between the left and right subtrees of that node is no more than 1.

B

BPDU. See “Bridge Protocol Data Unit” on page 398.

BootP. See “Bootstrap Protocol.” on page 398.

Bootstrap Protocol. An Internet protocol that enables a diskless workstation to discover its own IP address, the IP address of a BootP server on the network, and a file to be loaded into memory to boot the machine. This enables the workstation to boot without requiring a hard or floppy disk drive.

Bridge Protocol Data Unit. BPDU is the IEEE 802.1D MAC Bridge Management protocol that is the standard implementation of STP (Spanning Tree Protocol). It uses the STP algorithm to insure that physical loops in the network topology do not result in logical looping of network traffic. Using one bridge configured as root for reference, the BPDU switches one of two bridges forming a network loop into standby mode, so that only one side of a potential loop passes traffic. By examining frequent 802.1d configuration updates, a bridge in the standby mode can switch automatically into the forward mode if the other bridge forming the loop fails.

C

Checksum. A simple error-detection scheme in which each transmitted message is identified with a numerical value based on the number of set bits in the message. The receiving station then applies a formula to the message and checks to make sure the accompanying numerical value is the same. If not, the receiver can assume that the message has been corrupted.

CLI. See “Command Line Interface” on page 398.

Command Line Interface. CLI is a line-item interface for configuring systems.

Complex Programmable Logic Device. CPLD is a programmable circuit on which a logic network can be programmed after its construction.

CPLD. See “Complex Programmable Logic Device.” on page 399.

D

DAPI. See “Device Application Programming Interface” on page 399.

Device Application Programming Interface. DAPI is the software interface that facilitates communication of both data and control information between the Application Layer and HAPI, with support from System Support.

DHCP. See “Dynamic Host Configuration Protocol.” on page 399.

Differentiated Services. Diffserv is a protocol for specifying and controlling network traffic by class so that certain types of traffic get precedence - for example, voice traffic, which requires a relatively uninterrupted flow of data, might get precedence over other kinds of traffic. Differentiated Services is the most advanced method for managing traffic in terms of what is called Class of Service (CoS). Unlike the earlier mechanisms of 802.1P tagging and Type of Service

(ToS), Differentiated Services avoids simple priority tagging and depends on more complex policy or rule statements to determine how to forward a given network packet. An analogy is made to travel services, in which a person can choose among different modes of travel - train, bus, airplane - degree of comfort, the number of stops on the route, standby status, the time of day or period of year for the trip, and so forth. For a given set of packet travel rules, a packet is given one of 64 possible forwarding behaviors - known as per hop behaviors (PHBs). A six-bit field, known as the Differentiated Services Code Point (DSCP), in the Internet Protocol (Internet Protocol) header specifies the per hop behavior for a given flow of packets. Differentiated Services and the Class of Service approach provide a way to control traffic that is both more flexible and more scalability than the Quality of Service approach.

Diffserv. See “Differentiated Services.” on page 399..

Dynamic Host Configuration Protocol. DHCP is a protocol for assigning dynamic IP addresses to devices on a network. With dynamic addressing, a device can have a different IP address every time it connects to the network. In some systems, the device's IP address can even change while it is still connected. DHCP also supports a mix of static and dynamic IP

addresses. Dynamic addressing simplifies network administration because the software tracks IP addresses rather than requiring an administrator to manage the task. A new computer can be added to a network without the hassle of manually assigning it a unique IP address.

E

EEPROM. See “Electronically Erasable Programmable Read Only Memory” on page 400.

Electronically Erasable Programmable Read Only Memory. EEPROM is also known as Flash memory. This is re-programmable memory.

F

Fast STP. A high-performance Spanning Tree Protocol. See “STP” on page 409 for more information.

FIFO. First In First Out.

Flash Memory. See “EEPROM” on page 400.

Flow Control. The process of adjusting the flow of data from one network device to another to ensure that the receiving device can handle all of the incoming data. This is particularly important where the sending device is capable of sending data much faster than the receiving device can receive it.

There are many flow control mechanisms. One of the most common flow control protocols for asynchronous communication is called xon-xoff. In this case, the receiving device sends a an “xoff” message to the sending device when its buffer is full. The sending device then stops sending data. When the receiving device is ready to receive more data, it sends an “xon” signal.

Forwarding. When a frame is received on an input port on a switch, the address is checked against the lookup table. If the lookup table has recorded the destination address, the frame is automatically forwarded on an output port.

Frame Check Sequence. The extra characters added to a frame for error detection and correction. FCS is used in X.25, HDLC, Frame Relay, and other data link layer protocols.

G

GARP. See “Generic Attribute Registration Protocol.” on page 401.

GARP Information Propagation.

GIP is the propagation of information between GARP participants for the same application in a bridge is carried out by a GIP component.

GARP Multicast Registration Protocol. GMRP provides a mechanism that allows Bridges and end stations to dynamically register (and subsequently, de-register) Group membership information with the MAC Bridges attached to the same LAN segment, and for that information to be disseminated across all Bridges in the Bridged LAN that support Extended Filtering Services. The operation of GMRP relies upon the services provided by the GARP.

GARP VLAN Registration Protocol. GVRP allows workstations to request admission to a particular VLAN for multicast purposes.

GE. See “Gigabit Ethernet” on page 401.

General Purpose Chip-select Machine. GPCM provides interfacing for simpler, lower-performance memory resources and memory mapped-devices. The GPCM does not support bursting and is used primarily for boot-loading.

Generic Attribute Registration Protocol. GARP provides a generic attribute dissemination capability that is used by participants in GARP Applications (called GARP Participants) to register and de-register attribute values with other GARP Participants within a Bridged LAN. The definition of the attribute

types, the values that they can carry, and the semantics that are associated with those values when registered are specific to the operation of the GARP Application concerned.

Gigabit Ethernet. A high-speed Ethernet connection.

GIP. See “GARP Information Propagation” on page 400.

GMRP. See “GARP Multicast Registration Protocol” on page 401.

GPCM. See “General Purpose Chip-select Machine” on page 401.

GVD. GARP VLAN Database.

GVRP. See “GARP VLAN Registration Protocol.” on page 401.

H

.h file. Header file in C code. Contains function and coding definitions.

HAPI. See “Hardware Abstraction Programming Interface” on page 401.

Hardware Abstraction Programming Interface. HAPI is the module that contains the NP specific software that interacts with the hardware.

hop count. The number of routers that a data packet passes through on its way to its destination.

I

ICMP. See “Internet Control Message Protocol” on page 402.

IGMP. See “Internet Group Management Protocol” on page 402.

IGMP Snooping. A series of operations performed by intermediate systems to add logic to the network to optimize the flow of multicast traffic; these intermediate systems (such as Layer 2 switches) listen for IGMP messages and build mapping tables and associated forwarding filters, in addition to reducing the IGMP protocol traffic. See “Internet Group Management Protocol” on page 402 for more information.

Internet Control Message

Protocol. ICMP is an extension to the Internet Protocol (IP) that supports packets containing error, control, and informational messages. The PING command, for example, uses ICMP to test an Internet connection.

Internet Group Management

Protocol. IGMP is the standard for IP Multicasting on the Internet. IGMP is used to establish host memberships in particular multicast groups on a single network. The mechanisms of the protocol allow a host to inform its local router, using Host Membership Reports, that it wants to receive messages addressed to a specific multicast

group. All hosts conforming to Level 2 of the IP Multicasting specification require IGMP.

IP. See “Internet Protocol” on page 402.

IP Multicasting. Sending out data to distributed servers on the MBone (Multicast Backbone). For large amounts of data, IP Multicast is more efficient than normal Internet transmissions because the server can broadcast a message to many recipients simultaneously. Unlike traditional Internet traffic that requires separate connections for each source-destination pair, IP Multicasting allows many recipients to share the same source. This means that just one set of packets is transmitted for all the destinations.

Internet Protocol. The method or protocol by which data is sent from one computer to another on the Internet. Each computer (known as a host) on the Internet has at least one IP address that uniquely identifies it among all other computers on the Internet. When you send or receive data (for example, an e-mail note or a Web page), the message gets divided into little chunks called packets. Each of these packets contains both the sender's Internet address and the receiver's address. Any packet is sent first to a gateway computer that understands a small part of the Internet. The gateway computer reads the destination address and

forwards the packet to an adjacent gateway that in turn reads the destination address and so forth across the Internet until one gateway recognizes the packet as belonging to a computer within its immediate neighborhood or domain. That gateway then forwards the packet directly to the computer whose address is specified.

Because a message is divided into a number of packets, each packet can, if necessary, be sent by a different route across the Internet. Packets can arrive in a different order than they were sent. The Internet Protocol just delivers them. It's up to another protocol, the Transmission Control Protocol (TCP) to put them back in the right order. IP is a connectionless protocol, which means that there is no continuing connection between the end points that are communicating. Each packet that travels through the Internet is treated as an independent unit of data without any relation to any other unit of data. (The reason the packets do get put in the right order is because of TCP, the connection-oriented protocol that keeps track of the packet sequence in a message.) In the Open Systems Interconnection (OSI) communication model, IP is in Layer 3, the Networking Layer. The most widely used version of IP today is IP version 4 (IPv4). However, IP version 6 (IPv6) is also beginning to be supported. IPv6 provides for

much longer addresses and therefore for the possibility of many more Internet users. IPv6 includes the capabilities of IPv4 and any server that can support IPv6 packets can also support IPv4 packets.

J

Joint Test Action Group. An IEEE group that specifies test framework standards for electronic logic components.

JTAG. See “Joint Test Action Group” on page 403.

L

LAN. See “Local Area Network” on page 404.

LDAP. See “Lightweight Directory Access Protocol” on page 403.

Lightweight Directory Access Protocol. A set of protocols for accessing information directories. LDAP is based on the standards contained within the X.500 standard, but is significantly simpler. Unlike X.500, LDAP supports TCP/IP, which is necessary for any type of Internet access. Although not yet widely implemented, LDAP should eventually make it possible for almost any application running on virtually any computer platform to obtain directory information, such as e-mail addresses and public keys. Because LDAP is an open protocol, applications need not worry about

the type of server hosting the directory.

Learning. The bridge examines the Layer 2 source addresses of every frame on the attached networks (called listening) and then maintains a table, or cache, of which MAC addresses are attached to each of its ports.

Link-State. In routing protocols, the declared information about the available interfaces and available neighbors of a router or network. The protocol's topological database is formed from the collected link-state declarations.

LLDP. The IEEE 802.1AB standard for link layer discovery in Ethernet networks provides a method for switches, routers and access points to advertise their identification, configuration and capabilities to neighboring devices that store the data in a MIB (management information base). Link layer discovery allows a network management system to model the topology of the network by interrogating the MIB databases in the devices.

Local Area Network. A group of computers that are located in one area and are connected by less than 1,000 feet of cable. A typical LAN might interconnect computers and peripherals on a single floor or in a single building. LANs can be connected together, but if modems

and telephones connect two or more LANs, the larger network constitutes what is called a WAN or Wide Area Network.

M

MAC. (1) Medium Access Control. In LANs, the sublayer of the data link control layer that supports medium-dependent functions and uses the services of the physical layer to provide services to the logical link control (LLC) sublayer. The MAC sublayer includes the method of determining when a device has access to the transmission medium. (2) Message Authentication Code. In computer security, a value that is a part of a message or accompanies a message and is used to determine that the contents, origin, author, or other attributes of all or part of the message are as they appear to be. (*IBM Glossary of Computing Terms*)

Management Information Base.

When SNMP devices send SNMP messages to the management console (the device managing SNMP messages), it stores information in the MIB.

MBONE. See "Multicast Backbone" on page 405.

MDC. Management Data Clock.

MDI. Management Data Interface.

MDIO. Management Data Input/Output.

MDIX. Management Dependent Interface Crossover.

MIB. See “Management Information Base” on page 404.

MOSPF. See “Multicast OSPF” on page 405.

MPLS. See “Multi-Protocol Label Switching” on page 405.

Multicast Backbone. The MBONE is a virtual network. It is layered on top of portions of the physical Internet to support routing of IP multicast packets since that function has not yet been integrated into many production routers. The network is composed of islands that can directly support IP multicast, such as multicast LANs like Ethernet, linked by virtual point-to-point links called “tunnels”. The tunnel endpoints are typically workstation-class machines having operating system support for IP multicast and running the “mrouterd” multicast routing daemon.

Multicasting. To transmit a message to specific recipients across a network. A simple example of multicasting is sending an e-mail message to a mailing list. Teleconferencing and videoconferencing also use multicasting, but require more robust protocols and networks. Standards are being developed to support multicasting over a TCP/IP network such as the Internet. These standards, IP Multicast and Mbone,

will allow users to easily join multicast groups. Note that multicasting refers to sending a message to a select group whereas broadcasting refers to sending a message to everyone connected to a network. The terms multicast and narrowcast are often used interchangeably, although narrowcast usually refers to the business model whereas multicast refers to the actual technology used to transmit the data.

Multicast OSPF. With a MOSPF specification, an IP Multicast packet is routed based both on the packet's source and its multicast destination (commonly referred to as source/destination routing). As it is routed, the multicast packet follows a shortest path to each multicast destination. During packet forwarding, any commonality of paths is exploited; when multiple hosts belong to a single multicast group, a multicast packet will be replicated only when the paths to the separate hosts diverge. See “P” on page 407 for more information.

Multiplexing. A function within a layer that interleaves the information from multiple connections into one connection.

Multi-Protocol Label Switching.

An initiative that integrates Layer 2 information about network links (bandwidth, latency, utilization) into Layer 3 (IP) within a particular

autonomous system—or ISP—in order to simplify and improve IP-packet exchange. MPLS gives network operators a great deal of flexibility to divert and route traffic around link failures, congestion, and bottlenecks. From a QoS standpoint, ISPs will better be able to manage different kinds of data streams based on priority and service plan. For instance, those who subscribe to a premium service plan, or those who receive a lot of streaming media or high-bandwidth content can see minimal latency and packet loss. When packets enter into a MPLS-based network, Label Edge Routers (LERs) give them a label (identifier). These labels not only contain information based on the routing table entry (i.e., destination, bandwidth, delay, and other metrics), but also refer to the IP header field (source IP address), Layer 4 socket number information, and differentiated service. Once this classification is complete and mapped, different packets are assigned to corresponding Labeled Switch Paths (LSPs), where Label Switch Routers (LSRs) place outgoing labels on the packets. With these LSPs, network operators can divert and route traffic based on data-stream type and Internet-access customer.

MT-RJ connector. A type of fiber-optic cable jack that is similar in shape and concept to a standard telephone jack, enabling duplex

fiber-optic cables to be plugged into compatible devices as easily as plugging in a telephone cable.

MUX. See “Multiplexing” on page 405.

N

NM. Network Module.

nm. Nanometer (1×10^9) meters.

NP. Network Processor.

O

Open Systems Interconnection.

OSI is a seven (7) layer architecture model for communications systems developed by the ISO for the interconnection of data communications systems. Each layer uses and builds on the services provided by those below it.

Operating System Application Programming Interface. OSAPI is a module within the System Support software that provides a set of interfaces to OS support functions.

OS. Operating System.

OSAPI. See “Operating System Application Programming Interface” on page 406.

OSI. See “Open Systems Interconnection” on page 406.

P

PDU. See “Protocol Data Unit” on page 407.

PHY. The OSI Physical Layer: The physical layer provides for transmission of cells over a physical medium connecting two ATM devices. This physical layer is comprised of two sublayers: the Physical Medium Dependent (PMD) sublayer, and the Transmission Convergence (TC) sublayer.

PMC. Packet Mode Channel.

Port Mirroring. Also known as a roving analysis port. This is a method of monitoring network traffic that forwards a copy of each incoming and outgoing packet from one port of a network switch to another port where the packet can be studied. A network administrator uses port mirroring as a diagnostic tool or debugging feature, especially when fending off an attack. It enables the administrator to keep close track of switch performance and alter it if necessary. Port mirroring can be managed locally or remotely. An administrator configures port mirroring by assigning a port from which to copy all packets and another port where those packets will be sent. A packet bound for or heading away from the first port will be forwarded onto the second port as well. The administrator places a protocol analyzer on the port receiving the

mirrored data to monitor each segment separately. The analyzer captures and evaluates the data without affecting the client on the original port. The monitor port may be a port on the same SwitchModule with an attached RMON probe, a port on a different SwitchModule in the same hub, or the SwitchModule processor. Port mirroring can consume significant CPU resources while active. Better choices for long-term monitoring may include a passive tap like an optical probe or an Ethernet repeater.

Protocol Data Unit. PDU is a packet of data passed across a network. The term implies a specific layer of the OSI model and a specific protocol.

Q

QoS. See “Quality of Service” on page 407.

Quality of Service. QoS is a networking term that specifies a guaranteed level of throughput. Throughput is the amount of data transferred from one device to another or processed in a specified amount of time - typically, throughputs are measured in bytes per second (Bps).

R

Real-Time Operating System.

RTOS is a component of the OSAPI module that abstracts operating systems with which other systems can interface.

RFC. Request For Comment.

RMON. Short for remote monitoring, a network management protocol that allows network information to be gathered at a single workstation. Whereas SNMP gathers network data from a single type of Management Information Base (MIB), RMON 1 defines nine additional MIBs that provide a much richer set of data about network usage. For RMON to work, network devices, such as hubs and switches, must be designed to support it. The newest version of RMON, RMON 2, provides data about traffic at the network layer in addition to the physical layer. This allows administrators to analyze traffic by protocol.

RP. Rendezvous Point. Used with IP Multicast.

RPU. Remote Power Unit.

RTOS. See “Real-Time Operating System” on page 408.

S

SDL. Synchronous Data Link.

Simple Network Management Protocol. SNMP is the protocol governing network management and the monitoring of network devices and their functions. It is not necessarily limited to TCP/IP networks. The versions have the following differences:

SNMPv1 (full): Security is based on community strings.

SNMPsec (historic): Security is based on parties. Few, if any, vendors implemented this version of the protocol, which is now largely forgotten.

SNMPv2p (historic): For this version, much work was done to update the SNMPv1 protocol and the SMIv1, and not just security. The result was updated protocol operations, new protocol operations and data types, and party-based security from SNMPsec.

SNMPv2c (experimental): This version of the protocol is called community string-based SNMPv2. It is an update of the protocol operations and data types of SNMPv2p, and uses community-based security from SNMPv1.

SNMPv2u (experimental): This version of the protocol uses the protocol operations and data types of SNMPv2c and security based on users.

*SNMPv2** (experimental): This version combined the best features

of SNMPv2p and SNMPv2u. (It is also called SNMPv2star.) The documents defining this version were never published as RFCs.

SNMPv3 (proposed): This version of the protocol is a combination of user-based security and the protocol operations and data types from SNMPv2p and support for proxies. The security is based on that found in SNMPv2u and SNMPv2*, and updated after much review. The documents defining this protocol will soon be published as RFCs.

SimpleX signaling. SX is one of IEEE 802.3's designations for media. For example, 1000SX indicates 1000 Gigabit Ethernet over "short haul" or "short wavelength" optical fiber.

SMC1. A model of Serial Management Controller from Motorola.

SMII. Serial Media Independent Interface.

SNMP. See "Simple Network Management Protocol" on page 408.

SODIMM. Small Outline Dual Inline Memory Module.

SRAM. Static Random Access Memory.

STP. Spanning Tree Protocol. See "802.1D" on page 397 for more information.

T

TBI. Ten Bit Interface.

Telnet. A character-based UNIX application that enables users with a Telnet server account to log on to a UNIX computer and utilize its resources.

TFTP. See "Trivial File Transfer Protocol" on page 409.

Trivial File Transfer Protocol.

TFTP is a simple form of the File Transfer Protocol (FTP). TFTP uses the User Datagram Protocol (UDP, a direct protocol used to communicate datagrams over a network with little error recovery) and provides no security features. It is often used by servers to boot diskless workstations, X-terminals, and routers.

Trunking. The process of combining a set of trunks that are traffic-engineered as a unit for the establishment of connections between switching systems in which all of the communications paths are interchangeable.

U

UPM. User Programmable Machine.

UPMA. The first of two UPMs in Motorola's MPC855T processor.

UPMB. The second of two UPMs in Motorola's MPC855T processor.

USP. An abbreviation that represents Unit, Slot, Port.

V

Virtual Local Area Network.

Operating at the Data Link Layer (Layer 2 of the OSI model), the VLAN is a means of parsing a single network into logical user groups or organizations, as if they physically resided on a dedicated LAN segment of their own. In reality, this virtually defined community may have individual members peppered across a large, extended LAN. The VLAN identifier is part of the 802.1Q tag, which is added to an Ethernet frame by an 802.1Q-compliant switch or router. Devices recognizing 802.1Q-tagged frames maintain appropriate tables to track VLANs. The first three bits of the 802.1Q tag are used by 802.1P to establish priority for the packet.

VLAN. See "Virtual Local Area Network" on page 410.

vMAN. Virtual Metropolitan Area Network.

W

WAN. See "Wide Area Network" on page 410.

Web. Also known as World-Wide Web (WWW) or W3. An Internet

client-server system to distribute information, based upon the hypertext transfer protocol (HTTP).

Wide Area Network. A WAN is a computer network that spans a relatively large geographical area. Typically, a WAN consists of two or more local-area networks (LANs).

X

X.500. A directory standard that enables applications like e-mail to access information that can either be central or distributed. The benefit of a directory is the ability to minimize the impact on the user of changes to a network. The standard is broken down under subsequent standards, as follows:

X.501 Models

X.509 Authentication framework

X.511 Abstract service definition

X.518 Procedures for distributed operation

X.519 Protocol specifications

X.520 Selected attribute types

X.521 Selected object types

XModem. One of the most popular file transfer protocols (FTPs). Xmodem is fairly effective at detecting errors. It sends blocks of data together with a checksum and then waits for acknowledgment of the block's receipt. The waiting

slows down the rate of data transmission considerably, but it ensures accurate transmission. Xmodem can be implemented either in software or in hardware. Many modems, and almost all communications software packages, support Xmodem. However, it is useful only at relatively slow data transmission speeds (less than 4,800 bps). Enhanced versions of Xmodem that work at higher transmission speeds are known as Ymodem and Zmodem.

Further support

■ Technical Questions

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

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

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

You can contact us

in the EMEA region at:

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

in the America region at:

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

in the Asia-Pacific region at:

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

■ Hirschmann Competence Center

The Hirschmann Competence Center is ahead of its competitors:

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

With the Hirschmann Competence Center, you have decided against making any compromises. Our client-customized package leaves you free to choose the service components you want to use.

Internet: <http://www.hicomcenter.com>



HIRSCHMANN

A **BELDEN** BRAND



HIRSCHMANN

A **BELDEN** BRAND

User Manual

Basic Configuration

Industrial ETHERNET (Gigabit-)Switch

RS20/RS30/RS40, MS20/MS30

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.

© 2015 Hirschmann Automation and Control GmbH

Manuals and software are protected by copyright. All rights reserved. The copying, reproduction, translation, conversion into any electronic medium or machine scannable form is not permitted, either in whole or in part. An exception is the preparation of a backup copy of the software for your own use. For devices with embedded software, the end-user license agreement on the enclosed CD/DVD applies.

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

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

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

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

Contents

	Safety Information	9
	About this Manual	11
	Key	13
	Introduction	15
1	Access to the user interfaces	17
1.1	System Monitor	18
1.2	Command Line Interface	21
1.3	Graphical User Interface	24
2	Entering the IP Parameters	27
2.1	IP Parameter Basics	29
2.1.1	IP Address (Version 4)	29
2.1.2	Netmask	30
2.1.3	Classless Inter-Domain Routing	34
2.2	Entering IP parameters via CLI	36
2.3	Entering the IP Parameters via HiDiscovery	39
2.4	Loading the system configuration from the ACA	41
2.5	System configuration via BOOTP	43
2.6	System Configuration via DHCP	48
2.7	System Configuration via DHCP Option 82	51
2.8	Graphical User Interface IP Configuration	52
2.9	Faulty Device Replacement	55
3	Loading/saving settings	57
3.1	Loading settings	58
3.1.1	Loading from the local non-volatile memory	59
3.1.2	Loading from a file	60
3.1.3	Resetting the configuration to the default settings	62
3.1.4	Loading from the AutoConfiguration Adapter	63

3.2	Saving settings	64
3.2.1	Saving locally (and on the ACA)	64
3.2.2	Saving in a binary file on a URL	66
3.2.3	Saving as an offline configuration file on the PC	67
3.3	Configuration Signature	68
4	Loading Software Updates	69
4.1	Loading the Software manually from the ACA	71
4.1.1	Selecting the software to be loaded	72
4.1.2	Starting the software	73
4.1.3	Performing a cold start	74
4.2	Automatic software update by ACA	75
4.3	Loading the software from the TFTP server	77
4.4	Loading the Software via File Selection	79
4.5	Bootcode Update via TFTP	80
4.5.1	Updating the Bootcode file	80
5	Configuring the Ports	83
6	Assistance in the Protection from Unauthorized Access	89
6.1	Protecting the device	90
6.2	Password for SNMP access	91
6.2.1	Description of password for SNMP access	91
6.2.2	Entering the password for SNMP access	92
6.3	HiDiscovery Access	100
6.3.1	Description of the HiDiscovery Protocol	100
6.3.2	Enabling/disabling the HiDiscovery function	100
6.4	Port access control	101
6.4.1	Description of the port access control	101
6.4.2	Application Example for Port Access Control	102
6.5	Login Banner	104
6.6	CLI Banner	105

7	Synchronizing the System Time in the Network	107
7.1	Setting the time	108
7.2	SNTP	110
	7.2.1 Description of SNTP	110
	7.2.2 Preparing the SNTP Configuration	111
	7.2.3 Configuring SNTP	112
7.3	Precision Time Protocol	115
	7.3.1 Description of PTP Functions	115
8	Network Load Control	119
8.1	Direct Packet Distribution	120
	8.1.1 Store and Forward	120
	8.1.2 Multi-Address Capability	120
	8.1.3 Aging of learned MAC addresses	121
	8.1.4 Entering Static Addresses	122
	8.1.5 Disabling the Direct Packet Distribution	123
8.2	Multicast Application	124
	8.2.1 Description of the Multicast Application	124
	8.2.2 Example of a Multicast Application	125
	8.2.3 Description of IGMP Snooping	126
	8.2.4 Setting IGMP Snooping	127
8.3	Rate Limiter	133
	8.3.1 Description of the Rate Limiter	133
	8.3.2 Rate limiter settings	134
8.4	QoS/Priority	136
	8.4.1 Description of Prioritization	136
	8.4.2 VLAN tagging	137
	8.4.3 IP ToS / DiffServ	139
	8.4.4 Handling of Received Priority Information	142
	8.4.5 Handling of traffic classes	143
	8.4.6 Setting prioritization	143
8.5	Flow Control	148
	8.5.1 Description of Flow Control	148
	8.5.2 Setting the Flow Control	150
8.6	VLANs	151
	8.6.1 VLAN Description	151
	8.6.2 Examples of VLANs	152

9	Operation Diagnosis	165
9.1	Sending Traps	166
9.1.1	List of SNMP traps	167
9.1.2	SNMP Traps when Booting	168
9.1.3	Configuring Traps	169
9.2	Monitoring the Device Status	171
9.2.1	Configuring the Device Status	172
9.2.2	Displaying the Device Status	173
9.3	Out-of-band Signaling	175
9.3.1	Controlling the Signal Contact	176
9.3.2	Monitoring the Device Status via the Signal Contact	177
9.3.3	Monitoring the Device Functions via the Signal Contact	177
9.4	Port Status Indication	179
9.5	Event Counter at Port Level	181
9.5.1	Detecting Non-matching Duplex Modes	182
9.6	Displaying the SFP Status	185
9.7	Topology Discovery	186
9.7.1	Description of Topology-Detection	186
9.7.2	Displaying the Topology Discovery Results	187
9.8	Detecting IP Address Conflicts	189
9.8.1	Description of IP Address Conflicts	189
9.8.2	Configuring ACD	190
9.8.3	Displaying ACD	190
9.9	Detecting Loops	191
9.10	Reports	192
9.11	Syslog	194
9.12	Trap log	197
A	Setting up the Configuration Environment	199
A.1	Setting up a DHCP/BOOTP Server	200
A.2	Setting up a DHCP Server with Option 82	206
A.3	TFTP Server for Software Updates	210
A.3.1	Setting up the TFTP Process	211
A.3.2	Software Access Rights	214
A.4	Service Shell	215

B	General Information	217
B.1	Management Information Base (MIB)	218
B.2	Abbreviations used	221
B.3	Technical Data	222
B.4	Readers' Comments	223
C	Index	225
D	Further Support	229

Safety Information



WARNING

UNCONTROLLED MACHINE ACTIONS

To avoid uncontrolled machine actions caused by data loss, configure all the data transmission devices individually.

Before you start any machine which is controlled via data transmission, be sure to complete the configuration of all data transmission devices.

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

About this Manual

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

The following thematic sequence has proven itself in practice:

- ▶ Set up device access for operation by entering the IP parameters
- ▶ Check the status of the software and update it if necessary
- ▶ Load/store any existing configuration
- ▶ Configure the ports
- ▶ Set up protection from unauthorized access
- ▶ Optimize the data transmission with network load control
- ▶ Synchronize system time in the network
- ▶ Perform an operation diagnosis
- ▶ Store the newly created configuration in the non-volatile memory

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

The “Redundancy Configuration” user manual document contains the information you require to select the 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 IO.

The “GUI” reference manual contains detailed information on using the graphical interface to operate the individual functions of the device.

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

The Industrial HiVision network management software provides you with additional options for smooth configuration and monitoring:

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

■ **Maintenance**

Hirschmann are continually working on improving and developing their software. Check regularly whether there is an updated version of the software that provides you with additional benefits. You find information and software downloads on the Hirschmann product pages on the Internet (www.hirschmann.com).

Key

The designations used in this manual have the following meanings:

	List
<input type="checkbox"/>	Work step
	Subheading
Link	Cross-reference with link
Note:	A note emphasizes an important fact or draws your attention to a dependency.
<code>Courier</code>	ASCII representation in the graphical user interface
	Execution in the Graphical User Interface
	Execution in the Command Line Interface

Symbols used:

	WLAN access point
	Router with firewall
	Switch with firewall
	Router
	Switch

Key



Bridge



Hub



A random computer



Configuration Computer



Server



PLC -
Programmable logic
controller



I/O -
Robot

Introduction

The device has been developed for use in a harsh industrial environment. Accordingly, the installation process has been kept simple. Thanks to the selected default settings, you only have to enter a few settings before starting to operate the device.

Note: The changes you make in the dialogs are copied into the volatile memory of the device when you click on "Set". To save the changes to the device into permanent memory, select the saving location in the `Basic Settings:Load/Save` dialog box and click on "Save".

1 Access to the user interfaces

The device has 3 user interfaces, which you can access via different interfaces:

- ▶ System monitor via the V.24 interface (out-of-band)
- ▶ Command Line Interface (CLI) via the V.24 connection (out-of-band) and Telnet (in-band)
- ▶ Graphical User Interface via Ethernet (in-band).

1.1 System Monitor

The system monitor enables you to

- ▶ select the software to be loaded
- ▶ perform a software update
- ▶ start the selected software
- ▶ shut down the system monitor
- ▶ delete the configuration saved and
- ▶ display the boot code information.

■ Starting the System Monitor

Prerequisites

- ▶ Terminal cable for connecting the device to your PC (available as an optional accessory).
- ▶ PC with VT100 terminal emulation (such as PuTTY) or serial terminal

Perform the following work steps:

- Use the terminal cable to connect the V.24 port of the device with the “COM” port of the PC.
- Start the VT100 terminal emulation on the PC.
- Define the following transmission parameters:
 - Speed: 9600 Baud
 - Data: 8 bit
 - Parity: None
 - Stopbit: 1 bit
 - Flow control: None

Speed	9600 Baud
Data	8 bit
Parity	None
Stopbit	1 bit
Handshake	Off

Table 1: Data transfer parameters

- Start the terminal program on the PC and set up a connection with the device.

When you boot the device, the message "Press <1> to enter System Monitor 1" appears on the terminal.

```
< Device Name (Boot) Release: 1.00 Build: 2005-09-17 15:36 >
Press <1> to enter System Monitor 1 ...
1
```

Figure 1: Screen display during the boot process

- Press the <1> key within one second to start system monitor 1.

```
System Monitor
```

```
(Selected OS: L3P-06.0.00 (2010-09-09 09:09))
```

- ```
1 Select Boot Operating System
2 Update Operating System
3 Start Selected Operating System
4 End (reset and reboot)
5 Erase main configuration file
```

```
sysMon1>
```

---

*Figure 2: System monitor 1 screen display*

- Select a menu item by entering the number.
- To leave a submenu and return to the main menu of system monitor 1, press the <ESC> key.

## 1.2 Command Line Interface

The Command Line Interface enables you to use the functions of the device via a local or remote connection.

The Command Line Interface provides IT specialists with a familiar environment for configuring IT devices.

The script compatibility of the Command Line Interface enables you, among other things, to feed multiple devices with the same configuration data, to create and use partial configurations, or to compare 2 configurations using 2 script files.

You will find a detailed description of the Command Line Interface in the “Command Line Interface” reference manual.

You can access the Command Line Interface via:

- ▶ the V.24 port (out-of-band)
- ▶ Telnet (in-band)

**Note:** To facilitate making entries, the CLI gives you the option of abbreviating keywords. Type in the beginning of a keyword. When you press the tab key, the CLI finishes the keyword.

### ■ Opening the Command Line Interface

- Connect the device to a terminal or to a “COM” port of a PC using terminal emulation based on VT100, and press any key (see on page 18 “System Monitor”) or call up the Command Line Interface via Telnet. A window for entering the user name appears on the screen. Up to 5 users can access the Command Line Interface.

---

Copyright (c) 2004-2010 Hirschmann Automation and Control GmbH

All rights reserved

PowerMICE Release L3P-06.0.00

(Build date 2010-09-09 12:13)

```
System Name: PowerMICE
Mgmt-IP : 10.0.1.105
1.Router-IP: 0.0.0.0
Base-MAC : 00:80:63:51:74:00
System Time: 2010-09-09 13:14:15
```

User:

---

*Figure 3: Logging in to the Command Line Interface program*

- Enter a user name. The default setting for the user name is **admin** . Press the Enter key.
- Enter the password. The default setting for the password is **private** . Press the Enter key.  
You can change the user name and the password later in the Command Line Interface.  
Please note that these entries are case-sensitive.

The start screen appears.

---

NOTE: Enter '?' for Command Help. Command help displays all options that are valid for the 'normal' and 'no' command forms. For the syntax of a particular command form, please consult the documentation.

(Hirschmann Product) >

---

*Figure 4: CLI screen after login*

## 1.3 Graphical User Interface

The graphical user Interface (GUI) allows you to conveniently define and monitor the settings of the device from a computer on the network.

You reach the graphical user interface (GUI) with the following programs:

- ▶ HiView
- ▶ Web browser

### ■ System requirements

Use HiView to open the graphical user interface. This application offers you the possibility to use the graphical user interface without other applications such as a Web browser or an installed Java Runtime Environment (JRE).

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

### ■ Starting the graphical user interface

The prerequisite for starting the graphical user interface, first configure the IP parameters of the device correctly.

Starting the graphical user interface in HiView:

- Start HiView.
- In the URL field of the start window, enter the IP address of your device.
- Click "Open".

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

Start the graphical user interface in the Web browser:

- This requires that Java is enabled in the security settings of your Web browser.
- Start your Web browser.
- Write the IP address of the device in the address field of the Web browser. Use the following form: `https://xxx.xxx.xxx.xxx`

The Web browser sets up the connection to the device and displays the login window.

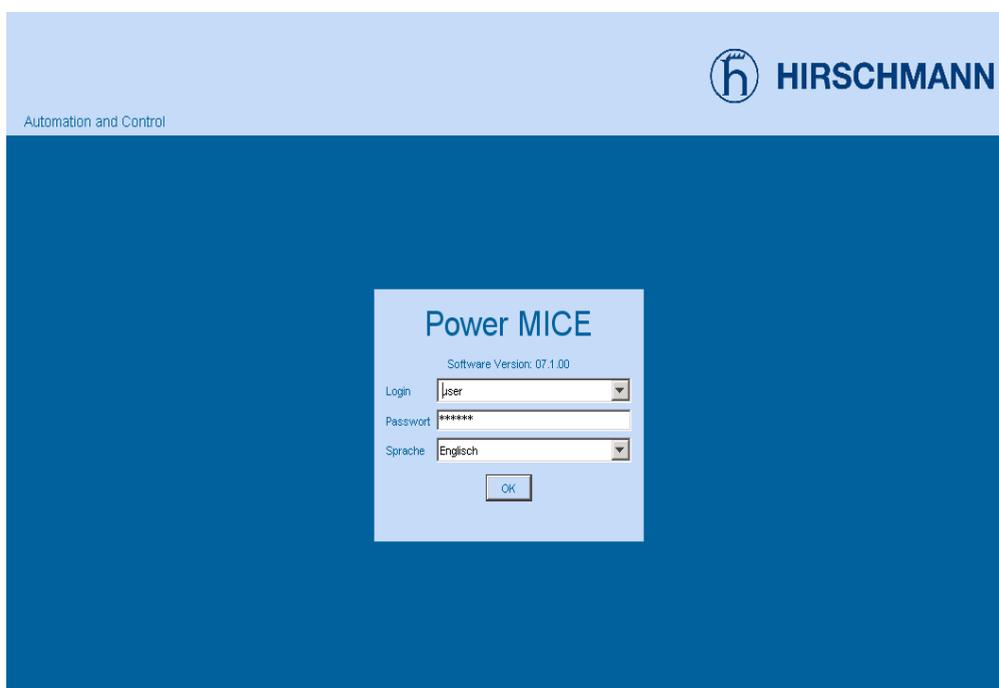


Figure 5: Login window

- Select the user name and enter the password.
  - Select the user name `user` to have read access to the device.
  - Select the user name `admin` to have read and write access to the device.
- Select the language in which you want to use the graphical user interface.
- Click "Ok".

The Web browser displays the graphical user interface.



## 2 Entering the IP Parameters

When you install the device for the first time enter the IP parameters.

The device provides the following options for entering the IP parameters during the first installation:

- ▶ Entry using the Command Line Interface (CLI).  
You choose this “out of band” method if
  - ▶ you preconfigure your device outside its operating environment, or
  - ▶ you need to restore network access (“in-band”) to the device
- ▶ Entry using the HiDiscovery protocol.  
You choose this “in-band” method on a previously installed network device or if you have another Ethernet connection between your PC and the device
- ▶ Configuration using the AutoConfiguration Adapter (ACA).  
You choose this method if you are replacing a device with a device of the same type and have already saved the configuration on anACA.
- ▶ Using BOOTP.  
You choose this “in-band” method to configure the installed device using BOOTP. You need a BOOTP server for this method. The BOOTP server assigns the configuration data to the device using its MAC address. The DHCP mode is the default mode for the configuration data reference, set the parameter to the BOOTP mode for this method.
- ▶ Configuration via DHCP.  
You choose this “in-band” method to configure the installed device using DHCP. You need a DHCP server for this method. The DHCP server assigns the configuration data to the device using its MAC address or its system name.

- ▶ Configuration via DHCP Option 82.  
You choose this “in-band” method if you want to configure the installed device using DHCP Option 82. You need a DHCP server with Option 82 for this. The DHCP server assigns the configuration data to the device using its physical connection ([see on page 51 “System Configuration via DHCP Option 82”](#)).
- ▶ Configuration using the graphical user interface.  
If the device already has an IP address and is reachable via the network, then the graphical user interface provides you with another option for configuring the IP parameters.

---

## 2.1 IP Parameter Basics

### 2.1.1 IP Address (Version 4)

The IP addresses consist of 4 bytes. These 4 bytes are written in decimal notation, separated by a decimal point.

Since 1992, five classes of IP address have been defined in the RFC 1340.

| Class | Network address | Host address | Address range                |
|-------|-----------------|--------------|------------------------------|
| A     | 1 byte          | 3 bytes      | 0.0.0.0 to 127.255.255.255   |
| B     | 2 bytes         | 2 bytes      | 128.0.0.0 to 191.255.255.255 |
| C     | 3 bytes         | 1 byte       | 192.0.0.0 to 223.255.255.255 |
| D     |                 |              | 224.0.0.0 to 239.255.255.255 |
| E     |                 |              | 240.0.0.0 to 255.255.255.255 |

Table 2: IP address classes

The network address is the fixed part of the IP address. The worldwide leading regulatory board for assigning network addresses is the IANA (Internet Assigned Numbers Authority). If you require an IP address block, contact your Internet service provider. Internet service providers should contact their local higher-level organization:

- ▶ APNIC (Asia Pacific Network Information Center) - Asia/Pacific Region
- ▶ ARIN (American Registry for Internet Numbers) - Americas and Sub-Saharan Africa
- ▶ LACNIC (Regional Latin-American and Caribbean IP Address Registry) – Latin America and some Caribbean Islands
- ▶ RIPE NCC (Réseaux IP Européens) - Europe and Surrounding Regions

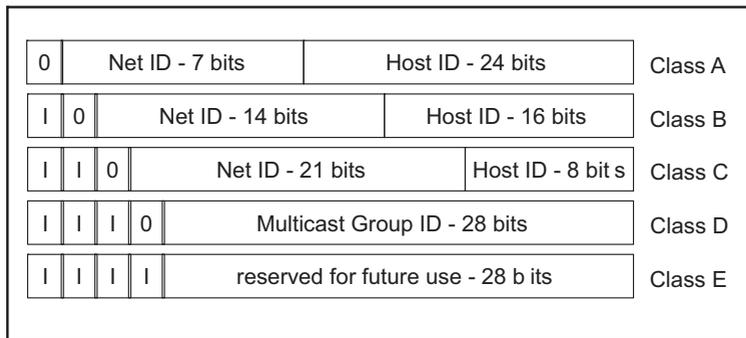


Figure 6: Bit representation of the IP address

All IP addresses belong to class A when their first bit is a zero, i.e. the first decimal number is less than 128.

The IP address belongs to class B if the first bit is a one and the second bit is a zero, i.e. the first decimal number is between 128 and 191.

The IP address belongs to class C if the first two bits are a one, i.e. the first decimal number is higher than 191.

Assigning the host address (host ID) is the responsibility of the network operator. He alone is responsible for the uniqueness of the IP addresses he assigns.

## 2.1.2 Netmask

Routers and gateways subdivide large networks into subnetworks. The netmask assigns the IP addresses of the individual devices to a particular subnetwork.

The division into subnetworks with the aid of the netmask is performed in much the same way as the division of the network addresses (net id) into classes A to C.

The bits of the host address (host id) that represent the mask are set to one. The remaining bits of the host address in the netmask are set to zero (see the following examples).

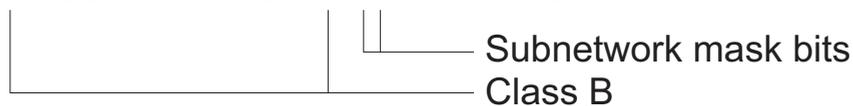
Example of a netmask:

Decimal notation

255.255.192.0

Binary notation

11111111.11111111.11000000.00000000

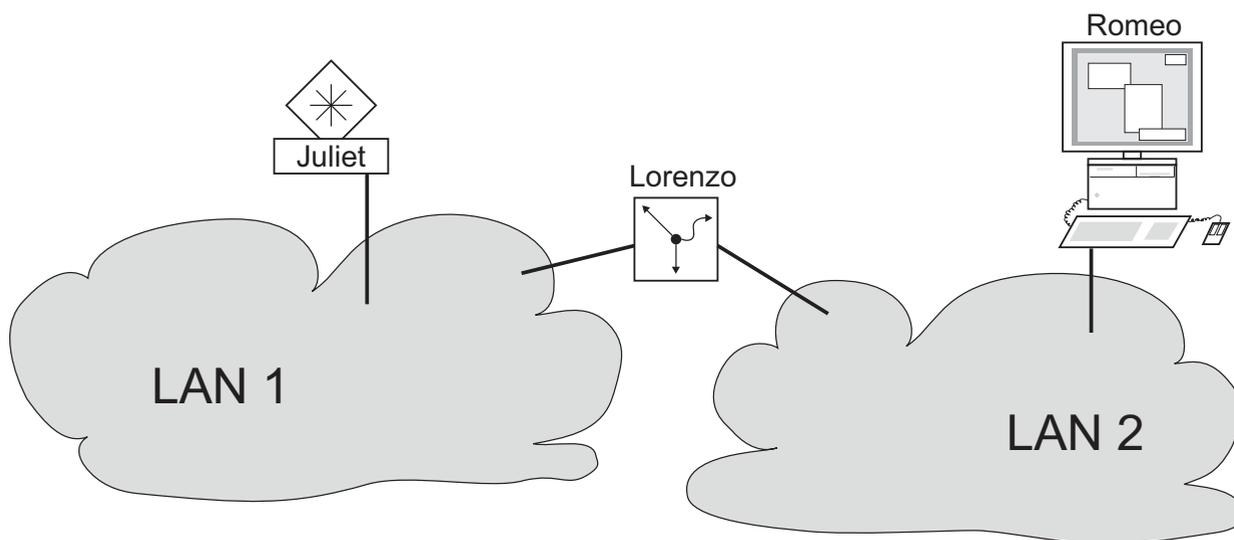


Example of IP addresses with subnetwork assignment when the above subnet mask is applied:



**■ Example of how the network mask is used**

In a large network it is possible that gateways and routers separate the management agent from its management station. How does addressing work in such a case?



*Figure 7: Management agent that is separated from its management station by a router*

The management station "Romeo" wants to send data to the management agent "Juliet". Romeo knows Juliet's IP address and also knows that the router "Lorenzo" knows the way to Juliet.

Romeo therefore puts his message in an envelope and writes Juliet's IP address as the destination address. For the source address he writes his own IP address on the envelope.

Romeo then places this envelope in a second one with Lorenzo's MAC address as the destination and his own MAC address as the source. This process is comparable to going from layer 3 to layer 2 of the ISO/OSI base reference model.

Finally, Romeo puts the entire data packet into the mailbox. This is comparable to going from layer 2 to layer 1, i.e. to sending the data packet over the Ethernet.

Lorenzo receives the letter and removes the outer envelope. From the inner envelope he recognizes that the letter is meant for Juliet. He places the inner envelope in a new outer envelope and searches his address list (the ARP table) for Juliet's MAC address. He writes her MAC address on the outer envelope as the destination address and his own MAC address as the source address. He then places the entire data packet in the mail box.

Juliet receives the letter and removes the outer envelope. She finds the inner envelope with Romeo's IP address. Opening the inner envelope and reading its contents corresponds to transferring the message to the higher protocol layers of the SO/OSI layer model.

Juliet would now like to send a reply to Romeo. She places her reply in an envelope with Romeo's IP address as destination and her own IP address as source. But where is she to send the answer? For she did not receive Romeo's MAC address. It was lost when Lorenzo replaced the outer envelope.

In the MIB, Juliet finds Lorenzo listed under the variable `hmNetGatewayIPAddr` as a means of communicating with Romeo. She therefore puts the envelope with the IP addresses in a further envelope with Lorenzo's MAC destination address.

The letter now travels back to Romeo via Lorenzo, the same way the first letter traveled from Romeo to Juliet.

### **2.1.3 Classless Inter-Domain Routing**

Class C with a maximum of 254 addresses was too small, and class B with a maximum of 65,534 addresses was too large for most users. This resulted in ineffective usage of the class B addresses available.

Class D contains reserved multicast addresses. Class E is reserved for experimental purposes. A gateway not participating in these experiments ignores datagrams with these destination addresses.

Since 1993, RFC 1519 has been using Classless Inter-Domain Routing (CIDR) to provide a solution. CIDR overcomes these class boundaries and supports classless address ranges.

With CIDR, you enter the number of bits that designate the IP address range. You represent the IP address range in binary form and count the mask bits that designate the netmask. The netmask indicates the number of bits that are identical to the network part for the IP addresses in a given address range. Example:

| IP address, decimal             | Network mask, decimal | IP address, binary                                                                 |
|---------------------------------|-----------------------|------------------------------------------------------------------------------------|
| 149.218.112.1                   | 255.255.255.128       | 10010101 11011010 01110000 00000001                                                |
| 149.218.112.127                 |                       | 10010101 11011010 01110000 01111111                                                |
|                                 |                       |  |
| CIDR notation: 149.218.112.0/25 |                       |                                                                                    |
|                                 |                       |   |

The combination of a number of class C address ranges is known as “supernetting”. This enables you to subdivide class B address ranges to a very fine degree.

## 2.2 Entering IP parameters via CLI

If you do not configure the system via BOOTP/DHCP, DHCP Option 82, the HiDiscovery protocol or the AutoConfiguration Adapter ACA, then you perform the configuration via the V.24 interface using the CLI.

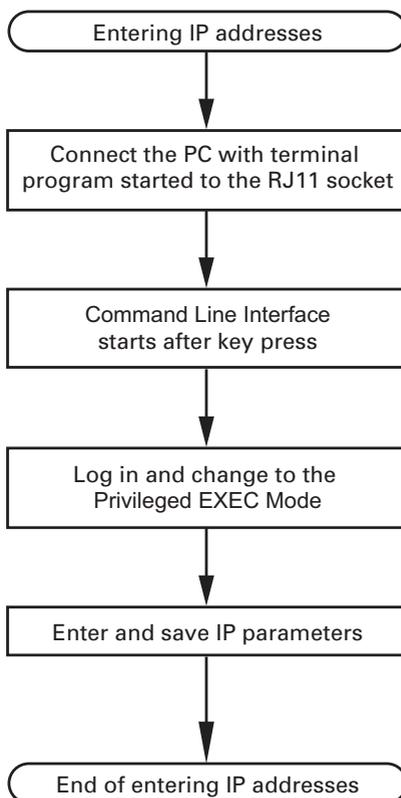


Figure 8: Flow chart for entering IP addresses

**Note:** If a terminal or PC with terminal emulation is unavailable in the vicinity of the installation location, you can configure the device at your own workstation, then take it to its final installation location.

- Set up a connection to the device (see on page 18 “Starting the System Monitor”).

The start screen appears.

---

NOTE: Enter '?' for Command Help. Command help displays all options that are valid for the 'normal' and 'no' command forms. For the syntax of a particular command form, please consult the documentation.

(Hirschmann PowerMICE) >

---

- Deactivate DHCP.
- Enter the IP parameters.
  - ▶ Local IP address  
On delivery, the device has the local IP address 0.0.0.0.
  - ▶ Netmask  
If you divided your network into subnetworks, and if these are identified with a netmask, then enter the netmask here.

The default setting of the netmask is 0.0.0.0.

► IP address of the gateway.

You require this entry when installing the device in a different subnetwork as the management station or TFTP server ([see on page 33 “Example of how the network mask is used”](#)).

Enter the IP address of the gateway between the subnetwork with the device and the path to the management station.

The default setting of the IP address is 0.0.0.0.

□ Save the configuration entered using

```
copy system:running-config nvram:startup-config.
```

```
enable
network protocol none
network parms 10.0.1.23
 255.255.255.0

copy system:running-config
 nvram:startup-config
```

Switch to the privileged EXEC mode.

Deactivate DHCP.

Assign the device the IP address 10.0.1.23 and the netmask 255.255.255.0. You have the option of also assigning a gateway address.

Save the current configuration to the non-volatile memory.

After entering the IP parameters, you easily configure the device via the graphical user interface (see the “GUI” reference manual).

## 2.3 Entering the IP Parameters via HiDiscovery

The HiDiscovery protocol enables you to assign IP parameters to the device via the Ethernet.

You can easily configure other parameters via the graphical user interface (see the "GUI" Graphic User Interface reference manual).

Install the HiDiscovery software on your PC. The software is on the CD supplied with the device.

To install it, you start the installation program on the CD.

Start the HiDiscovery program.

When you start HiDiscovery, it automatically searches the network for those devices which support the HiDiscovery protocol.

HiDiscovery uses the first network interface found for the PC. If your computer has several network cards, you select the one you desire in the HiDiscovery toolbar.

HiDiscovery displays a line for every device that reacts to the HiDiscovery protocol.

HiDiscovery enables you to identify the devices displayed.

Select a device line.

Click the „Signal“ symbol on the tool bar to set the LEDs for the selected device to flashing on. To switch off the flashing, click on the symbol again.

By double-clicking a line, you open a window in which you enter the device name and the IP parameters.

**Note:** When the IP address is entered, the device copies the local configuration settings ([see on page 57 “Loading/saving settings”](#)).

**Note:** For security reasons, switch off the HiDiscovery function for the device in the graphical user interface, after you have assigned the IP parameters to the device ([see on page 52 “Graphical User Interface IP Configuration”](#)).

**Note:** Save the settings so that you will still have the entries after a restart ([see on page 57 “Loading/saving settings”](#)).

## 2.4 Loading the system configuration from the ACA

The AutoConfiguration Adapter (ACA) is a device for

- ▶ for saving the device configuration data and
- ▶ saving the device software.

If a device becomes inoperative, the ACA allows you to transfer the configuration data to a replacement device of the same type.

When you start the device, it checks to see whether an ACA is present. If an ACA is present with a valid password and valid software, the device loads the configuration data from the ACA.

The password is valid if

- ▶ the entered password matches the password in the ACA, or
- ▶ the preset password in the device is entered.

To save the configuration data in the ACA, [See 64 “Saving locally \(and on the ACA\)”](#).

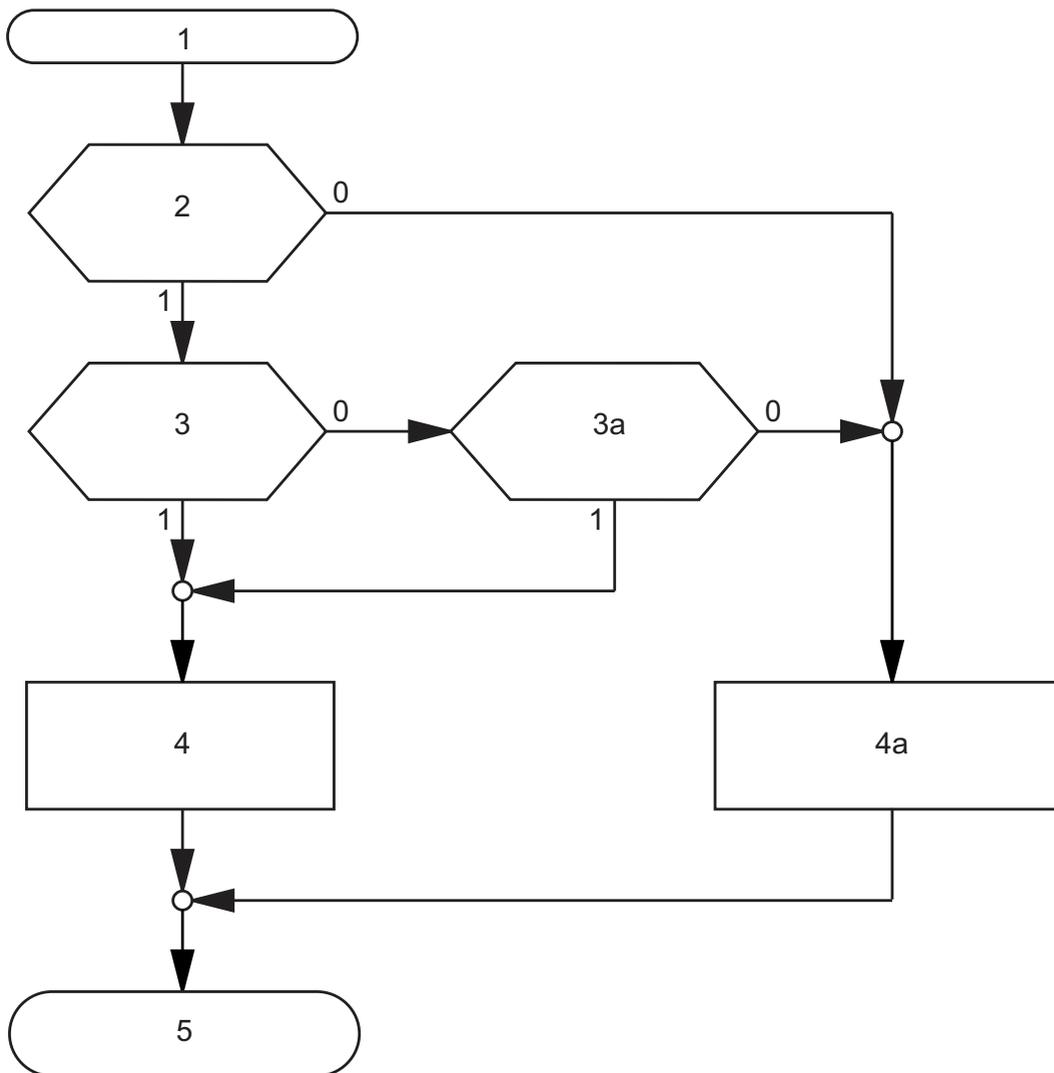


Figure 9: Flow chart of loading configuration data from the ACA

- 1 – Device start-up
- 2 – ACA plugged-in?
- 3 – Password in device and ACA identical?
- 3a – Default password in device?
- 4 – Load configuration from ACA, ACA LEDs flashing synchronously
- 4a – Load configuration from local memory, ACA LEDs flashing alternately
- 5 – Configuration data loaded

## 2.5 System configuration via BOOTP

When it is started up via BOOTP (bootstrap protocol), a device receives its configuration data in accordance with the “BOOTP process” flow chart ([see figure 10](#)).

**Note:** In its delivery state, the device gets its configuration data from the DHCP server.

- Activate BOOTP to receive the configuration data ([see on page 52 “Graphical User Interface IP Configuration”](#)), or see the CLI:

|                                                      |                                     |
|------------------------------------------------------|-------------------------------------|
| enable                                               | Switch to the privileged EXEC mode. |
| network protocol bootp                               | Activate BOOTP.                     |
| copy system:running-config<br>nvrnram:startup-config | Activate BOOTP.                     |
| y                                                    | Confirm save.                       |

- Provide the BOOTP server with the following data for a device:

```
/etc/bootptab for BOOTP-daemon bootpd
#
gw -- gateway
ha -- hardware address
ht -- hardware type
ip -- IP address
sm -- subnet mask
tc -- template

.global:\
:gw=0.0.0.0:\
:sm=255.255.240.0:
```

```
switch_01:ht=ethernet:ha=008063086501:ip=10.1.112.83:tc=.global:
switch_02:ht=ethernet:ha=008063086502:ip=10.1.112.84:tc=.global:
.
.
```

Lines that start with a '#' character are comment lines.

The lines under ".global:" make the configuration of several devices easier. With the template (tc) you allocate the global configuration data (tc=.global:) to each device .

The direct allocation of hardware address and IP address is performed in the device lines (switch-0...).

- Enter one line for each device.
- After ha= enter the hardware address of the device.
- After ip= enter the IP address of the device.

In the appendix, you will find an example for the configuration of a BOOTP/DHCP server.

[See "Setting up a DHCP/BOOTP Server" on page 200.](#)

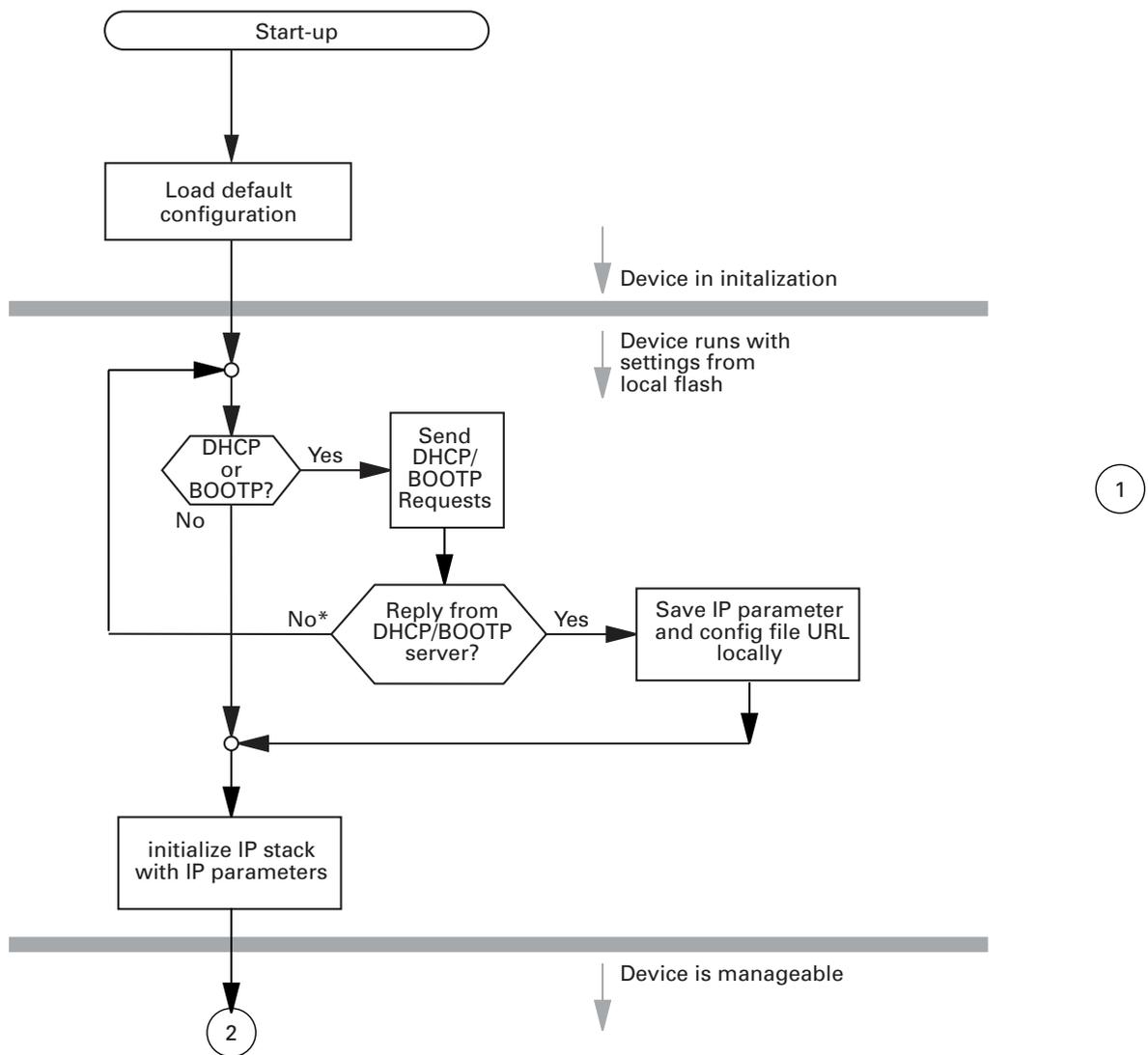


Figure 10: Flow chart for the BOOTP/DHCP process, part 1  
 \* see note [figure 11](#)

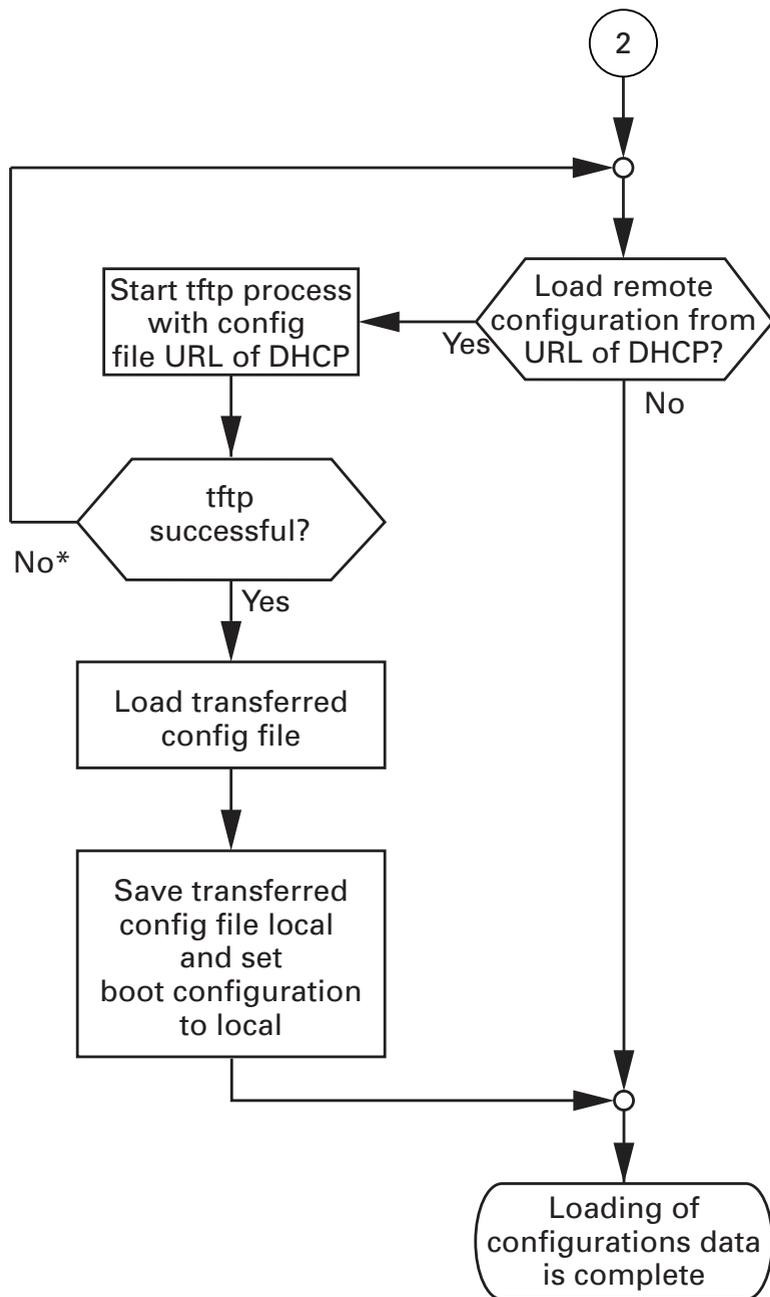


Figure 11: Flow chart for the BOOTP/DHCP process, part 2

**Note:** The loading process started by DHCP/BOOTP ([see on page 43 “System configuration via BOOTP”](#)) shows the selection of “from URL & save locally” 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.

## 2.6 System Configuration via DHCP

The DHCP (Dynamic Host Configuration Protocol) is a further development of BOOTP, which it has replaced. The DHCP additionally allows the configuration of a DHCP client via a name instead of via the MAC address. For the DHCP, this name is known as the “client identifier” in accordance with RFC 2131.

The device uses the name entered under sysName in the system group of the MIB II as the client identifier. You can enter this system name directly via SNMP, the Web-based management (see system dialog), or the Command Line Interface.

During startup operation, a device receives its configuration data according to the “DHCP process” flowchart ([see figure 10](#)).

The device sends its system name to the DHCP server. The DHCP server can then use the system name to allocate an IP address as an alternative to the MAC address.

In addition to the IP address, the DHCP server sends

- ▶ the netmask
- ▶ the default gateway (if available)
- ▶ the tftp URL of the configuration file (if available)

The device accepts this data as configuration parameters ([see on page 52 “Graphical User Interface IP Configuration”](#)). If an IP address was assigned by a DHCP server, it will be permanently saved locally.

| Option | Meaning     |
|--------|-------------|
| 1      | Subnet Mask |
| 2      | Time Offset |
| 3      | Router      |
| 4      | Time server |

Table 3: DHCP options which the device requests

| Option | Meaning           |
|--------|-------------------|
| 12     | Host Name         |
| 42     | NTP server        |
| 61     | Client Identifier |
| 66     | TFTP Server Name  |
| 67     | Bootfile Name     |

*Table 3: DHCP options which the device requests*

The advantage of using DHCP instead of BOOTP is that the DHCP server can restrict the validity of the configuration parameters (“Lease”) to a specific time period (known as dynamic address allocation). Before this period (“Lease Duration”) elapses, the DHCP client can attempt to renew this lease. Alternatively, the client can negotiate a new lease. The DHCP server then allocates a random free address.

To help avoid this, DHCP servers provide the explicit configuration option of assigning a specific client the same IP address based on a unique hardware ID (known as static address allocation).

On delivery, DHCP is activated. As long as DHCP is activated, the device attempts to obtain an IP address. If it cannot find a DHCP server after restarting, it will not have an IP address. Activate or deactivate DHCP in the `Basic Settings:Network:Global` dialog.

**Note:** When using Industrial HiVision network management, the user checks to see that DHCP allocates the original IP address to each device every time.

The appendix contains an example configuration of the BOOTP/DHCP-server .(see on page 200 “[Setting up a DHCP/BOOTP Server](#)”)

Example of a DHCP-configuration file:

```
/etc/dhcpd.conf for DHCP Daemon
#
subnet 10.1.112.0 netmask 255.255.240.0 {
option subnet-mask 255.255.240.0;
option routers 10.1.112.96;
```

```
}
#
Host berta requests IP configuration
with her MAC address
#
host berta {
hardware ethernet 00:80:63:08:65:42;
fixed-address 10.1.112.82;
}
#
Host hugo requests IP configuration
with his client identifier.
#
host hugo {
#
option dhcp-client-identifier "hugo";
option dhcp-client-identifier 00:68:75:67:6f;
fixed-address 10.1.112.83;
server-name "10.1.112.11";
filename "/agent/config.dat";
}
```

Lines that begin with the #-character contain comments.

The lines that precede the individual devices indicate settings that apply to the following device.

The fixed-address line assigns a fixed IP address to the device.

Please refer to your DHCP-Server manual for more details.

## 2.7 System Configuration via DHCP Option 82

As with the classic DHCP, on startup an agent receives its configuration data according to the “BOOTP/DHCP process” flow chart (see figure 10).

While the system configuration is based on the classic DHCP protocol on the device being configured (see on page 48 “System Configuration via DHCP”), Option 82 is based on the network topology. This procedure gives you the option of assigning the same IP address to any device which is connected to a particular location (port of a device) on the LAN.

The installation of a DHCP server is described in the chapter “Setting up a DHCP Server with Option 82” on page 206.

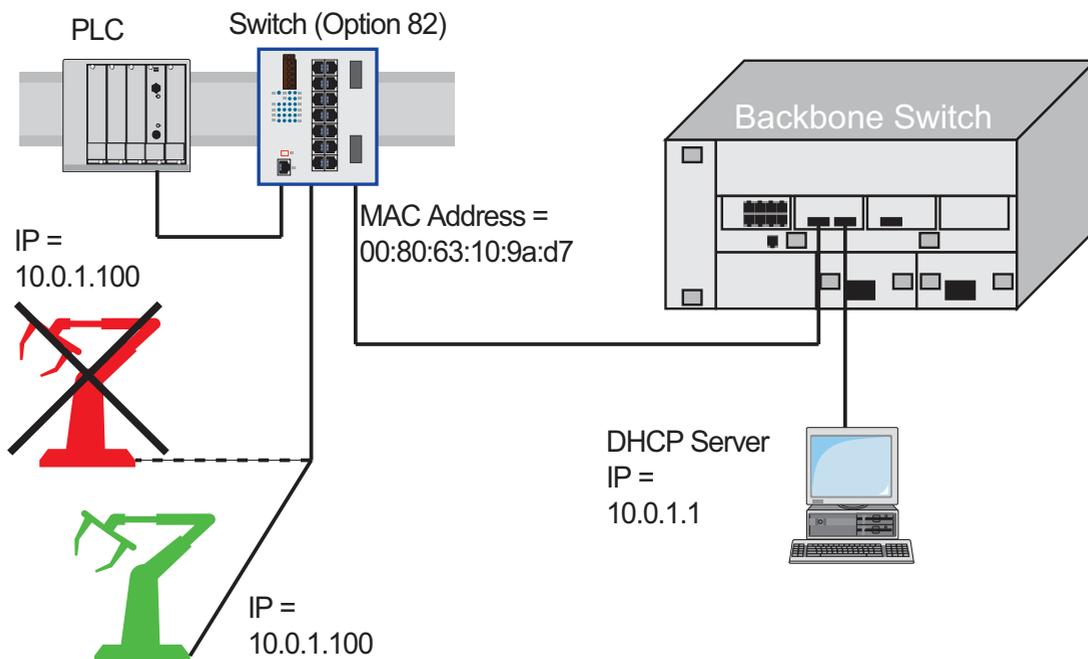


Figure 12: Application example of using Option 82

## 2.8 Graphical User Interface IP Configuration

Use the `Basic Settings:Network` dialog to define the source from which the device receives its IP parameters after startup, assign the IP parameters and VLAN ID, and configure the HiDiscovery access.

Figure 13: Network parameters dialog

- Under “Mode”, you enter where the device gets its IP parameters:
  - ▶ In the BOOTP mode, the configuration is via a BOOTP or DHCP server on the basis of the MAC address of the device.  
See [“Setting up a DHCP/BOOTP Server” on page 200.](#)
  - ▶ 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 [“Setting up a DHCP Server with Option 82” on page 206.](#)
  - ▶ 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 `Basic Settings: System` dialog of the graphical user interface.
- The “VLAN” frame enables you to assign a VLAN to the management CPU of the device. If you enter 0 here as the VLAN ID (not included in the VLAN standard version), the management CPU will then be accessible from all VLANs.
- The HiDiscovery protocol allows you to allocate an IP address to the device. Activate the HiDiscovery protocol if you want to allocate an IP address to the device from your PC with the enclosed HiDiscovery software (default setting: “Operation” On, “Access” read-write).

**Note:** Save the settings so that you will still have the entries after a restart (see on page 57 “Loading/saving settings”).

## 2.9 Faulty Device Replacement

The device provides 2 plug-and-play solutions for replacing a faulty device with a device of the same type (faulty device replacement):

- ▶ Configuring the new device using an AutoConfiguration Adapter ([see on page 41 “Loading the system configuration from the ACA”](#)) or
- ▶ configuration via DHCP Option 82 ([see on page 206 “Setting up a DHCP Server with Option 82”](#))

In both cases, when the new device is started, it is given the same configuration data that the replaced device had.

**Note:** If you are replacing a device with DIP switches, check the DIP switch settings to ensure they are the same.



## 3 Loading/saving settings

The device saves settings such as the IP parameters and the port configuration in the temporary memory. These settings are lost when you switch off or reboot the device.

The device allows you to do the following:

- ▶ Load settings from a non-volatile memory into the temporary memory
- ▶ Save settings from the temporary memory in a non-volatile memory

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

---

## 3.1 Loading settings

When it is restarted, the device loads its configuration data from the local non-volatile memory. The prerequisites for this are:

- ▶ You have not connected an AutoConfiguration Adapter (ACA) and
- ▶ the IP configuration is “local”.

During a restart, the device also allows you to load settings from the following sources:

- ▶ a binary file of the AutoConfiguration Adapter. If an ACA is connected to the device, the device automatically loads its configuration from the ACA during the boot procedure.

**Note:** Details of times required for a reboot:

- ▶ The time required for a cold start is the time taken by the device from the moment power is switched on until it is fully connected and its Management-CPU is fully accessible.
- ▶ Depending on the device type and the extent of the configuration settings, a cold start takes at least about 10 seconds.
- ▶ Extensive configuration settings will increase the time required for a reboot, especially if they contain a high number of VLANs. In extreme cases, a reboot can take up to about 200 seconds.
- ▶ A warm start is quicker, since in this case the device skips the software loading from NVRAM.

During operation, the device allows you to load settings from the following sources:

- ▶ the local non-volatile memory
- ▶ a file in the connected network (setting on delivery)
- ▶ a binary file and
- ▶ the firmware (restoration of the configuration on delivery).

**Note:** When loading a configuration, hold off any accesses to the device until it has loaded the configuration file and applied the new configuration settings. Depending on the device type and the extent of the configuration settings, this process can take between 10 and 200 seconds.

### 3.1.1 Loading from the local non-volatile memory

When loading the configuration data locally, the device loads the configuration data from the local non-volatile memory if no ACA is connected to the device.

- Select the `Basics: Load/Save` dialog.
- In the “Load” frame, click “from Device”.
- Click “Restore”.

```
enable
copy nvram:startup-config
system:running-config
```

Switch to the privileged EXEC mode.

The device loads the configuration data from the local non-volatile memory.

### 3.1.2 Loading from a file

The device allows you to load the configuration data from a file in the connected network if there is no AutoConfiguration Adapter connected to the device.

- Select the `Basics: Load/Save` dialog.
- In the “Load” frame, click
  - ▶ “from URL” if you want the device to load the configuration data from a file and retain the locally saved configuration.
  - ▶ “from URL & save to Switch” if you want the device to load the configuration data from a file and save this configuration locally.
  - ▶ “via PC” if you want the device to load the configuration data from a file on the PC and retain the locally saved configuration.
- In the “URL” frame, enter the path under which the device will find the configuration file, if you want to load from the URL.
- Click “Restore”.

**Note:** When restoring a configuration using one of the options in the “Load” frame, note the following particulars:

- ▶ The device can restore the configuration from a binary or script file:
  - The option “from Device” restores the configuration exclusively from the device-internal binary file.
  - The 3 options “from URL”, “from URL and save to Device” or “via PC” can restore the configuration both from a binary file and from a script file. The script file can be an offline configuration file (\*.ocf) or a CLI script file (\*.cli). The device determines the file type automatically.
- ▶ When restoring the configuration from a script file, you first delete the device configuration so that the default settings are overwritten correctly. For further information ([see on page 62 “Resetting the configuration to the default settings”](#))

The URL identifies the path to the tftp server from which the device loads the configuration file. The URL is in the format `tftp://IP address of the tftp server/path name/file name` (e.g. `tftp://10.1.112.5/switch/config.dat`).

### Example of loading from a tftp server

- Before downloading a file from the tftp server, you have to save the configuration file in the corresponding path of the tftp servers with the file name, e.g. `switch/switch_01.cfg` (see on page 66 “Saving in a binary file on a URL”).
- In the “URL” line, enter the path of the tftp server, e.g. `tftp://10.1.112.214/switch/switch_01.cfg`.

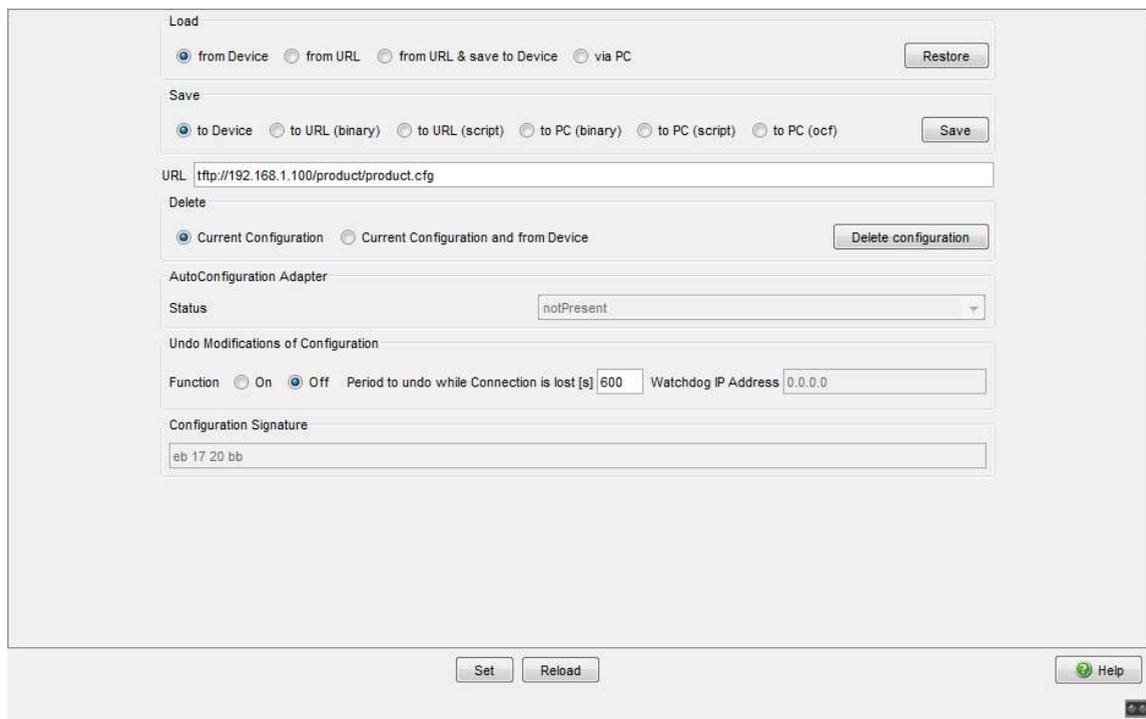


Figure 14: Load/Save dialog

```
enable
copy
tftp://10.1.112.159/switch/c
onfig.dat
nvram:startup-config
```

Switch to the privileged EXEC mode.

The device loads the configuration data from a tftp server in the connected network.

---

**Note:** The loading process started by DHCP/BOOTP ([see on page 43](#) “System configuration via BOOTP”) shows the selection of “from URL & save locally” 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.

### 3.1.3 Resetting the configuration to the default settings

The device enables you to

- ▶ reset the current configuration to the default setting. The locally saved configuration is kept.
- ▶ reset the device to the default setting. After the next restart, the IP address is also in the default setting.

- Select the Basics: Load/Save dialog.
- Make your selection in the "Delete" frame.
- Click "Delete configuration". The device will delete its configuration immediately.

Resetting the device using the system monitor

- Select 5 “Erase main configuration file”  
This menu item allows you to reset the current configuration, stored in non volatile memory, to its default setting. The device also stores a backup configuration, and a configuration associated with the firmware, in its Flash memory.
- Press the Enter key to delete the configuration file.

### 3.1.4 Loading from the AutoConfiguration Adapter

#### ■ Loading a configuration during the boot procedure

If you connect an ACA to the device and if the passwords on the device are in the default setting, missing, or the same as those on the ACA, the device automatically loads its configuration from the ACA during the boot procedure. After booting, the device updates its configuration in the local non-volatile memory with the configuration from the ACA.

**Note:** During the boot procedure, the configuration on the ACA has priority over the configuration in the local non-volatile memory.

The chapter [“Saving locally \(and on the ACA\)” on page 64](#) describes how you can save a configuration file on an ACA.

#### ■ Reporting configuration differences

The device allows you to trigger the following events when the configuration stored on the ACA does not match the configuration on the device:

- ▶ send a trap ([see on page 169 “Configuring Traps”](#)),
- ▶ update the device status ([see on page 172 “Configuring the Device Status”](#)),
- ▶ update the status of the signal contacts ([see on page 176 “Controlling the Signal Contact”](#)).

## 3.2 Saving settings

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,
- ▶ save the current configuration for the offline configurator on the PC in XML format.

### 3.2.1 Saving locally (and on the ACA)

The device allows you to save the current configuration data in the local non-volatile memory and in the ACA.

- Select the `Basics: Load/Save` dialog.
- In the "Load" options, click on "From device".
- Click on "Save".  
The device saves the current configuration data in the local non-volatile memory and also, if a ACA is connected, in the ACA.

```
enable
copy system:running-config
nvram:startup-config
```

Switch to the privileged EXEC mode.  
The device saves the current configuration data in the local non-volatile memory and also, if a ACA is connected, in the ACA

**Note:** After you have successfully saved the configuration on the device, the device sends a trap `hmConfigurationSavedTrap` together with the information about the AutoConfiguration Adapter (ACA), if one is connected. When you change the configuration for the first time after saving it, the device sends a trap `hmConfigurationChangedTrap`.

**Note:** The device allows you to trigger the following events when the configuration stored on the ACA does not match the configuration on the device:

- ▶ send a trap (see on page 169 “Configuring Traps”),
- ▶ update the device status (see on page 172 “Configuring the Device Status”),
- ▶ update the status of the signal contacts (see on page 176 “Controlling the Signal Contact”).

### ■ Skip ACA21 during the boot phase

The device allows you to skip the ACA21 AutoConfiguration Adapter (if connected) during the boot phase. In this case, the device ignores the ACA21 during the boot phase. This shortens the boot phase of the device by 1 to 4 seconds. If you have enabled this function, ACA21-functionality becomes available as usual after the boot phase. The device simply skips the ACA21-loading procedures during the boot phase.

|                                             |                                                                   |
|---------------------------------------------|-------------------------------------------------------------------|
| <code>enable</code>                         | Switch to Privileged EXEC mode..                                  |
| <code>configure</code>                      | Switch to Global Configure mode.                                  |
| <code>#boot skip-aca-on-boot enable</code>  | Skip ACA during the boot phase. (default setting: disabled).      |
| <code>#boot skip-aca-on-boot disable</code> | Include the ACA during the boot phase.                            |
| <code>#show boot skip-aca-on-boot</code>    | Show whether the "Skip ACA during boot phase"function is enabled. |

## 3.2.2 Saving in a binary file on a URL

The device allows you to save the current configuration data in a file in the connected network.

**Note:** The configuration file includes all configuration data, including the password. Therefore pay attention to the access rights on the tftp server.

- Select the `Basics: Load/Save` dialog.
- In the “Save” frame, click “to URL (binary)” to create a binary file.
- In the “URL” frame, enter the path under which you want the device to save the configuration file.

The URL identifies the path to the tftp server on which the device saves the configuration file. The URL is in the format `tftp://IP address of the tftp server/path name/file name` (e.g. `tftp://10.1.112.5/switch/config.dat`).

- Click "Save".

```
enable
copy nvram:startup-config
 tftp://10.1.112.159/
 switch/config.dat
```

Switch to the privileged EXEC mode.  
The device saves the configuration data in a binary file on a tftp server in the connected network

### 3.2.3 Saving as an offline configuration file on the PC

The device allows you to save the current configuration data for the offline configurator in XML form in a file on your PC.

- Select the `Basics: Load/Save` dialog.
- In the "Save" frame, click "to PC (ocf)".
- In the save dialog, enter the name of the file in which you want the device to save the configuration file.
- Click "Save".

## 3.3 Configuration Signature

The device assigns a checksum or signature to identify a configuration so that changes to that configuration are visible. Every time you save a configuration, the device generates a random sequence of numbers and/or letters for the configuration signature. This signature changes every time you change the configuration. Each configuration has a unique identifier.

The device stores the random generated signature with the configuration to verify that the device maintained the configuration after a reboot.

The signature consists of a configuration file checksum and a random number. The device checks the signature to verify that it is different from previous generated numbers.

## 4 Loading Software Updates

Hirschmann is working constantly to improve the performance of their products. Therefore, on the Hirschmann web page ([www.hirschmann.com](http://www.hirschmann.com)) you may find a newer release of the device software than the one installed on your device.

### ■ Checking the installed Software Release

- Open the `Basic Settings:Software` dialog.
- This dialog indicates the Release Number of the software installed in the device.

```

enable Switch to Privileged EXEC mode.
show sysinfo Show system information.

Alarm..... None

System Description..... Hirschmann Railswitch
System Name..... RS-1F1054
System Location..... Hirschmann Railswitch
System Contact..... Hirschmann Automation
 and Control GmbH
System Up Time..... 0 days 0 hrs 45 mins
 57 secs
System Date and Time (local time zone).... 2009-11-12 14:15:16
System IP Address..... 10.0.1.13
Boot Software Release..... L2B-05.2.00
Boot Software Build Date..... 2009-11-12 13:14
OS Software Release..... L2B-03.1.00
OS Software Build Date..... 2009-11-12 13:14
Hardware Revision..... 1.22 / 4 / 0103
Hardware Description..... RS20-1600T1T1SDAEHH
Serial Number..... 943434023000001191
Base MAC Address..... 00:80:63:1F:10:54
Number of MAC Addresses..... 32 (0x20)

```

### ■ **Loading the software**

The device gives you 4 options for loading the software:

- ▶ manually from the ACA (out-of-band),
- ▶ automatically from the ACA (out-of-band),
- ▶ via TFTP from a tftp server (in-band) and
- ▶ via a file selection dialog from your PC.

**Note:** The existing configuration of the device is still there after the new software is installed.

## 4.1 Loading the Software manually from the ACA

You can connect the AutoConfiguration Adapter (ACA) to a USB port of your PC like a conventional USB stick and copy the device software into the main directory of the ACA.

- Copy the device software from your computer to the ACA.
- Now connect the ACA to the device's USB port.
- Open the system monitor ([see on page 18 "Starting the System Monitor"](#)).
- Select 2 and press the Enter key to copy the software from the ACA into the local memory of the device.  
At the end of the update, the system monitor asks you to press any key to continue.
- Select 3 to start the new software on the device.

The system monitor offers you additional options in connection with the software on your device:

- ▶ selecting the software to be loaded
- ▶ starting the software
- ▶ performing a cold start

### 4.1.1 Selecting the software to be loaded

In this menu item of the system monitor, you select one of two possible software releases that you want to load.

The following window appears on the screen:

---

Select Operating System Image

(Available OS: Selected: 05.0.00 (2009-08-07 06:05), Backup: 04.2.00  
(2009-07-06 06:05 (Locally selected: 05.0.00 (2009-08-07 06:05))

- 1 Swap OS images
- 2 Copy image to backup
- 3 Test stored images in Flash mem.
- 4 Test stored images in USB mem.
- 5 Apply and store selection
- 6 Cancel selection

---

*Figure 15: Update operating system screen display*

**■ Swap OS images**

The memory of the device provides space for two images of the software. This allows you, for example, to load a new version of the software without deleting the existing version.

- Select 1 to load the other software in the next booting process.

**■ Copy image to backup**

- Select 2 to save a copy of the active software.

**■ Test stored images in flash memory**

- Select 3 to check whether the images of the software stored in the flash memory contain valid codes.

**■ Test stored images in USB memory**

- Select 4 to check whether the images of the software stored in the ACA contain valid codes.

**■ Apply and store selection**

- Select 5 to confirm the software selection and to save it.

**■ Cancel selection**

- Select 6 to leave this dialog without making any changes.

## 4.1.2 Starting the software

This menu item (Start Selected Operating System) of the system monitor

allows you to start the software selected.

### **4.1.3 Performing a cold start**

This menu item (End (reset and reboot)) of the system monitor allows you to reset the hardware of the device and perform a restart.

## 4.2 Automatic software update by ACA

- For a software update via the ACA, first copy the new device software into the main directory of the AutoConfiguration Adapter. If the version of the software on the ACA is newer or older than the version on the device, the device performs a software update.

**Note:** Software versions with release 06.0.00 and higher in the non-volatile memory of the device support the software update via the ACA. If the device software is older, you have the option of loading the software manually from the ACA. See [“Loading the Software manually from the ACA” on page 71](#).

- Give the file the name that matches the device type and the software variant, e.g. rsL2P.bin for device type RS2 with the software variant L2P. Please note the case-sensitivity here.  
If you have copied the software from a product CD or from a Web server of the manufacturer, the software already has the correct file name.
- Also create an empty file with the name “autoupdate.txt” in the main directory of the ACA. Please note the case-sensitivity here.
- Connect the AutoConfiguration Adapter to the device and restart the device.
- The device automatically performs the following steps:
  - During the booting process, it checks whether an ACA is connected.
  - It checks whether the ACA has a file with the name “autoupdate.txt” in the main directory.
  - It checks whether the ACA has a software file with a name that matches the device type in the main directory.
  - It compares the software version stored on the ACA with the one stored on the device.
  - If these conditions are fulfilled, the device loads the software from the ACA to its non-volatile memory as the main software.
  - The device then performs a cold start, during which it loads the new software from the non-volatile memory.

One of the following messages in the log file indicates the result of the update process:

- ▶ S\_watson\_AUTOMATIC\_SWUPDATE\_SUCCESSFUL: Update completed successfully.
  - ▶ S\_watson\_AUTOMATIC\_SWUPDATE\_FAILED\_WRONG\_FILE: Update failed. Reason: incorrect file.
  - ▶ S\_watson\_AUTOMATIC\_SWUPDATE\_FAILED\_SAVING\_FILE: Update failed. Reason: error when saving.
- In your browser, click on “Reload” so that you can use the graphical user interface to access the device again after it is booted.

## 4.3 Loading the software from the TFTP server

For a software update via TFTP, you need a TFTP server on which the software to be loaded is stored ([see on page 210 “TFTP Server for Software Updates”](#)).

- Select the `Basics:Software` dialog.

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

tftp://IP address of the tftp server/path name/file name  
(e.g. tftp://192.168.1.1/device/device.bin).

- Enter the path of the device software.
- Click on “tftp Update” to load the software from the tftp server to the device.

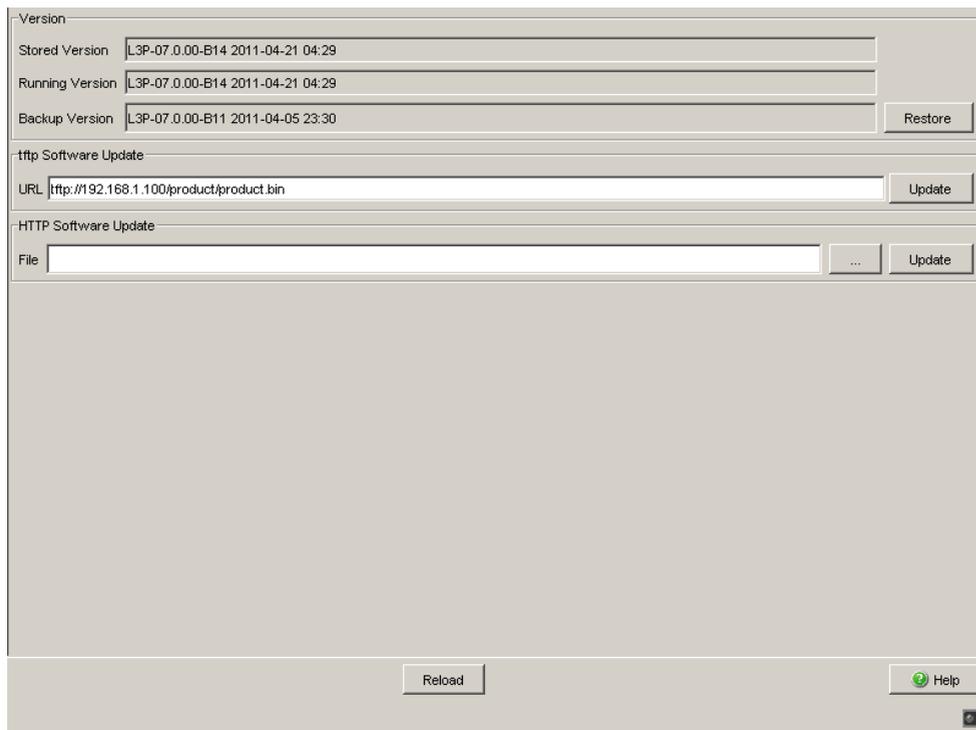


Figure 16: Software update dialog

- After successfully loading it, you 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 permanent memory, restarts, and performs a self-test.
- After booting the device, click “Reload” in your browser to access the device again.

```
enable
copy
tftp://10.0.1.159/product.b
in system:image
```

Switch to the privileged EXEC mode.  
Transfer the “product.bin” software file to the device from the tftp server with the IP address 10.0.1.159.

## 4.4 Loading the Software via File Selection

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

- Select the `Basics:Software` dialog.
- In the file selection frame, click on “...”.
- In the file selection window, select the device software (name type: \*.bin, e.g. device.bin) and click on “Open”.
- Click on “Update” to transfer the software to the device.

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

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

## 4.5 Bootcode Update via TFTP

In very rare cases, a bootcode with an expanded functionality is required to perform a software update. In such a case the service desk requests that you update the bootcode before performing the software update.

### 4.5.1 Updating the Bootcode file

For a tftp update, you need a tftp server to store the bootcode.

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

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

(for example: ).tftp://192.168.1.1/device/device\_bootrom.img

- Open the `Basic Settings:Software` dialog.
- In the "tftp Software Update" frame, click the "Bootcode" radio button.
- Enter the path to the bootcode bin file in the "URL" text box.
- To start the update, click "Update".
- To start the new bootcode after loading, open the `Basic Settings:Restart` dialog and click "Cold start...".

**Note:** You need read-write access for this dialog.

enable

Change to the privileged EXEC mode.

```
configure
copy <url> system:bootcode
```

Change to the Configuration mode.

Copy the bootcode bin file from the tftp server to the device.



## 5 Configuring the Ports

The port configuration consists of:

- ▶ Switching the port on and off
- ▶ Selecting the operating mode
- ▶ Activating the display of connection error messages
- ▶ Configuring Power over ETHERNET.

### ■ Switching the port on and off

In the default setting, every port is switched on. For a higher level of access security, switch off the ports for which you are not making any connection.

- Select the `Basics:Port Configuration` dialog.
- In the "Port on" column, select the ports that are connected to another device.

### ■ Selecting the operating mode

In the default setting, the ports are set to "Automatic Configuration" operating mode.

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

- Select the `Basics:Port Configuration` dialog.
- If the device connected to this port requires a fixed setting
  - select the operating mode (transmission rate, duplex mode) in the "Manual configuration" column and
  - deactivate the port in the "Automatic configuration" column.

### ■ **Disable unused module slots**

This function is available for the MS, PowerMICE, MACH102 and MACH4000 devices.

When you plug a module in an empty slot on modular devices, the device configures the module with the default settings. The default settings allow access to the network. To help prevent network access, the feature adds the possibility to disable an unused slot.

- Open the `Basics:Modules` dialog.
- Deactivate the unused slots in the "Enabled" column.

### ■ **Displaying detected loss of connection**

In the default setting, the device displays a detected connection error via the signal contact and the LED display. The device allows you to suppress this display, because you do not want to interpret a switched off device as an interrupted connection, for example.

- Select the `Basics:Port Configuration` dialog.
- In the "Propagate connection error" column, select the ports for which you want to have link monitoring.

### ■ **Power over Ethernet konfigurieren**

Devices with Power over ETHERNET (PoE) media modules or PoE ports enable you to supply current to terminal devices such as IP phones via the twisted-pair cable. PoE media modules and PoE ports support Power over ETHERNET in accordance with IEEE 802.3af.

The Power over ETHERNET function is globally active and the PoE-capable ports are active on delivery.

Nominal power for MS20/30, MACH 1000 and PowerMICE:

The device provides the nominal power for the sum of all PoE ports plus a surplus. Because the PoE media module gets its PoE voltage externally, the device does not know the possible nominal power.

The device therefore assumes a "nominal power" of 60 Watt per PoE media module for now.

Nominal power for OCTOPUS 8M-PoE:

The device provides the nominal power for the sum of all PoE ports, plus a power reserve. Since the device draws its PoE voltage from outside, it cannot know what the nominal power is.

Instead, the device therefore assumes a nominal power value of 15 Watt per PoE port.

### **Global settings**

- For devices with **PoE** select the `Basic Settings:Power over Ethernet` dialog.
- For devices with **PoE** select the `Basic Settings:Power over Ethernet Plus:Global` dialog.

### **Frame "Operation":**

- With "Function On/Off" you turn the PoE on or off.

### **Frame "Configuration":**

- 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 on at least one port.
- Enter the power threshold in "Threshold". When the device exceeds or is below this value, the device will send a trap, provided that you enable the "Send Trap" function. For the power threshold you enter the power yielded as a percentage of the nominal power.
- "Budget [W]" displays the power that the device nominally provides to the PoE ports.
- "Reserved [W]" displays the maximum power that the device provides to the connected PoE devices on the basis of their classification.
- "Delivered [W]" shows how large the current power requirement is on the PoE ports.

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

## Port settings

- For devices with **PoE** select the  
Basic Settings:Power over Ethernet dialog.
- For devices with **PoE+** select the  
Basic Settings:Power over Ethernet Plus:Port dialog.

The table only shows ports that support PoE.

- In the “POE on” column, you can enable/disable PoE at this port.
- The “Status” column indicates the PoE status of the port.
- The "Class" column indicates the class of the connected device:  
Class: Maximum delivered power  
0: 15.4 W = As-delivered state  
1: 4.0 W  
2: 7.0 W  
3: 15.4 W  
4: reserved, treated as Class 0
- The column „Consumption [W]“ displays the current power delivered at the respective port.
- The “Name” column indicates the name of the port, see  
Basic settings:Port configuration.

| Port | PoE enable                          | Status   | Priority | Class | Consumption [W] | Name |
|------|-------------------------------------|----------|----------|-------|-----------------|------|
| 1.5  | <input checked="" type="checkbox"/> | disabled | low      | -     | 0.0             |      |
| 1.6  | <input checked="" type="checkbox"/> | disabled | low      | -     | 0.0             |      |
| 1.7  | <input checked="" type="checkbox"/> | disabled | low      | -     | 0.0             |      |
| 1.8  | <input checked="" type="checkbox"/> | disabled | low      | -     | 0.0             |      |

Figure 17: Power over Ethernet dialog

### ■ Switch on PoE power supply

OCTOPUS PoE devices let you switch on the PoE power supply before loading and starting the software. This means that the connected PoE devices (powered devices) are supplied with the PoE voltage more quickly and the start phase of the whole network is shorter.

|                                                |                                                                                   |
|------------------------------------------------|-----------------------------------------------------------------------------------|
| <code>enable</code>                            | Switch to Privileged EXEC mode.                                                   |
| <code>configure</code>                         | Switch to Global Configure mode.                                                  |
| <code>#inlinepower fast-startup enable</code>  | Switch on Inline Power Fast Startup (disabled in the as-delivered state).         |
| <code>#inlinepower fast-startup disable</code> | Switch off Inline Power Fast Startup.                                             |
| <code>#show inlinepower</code>                 | Show Power over Ethernet System Information (Fast Startup and other information). |

### ■ Cold start with detected errors

This function lets you reset the device automatically with a cold start in the following cases:

- ▶ if an error is detected (selftest reboot-on-error enable) or
- ▶ only if a serious error is detected (selftest reboot-on-error seriousOnly)

If the function `selftest reboot-on-error seriousOnly` is enabled, the device behaves as follows:

- ▶ If an error is detected in a subsystem (for example, if an HDX/FDX mismatch is detected on a port), cold starts of the device are dropped.
- ▶ However, if an error affecting the function of the entire device is detected, the device still carries out a cold start.
- ▶ The device sends a trap ([see on page 166 “Sending Traps”](#)).

**Note:** If the `selftest reboot-on-error seriousOnly` function is enabled and the device detects an HDX/FDX mismatch, automatic cold starts of the device are dropped. In this case, to return the affected port(s) to a usable condition, open the `Basic Settings:Reboot` dialog and carry out a cold start of the device.

|                        |                                  |
|------------------------|----------------------------------|
| <code>enable</code>    | Switch to Privileged EXEC mode.  |
| <code>configure</code> | Switch to Global Configure mode. |

```
#selftest reboot-on-error
enable
#selftest reboot-on-error
seriousOnly
#selftest reboot-on-error
disable
#show selftest
```

Switch on the "Cold start if error detected" function.

Switch on the "Cold start only if serious error detected" function.

Switch off the "Cold start if error detected" function (enabled in the as-delivered state).

Show status of the "Cold start if error detected" function (Enabled/Disabled/seriousOnly).

## **6 Assistance in the Protection from Unauthorized Access**

The device provides the following functions to help prevent unauthorised accesses.

- ▶ Password for SNMP access
- ▶ Telnet/internet access can be switched off
- ▶ Restricted Management access
- ▶ HiDiscovery-Function can be switched off
- ▶ Port access control by IP or MAC address
- ▶ Login Banner

## 6.1 Protecting the device

If you want to maximize the protection of the device against unauthorized access in just a few steps, you can perform the following steps on the device as required:

- Deactivate SNMPv1 and SNMPv2 and select a password for SNMPv3 access other than the standard password ([see on page 92 “Entering the password for SNMP access”](#)).
- Deactivate the Web access after you have downloaded the applet for the graphical user interface onto your management station. You can start the applet as an independent program in order to have SNMPv3 access to the device.  
Deactivate Telnet access.  
[See “Enabling/disabling Telnet/Web Access” on page 96.](#)
- Deactivate HiDiscovery access.

**Note:** Retain at least one option to access the device. Connecting to the device via V.24 serial access is possible, since it cannot be deactivated.

## 6.2 Password for SNMP access

### 6.2.1 Description of password for SNMP access

A network management station communicates with the device via the Simple Network Management Protocol (SNMP).

Every SNMP packet contains the IP address of the sending computer and the password with which the sender of the packet wants to access the device MIB.

The device receives the SNMP packet and compares the IP address of the sending computer and the password with the entries in the device MIB.

If the password has the appropriate access right, and if the IP address of the sending computer has been entered, then the device will allow access.

In the delivery state, the device is accessible via the password "public" (read only) and "private" (read and write) to every computer.

To help protect your device from unwanted access:

- First define a new password with which you can access from your computer with all rights.
- Treat this password as confidential, because everyone who knows the password can access the device MIB with the IP address of your computer.
- Limit the access rights of the known passwords or delete their entries.

## 6.2.2 Entering the password for SNMP access

- Select the `Security:Password/SNMP Access` dialog.

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

Set different passwords for the read password and the read/write password so that a user that only has read access (user name “user”) does not know, or cannot guess, the password for read/write access (user name “admin”).

If you set identical passwords, when you attempt to write this data the device reports a general error.

The graphical user interface and the command line interface (CLI) use the same passwords as SNMPv3 for the users “admin” and “user”.

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

- Select “Modify Read-Only Password (User)” to enter the read password.
- Enter the new read password in the “New Password” line and repeat your entry in the “Please retype” line.
- Select “Modify Read-Write Password (Admin)” to enter the read/write password.
- Enter the read/write password and repeat your entry.

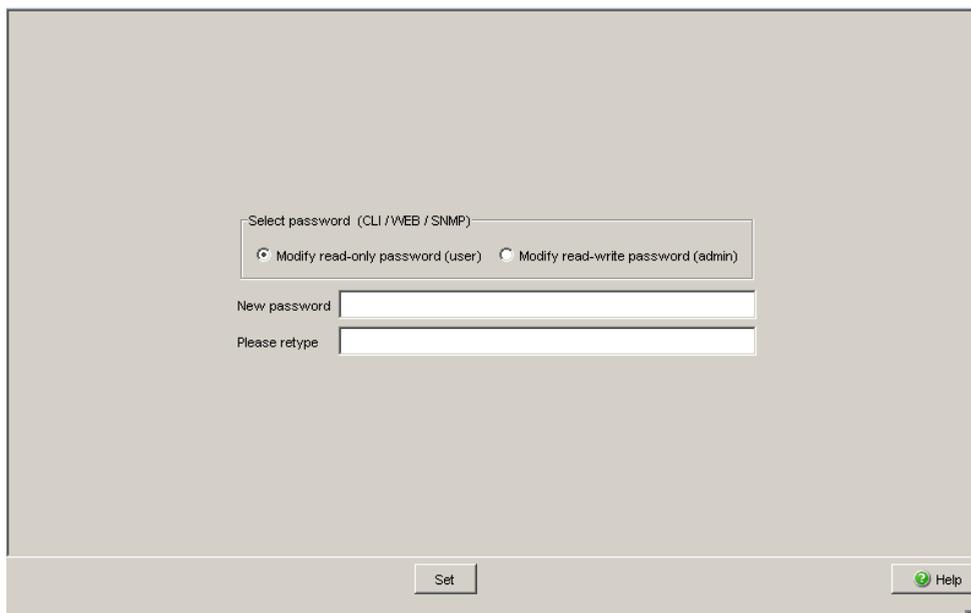


Figure 18: Password/SNMP Access dialog

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

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

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

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

- Select the Security:SNMPv1/v2 access dialog.  
With this dialog you can select the 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.

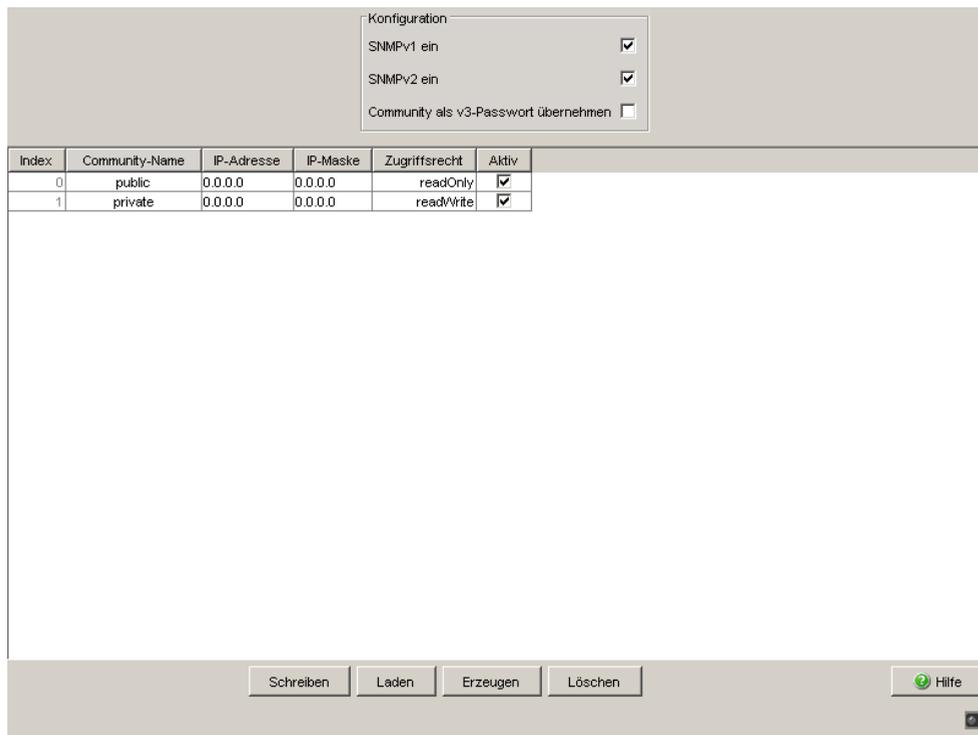
If you select SNMPv1 or SNMPv2, you can specify in the table via which IP addresses the device may be accessed, and what kinds of passwords are to be used.

Up to 8 entries can be made in the table.

For security reasons, the read password and the read/write password must not be identical.

Please note that passwords are case-sensitive.

|                |                                                                                                                                                                                                                                                                                                               |
|----------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Index          | Serial number for this table entry                                                                                                                                                                                                                                                                            |
| Community Name | Password with which this computer can access the device. This password is independent of the SNMPv3 password. If you activate the "Synchronize community to v3 password" function in the "Configuration" frame, the device synchronizes the corresponding SNMPv3 password when you change the community name. |
| IP Address     | IP address of the computer that can access the device.                                                                                                                                                                                                                                                        |
| IP Mask        | IP mask for the IP address                                                                                                                                                                                                                                                                                    |
| Access Mode    | The access mode determines whether the computer has read-only or read-write access.                                                                                                                                                                                                                           |
| Active         | Enable/disable this table entry.                                                                                                                                                                                                                                                                              |



The screenshot shows a configuration dialog for SNMP access. At the top, there is a 'Konfiguration' section with three checkboxes: 'SNMPv1 ein' (checked), 'SNMPv2 ein' (checked), and 'Community als v3-Passwort übernehmen' (unchecked). Below this is a table with the following data:

| Index | Community-Name | IP-Adresse | IP-Maske | Zugriffsrecht | Aktiv                               |
|-------|----------------|------------|----------|---------------|-------------------------------------|
| 0     | public         | 0.0.0.0    | 0.0.0.0  | readOnly      | <input checked="" type="checkbox"/> |
| 1     | private        | 0.0.0.0    | 0.0.0.0  | readWrite     | <input checked="" type="checkbox"/> |

At the bottom of the dialog, there are four buttons: 'Schreiben', 'Laden', 'Erzeugen', and 'Löschen'. To the right of these buttons is a 'Hilfe' button with a question mark icon.

Figure 19: SNMPv1/v2 access dialog

- To create a new line in the table click “Create”.
- To delete an entry, select the line in the table and click “Remove”.

### 6.2.3 Description of Telnet Access

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

The server is activated in its default setting.

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 retained.

**Note:** The Command Line Interface (out-of-band) and the `Security:Telnet/Web/SSH Access` dialog in the graphical user interface allows you to reactivate the Telnet server.

## 6.2.4 Description of Web Access (http)

The device's Web server allows you to configure the device by using the graphical user interface. You can deactivate the Web server to prevent Web access to the device.

The server is activated in its default setting.

After you switch the http Web server off, it is no longer possible to log in via a http Web browser. The http session in the open browser window remains active.

## 6.2.5 Enabling/disabling Telnet/Web Access

## 6.2.6 Switching Telnet/Internet/SSH access on/off

The Web server copies a Java applet for the graphical user interface onto your computer. The applet then communicates with the device by SNMPv3 (Simple Network Management Protocol). The Web server of the device allows you to configure the device using the graphical user interface. You can switch off the Web server in order to prevent the applet from being copied.

- Select the `Security:Telnet/Web` access dialog.
- Disable the server to which you want to refuse access.

|                                        |                                           |
|----------------------------------------|-------------------------------------------|
| <code>enable</code>                    | Switch to the privileged EXEC mode.       |
| <code>configure</code>                 | Switch to the Configuration mode.         |
| <code>lineconfig</code>                | Switch to the configuration mode for CLI. |
| <code>transport input telnet</code>    | Enable Telnet server.                     |
| <code>no transport input telnet</code> | Disable Telnet server.                    |
| <code>exit</code>                      | Switch to the Configuration mode.         |
| <code>exit</code>                      | Switch to the privileged EXEC mode.       |
| <code>ip http server</code>            | Enable Web server.                        |
| <code>no ip http server</code>         | Disable Web server.                       |

### 6.2.7 Web access through HTTPS

The HTTPS communication protocol (HyperText Transfer Protocol Secure) helps protect data transfers from interception. The device uses the HTTPS protocol to encrypt and authenticate the communications between web server and browser.

The Web server uses HTTP to load a Java applet for the graphical user interface onto your computer. This applet then communicates with the device by SNMP (Simple Network Management Protocol). If you have enabled the `Web Server (HTTPS)` function, the Java applet starts setting up a connection to the device via HTTPS. The device creates an HTTPS tunnel through the SNMP. It uses DES encoding on 56 bits. You can upload HTTPS certificates to the device.

## ■ Certificate

An X.509/PEM Standard certificate (Public Key Infrastructure) is required for the encryption. In the as-delivered state, a self-generated certificate is already present on the device.

- You can create an X509/PEM certificate using the following CLI command:  

```
ip https certgen
```
- You can upload a new certificate using the following CLI command:  

```
copy tftp://<server_ip>/<path_to_pem>
nvram:https-cert
```
- You can switch the HTTPS server off and on again using the following CLI command sequence:  

```
no ip https server
ip https server
```

**Note:** If you upload a new certificate, reboot the device or the HTTPS server in order to activate the certificate.

## ■ HTTPS connection

**Note:** The standard port for HTTPS connection is 443. If you change the number of the HTTPS port, reboot the device or the HTTPS server in order to make the change effective.

- You can change the HTTPS port number using the following CLI-command (where <port\_no> is the number of the HTTPS port):  

```
#ip https port <port_no>
```

**Note:** If you want to use HTTPS, switch on both HTTPS and HTTP. This is required in order to load the applet. In the as-delivered state, HTTPS is switched off.

- Open the `Security:Telnet/Internet Access` dialog.
- Tick the boxes `Telnet Server active`, `Web Server(http)` and `Web Server(https)`. In the `HTTPS Port Number` box, enter the value `443`.
- To access the device by HTTPS, enter HTTPS instead of HTTP in your browser, followed by the IP address of the device.

```
enable
ip https server
ip https port <port_no>

no ip https server
ip https server

show ip https

ip https certgen
copy
tftp://<server_ip>/<path_to_
pem> nvram:httpscert
no ip https server
ip https server
```

Switch to Privileged EXEC mode.  
Switch on HTTPS-server.  
Set the HTTPS port number for a secure HTTP connection.  
- As-delivered state: 443.  
- Value range: 1-65535  
If you change the HTTPS port number, switch the HTTPS server off and then on again in order to make the change effective.  
Optional: Show the status of the HTTPS server and HTTPS port number.  
Create X509/PEM certificates.  
Upload an X509/PEM certificate for HTTPS using TFTP.  
After uploading the HTTPS certificate, switch the HTTPS server off and then on again in order to activate the certificate.:

The device uses HTTPS protocol and establishes a new connection. When the session is ended and the user logs out, the device terminates the connection.

**Note:** The device allows you to open HTTPS- and HTTP connections at the same time. The maximum number of HTTP(S) connections that can be open at the same time is 16.

## 6.3 HiDiscovery Access

### 6.3.1 Description of the HiDiscovery Protocol

The HiDiscovery protocol allows you to allocate an IP address to the device (see on page 39 “Entering the IP Parameters via HiDiscovery”). HiDiscovery v1 is a Layer 2 protocol. HiDiscovery v2 is a Layer 3 protocol.

**Note:** For security reasons, restrict the HiDiscovery function for the device or disable it after you have assigned the IP parameters to the device.

### 6.3.2 Enabling/disabling the HiDiscovery function

- Select the `Basic settings:Network` dialog.
- Disable the "HiDiscovery function in the "HiDiscovery Protocol v1/v2" frame or limit the access to `read-only`.

|                                                    |                                                      |
|----------------------------------------------------|------------------------------------------------------|
| <pre>enable</pre>                                  | Switch to the privileged EXEC mode.                  |
| <pre>network protocol hidiscovery off</pre>        | Disable HiDiscovery function.                        |
| <pre>network protocol hidiscovery read-only</pre>  | Enable HiDiscovery function with “read-only” access  |
| <pre>network protocol hidiscovery read-write</pre> | Enable HiDiscovery function with “read-write” access |

## 6.4 Port access control

### 6.4.1 Description of the port access control

You can configure the device in such a way that it helps to protect every port from unauthorized access. Depending on your selection, the device checks the MAC address or the IP address of the connected device.

The following functions are available for monitoring every individual port:

- ▶ The device can distinguish between authorized and unauthorized access and supports 2 types of access control:
  - ▶ Access for all:
    - No access restriction.
    - MAC address 00:00:00:00:00:00 or
    - IP address 0.0.0.0.
  - ▶ Access exclusively for defined MAC and IP addresses:
    - Only devices with defined MAC or IP addresses have access.
    - You can define up to 10 IP addresses and up to 50 MAC addresses or maskable MAC addresses.
- ▶ The device reacts to an unauthorized access with the following selectable actions:
  - ▶ none: no reaction
  - ▶ trapOnly: message by sending a trap
  - ▶ portDisable: message by sending a trap and disabling the port
  - ▶ autoDisable: disabling the port via the AutoDisable function with the option to enable the port again after a definable time has elapsed.

## 6.4.2 Application Example for Port Access Control

You have a LAN connection in a room that is accessible to everyone. To set the device so that only defined users can use this LAN connection, activate the port access control on this port. An unauthorized access attempt will cause the device to shut down the port and alert you with an alarm message. The following is known:

| Parameter            | Value                    | Explanation                                                                                                                                               |
|----------------------|--------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------|
| Allowed IP Addresses | 10.0.1.228<br>10.0.1.229 | The defined users are the device with the IP address 10.0.1.228 and the device with the IP address 10.0.1.229                                             |
| Action               | portDisable              | Disable the port with the corresponding entry in the port configuration table ( <a href="#">see on page 83</a> “Configuring the Ports”) and send an alarm |

Prerequisites for further configuration:

- ▶ The port for the LAN connection is enabled and configured correctly ([see on page 83](#) “Configuring the Ports”)
- ▶ Prerequisites for the device to be able to send an alarm (trap) ([see on page 169](#) “Configuring Traps”):
  - You have entered at least one recipient
  - You have set the flag in the “Active” column for at least one recipient
  - In the “Selection” frame, you have selected “Port Security”

Configure the port security.

Select the `Security:Port Security` dialog.

In the “Configuration” frame, select “IP-Based Port Security”.

- In the table, click on the row of the port to be protected, in the “Allowed IP addresses” cell.
- Enter in sequence:
  - the IP subnetwork group: 10.0.1.228
  - a space character as a separator
  - the IP address: 10.0.1.229
 Entry: 10.0.1.228 10.0.1.229
- In the table, click on the row of the port to be protected, in the “Action” cell, and select portDisable.

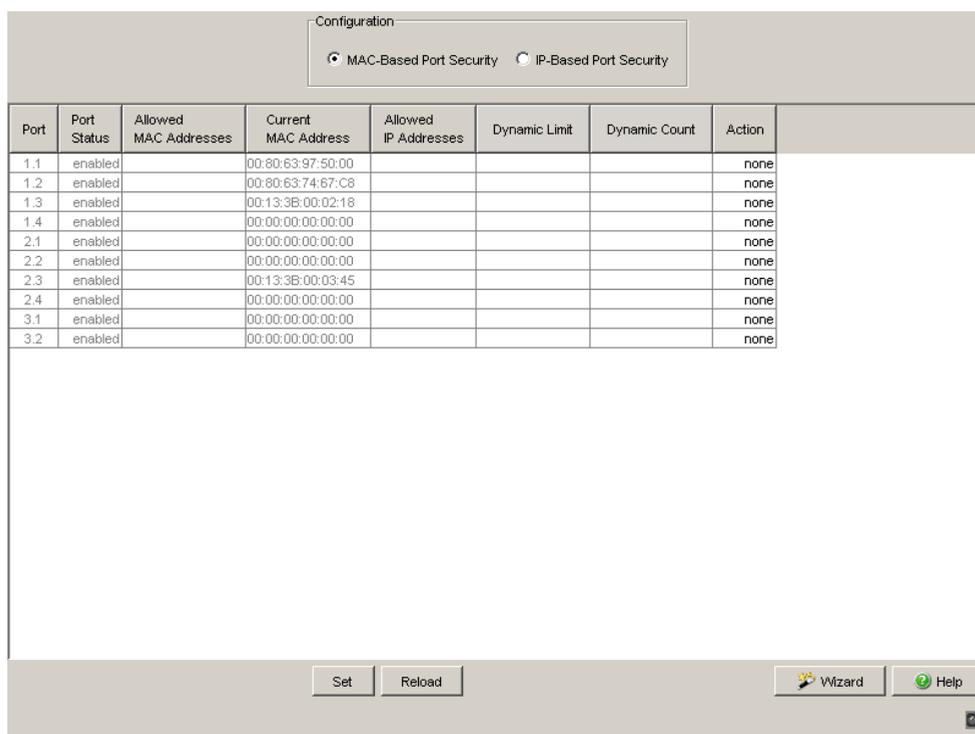


Figure 20: Port Security dialog

- Save the settings in the non-volatile memory.

- Select the dialog  
Basic Settings:Load/Save.
- In the “Save” frame, select “To Device” for the location and click “Save” to permanently save the configuration in the active configuration.

## 6.5 Login Banner

The device gives you the option of displaying a greeting text to users before they login to the device. The users see this greeting text in the login dialog of the graphical user interface (GUI) and of the Command Line Interface (CLI).

Users logging in with SSH see the greeting text - depending on the client used - before or during the login.

Perform the following work steps:

- Open the `Security:Login Banner` dialog, "Login Banner" tab.
- Enter the greeting text in the "Banner Text" frame.  
Max. 255 characters allowed.
- To switch on the function, in the "Operation" frame, mark the "On" radio button.
- Click "Set" to save the changes temporarily.

```
enable
set pre-login-banner text
 "<string>"
```

```
set pre-login-banner
operation
logout
```

Change to the privileged EXEC mode.

Assign the greeting text:

- Put the text in quotation marks.
- Max. 255 characters allowed.
- Insert tab using string `\\t`.
- Insert line break using string `\\n`.

Switching the function on.

Logout from device.

The text is visible before you login again.

## 6.6 CLI Banner

In the default setting, the CLI start screen shows information about the device, such as the software version and the device settings. The "CLI Banner" function allows you to replace this information with an individual text.

Perform the following work steps:

- Open the `Security:Login/CLI Banner` dialog, "CLI Banner" tab.
- In the "Banner Text" frame, enter the text of your choice.  
Max. 2048 characters allowed.
- To switch on the function, in the "Operation" frame, mark the "On" radio button.
- Click "Set" to save the changes temporarily.

```
enable
set clibanner text
 "<string>"

set clibanner operation
logout
```

Change to the privileged EXEC mode.

Assign the text to:

- Put the text in quotation marks.
- Max. 2048 characters allowed.
- Insert tab using string `\\t`.
- Insert line break using string `\\n`.

Switching the function on.

Logout from device.

The text is visible before you login again.



## 7 Synchronizing the System Time in the Network

The actual meaning of the term “real time” depends on the time requirements of the application.

The device provides two options with different levels of accuracy for synchronizing the time in your network.

The Simple Network Time Protocol (SNTP) is a simple solution for low accuracy requirements. Under ideal conditions, SNTP achieves an accuracy in the millisecond range. The accuracy depends on the signal delay.

IEEE 1588 with the Precision Time Protocol (PTP) achieves accuracies on the order of fractions of microseconds. This method is suitable even for demanding applications up to and including process control.

Examples of application areas include:

- ▶ Log entries
- ▶ Time stamping of production data
- ▶ Process control

Select the method (SNMP or PTP) that best suits your requirements. You can also use both methods simultaneously if you consider that they interact.

## 7.1 Setting the time

If no reference clock is available, you have the option of entering the system time in a device and then using it like a reference clock ([see on page 112 “Configuring SNTP”](#)).

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

**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.

- Open the `Time:Basic Settings` dialog.

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

- ▶ “System time (UTC)” displays the time determined using SNTP or PTP.

The display is the same worldwide. Local time differences are not taken into account.

**Note:** If the time source is PTP, consider that the PTP time uses the TAI time scale. TAI time is 34 s ahead of UTC time (as of 01.01.2011).

If the UTC offset is configured correctly on the PTP reference clock, the device corrects this difference automatically when displaying “System time (UTC)”.

- ▶ The "System Time" uses "System Time (UTC)", allowing for the local time difference from "System Time (UTC)".  
"System Time" = "System Time (UTC)" + "Local Offset".

- ▶ Time Source displays the source of the following time data. The device automatically selects the source with the greatest accuracy. Possible sources are: `local`, `ptp` and `sntp`. The source is initially `local`.

If PTP is activated and the device receives a valid PTP frame, it sets its time source to `ptp`. If SNTP is activated and if the device receives a valid SNTP packet, the device sets its time source to `sntp`. The device gives the PTP time source priority over SNTP.

- With "Set Time from PC", the device takes the PC time as the system time and calculates the "System Time (UTC)" using the local time difference.  
"System Time (UTC)" = "System Time" - "Local Offset"
- The "Local Offset" is for displaying/entering the time difference between the local time and the "System Time (UTC)".

With "Set Offset from PC", the device determines the time zone on your PC and uses it to calculate the local time difference.

```
enable
configure
sntp time <YYYY-MM-DD
 HH:MM:SS>
sntp client offset
 <-1000 to 1000>
```

Switch to the privileged EXEC mode.

Switch to the Configuration mode.

Set the system time of the device.

Enter the time difference between the local time and the "System Time (UTC)".

## 7.2 SNTP

### 7.2.1 Description of SNTP

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

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

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

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

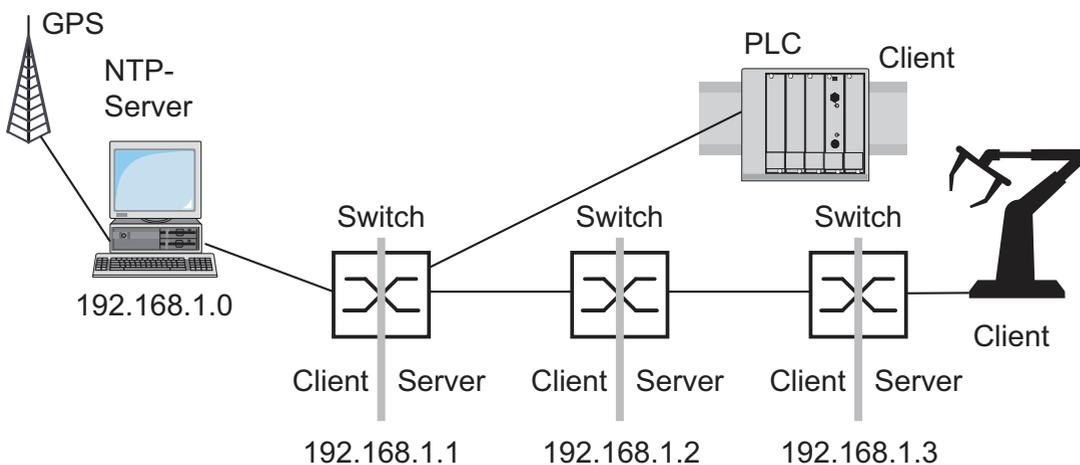


Figure 21: SNTP cascade

## 7.2.2 Preparing the SNTP Configuration

- To get an overview of how the time is passed on, draw a network plan with the devices participating in SNTP. When planning, bear in mind that the accuracy of the time depends on the signal runtime.

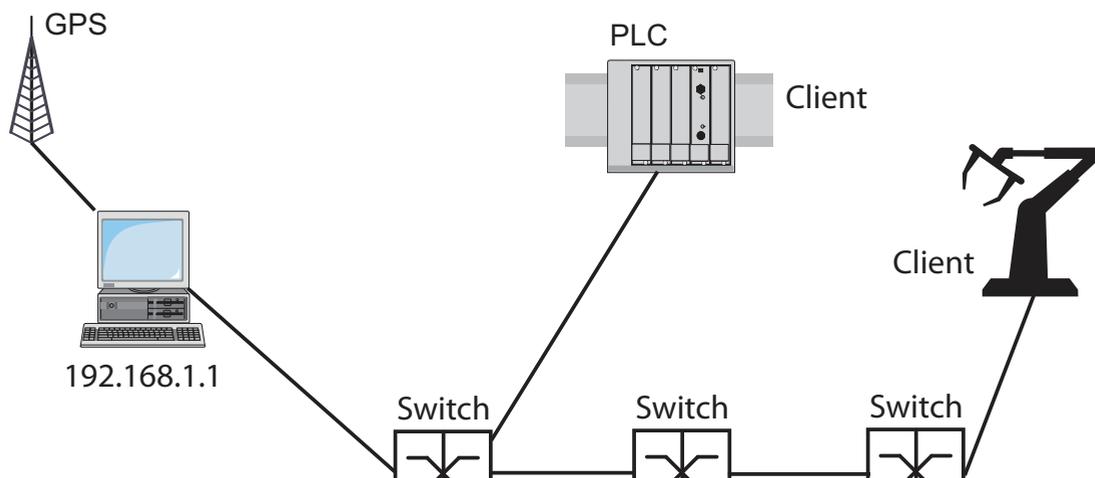


Figure 22: Example of SNTP cascade

- Enable the SNTP function on the devices whose time you want to set using SNTP.  
The SNTP server of the device responds to Unicast requests as soon as it is enabled.
- If no reference clock is available, specify a device as the reference clock and set its system time as accurately as possible.

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

### 7.2.3 Configuring SNTP

- Select the `Time : SNTP` dialog.
- ▶ Operation
  - In this frame you switch the SNTP function on/off globally.
- ▶ SNTP Status
  - The “Status message” displays statuses of the SNTP client as one or more test messages, e.g. `Server 2 not responding`.
- ▶ Configuration SNTP Client
  - In “Client status” you switch the SNTP client of the device on/off.
  - 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 1 second.

**Note:** If you are receiving the system time from an external/redundant server address, enter the dedicated server address(es) and disable the setting `Accept SNTP Broadcasts` (see below). You thus ensure that the device uses the time of the server(s) entered and does not synchronize to broadcasts that might not be trustworthy.

- In “Server request interval” you specify the interval at which the device requests SNTP packets (valid entries: 1 s to 3600 s, on delivery: 30 s).
- With “Accept SNTP Broadcasts” the device takes the system time from SNTP Broadcast/Multicast packets that it receives.
- With “Deactivate client after synchronization”, the device only synchronizes its system time with the SNTP server one time after the client status is activated, then it switches the client off.

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

 ▶ SNTP server configuration

- In "Server-Status", switch the device's SNTP server on/off.
- In "Anycast destination address" you enter the IP address to which the SNTP server of the device sends its SNTP packets (see table 4).
- In "VLAN ID", enter the VLAN over which the device will be cyclically sending its SNTP packets.
- In "Anycast send interval" you specify the interval at which the device sends SNTP packets (valid entries: 1 s to 3600 s, on delivery: 120 s).
- With "Disable Server at local time source" the device disables the SNTP server function if the source of the time is `local` (see `Time` dialog).

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

*Table 4: Destination address classes for SNTP and NTP packets*

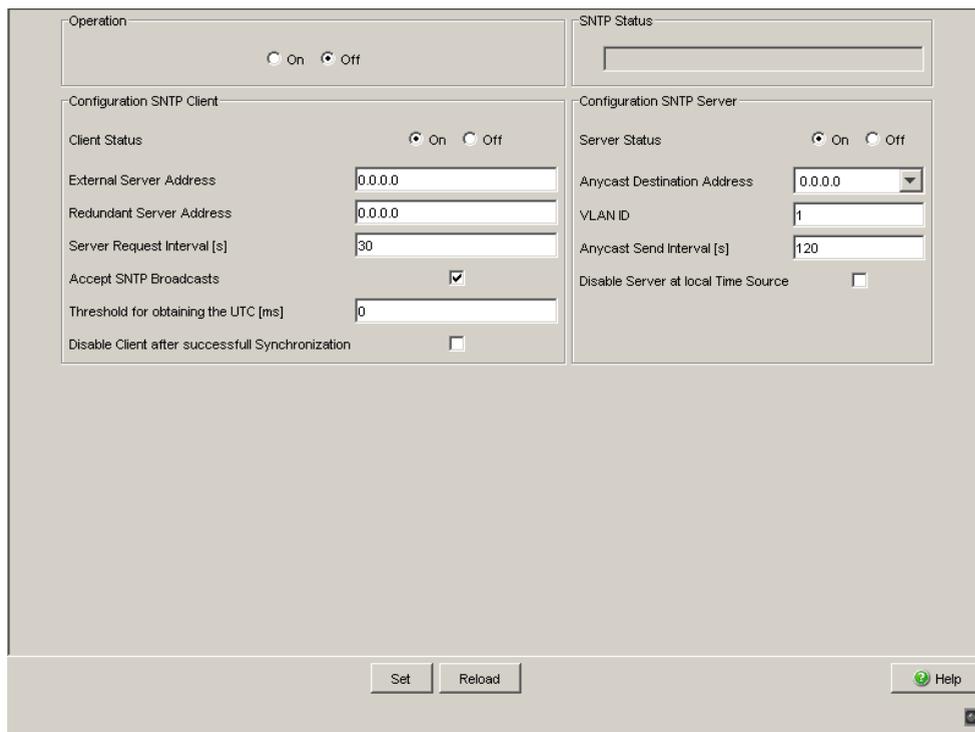


Figure 23: SNTP Dialog

| Device                         | 192.168.1.1 | 192.168.1.2 | 192.168.1.3 |
|--------------------------------|-------------|-------------|-------------|
| Operation                      | On          | On          | On          |
| Server destination address     | 0.0.0.0     | 0.0.0.0     | 0.0.0.0     |
| Server VLAN ID                 | 1           | 1           | 1           |
| Send interval                  | 120         | 120         | 120         |
| Client external server address | 192.168.1.0 | 192.168.1.1 | 192.168.1.2 |
| Request interval               | 30          | 30          | 30          |
| Accept Broadcasts              | No          | No          | No          |

Table 5: Settings for the example (see figure 22)

## 7.3 Precision Time Protocol

### 7.3.1 Description of PTP Functions

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

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

This procedure enable the synchronization of the clocks involved to an accuracy of a few 100 ns. The synchronization messages have virtually no effect on the network load. PTP uses Multicast communication.

Factors influencing precision are:

- ▶ Accuracy of the reference clock  
IEEE 1588 classifies clocks according to their accuracy. An algorithm that measures the accuracy of the clocks available in the network specifies the most accurate clock as the "Grandmaster" clock.

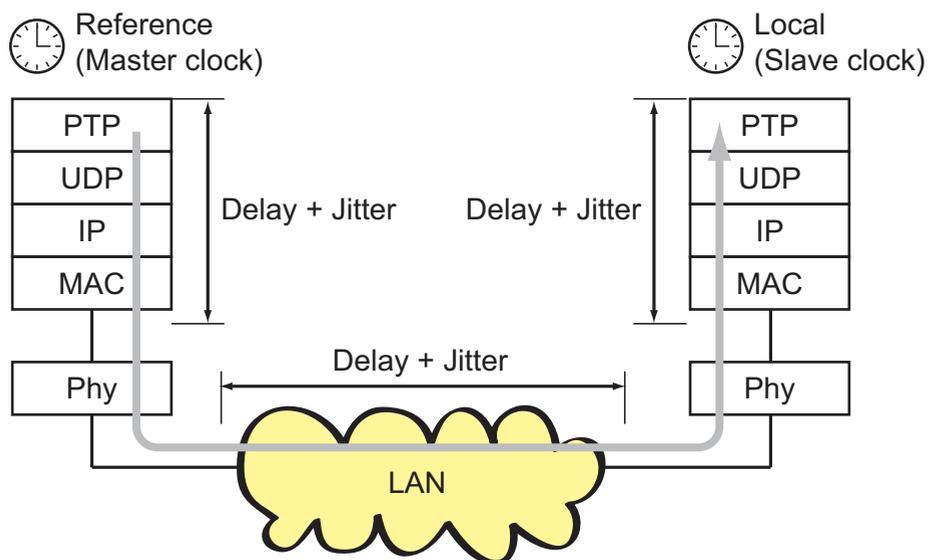
| PTPv1<br>Stratum<br>number | PTPv2<br>Clock class | Specification                                                                                                                                                                                                                                                                                                  |
|----------------------------|----------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 0                          | – (priority 1 = 0)   | For temporary, special purposes, in order to assign a higher accuracy to one clock than to all other clocks in the network.                                                                                                                                                                                    |
| 1                          | 6                    | Indicates the reference clock with the highest degree of accuracy. The clock can be both a boundary clock and an ordinary clock. Stratum 1/ clock class 6 clocks include GPS clocks and calibrated atomic clocks. A stratum 1 clock cannot be synchronized using the PTP from another clock in the PTP system. |
| 2                          | 6                    | Indicates the second-choice reference clock.                                                                                                                                                                                                                                                                   |

Table 6: Stratum – classifying the clocks

| PTPv1 Stratum number | PTPv2 Clock class | Specification                                                                                                                           |
|----------------------|-------------------|-----------------------------------------------------------------------------------------------------------------------------------------|
| 3                    | 187               | Indicates the reference clock that can be synchronized via an external connection.                                                      |
| 4                    | 248               | Indicates the reference clock that cannot be synchronized via an external connection. This is the standard setting for boundary clocks. |
| 5–254                | –                 | Reserved.                                                                                                                               |
| 255                  | 255               | Such a clock should never be used as the so-called best master clock.                                                                   |

Table 6: *Stratum – classifying the clocks*

- ▶ Cable delays; device delays  
The communication protocol specified by IEEE 1588 enables delays to be determined. Algorithms for calculating the current time cancel out these delays.
- ▶ Accuracy of local clocks  
The communication protocol specified by IEEE 1588 takes into account the inaccuracy of local clocks in relation to the reference clock. Calculation formulas permit the synchronization of the local time, taking into account the inaccuracy of the local clock in relation to the reference clock.



PTP Precision Time Protocol (Application Layer)  
 UDP User Datagramm Protocol (Transport Layer)  
 IP Internet Protocol (Network Layer)  
 MAC Media Access Control  
 Phy Physical Layer

Figure 24: Delay and jitter for clock synchronization



## 8 Network Load Control

To optimize the data transmission, the device provides you with the following functions for controlling the network load:

- ▶ Settings for direct packet distribution (MAC address filter)
- ▶ Multicast settings
- ▶ Rate limiter
- ▶ Prioritization - QoS
- ▶ Flow control
- ▶ Virtual LANs (VLANs)

## 8.1 Direct Packet Distribution

With direct packet distribution, you help protect the device from unnecessary network loads. The device provides you with the following functions for direct packet distribution:

- ▶ Store-and-forward
- ▶ Multi-address capability
- ▶ Aging of learned addresses
- ▶ Static address entries
- ▶ Disabling the direct packet distribution

### 8.1.1 Store and Forward

The device stores receive data and checks the validity. The device rejects invalid and defective data packets (> 1522 bytes or CRC errors) as well as fragments (> 64 bytes). The device then forwards valid data packets.

### 8.1.2 Multi-Address Capability

The device learns all the source addresses for a port. Only packets with

- ▶ unknown destination addresses
- ▶ these destination addresses or
- ▶ a multi/broadcast destination address

in the destination address field are sent to this port. The device enters learned source addresses in its filter table ([see on page 122 “Entering Static Addresses”](#)).

The device can learn up to 8,000 addresses. This is necessary if more than one terminal device is connected to one or more ports. It is thus possible to connect several independent subnets to the device.

### 8.1.3 Aging of learned MAC addresses

The device monitors the age of the learned addresses. Address entries which exceed a particular age - the aging time - are deleted by the device from its address table.

Data packets with an unknown destination address are flooded by the device.

Data packets with known destination addresses are selectively transmitted by the device.

**Note:** A reboot deletes the learned address entries.

- Select the `Switching:Global` dialog.
- Enter the aging time for all dynamic entries in the range from 10 to 630 seconds (unit: 1 second; default setting: 30).  
In connection with the router redundancy, select a time  $\geq 30$  seconds.

### 8.1.4 Entering Static Addresses

An important function of the device is the filter function. It selects data packets according to defined patterns, known as filters. These patterns are assigned distribution rules. This means that a data packet received by a device at a port is compared with the patterns. If there is a pattern that matches the data packet, a device then sends or blocks this data packet according to the distribution rules at the relevant ports.

The following are valid filter criteria:

- ▶ Destination address
- ▶ Broadcast address
- ▶ Multicast address
- ▶ VLAN membership

The individual filters are stored in the filter table (Forwarding Database, FDB). It consists of 3 parts: a static part and two dynamic parts.

- ▶ The management administrator describes the static part of the filter table (`dot1qStaticTable`).
- ▶ During operation, the device is capable of learning which of its ports receive data packets from which source address ([see on page 120 “Multi-Address Capability”](#)). This information is written to a dynamic part (`dot1qTpFdbTable`).
- ▶ Addresses learned dynamically from neighboring agents and those learned via GMRP are written to the other dynamic part.

Addresses already located in the static filter table are automatically transferred to the dynamic part by the device.

An address entered statically cannot be overwritten through learning.

**Note:** If the ring manager is active, it is not possible to make permanent unicast entries.

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

- Select the `Switching:Filters for MAC Addresses` dialog.

Each row of the filter table represents one filter. Filters specify the way in which data packets are sent. They are set automatically by the Switch (learned status) or created 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. In the "Create filter" dialog you can set up new filters. The following status settings are possible:

- ▶ `learned`: The filter was created automatically by the device.
- ▶ `permanent`: The filter is stored permanently in the device or on the URL (see on page 64 "Saving settings")
- ▶ `invalid`: With this status you delete a manually created filter.
- ▶ `igmp`: The filter was created by IGMP Snooping.

To delete entries with the "learned" status from the filter table, select the `Basics:Restart` dialog and click "Reset MAC address table".

### 8.1.5 Disabling the Direct Packet Distribution

To enable you to observe the data at all the ports, the device allows you to disable the learning of addresses. When the learning of addresses is disabled, the device transfers all the data from all ports to all ports.

- Select the `Switching:Global` dialog.

Uncheck "Address Learning" to observe the data at all ports.

## 8.2 Multicast Application

### 8.2.1 Description of the Multicast Application

The data distribution in the LAN differentiates between 3 distribution classes on the basis of the addressed recipients:

- ▶ Unicast - one recipient
- ▶ Multicast - a group of recipients
- ▶ Broadcast - every recipient that can be reached

In the case of a Multicast address, the device forwards all data packets with a Multicast address to all ports. This leads to an increased bandwidth requirement.

Protocols such as GMRP and procedures such as IGMP Snooping enable the device to exchange information via the direct transmission of Multicast data packets. The bandwidth requirement can be reduced by distributing the Multicast data packets only to those ports to which recipients of these Multicast packets are connected.

You can recognize IGMP Multicast addresses by the range in which the address lies:

- ▶ MAC Multicast Address  
01:00:5E:00:00:00 - 01:00:5E:FF:FF:FF  
(in mask form 01:00:5E:00:00:00/24)
- ▶ Class D IP Multicast address  
224.0.0.0 - 239.255.255.255  
(in mask form 224.0.0.0/4)

### 8.2.2 Example of a Multicast Application

The cameras for monitoring machines normally transmit their images to monitors located in the machine room and to the control room. In an IP transmission, a camera sends its image data with a Multicast address via the network.

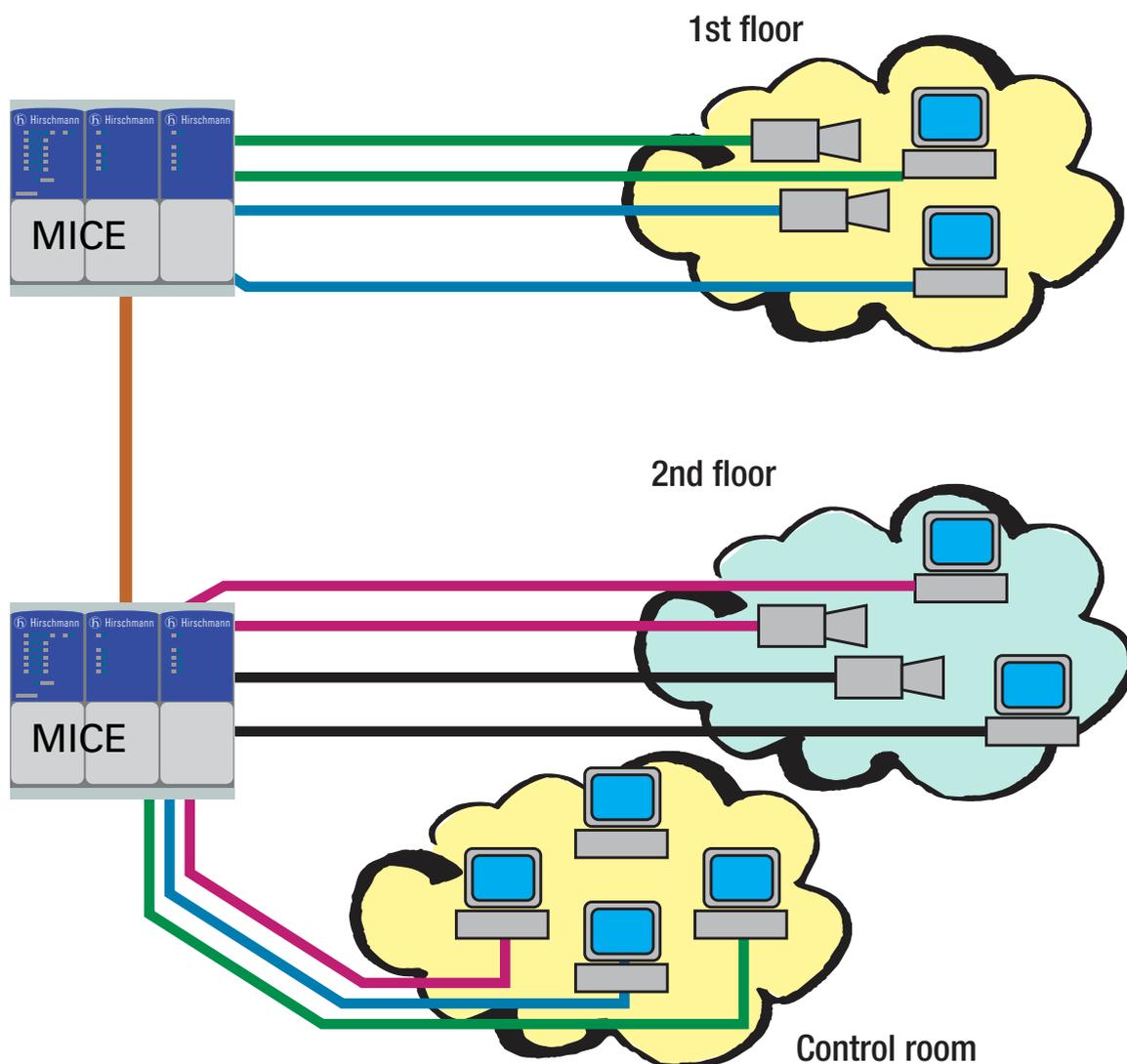


Figure 25: Example: Video surveillance in machine rooms

### 8.2.3 Description of IGMP Snooping

The Internet Group Management Protocol (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 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 a number of routers with an active IGMP function in the network, then they work out among themselves (in IGMP version 2) which router carries out 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 using 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 records the MAC addresses of the Multicast receivers, which are obtained via IGMP Snooping from the IP addresses, in the static address table. The Switch thus transmits these Multicast packets exclusively at the ports at which Multicast receivers are connected. The other ports are not affected by these packets.

A special feature of the device is that you can specify whether it should drop data packets with unregistered Multicast addresses, transmit them to all ports, or only to those ports at which the device received query packets. You also have the option of additionally sending known Multicast packets to query ports.

Default setting: "Off".

## 8.2.4 Setting IGMP Snooping

- Select the `Switching:Multicast:IGMP` dialog.

### ■ Operation

The “Operation” frame allows you to enable/disable 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 every port.

### ■ Settings for IGMP Querier and IGMP

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

Prerequisite: The IGMP Snooping function is activated globally.

#### IGMP Querier

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

“Protocol version” allow you to select IGMP version 1, 2 or 3.

In “Send interval [s]” you specify the interval at which the device sends query packets (valid entries: 2-3,599 s, default setting: 125 s).

Note the connection between the parameters Max. Response Time, Send Interval and Group Membership Interval ([see on page 128 “Parameter Values”](#)).

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.

## IGMP Settings

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

In “Max. Response Time” you specify the period within which the Multicast group members respond to a query (valid values: 1-3,598 s, default setting: 10 s).

Note the connection between the parameters Max. Response Time, Send Interval and Group Membership Interval ([see on page 128 “Parameter Values”](#)).

The Multicast group members select a random value within the maximum 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: 3-3,600 s, default setting: 260 s).

Note the connection between the parameters Max. Response Time, Send Interval and Group Membership Interval ([see on page 128 “Parameter Values”](#)).

## ■ Parameter Values

The parameters

- Max. Response Time,
- Transmit Interval and
- Group Membership Interval

have a relationship to one another:

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

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

| Parameter                 | Protocol Version | Value Range     | Default Setting |
|---------------------------|------------------|-----------------|-----------------|
| Max. Response Time        | 1, 2             | 1-25 seconds    | 10 seconds      |
|                           | 3                | 1-3,598 seconds |                 |
| Transmit Interval         | 1, 2, 3          | 2-3,599 seconds | 125 seconds     |
| Group Membership Interval | 1, 2, 3          | 3-3,600 seconds | 260 seconds     |

*Table 7: Value range for Max. Response Time, Transmit Interval and Group Membership Interval*

## ■ Multicasts

With these frames you can enter global settings for the Multicast functions.

Prerequisite: The IGMP Snooping function is activated globally.

### Unknown Multicasts

In this frame you can determine how the device in IGMP mode sends packets with known and unknown MAC/IP Multicast addresses that were not learned through IGMP Snooping..

“Unknown Multicasts” allows you to specify how the device transmits unknown Multicast packets:

- ▶ “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 IP 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.

### 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.

### ■ Settings per Port (Table)

- ▶ “IGMP on”  
This table column enables you to enable/disable the IGMP for each port when the global IGMP Snooping is enabled. Port registration will not occur if IGMP is disabled.

▶ “IGMP Forward All”

This table column enables you to enable/disable the “Forward All” IGMP Snooping function when the global IGMP Snooping is enabled. With the “Forward All” setting, 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 use IGMP version 1 in a subnetwork, then 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 on which it receives IGMP requests (disabled=as-delivered state).

This table column also lets you send IGMP Report messages to: other selected ports (enable) or 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 incorporated into a HIPER-Ring, you can use the following settings to quickly reconfigure the network for data packets with registered Multicast destination addresses after the ring is switched:

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

**Funktion**

An  Aus

**IGMP Querier**

IGMP Querier aktiv

Protokoll Version  1  2  3

Sende Intervall [s]

**IGMP Einstellungen**

Aktuelle Querier IP-Adresse

Max Response Time [s]

Group Membership Intervall [s]

**Multicasts**

Unbekannte Multicasts  An Query Ports senden  An alle Ports senden  Verwerfen

Bekannte Multicasts  An Query und registrierte Ports senden  An registrierte Ports senden

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

Figure 26: IGMP Snooping dialog

## 8.3 Rate Limiter

### 8.3.1 Description of the Rate Limiter

To ensure reliable operation at a high level of traffic, the device allows you to limit the rate of traffic at the ports.

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

If the traffic at this port exceeds the maximum rate entered, then the device suppresses the overload at this port.

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

**Note:** The limiter functions only work on Layer 2 and are used to limit the effect of storms by frame types that the Switch floods (typically broadcasts). In doing so, the limiter function disregards the protocol information of higher layers, such as IP or TCP. This can affect on TCP traffic, for example.

To minimize these effects, use the following options:

- ▶ limiting the limiter function to particular frame types (e.g. to broadcasts, multicasts and unicasts with unlearned destination addresses) and receiving unicasts with destination addresses established by the limitation,
- ▶ using the output limiter function instead of the input limiter function because the former works slightly better together with the TCP flow control due to switch-internal buffering.
- ▶ increasing the aging time for learned unicast addresses.

## 8.3.2 Rate limiter settings

- Select the `Switching:Rate Limiter` dialog.
- ▶ "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 ingress data volume at this port.
  - ▶ BC, limits the broadcast packets received at this port.
  - ▶ BC + MC, limits broadcast packets and multicast packets received on this port.
  - ▶ BC + MC + uUC, limits broadcast packets, multicast packets, and unknown unicast packets received on this port.
- ▶ Ingress Limiter Rate (kbit/s) for the ingress packet type selected:
  - ▶ = 0, no ingress limit at this port.
  - ▶ > 0, maximum ingress traffic rate in kbit/s that can be received on this port.
- ▶ Egress Limit (Pkt/s) for broadcast packets:
  - ▶ = 0, no rate limit for egress broadcast packets at this port.
  - ▶ > 0, maximum number of egress broadcasts per second that can be sent on this port.
- ▶ Egress Limit (kbit/s) for the entire data stream:
  - ▶ = 0, no rate limit for egress data stream at this port.
  - ▶ > 0, maximum egress traffic rate in kbit/s sent on this port.

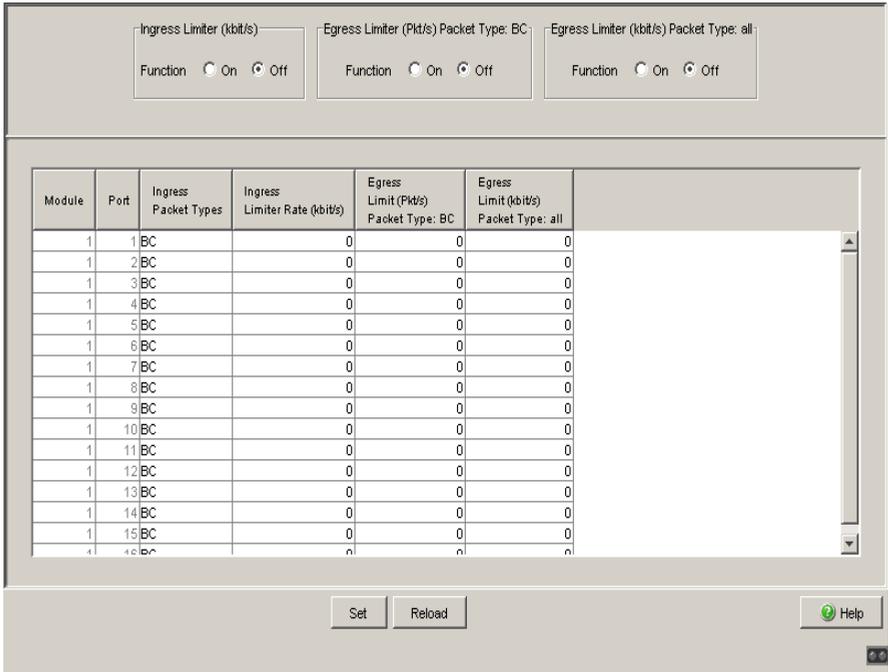


Figure 27: Rate limiter

---

## 8.4 QoS/Priority

### 8.4.1 Description of Prioritization

This function helps prevent time-critical data traffic such as language/video or real-time data from being disrupted by less time-critical data traffic during periods of heavy traffic. By assigning high traffic classes for time-critical data and low traffic classes for less time-critical data, this provides optimal data flow for time-critical data traffic.

The device supports 4 priority queues (IEEE 802.1D standard traffic classes). Received data packets are assigned to these classes by

- ▶ the priority of the data packet contained in the VLAN tag when the receiving port was configured to “trust dot1p”.
- ▶ the QoS information (ToS/DiffServ) contained in the IP header when the receiving port was configured to “trust ip-dscp”.
- ▶ the port priority when the port was configured to “untrusted”.
- ▶ the port priority when receiving non-IP packets when the port was configured to “trust ip-dscp”.
- ▶ the port priority when receiving data packets without a VLAN tag ([see on page 83 “Configuring the Ports”](#)) and when the port was configured to “trust dot1p”.  
Default setting: “trust dot1p”.

The device takes account of the classification mechanisms in the above order.

Data packets can contain prioritizing/QoS information:

- ▶ VLAN priority based on IEEE 802.1Q/ 802.1D (Layer 2)

## 8.4.2 VLAN tagging

The VLAN tag is integrated into the MAC data frame for the VLAN and Prioritization functions in accordance with the IEEE 802 1Q standard. The VLAN tag consists of 4 bytes. It is inserted between the source address field and the type field.

For data packets with a VLAN tag, the device evaluates:

- ▶ the priority information and
- ▶ the VLAN information if VLANs have been set.

Data packets with VLAN tags containing priority information but no VLAN information (VLAN ID = 0), are known as Priority Tagged Frames.

| Priority entered | 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: Assignment of the priority entered in the tag to the traffic classes*

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

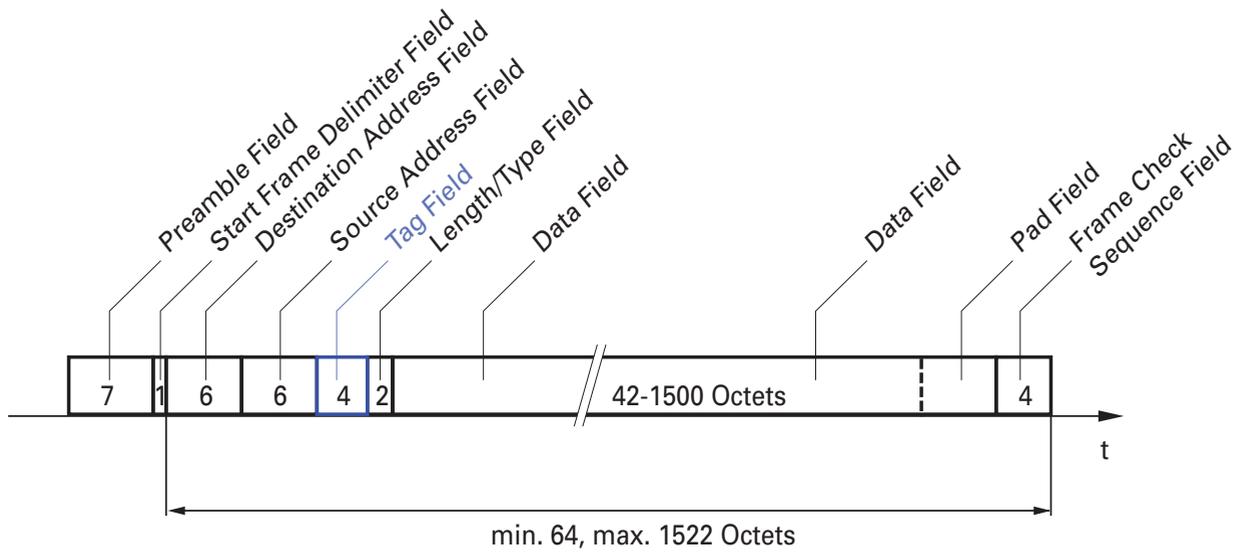


Figure 28: Ethernet data packet with tag

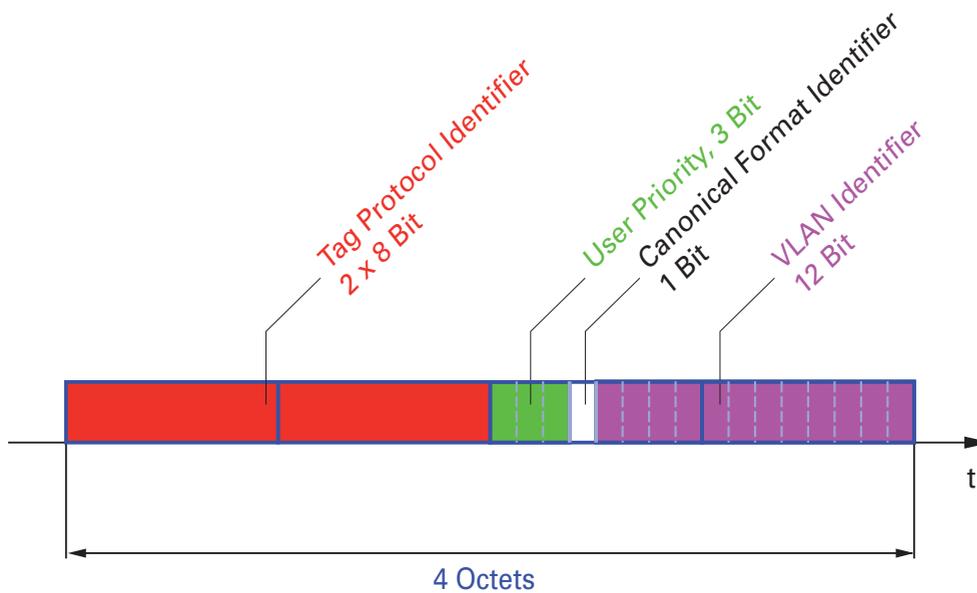


Figure 29: Tag format

When using VLAN prioritizing, note the following special features:

- ▶ End-to-end prioritizing requires the VLAN tags to be transmitted to the entire network, which means that all network components must be VLAN-capable.
- ▶ Routers cannot receive or send packets with VLAN tags via port-based router interfaces.

### 8.4.3 IP ToS / DiffServ

#### ■ TYPE of Service

The Type of Service (ToS) field in the IP header (see table 9) has been part of the IP protocol from the start, and it is used to differentiate various services in IP networks. Even back then, there were ideas about differentiated treatment of IP packets, due to the limited bandwidth available and the unreliable connection paths. Because of the continuous increase in the available bandwidth, there was no need to use the ToS field. Only with the real-time requirements of today's networks has the ToS field become significant again. Selecting the ToS byte of the IP header enables you to differentiate between different services. However, this field is not widely used in practice.



| Bits (0-2): IP Precedence Defined | Bits (3-6): Type of Service Defined | Bit (7)          |
|-----------------------------------|-------------------------------------|------------------|
| 111 - Network Control             | 0000 - [all normal]                 | 0 - Must be zero |
| 110 - Internetwork Control        | 1000 - [minimize delay]             |                  |
| 101 - CRITIC / ECP                | 0100 - [maximize throughput]        |                  |
| 100 - Flash Override              | 0010 - [maximize reliability]       |                  |
| 011 - Flash                       | 0001 - [minimize monetary cost]     |                  |

Table 9: ToS field in the IP header

| Bits (0-2): IP Precedence Defined | Bits (3-6): Type of Service Defined | Bit (7) |
|-----------------------------------|-------------------------------------|---------|
| 010 - Immediate                   |                                     |         |
| 001 - Priority                    |                                     |         |
| 000 - Routine                     |                                     |         |

Table 9: ToS field in the IP header

## ■ Differentiated Services

The Differentiated Services field in the IP header (see figure 30) newly defined in RFC 2474 - often known as the DiffServ code point or DSCP - replaces the ToS field and is used to mark the individual packets with a DSCP. Here the packets are divided into different quality classes. The first 3 bits of the DSCP are used to divide the packets into classes. The next 3 bits are used to further divide the classes on the basis of different criteria. In contrast to the ToS byte, DiffServ uses 6 bits for the division into classes. This results in up to 64 different service classes.

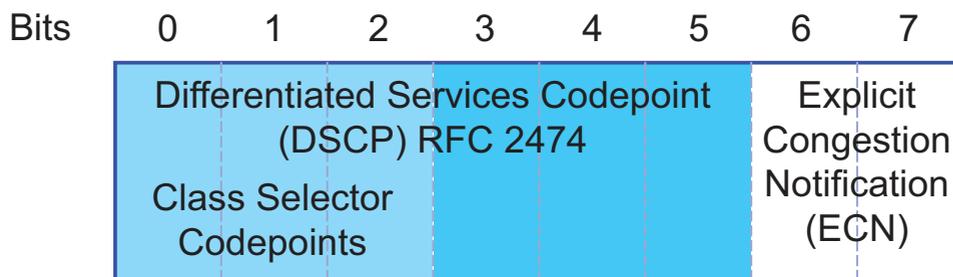


Figure 30: Differentiated Services field in the IP header

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

- ▶ Class Selector (CS0-CS7): For reasons of compatibility to TOS/IP Precedence
- ▶ Expedited Forwarding (EF): Premium service. Reduced delay, jitter + packet loss (RFC 2598)
- ▶ Assured Forwarding (AF): Provides a differentiated schema for handling different data traffic (RFC 2597).
- ▶ Default Forwarding/Best Effort: No particular prioritizing.

The PHB class selector assigns the 7 possible IP precedence values from the old ToS field to specific DSCP values, thus ensuring the downwards compatibility.

| ToS Meaning          | Precedence Value | Assigned DSCP |
|----------------------|------------------|---------------|
| Network Control      | 111              | CS7 (111000)  |
| Internetwork Control | 110              | CS6 (110000)  |
| Critical             | 101              | CS5 (101000)  |
| Flash Override       | 100              | CS4 (100000)  |
| Flash                | 011              | CS3 (011000)  |
| Immmediate           | 010              | CS2 (010000)  |
| Priority             | 001              | CS1 (001000)  |
| Routine              | 000              | CS0 (000000)  |

*Table 10: Assigning the IP precedence values to the DSCP value*

| 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 11: Mapping the DSCP values onto the traffic classes*

## 8.4.4 Handling of Received Priority Information

The device offers three options, which can be applied globally to all ports and determine how it treats received data packets that contain a priority indicator.

- ▶ **trust dot1p**  
The device assigns VLAN-tagged packets to the different traffic classes according to their VLAN priorities. The assignment is based on the pre-defined table ([see on page 137 “VLAN tagging”](#)). You can modify this assignment. The device assigns the port priority to packets that it receives without a tag.
- ▶ **untrusted**  
The device ignores the priority information in the packet and always assigns the packets the port priority of the receiving port.
- ▶ **trust ip-dscp**  
The device assigns the IP packets to the different traffic classes according to the DSCP value in the IP header, even if the packet was also VLAN-tagged. The assignment is based on the pre-defined values ([see table 11](#)). You can modify this assignment.  
The device prioritizes non-IP packets according to the port priority.

## 8.4.5 Handling of traffic classes

For the handling of traffic classes, the device provides:

► Strict Priority

### ■ Description of Strict Priority

With the Strict Priority setting, the device first transmits data packets that have a higher traffic class (higher priority) before transmitting a data packet with the next highest traffic class. The device transmits a data packet with the lowest traffic class (lowest priority) when there are no other data packets remaining in the queue. In unfortunate cases, the device never sends packets with a low priority if there is a high volume of high-priority traffic waiting to be sent on this port.

In delay-sensitive applications, such as VoIP or video, Strict Priority allows Strict Priority data to be sent immediately.

## 8.4.6 Setting prioritization

### ■ Assigning the Port Priority

- Select the `QoS/Priority:Port Configuration` dialog.
- In the “Port Priority” column, you can specify the priority (0-7) with which the device sends data packets which it receives without a VLAN tag at this port.
- In the column “Trust Mode“, you have the option to control which criterion the the device uses to assign a traffic class to received data packets ([see on page 136 “Description of Prioritization”](#)).

**Note:** If you have set up VLANs, pay attention to the “VLAN 0 Transparent mode” (see `Switching:VLAN:Global`)

|                 |                                                              |
|-----------------|--------------------------------------------------------------|
| enable          | Switch to the privileged EXEC mode.                          |
| configure       | Switch to the Configuration mode.                            |
| interface 1/1   | Switch to the Interface Configuration mode of interface 1/1. |
| vlan priority 3 | Assigns port priority 3 to interface 1/1.                    |
| exit            | Switch to the Configuration mode.                            |

## ■ Assigning VLAN priority to a traffic class

- Select the QOS/Priority:802.1D/p-Mapping dialog.
- In the "Traffic Class" column, enter the desired values.

|                                   |                                                 |
|-----------------------------------|-------------------------------------------------|
| enable                            | Switch to the privileged EXEC mode.             |
| configure                         | Switch to the Configuration mode.               |
| classofservice dot1p-mapping 0 2  | Assign traffic class 2 to VLAN priority 0.      |
| classofservice dot1p-mapping 1 2  | Also assign traffic class 2 to VLAN priority 1. |
| exit                              | Switch to the privileged EXEC mode.             |
| show classofservice dot1p-mapping | Display the assignment.                         |

| User Priority<br>----- | Traffic Class<br>----- |
|------------------------|------------------------|
| 0                      | 2                      |
| 1                      | 2                      |
| 2                      | 0                      |
| 3                      | 1                      |
| 4                      | 2                      |
| 5                      | 2                      |
| 6                      | 3                      |
| 7                      | 3                      |

## ■ Assigning the traffic class to a DSCP

- Select the QOS/Priority:IP DSCP Mapping dialog.
- In the "Traffic Class" column, enter the desired values.

```

enable
configure
classofservice
 ip-dscp-mapping cs1 1
show classofservice ip-dscp-mapping

```

Switch to the privileged EXEC mode.

Switch to the Configuration mode.

Assign traffic class 1 to DSCP CS1.

| IP DSCP    | Traffic Class |
|------------|---------------|
| -----      | -----         |
| 0 (be/cs0) | 2             |
| 1          | 2             |
| .          |               |
| .          |               |
| 8 (cs1)    | 1             |
| .          |               |

### ■ Always assign the DSCP priority to received IP data packets globally

- Open the `QoS/Priority:Global` dialog.
- Select `trustIPDSCP` in the "Trust Mode" line.

```

enable
configure
classofservice trust ip-
dscp
exit
exit
show classofservice trust
Class of Service Trust Mode: IP DSCP

```

Switch to the privileged EXEC mode.

Switch to the Configuration mode.

Assign the "trust ip-dscp" mode globally.

Switch to the Configuration mode.

Switch to the privileged EXEC mode.

Display the trust mode.

### ■ Configuring Layer 2 management priority

- Configure the VLAN ports to which the device sends management packets as a member of the VLAN that sends data packets with a tag (see on page 152 "Examples of VLANs").

- Open the `QoS/Priority:Global` dialog.
- In the "VLAN Priority for Management packets" field, you enter the value of the VLAN priority.

```

enable Switch to the privileged EXEC mode.
network priority dot1p-vlan Assign the value 7 to the management priority so
7 that management packets with the highest priority
 are sent.

exit Switch to the privileged EXEC mode.
show network Displays the management VLAN priority.

System IP Address..... 10.0.1.116
Subnet Mask..... 255.255.255.0
Default Gateway..... 10.0.1.200
Burned In MAC Address..... 00:80:63:51:7A:80
Network Configuration Protocol (BootP/DHCP).... None
DHCP Client ID (same as SNMP System Name)..... "PowerMICE-517A80"
Network Configuration Protocol HiDiscovery..... Read-Write
HiDiscovery Version..... v1, v2
Management VLAN ID..... 1
Management VLAN Priority..... 7
Management IP-DSCP Value..... 0 (be/cs0)
Web Mode..... Enable

```

### ■ Configuring Layer 3 management priority

- Open the `QoS/Priority:Global` dialog.
- In the "IP DSCP Value for Management packets" field, you enter the IP DSCP value with which the device sends management packets.

```

enable Switch to the privileged EXEC mode.
network priority ip-dscp Assign the value cs7 to the management priority so
cs7 that management packets with the highest priority
 are handled.

exit Switch to the privileged EXEC mode.
show network Displays the management VLAN priority.

```

---

```
System IP Address..... 10.0.1.116
Subnet Mask..... 255.255.255.0
Default Gateway..... 10.0.1.200
Burned In MAC Address..... 00:80:63:51:7A:80
Network Configuration Protocol (BootP/DHCP).... None
DHCP Client ID (same as SNMP System Name)..... "PowerMICE-517A80"
Network Configuration Protocol HiDiscovery..... Read-Write
HiDiscovery Version..... v1, v2
Management VLAN ID..... 1
Management VLAN Priority..... 7
Management IP-DSCP Value..... 56(cs7)
Web Mode..... Enable
```

## 8.5 Flow Control

### 8.5.1 Description of Flow Control

Flow control is a mechanism which acts as an overload protection for the device. During periods of heavy traffic, it holds off additional traffic from the network.

The example ([see figure 31](#)) shows a graphic illustration of how the flow control works. Workstations 1, 2 and 3 want to simultaneously transmit a large amount of data to Workstation 4. The combined bandwidth of Workstations 1, 2 and 3 to the device is larger than the bandwidth of Workstation 4 to the device. This leads to an overflow of the send queue of port 4. The funnel on the left symbolizes this status.

If the flow control function at ports 1, 2 and 3 of the device is turned on, the device reacts before the funnel overflows. Ports 1, 2 and 3 send a message to the connected devices that no data can be received at present.

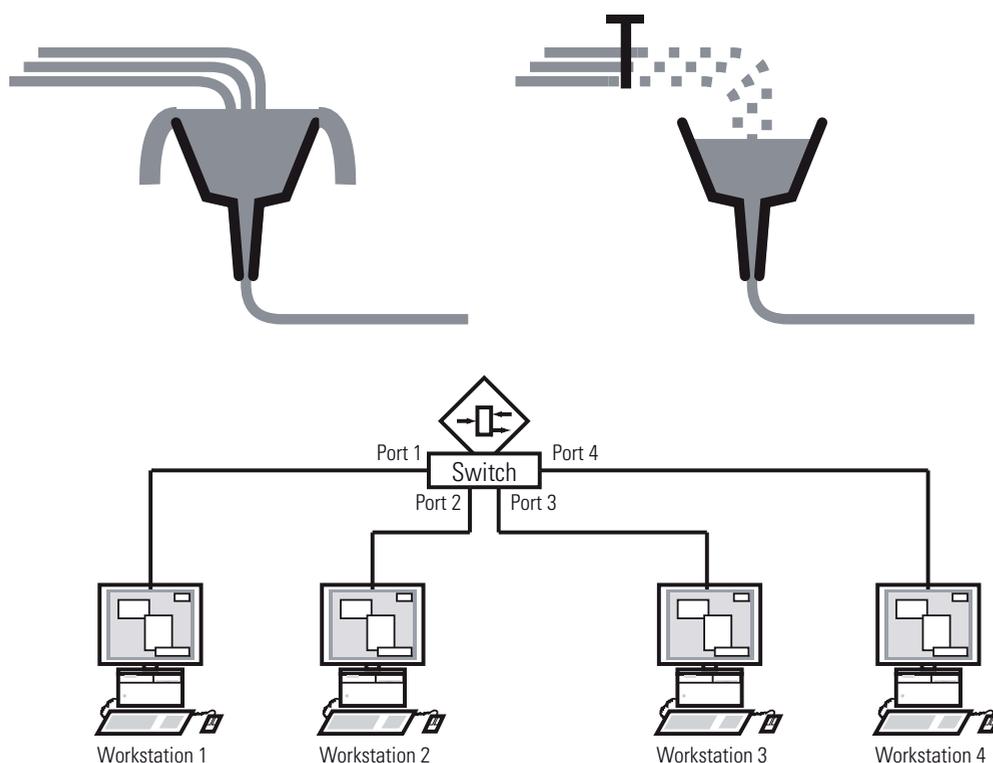


Figure 31: Example of flow control

### ■ Flow Control with a full duplex link

In the example (see [figure 31](#)) there is a full duplex link between Workstation 2 and the device.

Before the send queue of port 2 overflows, the device sends a request to Workstation 2 to include a small break in the sending transmission.

**Note:** The devices RS20/30/40, MS20/30, Octopus, MACH 100, RSR and MACH 1000 support flow control in full duplex mode only.

### ■ Flow Control with a half duplex link

In the example (see [figure 31](#)) there is a half duplex link between Workstation 2 and the device.

Before the send queue of port 2 overflows, the device sends data back so that Workstation 2 detects a collision and interrupts the sending process.

**Note:** The devices RS20/30/40, MS20/30, Octopus, MACH 100, RSR and MACH 1000 do not support flow control in half duplex mode.

## 8.5.2 Setting the Flow Control

- Select the `Basics:Port Configuration` dialog.  
In the "Flow Control on" 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.
- Select the `Switching:Global` dialog.  
With this dialog you can
  - ▶ switch off the flow control at all ports or
  - ▶ switch on the flow control at those ports for which the flow control is selected in the port configuration table.

**Note:** When you are using a redundancy function, you deactivate the flow control on the participating device ports. If the flow control and the redundancy function are active at the same time, there is a risk that the redundancy function will not operate as intended.

## 8.6 VLANs

### 8.6.1 VLAN Description

In the simplest case, a virtual LAN (VLAN) consists of a group of network participants in one network segment who can communicate with each other as if they belonged to a separate LAN.

More complex VLANs span out over multiple network segments and are also based on logical (instead of only physical) connections between network participants. Thus VLANs are an element of flexible network design, as you can reconfigure logical connections centrally more easily than cable connections.

The IEEE 802.1Q standard defines the VLAN function.

The most important benefits of VLANs are:

- ▶ **Network load limiting**  
VLANs reduce the network load considerably as the devices transmit broadcast, multicast, and unicast packets with unknown (unlearned) destination addresses exclusively inside the virtual LAN. The rest of the data network forwards traffic as normal.
- ▶ **Flexibility**  
You have the option of forming user groups flexibly based on the function of the participants and not on their physical location or medium.
- ▶ **Clarity**  
VLANs give networks a clear structure and make maintenance easier.

## 8.6.2 Examples of VLANs

The following practical examples provide a quick introduction to the structure of a VLAN.

### ■ Example 1

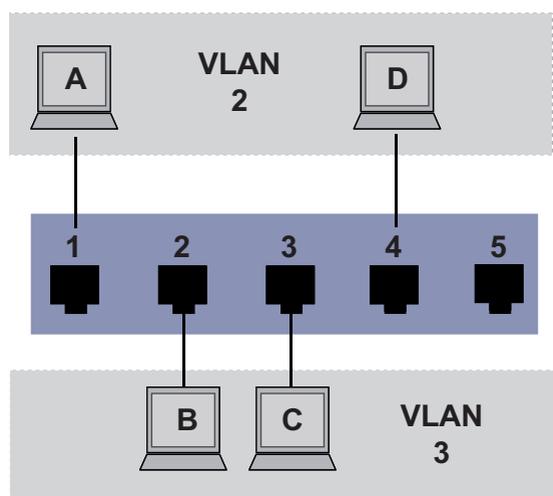


Figure 32: Example of a simple port-based VLAN

The example shows a minimal VLAN configuration (port-based VLAN). An administrator has connected multiple terminal devices to a transmission device and assigned them to 2 VLANs. This effectively prohibits any data transmission between the VLANs, whose members communicate only within their own VLANs.

When setting up the VLANs, you create communication rules for every port, which you enter in incoming (ingress) and outgoing (egress) tables. The ingress table specifies which VLAN ID a port assigns to the incoming data packets. Hereby, you use the port address of the terminal device to assign it to a VLAN.

The egress table specifies at which ports the Switch may send the frames from this VLAN. Your entry also defines whether the Switch marks (tags) the Ethernet frames sent from this port.

- ▶ T = with tag field (T = tagged, marked)
- ▶ U = without tag field (U = untagged, not marked)

For this example, the status of the TAG field of the data packets has no relevance, so you set it to "U".

| Terminal | Port | Port VLAN identifier (PVID) |
|----------|------|-----------------------------|
| A        | 1    | 2                           |
| B        | 2    | 3                           |
| C        | 3    | 3                           |
| D        | 4    | 2                           |
|          | 5    | 1                           |

Table 12: Ingress table

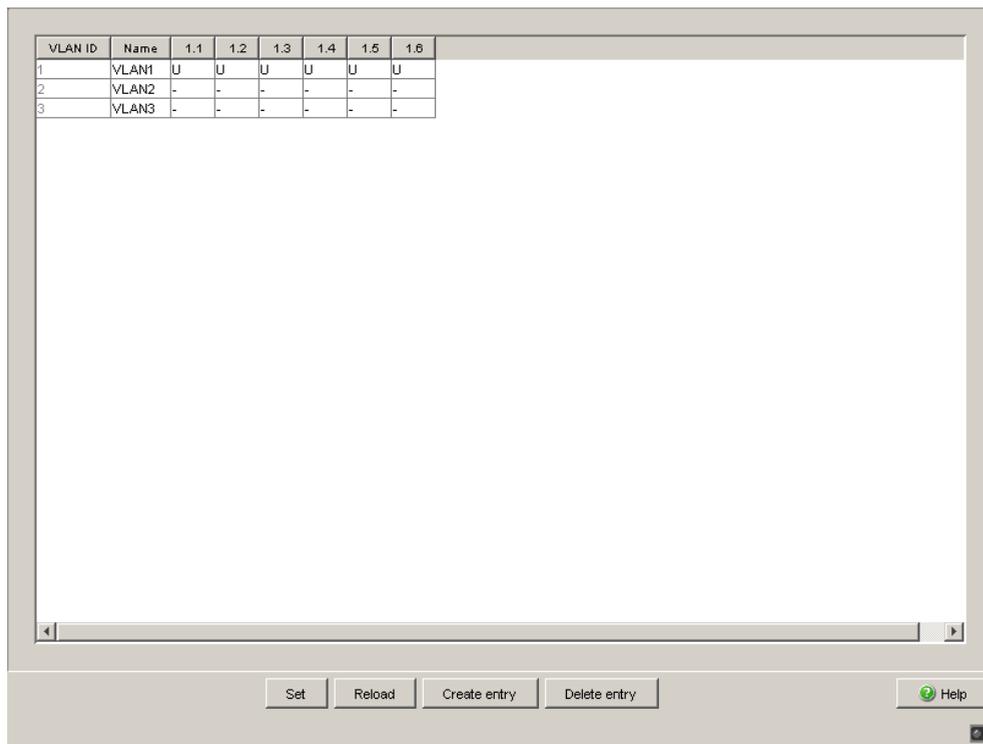
| VLANID | Port |   |   |   |   |
|--------|------|---|---|---|---|
|        | 1    | 2 | 3 | 4 | 5 |
| 1      |      |   |   |   | U |
| 2      | U    |   |   | U |   |
| 3      |      | U | U |   |   |

Table 13: Egress table

Proceed as follows to perform the example configuration:

Configure VLAN

Open the `Switching:VLAN:Static` dialog.



*Figure 33: Creating and naming new VLANs*

- Click on "Create" to open the window for entering the VLAN ID.
- Assign VLAN ID 2 to the VLAN.
- Click "OK".
- You give this VLAN the name VLAN2 by clicking on the field and entering the name. Also change the name for VLAN 1 from `Default` to `VLAN1`.
- Repeat the previous steps and create another VLAN with the VLAN ID 3 and the name `VLAN3`.

```
enable
vlan database
vlan 2
vlan name 2 VLAN2

vlan 3
vlan name 3 VLAN3

vlan name 1 VLAN1

exit
```

Switch to the privileged EXEC mode.  
 Switch to the VLAN configuration mode.  
 Create a new VLAN with the VLAN ID 2.  
 Give the VLAN with the VLAN ID 2 the name `VLAN2`.  
 Create a new VLAN with the VLAN ID 3.  
 Give the VLAN with the VLAN ID 3 the name `VLAN3`.  
 Give the VLAN with the VLAN ID 1 the name `VLAN1`.  
 Leave the VLAN configuration mode.

```

show vlan brief Display the current VLAN configuration.
Max. VLAN ID..... 4042
Max. supported VLANs..... 255
Number of currently configured VLANs..... 3
VLAN 0 Transparent Mode (Prio. Tagged Frames).. Disabled
VLAN ID VLAN Name VLAN Type VLAN Creation Time

1 VLAN1 Default 0 days, 00:00:05
2 VLAN2 Static 0 days, 02:44:29
3 VLAN3 Static 0 days, 02:52:26

```

## Configuring the ports

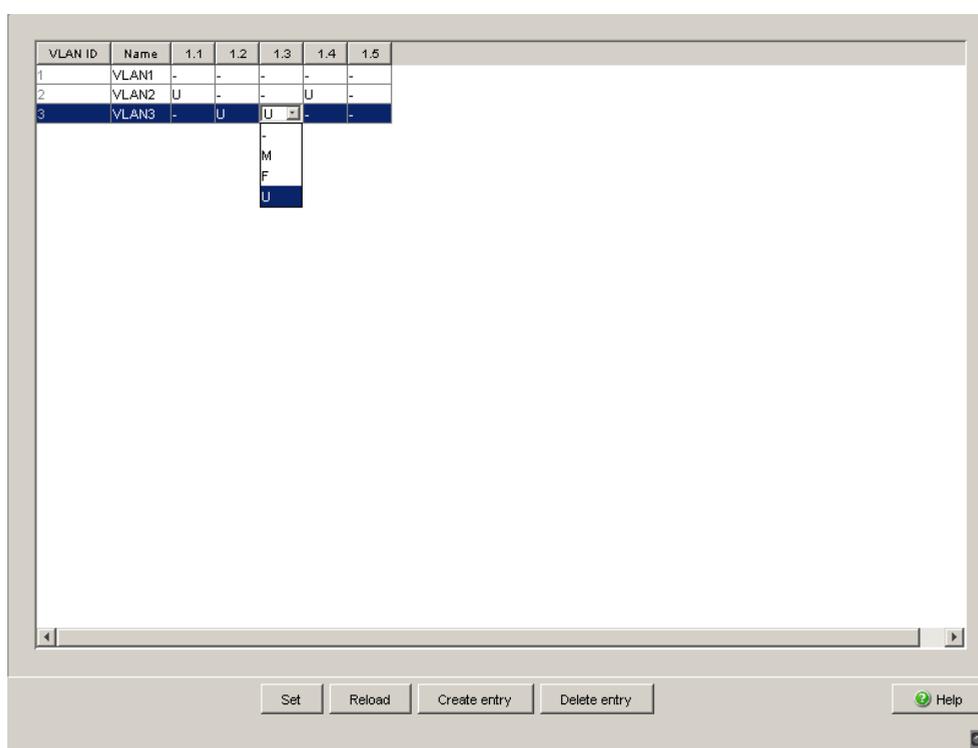


Figure 34: Defining the VLAN membership of the ports.

- Assign the ports of the device to the corresponding VLANs by clicking on the related table cell to open the selection menu and define the status. The selection options are:

- ▶ - = currently not a member of this VLAN (GVRP allowed)
- ▶ T = member of VLAN; send data packets with tag
- ▶ U = Member of the VLAN; send data packets without tag
- ▶ F = not a member of the VLAN (also disabled for GVRP)

Because terminal devices usually interpret untagged data packets exclusively, you select the U setting here.

- To temporarily save the changes, click "Set".
- Open the `Switching:VLAN:Port` dialog.

| Port | Port-VLAN-ID | Acceptable Frame Types | Ingress Filtering        |
|------|--------------|------------------------|--------------------------|
| 1.1  | 1            | admitAll               | <input type="checkbox"/> |
| 1.2  | 1            | admitAll               | <input type="checkbox"/> |
| 1.3  | 1            | admitAll               | <input type="checkbox"/> |
| 1.4  | 1            | admitAll               | <input type="checkbox"/> |
| 1.5  | 1            | admitAll               | <input type="checkbox"/> |
| 1.6  | 1            | admitOnlyVlanTag       | <input type="checkbox"/> |
| 1.7  | 1            | admitAll               | <input type="checkbox"/> |
| 1.8  | 1            | admitAll               | <input type="checkbox"/> |
| 1.9  | 1            | admitAll               | <input type="checkbox"/> |
| 1.10 | 1            | admitAll               | <input type="checkbox"/> |
| 1.11 | 1            | admitAll               | <input type="checkbox"/> |
| 1.12 | 1            | admitAll               | <input type="checkbox"/> |
| 1.13 | 1            | admitAll               | <input type="checkbox"/> |
| 1.14 | 1            | admitAll               | <input type="checkbox"/> |
| 1.15 | 1            | admitAll               | <input type="checkbox"/> |
| 1.16 | 1            | admitAll               | <input type="checkbox"/> |

*Figure 35: Assigning and saving "Port VLAN ID", "Acceptable Frame Types" and "Ingress Filtering"*

- Assign the Port VLAN ID of the related VLANs (2 or 3) to the individual ports - see table.
- Because terminal devices usually send data packets as untagged, you select the `admitAll` setting for the "Acceptable Frame Types".
- The setting for `Ingress Filter` does not affect how this example functions.
- Click "Set" to save the changes temporarily.
- Select the `Basics: Load/Save` dialog.
- In the "Save" frame, select "To Device" for the location and click "Save" to permanently save the configuration in the active configuration.

```
enable
configure
interface 1/1
```

```
vlan participation include 2
vlan pvid 2
exit
```

Switch to the privileged EXEC mode.

Switch to the Configuration mode.

Switch to the Interface Configuration mode of interface 1/1.

Port 1/1 becomes member untagged in VLAN 2.

Port 1/1 is assigned the port VLAN ID 2.

Switch to the Configuration mode.

```

interface 1/2
vlan participation include 3
vlan pvid 3
exit
interface 1/3
vlan participation include 3
vlan pvid 3
exit
interface 1/4
vlan participation include 2
vlan pvid 2
exit
exit
show VLAN 3
VLAN ID : 3
VLAN Name : VLAN3
VLAN Type : Static
VLAN Creation Time: 0 days, 02:52:26 (System Uptime)
Interface Current Configured Tagging
----- -
1/1 Exclude Autodetect Tagged
1/2 Include Include Untagged
1/3 Include Include Untagged
1/4 Exclude Autodetect Tagged
1/5 Exclude Autodetect Tagged

```

Switch to the interface configuration mode for port 1.2.  
Port 1/2 becomes member untagged in VLAN 3.  
Port 1/2 is assigned the port VLAN ID 3.  
Switch to the Configuration mode.  
Switch to the Interface Configuration mode of Interface 1/3.  
Port 1/3 becomes member untagged in VLAN 3.  
Port 1/3 is assigned the port VLAN ID 3.  
Switch to the Configuration mode.  
Switch to the interface configuration mode of interface 1/4.  
Port 1/4 becomes member untagged in VLAN 2.  
Port 1/4 is assigned the port VLAN ID 2.  
Switch to the Configuration mode.  
Switch to the privileged EXEC mode.  
Show details for VLAN 3.

## ■ Example 2

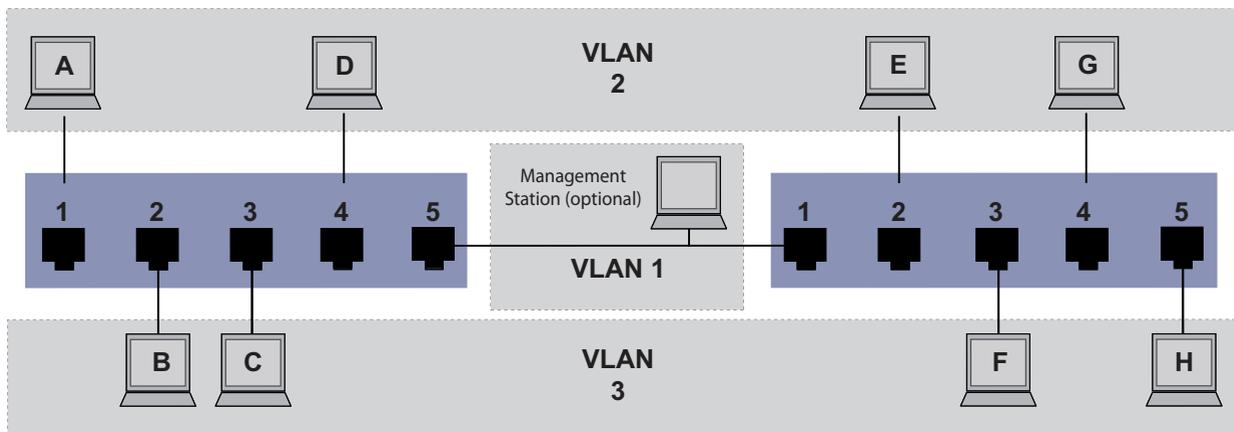


Figure 36: Example of a more complex VLAN configuration

The second example shows a more complex configuration with 3 VLANs (1 to 3). Along with the Switch from example 1, you use a 2nd Switch (on the right in the example).

The simple network divides the terminal devices, A - H, of the individual VLANs over 2 transmission devices (Switches). VLANs configured in this manner are „distributed VLANs“. When configured correctly the VLANs allow the optional Management Station to access the network components.

**Note:** In this case, VLAN 1 has no significance for the terminal device communication, but it is required for the administration of the transmission devices via what is known as the Management VLAN.

As in the previous example, uniquely assign the ports with their connected terminal devices to a VLAN. With the direct connection between the 2 transmission devices (uplink), the ports transport packets for both VLANs. To differentiate these uplinks you use “VLAN tagging”, which handles the frames accordingly. Thus, you maintain the assignment to the respective VLANs.

Proceed as follows to perform the example configuration:

Add Uplink Port 5 to the ingress and egress tables from example 1.  
Create new ingress and egress tables for the right switch, as described in the first example.

The egress table specifies at which ports the Switch may send the frames from this VLAN. Your entry also defines whether the Switch marks (tags) the Ethernet frames sent from this port.

- ▶ T = with tag field (T = tagged, marked)
- ▶ U = without tag field (U = untagged, not marked)

In this example, the devices use tagged frames in the communication between the transmission devices (uplink), the ports differentiate the frames for different VLANs.

| Terminal | Port | Port VLAN identifier (PVID) |
|----------|------|-----------------------------|
| A        | 1    | 2                           |
| B        | 2    | 3                           |
| C        | 3    | 3                           |
| D        | 4    | 2                           |
| Uplink   | 5    | 1                           |

Table 14: Ingress table for device on left

| Terminal | Port | Port VLAN identifier (PVID) |
|----------|------|-----------------------------|
| Uplink   | 1    | 1                           |
| E        | 2    | 2                           |
| F        | 3    | 3                           |
| G        | 4    | 2                           |
| H        | 5    | 3                           |

Table 15: Ingress table for device on right

| VLAN ID | Port |   |   |   |   |
|---------|------|---|---|---|---|
|         | 1    | 2 | 3 | 4 | 5 |
| 1       |      |   |   |   | U |
| 2       | U    |   |   | U | T |
| 3       |      | U | U |   | T |

Table 16: Egress table for device on left

| VLAN ID | Port |   |   |   |   |
|---------|------|---|---|---|---|
|         | 1    | 2 | 3 | 4 | 5 |
| 1       | U    |   |   |   |   |

Table 17: Egress table for device on right

| VLAN ID | Port |   |   |
|---------|------|---|---|
| 2       | T    | U | U |
| 3       | T    | U | U |

Table 17: Egress table for device on right

The communication relationships here are as follows: terminal devices at ports 1 and 4 of the left device and terminal devices at ports 2 and 4 of the right device are members of VLAN 2 and can thus communicate with each other. The behavior is the same for the terminal devices at ports 2 and 3 of the left device and the terminal devices at ports 3 and 5 of the right device. These belong to VLAN 3.

The terminal devices “see” their respective part of the network. Participants outside this VLAN cannot be reached. The device also sends broadcast, multicast, and unicast packets with unknown (unlearned) destination addresses exclusively inside a VLAN.

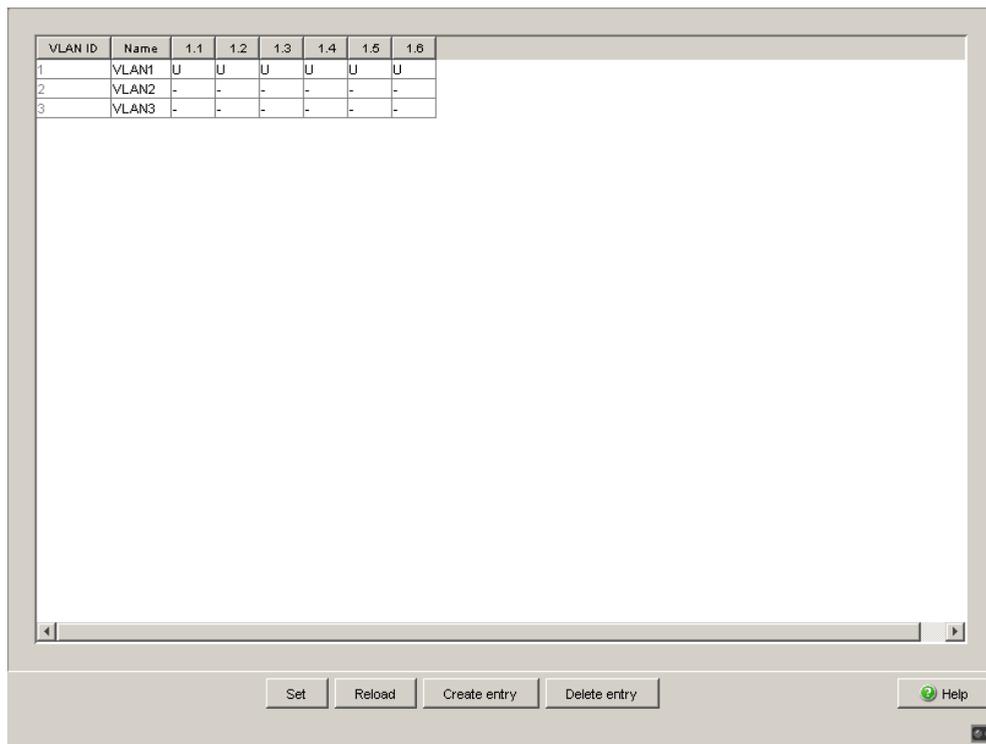
Here, VLAN tagging (IEEE 801.1Q) is used within the VLAN with the ID 1 (Uplink). You can see this from the letter T in the egress table of the ports.

The configuration of the example is the same for the device on the right. Proceed in the same way, using the ingress and egress tables created above to adapt the previously configured left device to the new environment.

Proceed as follows to perform the example configuration:

Configure VLAN

Open the `Switching:VLAN:Static` dialog.



*Figure 37: Creating and naming new VLANs*

- Click on "Create" to open the window for entering the VLAN ID.
- Assign VLAN ID 2 to the VLAN.
- You give this VLAN the name VLAN2 by clicking on the field and entering the name. Also change the name for VLAN 1 from `Default` to `VLAN1`.
- Repeat the previous steps and create another VLAN with the VLAN ID 3 and the name `VLAN3`.

```
enable
vlan database
vlan 2
vlan name 2 VLAN2

vlan 3
vlan name 3 VLAN3

vlan name 1 VLAN1

exit
```

Switch to the privileged EXEC mode.

Switch to the VLAN configuration mode.

Create a new VLAN with the VLAN ID 2.

Give the VLAN with the VLAN ID 2 the name `VLAN2`.

Create a new VLAN with the VLAN ID 3.

Give the VLAN with the VLAN ID 3 the name `VLAN3`.

Give the VLAN with the VLAN ID 1 the name `VLAN1`.

Switch to the privileged EXEC mode.

```

show vlan brief Display the current VLAN configuration.
Max. VLAN ID..... 4042
Max. supported VLANs..... 255
Number of currently configured VLANs..... 3
VLAN 0 Transparent Mode (Prio. Tagged Frames).. Disabled
VLAN ID VLAN Name VLAN Type VLAN Creation Time

1 VLAN1 Default 0 days, 00:00:05
2 VLAN2 Static 0 days, 02:44:29
3 VLAN3 Static 0 days, 02:52:26

```

## □ Configuring the ports

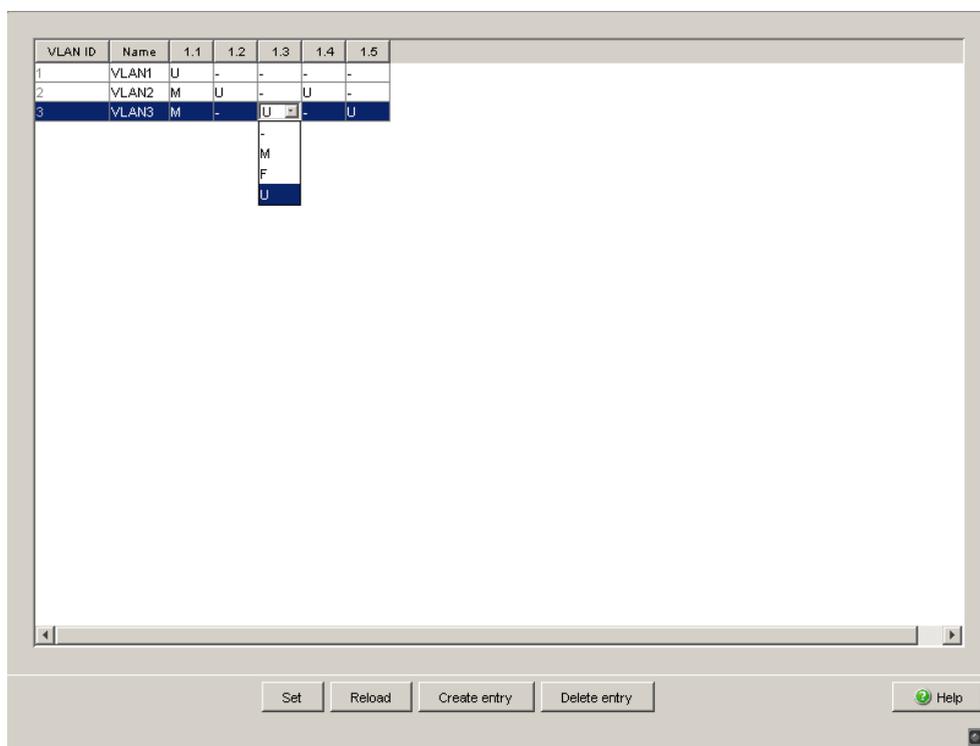


Figure 38: Defining the VLAN membership of the ports.

- Assign the ports of the device to the corresponding VLANs by clicking on the related table cell to open the selection menu and define the status. The selection options are:

- ▶ - = currently not a member of this VLAN (GVRP allowed)
- ▶ T = member of VLAN; send data packets with tag
- ▶ U = Member of the VLAN; send data packets without tag
- ▶ F = not a member of the VLAN (also disabled for GVRP)

Because terminal devices usually interpret untagged data packets, you select the **U** setting. You select the **T** setting on the uplink port on which the VLANs communicate with each other.

- Click "Set" to save the changes temporarily.

Open the Switching:VLAN:Port dialog.

| Port | Port-VLAN-ID | Acceptable Frame Types | Ingress Filtering        |
|------|--------------|------------------------|--------------------------|
| 1.1  | 1            | admitAll               | <input type="checkbox"/> |
| 1.2  | 1            | admitAll               | <input type="checkbox"/> |
| 1.3  | 1            | admitAll               | <input type="checkbox"/> |
| 1.4  | 1            | admitAll               | <input type="checkbox"/> |
| 1.5  | 1            | admitAll               | <input type="checkbox"/> |
| 1.6  | 1            | admitOnlyVlanTag       | <input type="checkbox"/> |
| 1.7  | 1            | admitAll               | <input type="checkbox"/> |
| 1.8  | 1            | admitAll               | <input type="checkbox"/> |
| 1.9  | 1            | admitAll               | <input type="checkbox"/> |
| 1.10 | 1            | admitAll               | <input type="checkbox"/> |
| 1.11 | 1            | admitAll               | <input type="checkbox"/> |
| 1.12 | 1            | admitAll               | <input type="checkbox"/> |
| 1.13 | 1            | admitAll               | <input type="checkbox"/> |
| 1.14 | 1            | admitAll               | <input type="checkbox"/> |
| 1.15 | 1            | admitAll               | <input type="checkbox"/> |
| 1.16 | 1            | admitAll               | <input type="checkbox"/> |

*Figure 39: Assigning and saving "Port VLAN ID", "Acceptable Frame Types" and "Ingress Filtering"*

- Assign the ID of the related VLANs (1 to 3) to the individual ports.
- Because terminal devices usually send data packets as untagged, you select the `admitAll` setting for the terminal device ports. Configure the uplink port with `admit only VLAN tags`.
- To evaluate the VLAN tag on this port, activate "Ingress Filtering" on the uplink port.
- Click "Set" to save the changes temporarily.
- Select the `Basics: Load/Save dialog`.
- In the "Save" frame, select "To Device" for the location and click "Save" to permanently save the configuration in the active configuration.

```
enable
configure
interface 1/1
```

```
vlan participation include 1
vlan participation include 2
vlan tagging 2
```

Switch to the privileged EXEC mode.

Switch to the Configuration mode.

Switch to the Interface Configuration mode of interface 1/1.

Port 1/1 becomes member untagged in VLAN 1.

Port 1/1 becomes member untagged in VLAN 2.

Port 1/1 becomes member tagged in VLAN 2.

```

vlan participation include 3 Port 1/1 becomes member untagged in VLAN 3.
vlan tagging 3 Port 1/1 becomes member tagged in VLAN 3.
vlan pvid 1 Port 1/1 is assigned the port VLAN ID 1.
vlan ingressfilter Port 1/1 ingress filtering is activated.
vlan acceptframe vlanonly Port 1/1 only forwards frames with a VLAN tag.
exit Switch to the Configuration mode.
interface 1/2 Switch to the interface configuration mode for
port 1.2.

vlan participation include 2 Port 1/2 becomes member untagged in VLAN 2.
vlan pvid 2 Port 1/2 is assigned the port VLAN ID 2.
exit Switch to the Configuration mode.
interface 1/3 Switch to the Interface Configuration mode of
Interface 1/3.

vlan participation include 3 Port 1/3 becomes member untagged in VLAN 3.
vlan pvid 3 Port 1/3 is assigned the port VLAN ID 3.
exit Switch to the Configuration mode.
interface 1/4 Switch to the interface configuration mode of
interface 1/4.

vlan participation include 2 Port 1/4 becomes member untagged in VLAN 2.
vlan pvid 2 Port 1/4 is assigned the port VLAN ID 2.
exit Switch to the Configuration mode.
interface 1/5 Switch to the interface configuration mode for port
1.5.

vlan participation include 3 Port 1/5 becomes member untagged in VLAN 3.
vlan pvid 3 Port 1/5 is assigned the port VLAN ID 3.
exit Switch to the Configuration mode.
exit Switch to the privileged EXEC mode.
show vlan 3 Show details for VLAN 3.
VLAN ID : 3
VLAN Name : VLAN3
VLAN Type : Static
VLAN Creation Time: 0 days, 00:07:47 (System Uptime)
Interface Current Configured Tagging

1/1 Include Include Tagged
1/2 Exclude Autodetect Untagged
1/3 Include Include Untagged
1/4 Exclude Autodetect Untagged
1/5 Include Include Untagged

```

For further information on VLANs, see the reference manual and the integrated help function in the program.

## 9 Operation Diagnosis

The device provides you with the following diagnostic tools:

- ▶ Sending traps
- ▶ Monitoring the device status
- ▶ Out-of-band signaling via signal contact
- ▶ Port status indication
- ▶ Event counter at port level
- ▶ Detecting non-matching duplex modes
- ▶ SFP status display
- ▶ Topology Discovery
- ▶ Detecting IP address conflicts
- ▶ Detecting loops
- ▶ Reports
- ▶ Monitoring data traffic at a port (port mirroring)
- ▶ Syslog
- ▶ Event log

## 9.1 Sending Traps

The device reports unusual events which occur during normal operation immediately to the management station. This is done by messages called traps that bypass the polling procedure ("Polling" means querying the data stations at regular intervals). Traps allow you to react quickly to unusual events.

Examples of such events are:

- ▶ Hardware reset
- ▶ Changes to the configuration
- ▶ Segmentation of a port

The device sends traps to various hosts to increase the transmission reliability for the messages. The unacknowledged trap message consists of a packet containing information about an unusual event.

The device sends traps to those hosts entered in the trap destination table. The device allows you to configure the trap destination table with the management station via SNMP.

### 9.1.1 List of SNMP traps

The following table shows a list of the traps that can be sent by the device.

| Trap name                  | Meaning                                                                                                                                                                                                    |
|----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| authenticationFailure      | this is sent if a station attempts to access an agent without authorisation.                                                                                                                               |
| coldStart                  | this is sent during the boot phase for both cold starts and warm starts, after successful initialisation of the network management.                                                                        |
| hmAutoconfigAdapterTrap    | this is sent when the AutoConfiguration AdapterACA is disconnected or connected.                                                                                                                           |
| linkDown                   | this is sent if the connection to a port is interrupted.                                                                                                                                                   |
| linkUp                     | this is sent when connection is established to a port.                                                                                                                                                     |
| hmTemperature              | this is sent if the temperature exceeds the set threshold limits.                                                                                                                                          |
| hmPowerSupply              | this is sent if the power supply status changes.                                                                                                                                                           |
| hmSigConRelayChange        | this is sent if the status of the signal contact changes in the function monitoring.                                                                                                                       |
| newRoot                    | this is sent if the sending agent becomes the new root of the spanning tree.                                                                                                                               |
| topologyChange             | this is sent if the switching mode of a port changes.                                                                                                                                                      |
| risingAlarm                | this is sent if an RMON alarm input exceeds its upper threshold.                                                                                                                                           |
| fallingAlarm               | this is sent if an RMON alarm input goes below its lower threshold.                                                                                                                                        |
| hmPortSecurityTrap         | this is sent if an MAC/IP address detected on this port does not correspond to the current settings for<br>– hmPortSecPermission and<br>– hmPorSecAction is set to either trapOnly (2) or portDisable (3). |
| hmModuleMapChange          | this is sent if the hardware configuration changes.                                                                                                                                                        |
| hmBPDUGuardTrap            | this is sent if a BPDU is received on a port while the BPDU Guard function is active.                                                                                                                      |
| hmMrpReconfig              | this is sent if the configuration of the MRP Ring changes.                                                                                                                                                 |
| hmRingRedReconfig          | this is sent if the configuration of the HIPER Ring changes.                                                                                                                                               |
| hmRingRedCplReconfig       | this is sent if the configuration of the redundant ring/network coupling changes.                                                                                                                          |
| hmSNTPTrap                 | this is sent if an error occurs in relation to the SNTP (e.g. server not available).                                                                                                                       |
| hmRelayDuplicateTrap       | this is sent if a duplicate IP address is detected in relation to DHCP Option 82.                                                                                                                          |
| lldpRemTablesChangeTrap    | this is sent if an entry in the Remote Table topology changes.                                                                                                                                             |
| hmConfigurationSavedTrap   | this is sent after the device has successfully saved its configuration locally.                                                                                                                            |
| hmConfigurationChangedTrap | this is sent if you change the configuration of the device after saving locally for the first time.                                                                                                        |

Table 18: Possible traps

---

| Trap name                  | Meaning                                                                                                                                                                                                     |
|----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| hmAddressRelearnDetectTrap | this is sent if Address Relearn Detection is active and the relearn threshold for MAC addresses on different ports is exceeded. This process indicates high probability of a loop situation on the network. |
| hmDuplexMismatchTrap       | this is sent if the device detects a possible problem with duplex mode on a port.                                                                                                                           |
| hmTrapRebootOnError        | this is sent if the device detects an error which is to be corrected by a cold start.                                                                                                                       |

---

*Table 18: Possible traps*

## 9.1.2 SNMP Traps when Booting

The device sends the ColdStart trap during every booting.

### 9.1.3 Configuring Traps

- Open the `Diagnostics:Alarms (Traps)` dialog. This dialog allows you to determine which events trigger an alarm (trap) and where these alarms should be sent.
- Click "Create".
- In the "IP Address" column, enter the IP address of the management station to which the traps should be sent.
- In the "Enabled" column, you mark the entries that the device should take into account when it sends traps. Default setting: inactive.
- In the column "Password", enter the community name that the device uses to identify itself as the trap's source.
- In the "Configuration" frame, select the trap categories from which you want to send traps. Default setting: all trap categories are active.

**Note:** You need read-write access for this dialog.

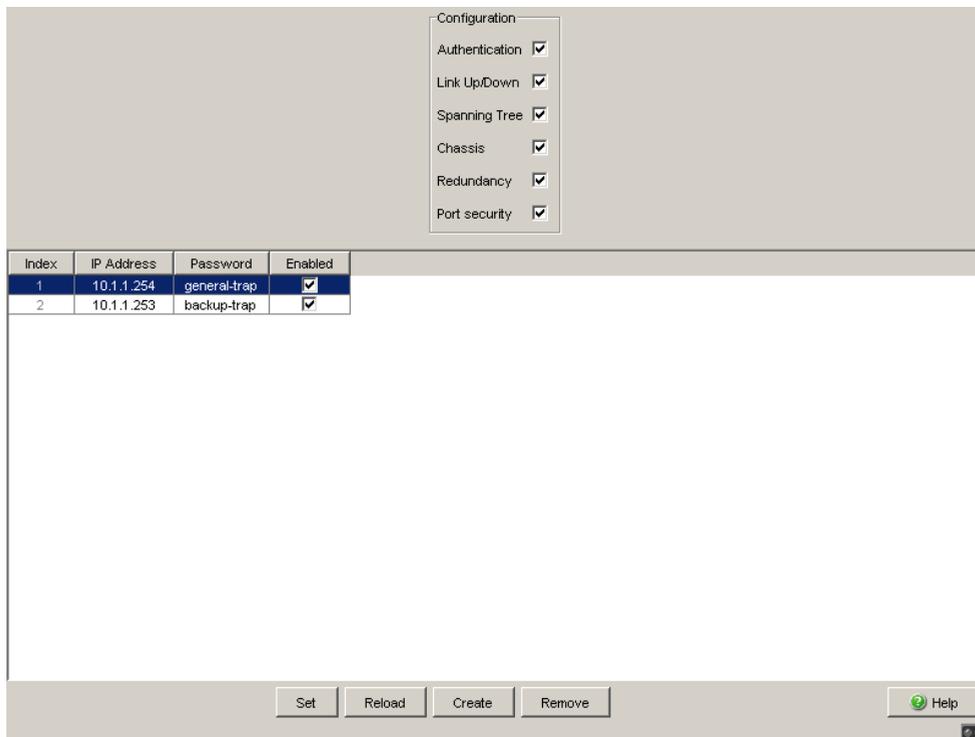


Figure 40: Alarms dialog

The events which can be selected are:

| Name           | Meaning                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|----------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Authentication | The device has rejected an unauthorized access attempt (see the <code>Access for IP Addresses and Port Security</code> dialog).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Link Up/Down   | At one port of the device, the link to another device has been established/interrupted.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Spanning Tree  | The topology of the Rapid Spanning Tree has changed.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Chassis        | <p>Summarizes the following events:</p> <ul style="list-style-type: none"> <li>– The status of a supply voltage has changed (see the <code>System</code> dialog).</li> <li>– The status of the signal contact has changed.</li> </ul> <p>To take this event into account, you activate “Create trap when status changes” in the <code>Diagnostics:Signal Contact 1/2</code> dialog.</p> <ul style="list-style-type: none"> <li>- The AutoConfiguration Adapter (ACA), has been added or removed.</li> <li>- The configuration on the AutoConfiguration Adapter(ACA) does not match that in the device.</li> <li>– The temperature thresholds have been exceeded/not reached.</li> <li>– A media module has been added or removed (only for modular devices).</li> <li>– The receiver power status of a port with an SFP module has changed (see dialog <code>Diagnostics:Ports:SFP Modules</code>).</li> </ul> <p>The redundancy status of the ring redundancy (redundant line active/inactive) or (for devices that support redundant ring/network coupling) the redundant ring/network coupling (redundancy exists) has changed.</p> |
| Port security  | On one port a data packet has been received from an unauthorized terminal device (see the <code>Port Security</code> dialog).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |

*Table 19: Trap categories*

---

## 9.2 Monitoring the Device Status

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

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

The device enables you to

- ▶ signal the device status out-of-band via a signal contact  
(see on page 177 "Monitoring the Device Status via the Signal Contact")
- ▶ signal the device status by sending a trap when the device status changes
- ▶ detect the device status in the graphical user interface on the system side.
- ▶ query the device status in the Command Line Interface.

The `Diagnostics:Device Status` dialog of the device includes:

- ▶ Incorrect supply voltage
  - at least one of the 2 supply voltages is not operating,
  - the internal supply voltage is not operating.
- ▶ The temperature threshold has been exceeded or has not been reached.
- ▶ The removal of a module (for modular devices).
- ▶ The removal of the ACA.
- ▶ The configuration on the external memory does not match that in the device.
- ▶ The interruption of the connection at at least one port. In the `Basic Settings:Port Configuration` menu, you define which ports the device signals if the connection is down (see on page 84 "Displaying detected loss of connection"). On delivery, there is no link monitoring.

- ▶ Events for ring redundancy:  
Loss of the redundancy (in ring manager mode). On delivery, ring redundancy monitoring is inactive.  
The device is a normal ring participant and detects an error in the local configuration.
- ▶ Event in the ring/network coupling:  
Loss of the redundancy. On delivery, there is no ring redundancy monitoring.  
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

Select the corresponding entries to decide which events the device status includes.

**Note:** With a non-redundant voltage supply, the device reports the absence of a supply voltage. If you do not want this message to be displayed, feed the supply voltage over both inputs or switch off the monitoring ([see on page 177 “Monitoring the Device Status via the Signal Contact”](#)).

## 9.2.1 Configuring the Device Status

- Open the `Diagnostics:Device Status` dialog.
- In the “Monitoring” field, you select the events you want to monitor.
- To monitor the temperature, you also set the temperature thresholds in the `Basic settings:System` dialog at the end of the system data.

enable  
configure

Change to the privileged EXEC mode.  
Change to the Configuration mode.

```
device-status monitor all
error
device-status trap enable
```

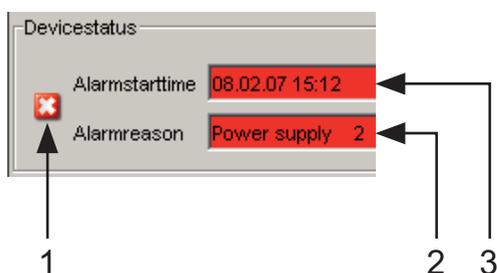
Include all the possible events in the device status determination.

Enable a trap to be sent if the device status changes.

**Note:** The above CLI commands activate the monitoring and the trapping respectively for all the supported components. If you want to activate or deactivate monitoring only for individual components, you will find the corresponding syntax in the CLI manual or in the help of the CLI console (enter a question mark “?” at the CLI prompt).

## 9.2.2 Displaying the Device Status

Select the `Basics: System` dialog.



*Figure 41: Device status and alarm display*

*1 - The symbol displays the device status*

*2 - Cause of the oldest existing alarm*

*3 - Start of the oldest existing alarm*

 `exit``show device-status`

Change to the privileged EXEC mode.

Display the device status and the setting for the device status determination.

---

## 9.3 Out-of-band Signaling

The signal contact is used to control external devices and monitor the operation of the device. Function monitoring enables you to perform remote diagnostics.

The device reports the operating status via a break in the potential-free signal contact (relay contact, closed circuit):

- ▶ Incorrect supply voltage
  - at least one of the 2 supply voltages is not operating,
  - the internal supply voltage is not operating.
- ▶ The temperature threshold has been exceeded or has not been reached.
- ▶ The removal of a module (for modular devices).
- ▶ The removal of the ACA.
- ▶ The configuration on the external memory does not match that in the device.
- ▶ The interruption of the connection at at least one port. In the `Basic Settings:Port Configuration` menu, you define which ports the device signals if the connection is down ([see on page 84 “Displaying detected loss of connection”](#)). On delivery, there is no link monitoring.
- ▶ Events for ring redundancy:
  - Loss of the redundancy (in ring manager mode). On delivery, ring redundancy monitoring is inactive.
  - The device is a normal ring participant and detects an error in the local configuration.
- ▶ Event in the ring/network coupling:
  - Loss of the redundancy. On delivery, there is no ring redundancy monitoring.
  - 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

Select the corresponding entries to decide which events the device status includes.

**Note:** With a non-redundant voltage supply, the device reports the absence of a supply voltage. If you do not want this message to be displayed, feed the supply voltage over both inputs or switch off the monitoring ([see on page 177 “Monitoring the Device Status via the Signal Contact”](#)).

### 9.3.1 Controlling the Signal Contact

With this mode you control this signal contact remotely.

Application options:

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

- Select the `Diagnostics:Signal Contact 1/2` dialog.
- In the "Mode Signal contact" frame, you select the "Manual setting" mode to switch the contact manually.
- Select "Opened" in the "Manual setting" frame to open the contact.
- Select "Closed" in the "Manual setting" frame to close the contact.

|                              |                                                      |
|------------------------------|------------------------------------------------------|
| enable                       | Switch to the privileged EXEC mode.                  |
| configure                    | Switch to the Configuration mode.                    |
| signal-contact 1 mode manual | Select the manual setting mode for signal contact 1. |
| signal-contact 1 state open  | Open signal contact 1.                               |
| signal-contact 1 state close | Close signal contact 1.                              |

## 9.3.2 Monitoring the Device Status via the Signal Contact

The "Device Status" option enables you, like in the operation monitoring, to monitor the device state (see on page 177 "Monitoring the Device Status via the Signal Contact") via the signal contact.

## 9.3.3 Monitoring the Device Functions via the Signal Contact

### ■ Configuring the operation monitoring

- Select the `Diagnostics:Signal Contact` dialog.
- Select "Monitoring correct operation" in the "Mode signal contact" frame to use the contact for operation monitoring.
- In the "Monitoring correct operation" frame, 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.

|                                           |                                                                              |
|-------------------------------------------|------------------------------------------------------------------------------|
| <code>enable</code>                       | Switch to the privileged EXEC mode.                                          |
| <code>configure</code>                    | Switch to the Configuration mode.                                            |
| <code>signal-contact 1 monitor all</code> | Includes all the possible events in the operation monitoring.                |
| <code>signal-contact 1 trap enable</code> | Enables a trap to be sent if the status of the operation monitoring changes. |

### ■ Displaying the signal contact's status

The device gives you 3 additional options for displaying the status of the signal contact:

- ▶ LED display on device,
- ▶ display in the graphical user interface,
- ▶ query in the Command Line Interface.

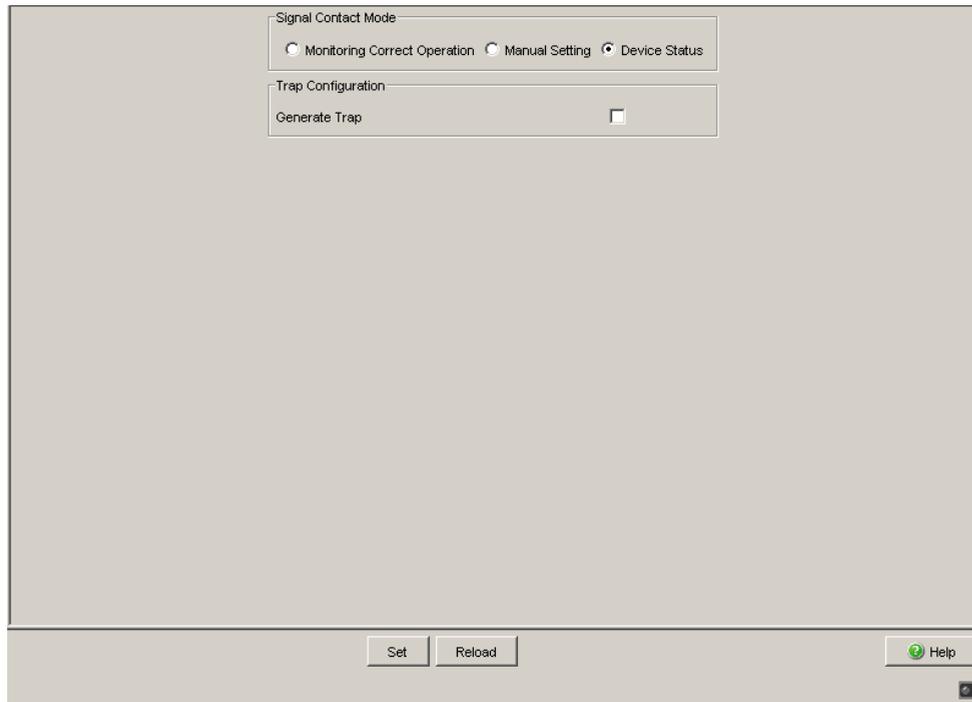


Figure 42: Signal Contact dialog

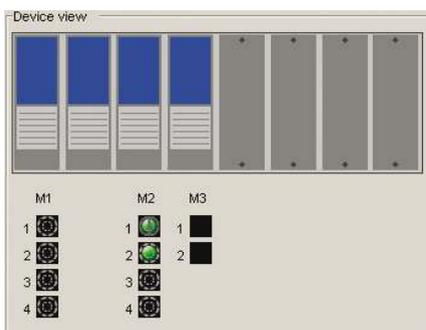
```
exit
show signal-contact 1
```

Change to the privileged EXEC mode.  
Displays the status of the operation monitoring  
and the setting for the status determination.

## 9.4 Port Status Indication

- Select the `Basics: System` dialog.

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



*Figure 43: 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 (100 MBit/s) is in the discarding mode of a redundancy protocol such as Spanning Tree or HIPER-Ring.



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

## 9.5 Event Counter at Port Level

The port statistics table enables experienced network administrators to identify possible detected problems in the network.

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

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

| Counter            | Indication of known possible weakness                                                                                                                                                                                    |
|--------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Received fragments | <ul style="list-style-type: none"> <li>– Non-functioning controller of the connected device</li> <li>– Electromagnetic interference in the transmission medium</li> </ul>                                                |
| CRC error          | <ul style="list-style-type: none"> <li>– Non-functioning controller of the connected device</li> <li>– Electromagnetic interference in the transmission medium</li> <li>– Inoperable component in the network</li> </ul> |
| Collisions         | <ul style="list-style-type: none"> <li>– Non-functioning controller of the connected device</li> <li>– Network over extended/lines too long</li> <li>– Collision or a detected fault with a data packet</li> </ul>       |

*Table 20: Examples indicating known weaknesses*

- Select the `Diagnostics:Ports:Statistics` dialog.
- To reset the counters, click on "Reset port counters" in the Basic Settings:Restart dialog.

| Port | Transmitted Packets | Transmitted Unicast Packets | Transmitted Non Unicast Packets | Received Packets | Received Octets | Received Fragments | Detected CRC errors | Detected Collisions | Detected Late Collisions |
|------|---------------------|-----------------------------|---------------------------------|------------------|-----------------|--------------------|---------------------|---------------------|--------------------------|
| 1.1  | 95814               | 47099                       | 48715                           | 49154            | 5913348         | 0                  | 0                   | 0                   | 0                        |
| 1.2  | 576243              | 553589                      | 22654                           | 740869           | 129805821       | 0                  | 0                   | 0                   | 0                        |
| 1.3  | 297568              | 249662                      | 47906                           | 279692           | 54137857        | 0                  | 0                   | 0                   | 0                        |
| 1.4  | 0                   | 0                           | 0                               | 0                | 0               | 0                  | 0                   | 0                   | 0                        |
| 2.1  | 243648              | 34570                       | 209078                          | 52045            | 10200063        | 0                  | 0                   | 0                   | 0                        |
| 2.2  | 0                   | 0                           | 0                               | 0                | 0               | 0                  | 0                   | 0                   | 0                        |
| 2.3  | 0                   | 0                           | 0                               | 0                | 0               | 0                  | 0                   | 0                   | 0                        |
| 2.4  | 232380              | 24750                       | 207630                          | 31423            | 7025437         | 0                  | 3                   | 0                   | 0                        |
| 3.1  | 0                   | 0                           | 0                               | 0                | 0               | 0                  | 0                   | 0                   | 0                        |
| 3.2  | 0                   | 0                           | 0                               | 0                | 0               | 0                  | 0                   | 0                   | 0                        |

Figure 44: Port Statistics dialog

### 9.5.1 Detecting Non-matching Duplex Modes

If the duplex modes of 2 ports directly connected to each other do not match, this can cause problems that are difficult to track down. The automatic detection and reporting of this situation has the benefit of recognizing it before problems occur.

This situation can arise from an incorrect configuration, e.g. if you deactivate the automatic configuration at the remote port.

A typical effect of this non-matching is that at a low data rate, the connection seems to be functioning, but at a higher bi-directional traffic level the local device records a lot of CRC errors, and the connection falls significantly below its nominal capacity.

The device allows you to detect this situation and report it to the network management station. In the process, the device evaluates the error counters of the port in the context of the port settings.

### ■ Possible causes of port error events

The following table lists the duplex operating modes for TX ports, with the possible fault events. The meanings of terms used in the table are as follows:

- ▶ Collisions: In half-duplex mode, collisions mean normal operation.
- ▶ Duplex problem: Mismatching duplex modes.
- ▶ EMI: Electromagnetic interference.
- ▶ Network extension: The network extension is too great, or too many cascading hubs.
- ▶ Collisions, late collisions: In full-duplex mode, no incrementation of the port counters for collisions or late collisions.
- ▶ CRC error: The device evaluates these errors as non-matching duplex modes in the manual full duplex mode.

| No. | Automatic configuration | Current duplex mode | Detected error events (≥ 10 after link up) | Duplex modes            | Possible causes                        |
|-----|-------------------------|---------------------|--------------------------------------------|-------------------------|----------------------------------------|
| 1   | On                      | Half duplex         | None                                       | OK                      |                                        |
| 2   | On                      | Half duplex         | Collisions                                 | OK                      |                                        |
| 3   | On                      | Half duplex         | Late collisions                            | Duplex problem detected | Duplex problem, EMI, network extension |
| 4   | On                      | Half duplex         | CRC error                                  | OK                      | EMI                                    |
| 5   | On                      | Full duplex         | None                                       | OK                      |                                        |
| 6   | On                      | Full duplex         | Collisions                                 | OK                      | EMI                                    |
| 7   | On                      | Full duplex         | Late collisions                            | OK                      | EMI                                    |
| 8   | On                      | Full duplex         | CRC error                                  | OK                      | EMI                                    |
| 9   | Off                     | Half duplex         | None                                       | OK                      |                                        |
| 10  | Off                     | Half duplex         | Collisions                                 | OK                      |                                        |
| 11  | Off                     | Half duplex         | Late collisions                            | Duplex problem detected | Duplex problem, EMI, network extension |
| 12  | Off                     | Half duplex         | CRC error                                  | OK                      | EMI                                    |
| 13  | Off                     | Full duplex         | None                                       | OK                      |                                        |
| 14  | Off                     | Full duplex         | Collisions                                 | OK                      | EMI                                    |

Table 21: Evaluation of non-matching of the duplex mode

| No. | Automatic configuration | Current duplex mode | Detected error events (≥ 10 after link up) | Duplex modes            | Possible causes     |
|-----|-------------------------|---------------------|--------------------------------------------|-------------------------|---------------------|
| 15  | Off                     | Full duplex         | Late collisions                            | OK                      | EMI                 |
| 16  | Off                     | Full duplex         | CRC error                                  | Duplex problem detected | Duplex problem, EMI |

Table 21: Evaluation of non-matching of the duplex mode (cont.)

### ■ Activating the detection

- Select the `Switching:Switching` Global dialog.
- Select “Activate Duplex Mismatch Detection”. The device then checks whether the duplex mode of a port might not match that of the remote port.  
If the device detects a potential mismatch, it creates an entry in the event log and sends an alarm (trap).

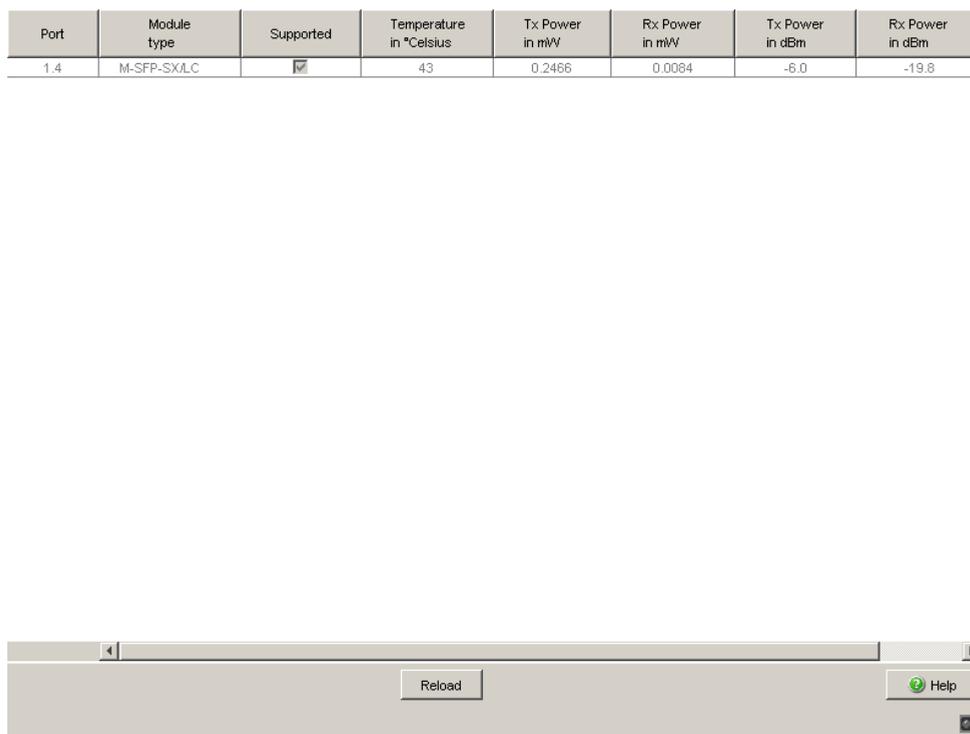
|                                                                                                                            |                                                                                                                                                                                                                                             |
|----------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <pre>enable configure bridge duplex-mismatch-detect operation enable bridge duplex-mismatch-detect operation disable</pre> | <p>Change to the privileged EXEC mode.</p> <p>Change to the Configuration mode.</p> <p>Activates the detection and reporting of non-matching duplex modes.</p> <p>Deactivates the detection and reporting of non-matching duplex modes.</p> |
|----------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

## 9.6 Displaying the SFP Status

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

- ▶ module type
- ▶ support provided in media module
- ▶ temperature in ° C
- ▶ transmission power in mW
- ▶ receive power in mW

Select the `Diagnostics:Ports:SFP` modules dialog.



| Port | Module type | Supported                           | Temperature in °Celsius | Tx Power in mW | Rx Power in mW | Tx Power in dBm | Rx Power in dBm |
|------|-------------|-------------------------------------|-------------------------|----------------|----------------|-----------------|-----------------|
| 1.4  | M-SFP-SX/LC | <input checked="" type="checkbox"/> | 43                      | 0.2466         | 0.0084         | -6.0            | -19.8           |

Figure 45: SFP Modules dialog

---

## 9.7 Topology Discovery

### 9.7.1 Description of Topology-Detection

IEEE 802.1AB defines the Link Layer Discovery Protocol (LLDP). LLDP allows the user to automatically detect the LAN network topology.

Devices with LLDP active

- ▶ broadcast their connection and management information to adjacent devices on the shared LAN. These devices can then be evaluated provided they also have LLDP active.
- ▶ receive connection and management information from adjacent devices on the shared LAN, provided these devices also have LLDP active.
- ▶ builds a management-information table and object definitions for storing information about adjacent devices with LLDP active.

As the main element, the connection information contains an exact, unique identifier for the connection end point: MSAP (MAC Service Access Point). This is made up of a device identifier which is unique on the entire network and a unique port identifier for this device.

Content of the connection and management-information:

- ▶ Chassis identifier (its MAC address)
- ▶ Port identifier (its port-MAC address)
- ▶ Description of port
- ▶ System name
- ▶ System description
- ▶ Supported system capabilities
- ▶ System capabilities currently active
- ▶ Interface ID of the management address
- ▶ VLAN-ID of the port
- ▶ Auto-negotiation status at the port
- ▶ Medium, half/full duplex setting and port speed setting

- ▶ Indication whether a redundancy protocol is enabled at the port, and which one (e.g. RSTP, HIPER-Ring, FastHIPER Ring, MRP, ring coupling).
- ▶ Information about the VLANs installed in the device (VLAN-ID and VLAN name, irrespective of whether the port is a VLAN participant).

A network management station can query this information from devices that have LLDP active. This information allows the network management station to form a description of the network topology.

For information exchanges, the LLDP uses an IEEE MAC address, which devices do not normally communicate. Devices without LLDP therefore do not allow support for LLDP packets. If a device without LLDP capability is located between two devices with LLDP capability, then LLDP information exchanges are prevented between these two devices. To work around this, Hirschmann devices send and receive additional LLDP packets with the Hirschmann Multicast-MAC address 01:80:63:2F:FF:0B. Hirschmann-Devices with the LLDP function are therefore able to exchange LLDP information with each other even across devices that do not have LLDP capability.

The Management Information Base (MIB) for a Hirschmann device with LLDP capability holds the LLDP information in the `lldp` MIB and in the private `hmLLDP`.

## 9.7.2 Displaying the Topology Discovery Results

- Select the `Diagnostics:Topology Discovery` dialog.

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

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

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

If

- ▶ devices with active topology discovery function and
- ▶ devices without active topology discovery function are connected to a port

then

- ▶ the topology table hides the devices without active topology discovery.

If

- ▶ only devices without active topology discovery are connected to a port

then

- ▶ 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 122 “Entering Static Addresses”](#)).

## 9.8 Detecting IP Address Conflicts

### 9.8.1 Description of IP Address Conflicts

By definition, each IP address may only be assigned once within a subnetwork. Should two or more devices erroneously share the same IP address within one subnetwork, this will inevitably lead to communication disruptions with devices that have this IP address. In his Internet draft, Stuart Cheshire describes a mechanism that industrial Ethernet devices can use to detect and eliminate address conflicts (Address Conflict Detection, ACD).

| 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.<br>If the IP address already exists, the device will return to the previous configuration, if possible, and make another attempt after 15 seconds. The device therefore avoids to participate in the network traffic with a duplicate IP address.                                                                                                                            |
| passiveOnly         | Enables passive detection only. The device listens passively on the network to determine whether its IP address already exists. If it detects a duplicate IP address, it will initially defend its address by employing the ACD mechanism and sending out gratuitous ARPs. If the remote device does not disconnect from the network, the management interface of the local device will then disconnect from the network. Every 15 seconds, it will poll the network to determine if there is still an address conflict. If there isn't, it will connect back to the network. |

*Table 22: Possible address conflict operation modes*

## 9.8.2 Configuring ACD

- Select the Diagnostics:IP Address Conflict Detection dialog.
- With "Status" you enable/disable the IP address conflict detection or select the operating mode ([see table 22](#)).

## 9.8.3 Displaying ACD

- Select the Diagnostics:IP Address Conflict Detection dialog.
  - ▶ In the table, the device logs IP address conflicts with its IP address. The device logs the following data for each conflict:
    - ▶ the time („Timestamp“ column)
    - ▶ the conflicting IP address („IP Address“ column)
    - ▶ the MAC address of the device with which the IP address conflicted („MAC Address“ column).
  - For each IP address, the device logs a line with the last conflict that occurred.
- During a restart, the device deletes the table.

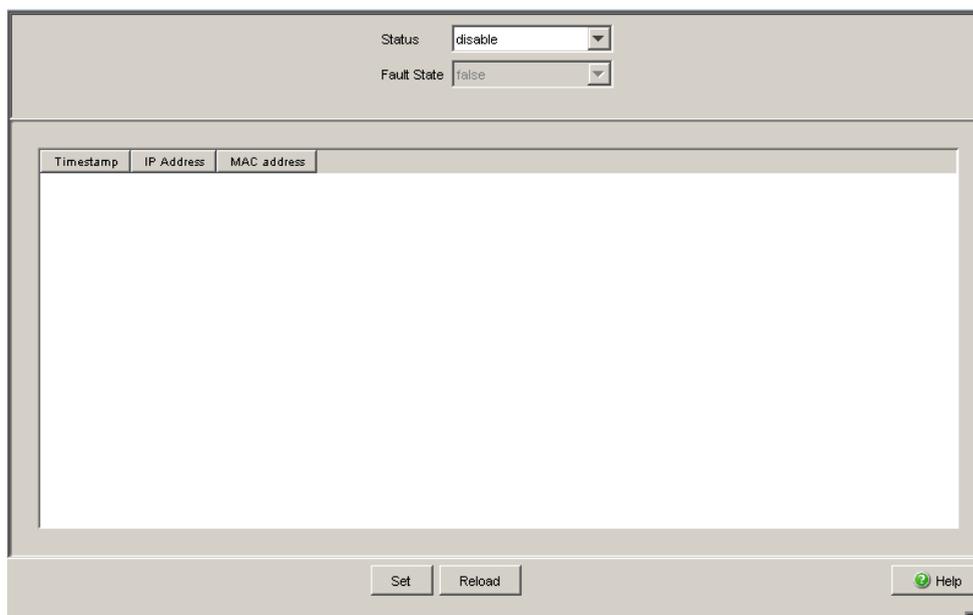


Figure 46: IP Address Conflict Detection dialog

## 9.9 Detecting Loops

Loops in the network, even temporary loops, can cause connection interruptions or data losses that may cause unintended equipment operation. The automatic detection and reporting of this situation allows you to detect it faster and diagnose it more easily.

An incorrect configuration can cause a loop, for example, if you deactivate Spanning Tree.

The device allows you to detect the effects typically caused by loops and report this situation automatically to the network management station. You have the option here to specify the magnitude of the loop effects that triggers the device to send a report.

A typical effect of a loop is that frames from multiple different MAC source addresses can be received at different ports of the device within a short time. The device evaluates how many of the same MAC source addresses it has learned at different ports within a time period. This process detects loops when the same MAC address is received at different ports. Conversely, the same MAC address being received at different ports can also have other causes than a loop.

- Select the `Switching:Switching Global` dialog.
- Select "Enable address relearn detection". Enter the desired threshold value in the "Address relearn threshold" field.

If the address relearn detection is enabled, the device checks whether it has repeatedly learned the same MAC source addresses at different ports. This process very probably indicates a loop situation.

If the device detects that the threshold value set for the MAC addresses has been exceeded at its ports during the evaluation period (a few seconds), the device creates an entry in the log file and sends an alarm (trap). The preset threshold value is 1.

---

## 9.10 Reports

The following reports and buttons 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 the system-relevant data.
- ▶ **Download Support Information.**  
This button allows you to download system information as files in a ZIP archive.

In service situations, these reports provide the technician with the necessary information.

The following button is available as an alternative for operating the Web-based interface:

- ▶ **Download JAR file.**  
This button allows you to download the applet of the Web-based interface as a JAR file. Then you have the option to start the applet outside of a browser.  
This facilitates the device administration even when you have disabled its web server for security reasons.

- To display the HTML file with system-relevant data, select the dialog `Diagnosis:Report:System Information`.
- To view the log file with important device-internal events, select the dialog `Diagnosis:Report:Event Log`.

- Select the `Diagnosis:Report` dialog.
- Click “Download Switch Dump”.
- Select the directory in which you want to save the switch dump.
- Click “Save”.

The device creates the file name of the switch dumps automatically in the format `<IP address>_<system name>.zip`, e.g. for a device of the type PowerMICE: “10.0.1.112\_PowerMICE-517A80.zip”.

- Click “Download JAR-File”.
- Select the directory in which you want to save the applet.
- Click “Save”.

The device creates the file name of the applet automatically in the format `<device type><software variant><software version>_<software revision of applet>.jar`, e.g. for a device of type PowerMICE with software variant L3P: “pmL3P06000\_00.jar”.

## 9.11 Syslog

The device enables you to send messages about important device-internal events to one or more syslog servers (up to 8). Additionally, you can also include SNMP requests to the device as events in the syslog.

**Note:** You will find the actual events that the device has logged in the “Event Log” (see on page 197 “Trap log”) and in the log file (see on page 192 “Reports”), a HTML page with the title “Event Log”.

- Select the `Diagnostics:Syslog` dialog.
- Activate the syslog function in the “Operation” frame.
- Click on “Create”
- In the “IP Address” column, enter the IP address of the syslog server to which the log entries should be sent.
- In the “Port” column, enter the UDP port of the syslog server at which the syslog receives log entries. The default setting is 514.
- In the “Minimum level to report” column, you enter the minimum level of seriousness an event must attain for the device to send a log entry to this syslog server.
- In the “Active” column, you select the syslog servers that the device takes into account when it is sending logs.

“SNMP Logging” frame:

- Activate “Log SNMP Get Request” if you want to send reading SNMP requests to the device as events to the syslog server.
- Select the level to report at which the device creates the events from reading SNMP requests.
- Activate “Log SNMP Set Request” if you want to send writing SNMP requests to the device as events to the syslog server.
- Activate “Log SNMP Set Request” if you want to send writing SNMP requests to the device as events to the syslog server.

**Note:** For more details on setting the SNMP logging, see the “Syslog” chapter in the “GUI” (Graphical User Interface / Web-based Interface) reference manual.

|                                                                                                                                                                                                                               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <pre>enable configure logging host 10.0.1.159 514 3  logging syslog exit show logging hosts Index      IP Address      Severity      Port      Status ----- 1          10.0.1.159      error          514      Active</pre>   | <p>Switch to the privileged EXEC mode.</p> <p>Switch to the Configuration mode.</p> <p>Select the recipient of the log messages and its port 514. The “3” indicates the seriousness of the message sent by the device. “3” means “error”.</p> <p>Enable the Syslog function.</p> <p>Switch to the privileged EXEC mode.</p> <p>Display the syslog host settings.</p>                                                                                                                                                                                                       |
| <pre>enable configure logging snmp-requests get operation enable logging snmp-requests get severity 5  logging snmp-requests set operation enable logging snmp-requests set severity 5  exit show logging snmp-requests</pre> | <p>Switch to the privileged EXEC mode.</p> <p>Switch to the Configuration mode.</p> <p>Create log events from reading SNMP requests.</p> <p>The “5” indicates the seriousness of the message that the device allocates to messages from reading SNMP requests. “5” means “note”.</p> <p>Create log events from writing SNMP requests.</p> <p>The “5” indicates the seriousness of the message that the device allocates to messages from writing SNMP requests. “5” means “note”.</p> <p>Switch to the privileged EXEC mode.</p> <p>Display the SNMP logging settings.</p> |

```
Log SNMP SET requests : enabled
Log SNMP SET severity : notice
Log SNMP GET requests : enabled
Log SNMP GET severity : notice
```

## 9.12 Trap log

The device allows you to call up a log of the system events. The table of the “Trap Log” dialog lists the logged events with a time stamp.

- Click “Reload” to update the content of the trap log.
- Click “Clear” to delete the content of the trap log.

**Note:** You have the option to also send the logged events to one or more syslog servers ([see on page 194 “Syslog”](#)).



# **A Setting up the Configuration Environment**

## A.1 Setting up a DHCP/BOOTP Server

On the product CD supplied with the device you will find the software for a DHCP server from the software development company IT-Consulting Dr. Herbert Hanewinkel. You can test the software for 30 calendar days from the date of the first installation, and then decide whether you want to purchase a license.

- To install the DHCP servers on your PC  
put the product CD in the CD drive of your PC and under Additional Software select “haneWIN DHCP-Server”.  
To carry out the installation, follow the installation assistant.
- Start the DHCP Server program.



Figure 47: Start window of the DHCP server

**Note:** The installation procedure includes a service that is automatically started in the basic configuration when Windows is activated. This service is also active if the program itself has not been started. When started, the service responds to DHCP queries.

- Open the window for the program settings in the menu bar: `Options: Preferences` and select the `DHCP` tab page.
- Enter the settings shown in the illustration and click `OK`.

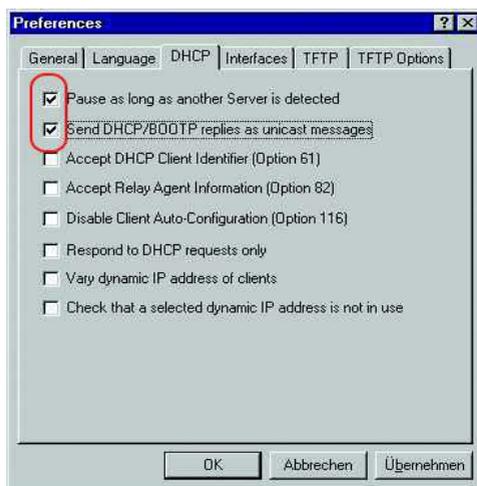


Figure 48: DHCP setting

- To enter the configuration profiles, select `Options: Configuration Profiles` in the menu bar.
- Enter the name of the new configuration profile and click `Add`.

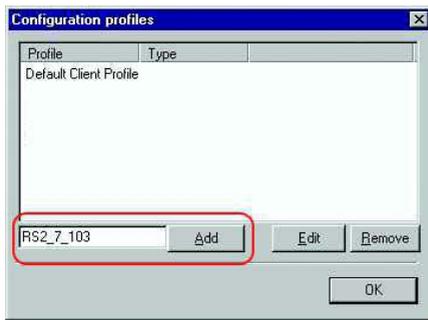


Figure 49: Adding configuration profiles

- Enter the netmask and click `Apply`.

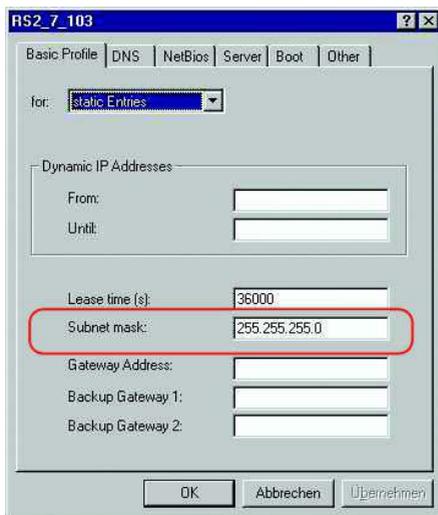


Figure 50: Netmask in the configuration profile

- Select the `Boot` tab page.
- Enter the IP address of your tftp server.
- Enter the path and the file name for the configuration file.
- Click `Apply` and then `OK`.

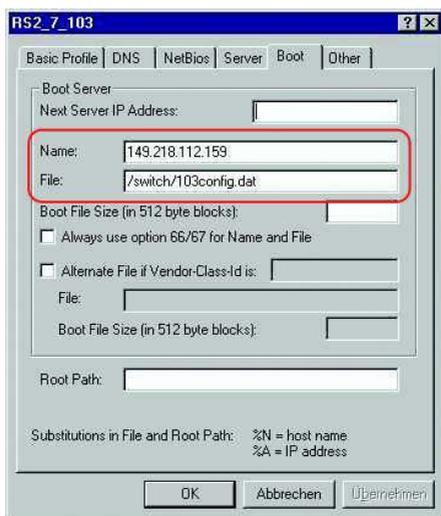


Figure 51: Configuration file on the tftp server

- Add a profile for each device type.  
If devices of the same type have different configurations, then you add a profile for each configuration.  
To complete the addition of the configuration profiles, click **OK**.

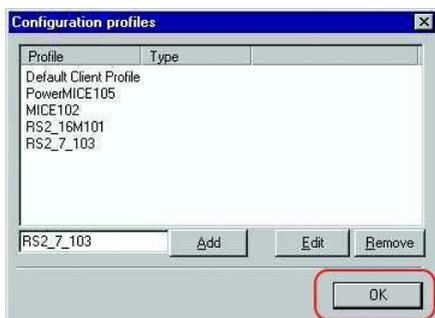


Figure 52: Managing configuration profiles

- To enter the static addresses, click `Static` in the main window.

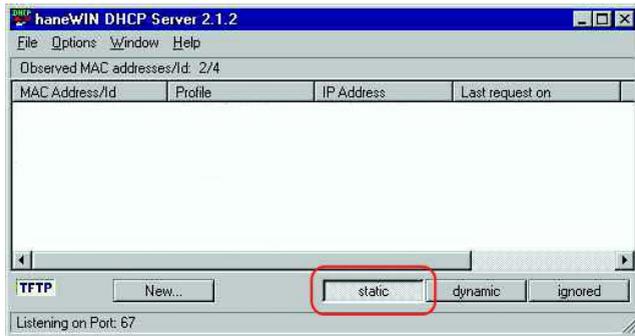


Figure 53: Static address input

- Click New.



Figure 54: Adding static addresses

- Enter the MAC address of the device.
- Enter the IP address of the device.
- Select the configuration profile of the device.
- Click Apply and then OK.

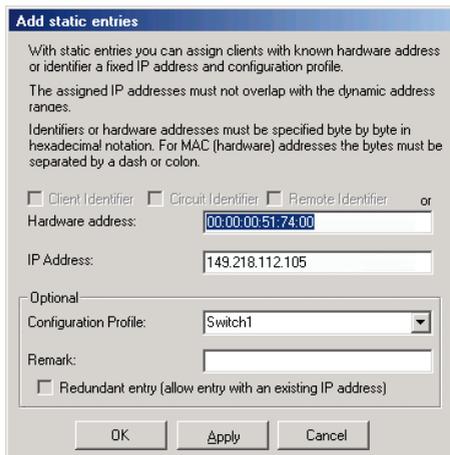


Figure 55: Entries for static addresses

- Add an entry for each device that will get its parameters from the DHCP server.

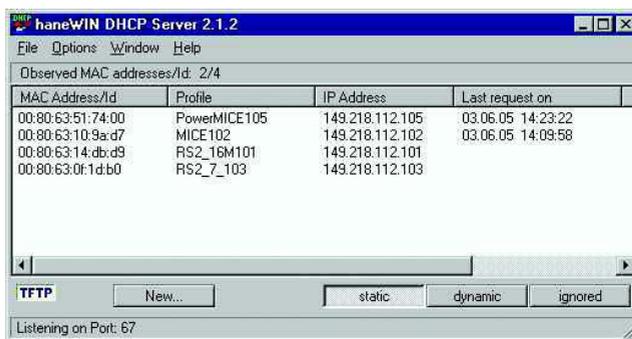


Figure 56: DHCP server with entries

## A.2 Setting up a DHCP Server with Option 82

On the product CD supplied with the device you will find the software for a DHCP server from the software development company IT-Consulting Dr. Herbert Hanewinkel. You can test the software for 30 calendar days from the date of the first installation, and then decide whether you want to purchase a license.

- To install the DHCP servers on your PC  
put the product CD in the CD drive of your PC and under Additional Software select “haneWIN DHCP-Server”.  
To carry out the installation, follow the installation assistant.
- Start the DHCP Server program.



Figure 57: Start window of the DHCP server

**Note:** The installation procedure includes a service that is automatically started in the basic configuration when Windows is activated. This service is also active if the program itself has not been started. When started, the service responds to DHCP queries.

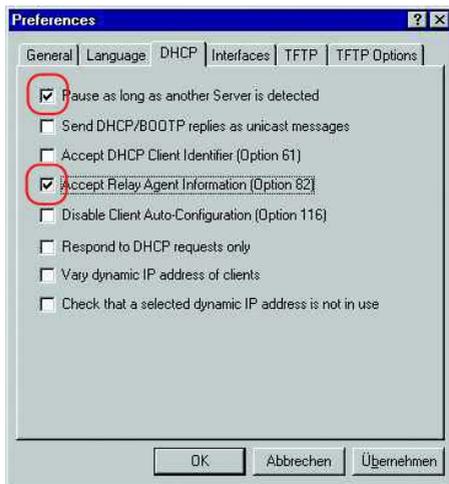


Figure 58: DHCP setting

- To enter the static addresses, click **New**.



Figure 59: Adding static addresses

- Select **Circuit Identifier** and **Remote Identifier**.

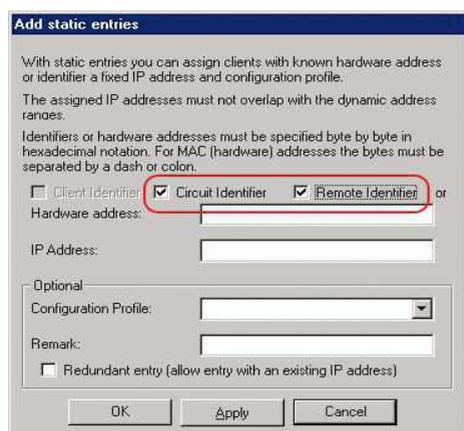


Figure 60: Default setting for the fixed address assignment

- In the `Hardware address` field, you enter the `Circuit Identifier` and the `Remote Identifier` (see "DHCP Relay Agent" in the "Web-based Interface" reference manual).

With `Hardware address` you identify the device and the port to which that device is connected, to which you want to assign the `IP address` in the line below it.

The hardware address is in the following form:

`ciclhvVVVSSmmppriRxxxxxxxxxxxx`

- ▶ `ci`: sub-identifier for the type of the circuit ID
- ▶ `cl`: length of the circuit ID
- ▶ `hh`: Hirschmann ID: 01 if a Hirschmann device is connected to the port, otherwise 00.
- ▶ `VVVV`: VLAN ID of the DHCP request (default: 0001 = VLAN 1)
- ▶ `ss`: socket of device at which the module with that port is located to which the device is connected. Enter the value 00.
- ▶ `mm`: module with the port to which the device is connected.
- ▶ `pp`: port to which the device is connected.
- ▶ `ri`: sub-identifier for the type of the remote ID
- ▶ `rl`: length of the remote ID
- ▶ `xxxxxxxxxxxx`: remote ID of the device (e.g. MAC address) to which a device is connected.

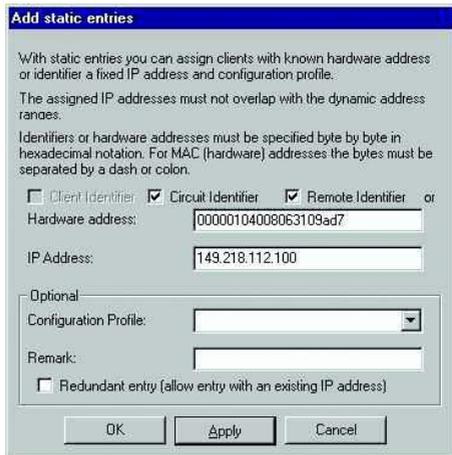


Figure 61: Entering the addresses

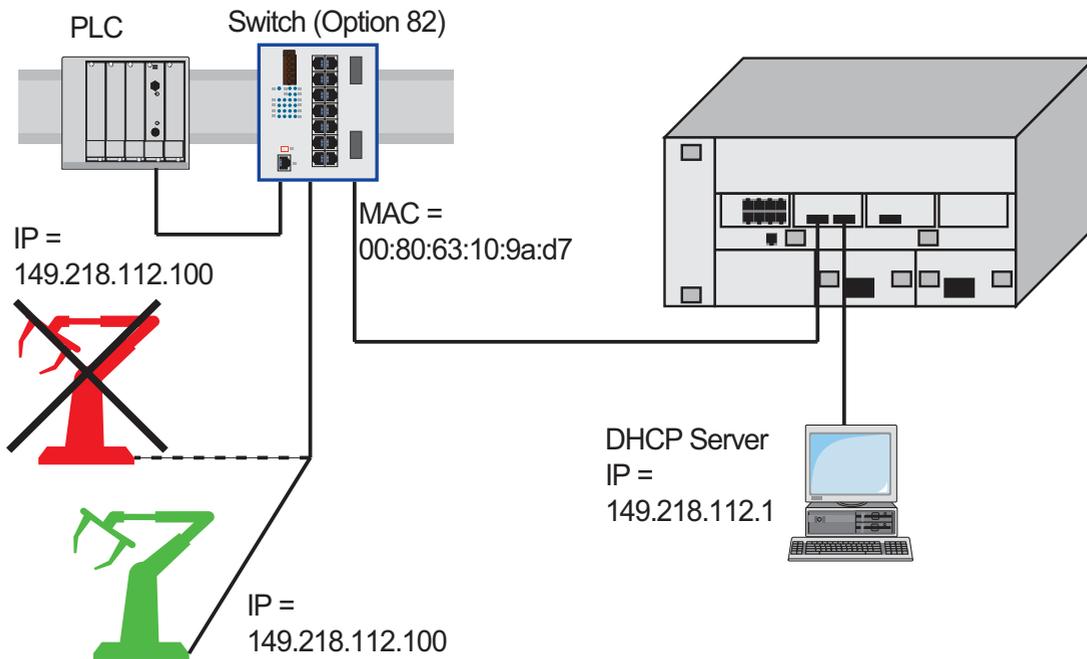


Figure 62: Application example of using Option 82

## A.3 TFTP Server for Software Updates

On delivery, the device software is held in the local flash memory. The device boots the software from the flash memory.

Software updates can be performed via a TFTP server. This presupposes that a TFTP server has been installed in the connected network and that it is active.

**Note:** An alternative to the TFTP update is the HTTP update. The HTTP update saves you having to configure the TFTP server.

The device requires the following information to be able to perform a software update from the TFTP server:

- ▶ its own IP address (entered permanently),
- ▶ the IP address of the TFTP server or of the gateway to the TFTP server,
- ▶ the path in which the operating system of the TFTP server is kept

The file transfer between the device and the TFTP server is performed via the Trivial File Transfer Protocol (tftp).

The management station and the TFTP server may be made up of one or more computers.

The preparation of the TFTP server for the device software involves the following steps:

- ▶ Setting up the device directory and copying the device software
- ▶ Setting up the TFTP process

## A.3.1 Setting up the TFTP Process

General prerequisites:

- ▶ The local IP address of the device and the IP address of the TFTP server or the gateway are known to the device.
- ▶ The TCP/IP stack with tftp is installed on TFTP server.

The following sections contain information on setting up the TFTP process, arranged according to operating system and application.

### ■ SunOS and HP

- First check whether the tftp daemon (background process) is running, i.e. whether the file `/etc/inetd.conf` contains the following line (see [figure 63](#)) and whether the status of this process is "IW":

#### SunOS

```
tftp dgram udp wait root /usr/etc/in.tftpd in.tftpd -
s /tftpboot
```

#### HP

```
tftp dgram udp wait root /usr/etc/in.tftpd tftpd
```

If the process is not entered or only entered as a comment line (`#`), modify `/etc/inetd.conf` accordingly and then re-initialize the INET daemon. This is performed with the command "kill -1 PID", where PID is the process number of inetd.

This re-initialization can be executed automatically by entering the following UNIX commands:

#### SunOS

```
ps -ax | grep inetd | head -1 | awk -e {print $1} |
kill -1
```

#### HP

```
/etc/inetd -c
```

You can obtain additional information about the tftpd daemon tftpd with the UNIX command "man tftpd".

**Note:** The command "ps" does not show the tftp daemon every time, although it is actually running.

Special steps for HP workstations:

- During installation on an HP workstation, enter the user tftp in the /etc/passwd file.

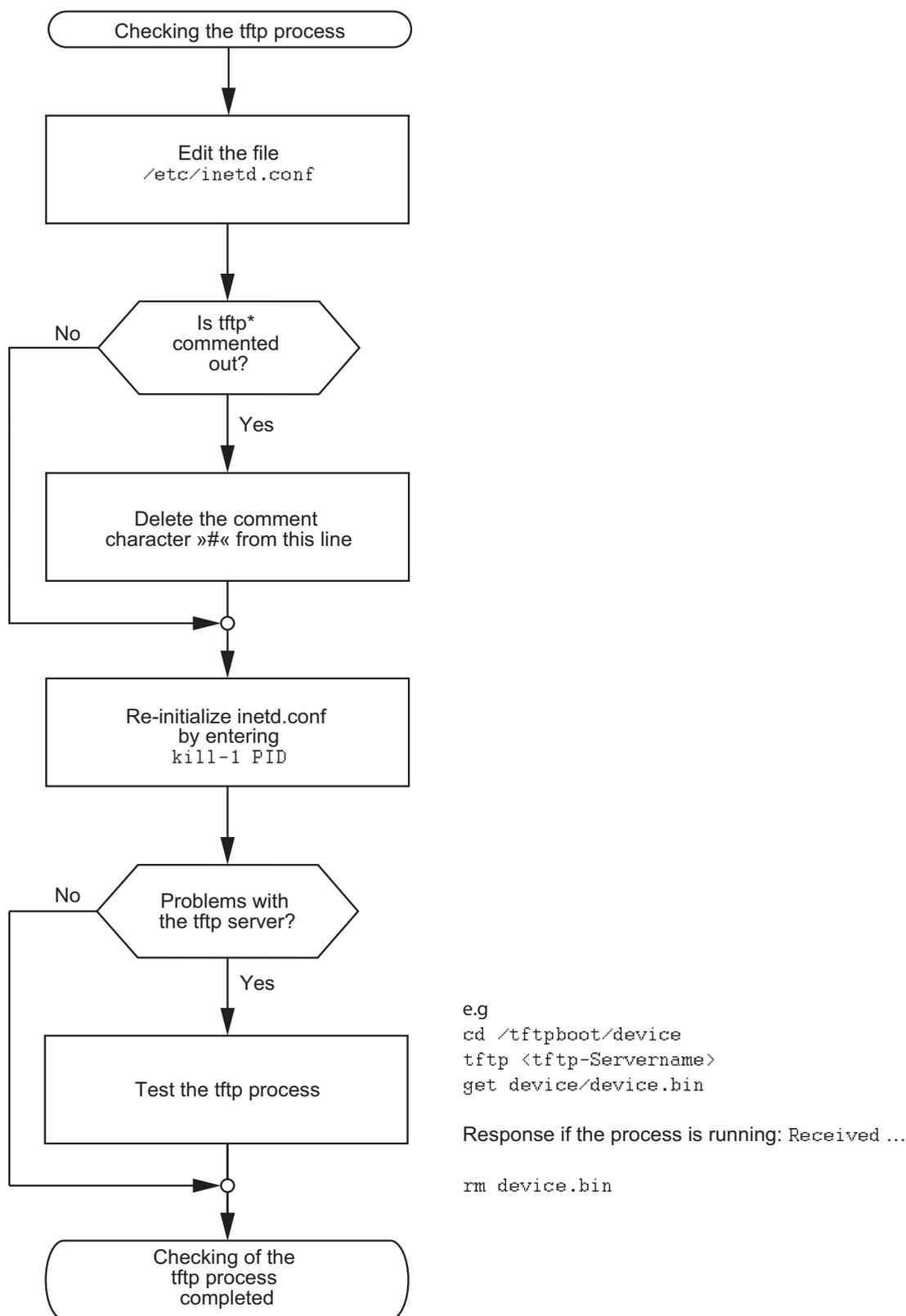
For example:

```
tftp:*:510:20:tftp server:/usr/tftpdire:/bin/false
```

```
tftpuser ID,
* is in the password field,
510 sample user number,
20 sample group number.,
tftp server any meaningful name ,
/bin/false mandatory entry (login shell)
```

- Test the tftp process with, for example:

```
cd /tftpboot/device
tftp <tftp-Servername>
get device/device.bin
rm device.bin
```



\* tftp dgram udp wait root/usr/etc/in.tftpd in.tftpd /tftpboot

Figure 63: Flow chart for setting up TFTP server with SunOS and HP

## A.3.2 Software Access Rights

The agent needs read permission for the TFTP directory on which the device software is stored.

### ■ Example of a UNIX tftp Server

Once the device software has been installed, the TFTP server should have the following directory structure with the stated access rights:

| File name  | Access     |
|------------|------------|
| device.bin | -rw-r--r-- |

Table 23: Directory structure of the software

l = link; d = directory; r = read; w = write; x = execute

1<sup>st</sup> position denotes the file type (- = normal file),

2<sup>nd</sup> to 4<sup>th</sup> positions designate user access rights,

5<sup>th</sup> to 7<sup>th</sup> positions designate access rights for users from other groups,

8<sup>th</sup> to 10<sup>th</sup> positions designate access rights of every other user.

## A.4 Service Shell

When you need assistance with your device, then the service personnel use the Service Shell function to monitor internal conditions, for example switch or CPU registers.

The CLI Reference Manual contains a description of deactivating the Service Shell.

**Note:** When you deactivate the Service Shell, then you are still able to configure the device, but you limit the service personnel to system diagnostics. In order to reactivate the Service Shell function, the device requires disassembly by the manufacturer.



# **B General Information**

## B.1 Management Information Base (MIB)

The Management Information Base (MIB) is designed in the form of an abstract tree structure.

The branching points are the object classes. The "leaves" of the MIB are called generic object classes.

If this is required for unique identification, the generic object classes are instantiated, i.e. the abstract structure is mapped onto reality, by specifying the port or the source address.

Values (integers, time ticks, counters or octet strings) are assigned to these instances; these values can be read and, in some cases, modified. The object description or object ID (OID) identifies the object class. The subidentifier (SID) is used to instantiate them.

Example:

The generic object class

`hmPSState` (OID = 1.3.6.1.4.1.248.14.1.2.1.3)

is the description of the abstract information "power supply status". However, it is not possible to read any information from this, as the system does not know which power supply is meant.

Specifying the subidentifier (2) maps this abstract information onto reality (instantiates it), thus indicating the operating status of power supply 2. A value is assigned to this instance and can then be read. The instance "get 1.3.6.1.4.1.248.14.1.2.1.3.2" returns the response "1", which means that the power supply is ready for operation.

### The following abbreviations are used in the MIB:

|       |                              |
|-------|------------------------------|
| Comm  | Group access rights          |
| con   | Configuration                |
| Descr | Description                  |
| Fan   | Fan                          |
| ID    | Identifier                   |
| Lwr   | Lower (e.g. threshold value) |
| PS    | Power supply                 |
| Pwr   | Power supply                 |
| sys   | System                       |

**The following abbreviations are used in the MIB:**

|     |                                    |
|-----|------------------------------------|
| UI  | User interface                     |
| Upr | Upper (e.g. threshold value)       |
| ven | Vendor = manufacturer (Hirschmann) |

**Definition of the syntax terms used:**

|                   |                                                                                                                    |
|-------------------|--------------------------------------------------------------------------------------------------------------------|
| Integer           | An integer in the range $-2^{31} - 2^{31}-1$                                                                       |
| IP Address        | xxx.xxx.xxx.xxx<br>(xxx = integer in the range 0-255)                                                              |
| MAC Address       | 12-digit hexadecimal number in accordance with ISO/IEC 8802-3                                                      |
| Object identifier | x.x.x.x... (e.g. 1.3.6.1.1.4.1.248...)                                                                             |
| Octet string      | ASCII character string                                                                                             |
| PSID              | Power supply identifier<br>(number of the power supply unit)                                                       |
| TimeTicks         | Stopwatch,<br>Elapsed time (in seconds) = numerical value / 100<br>Numerical value = integer in range $0-2^{32}-1$ |
| Timeout           | Time value in hundredths of a second<br>Time value = integer in range $0-2^{32}-1$                                 |
| Type field        | 4-digit hexadecimal number in accordance with ISO/IEC 8802-3                                                       |
| Counter           | Integer ( $0-2^{32}-1$ ), whose value is increased by 1 when certain events occur.                                 |

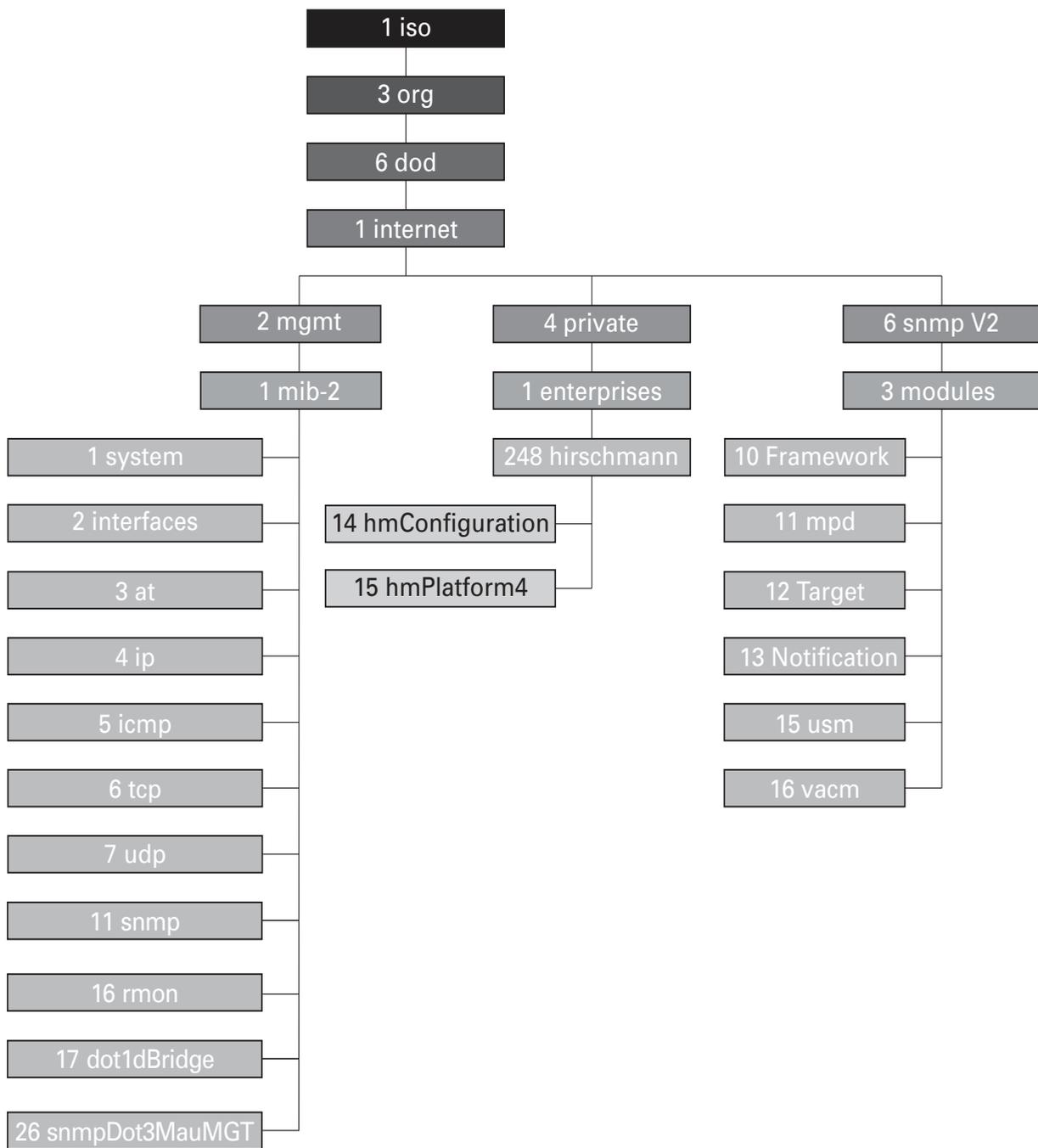


Figure 64: Tree structure of the Hirschmann MIB

A complete description of the MIB can be found on the product CD provided with the device.

---

## B.2 Abbreviations used

|       |                                         |
|-------|-----------------------------------------|
| ACA   | AutoConfiguration Adapter               |
| BOOTP | Bootstrap Protocol                      |
| CLI   | Command Line Interface                  |
| DHCP  | Dynamic Host Configuration Protocol     |
| FDB   | Forwarding Database                     |
| GARP  | General Attribute Registration Protocol |
| GMRP  | GARP Multicast Registration Protocol    |
| HTTP  | Hypertext Transfer Protocol             |
| ICMP  | Internet Control Message Protocol       |
| IGMP  | Internet Group Management Protocol      |
| IP    | Internet Protocol                       |
| LED   | Light Emitting Diode                    |
| LLDP  | Link Layer Discovery Protocol           |
| F/O   | Optical Fiber                           |
| MAC   | Media Access Control                    |
| MSTP  | Multiple Spanning Tree Protocol         |
| NTP   | Network Time Protocol                   |
| PC    | Personal Computer                       |
| PTP   | Precision Time Protocol                 |
| QoS   | Quality of Service                      |
| RFC   | Request For Comment                     |
| RM    | Redundancy Manager                      |
| RS    | Rail Switch                             |
| RSTP  | Rapid Spanning Tree Protocol            |
| SFP   | Small Form-factor Pluggable             |
| SNMP  | Simple Network Management Protocol      |
| SNTP  | Simple Network Time Protocol            |
| TCP   | Transmission Control Protocol           |
| TFTP  | Trivial File Transfer Protocol          |
| TP    | Twisted Pair                            |
| UDP   | User Datagram Protocol                  |
| URL   | Uniform Resource Locator                |
| UTC   | Coordinated Universal Time              |
| VLAN  | Virtual Local Area Network              |

## **B.3 Technical Data**

You will find the technical data in the document “GUI Reference Manual”.

## B.4 Readers' Comments

What is your opinion of this manual? We are constantly striving to provide as comprehensive a description of our product as possible, as well as important information to assist you in the operation of this product. Your comments and suggestions help us to further improve the quality of our documentation.

Your assessment of this manual:

|                     | Very Good             | Good                  | Satisfactory          | Mediocre              | Poor                  |
|---------------------|-----------------------|-----------------------|-----------------------|-----------------------|-----------------------|
| Precise description | <input type="radio"/> |
| Readability         | <input type="radio"/> |
| Understandability   | <input type="radio"/> |
| Examples            | <input type="radio"/> |
| Structure           | <input type="radio"/> |
| Comprehensive       | <input type="radio"/> |
| Graphics            | <input type="radio"/> |
| Drawings            | <input type="radio"/> |
| Tables              | <input type="radio"/> |

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

---



---



---



---



---



---



---



---

---

Suggestions for improvement and additional information:

---

---

---

---

General comments:

---

---

---

---

Sender:

---

Company / Department:

---

Name / Telephone number:

---

Street:

---

Zip code / City:

---

E-mail:

---

Date / Signature:

---

Dear User,

Please fill out and return this page

- ▶ as a fax to the number +49 (0)7127/14-1600 or
- ▶ per mail to

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

# C Index

|                                |                 |                                |               |
|--------------------------------|-----------------|--------------------------------|---------------|
| <b>A</b>                       |                 |                                |               |
| ACA                            | 58, 71, 73, 170 | DHCP                           | 27, 48, 51    |
| ACA31                          | 41              | DHCP Client                    | 48            |
| ACD                            | 189             | DHCP Option 82                 | 51            |
| Access                         | 170             | DHCP server                    | 108, 200, 206 |
| Access rights                  | 66, 91          | Differentiated Services        | 140           |
| Access security                | 83              | DiffServ                       | 136           |
| Address Conflict Detection     | 189             | DiffServ codepoint             | 140           |
| Address table                  | 121             | DSCP                           | 140, 142, 145 |
| AF                             | 140             | Dynamic                        | 122           |
| Aging Time                     | 121, 126, 126   | <b>E</b>                       |               |
| Alarm                          | 169             | EF                             | 140           |
| Alarm messages                 | 166             | Event Log                      | 197           |
| APNIC                          | 29              | Expedited Forwarding           | 140           |
| ARIN                           | 29              | <b>F</b>                       |               |
| ARP                            | 34              | FAQ                            | 229           |
| Assured Forwarding             | 140             | Faulty device replacement      | 55            |
| Authentication                 | 170             | FDB                            | 122           |
| AutoConfiguration Adapter      | 41, 170         | Filter                         | 122           |
| Automatic Configuration        | 83              | Filter table                   | 122           |
| <b>B</b>                       |                 | First installation             | 27            |
| Bandwidth                      | 124, 148        | Flash memory                   | 62, 73        |
| BOOTP                          | 27              | Flow control                   | 148           |
| Booting                        | 19              | Forwarding database            | 122           |
| Broadcast                      | 120, 122, 124   | <b>G</b>                       |               |
| Broadcast Limiter              | 134             | Gateway                        | 30, 38        |
| <b>C</b>                       |                 | Generic object classes         | 218           |
| CD-ROM                         | 200, 206        | GMRP                           | 124           |
| CIDR                           | 34              | Grandmaster                    | 115           |
| CLI Banner                     | 105             | <b>H</b>                       |               |
| Classless Inter-Domain Routing | 34              | HaneWin                        | 200, 206      |
| Class Selector                 | 140             | Hardware address               | 44            |
| Clock                          | 115             | Hardware reset                 | 166           |
| Clock synchronization          | 117             | HIPER-Ring (source for alarms) | 170           |
| Closed circuit                 | 175             | HiDiscovery                    | 39, 100       |
| Cold start                     | 74              | HiView                         | 24            |
| Command Line Interface         | 21              | Host address                   | 30            |
| Configuration                  | 62              | <b>I</b>                       |               |
| Configuration changes          | 166             | IANA                           | 29            |
| Configuration data             | 43, 51, 60, 64  | IEEE 1588 time                 | 108           |
| Configuration file             | 48, 63          | IEEE 802.1 Q                   | 137           |
| Connection error               | 84              | IEEE MAC Address               | 187           |
| <b>D</b>                       |                 | IGMP                           | 126           |
| Data transfer parameters       | 18              | IGMP Querier                   | 127           |
| Destination address            | 120, 122, 123   | IGMP Snooping                  | 124, 126      |
| Device Status                  | 171             |                                |               |

|                                                      |                     |                                           |               |
|------------------------------------------------------|---------------------|-------------------------------------------|---------------|
| Industrial HiVision                                  | 12, 49              | Priority Queues                           | 136           |
| Industry Protocols                                   | 11                  | Priority tagged frames                    | 137           |
| Instantiation                                        | 218                 | PTP                                       | 107, 108, 115 |
| Internet Assigned Numbers Authority                  | 29                  | <b>Q</b>                                  |               |
| Internet service provider                            | 29                  | QoS                                       | 137           |
| In-band                                              | 21                  | Query                                     | 126           |
| IP Address                                           | 29, 37, 44, 48, 189 | Query function                            | 127           |
| IP header                                            | 136, 139, 140       | Queue                                     | 143           |
| IP Parameter                                         | 27                  | <b>R</b>                                  |               |
| ISO/OSI layer model                                  | 34                  | Rate Limiter Settings                     | 134           |
| <b>L</b>                                             |                     | Real time                                 | 107, 136      |
| LACNIC                                               | 29                  | Reboot                                    | 74            |
| Leave                                                | 126                 | Receiver power status (source for alarms) | 170           |
| Link monitoring                                      | 171, 175            | Receiving port                            | 123           |
| Local clock                                          | 116                 | Redundancy                                | 11            |
| Login banner                                         | 104                 | Reference clock                           | 108, 111, 115 |
| Login window                                         | 25                  | Relay contact                             | 175           |
| <b>M</b>                                             |                     | Release                                   | 69            |
| MAC destination address                              | 34                  | Remote diagnostics                        | 175           |
| Media module for modular devices (source for alarms) | 170                 | Report                                    | 126, 192      |
| Message                                              | 166                 | Request interval (SNTP)                   | 112           |
| Mode                                                 | 83                  | Reset                                     | 74            |
| Multicast                                            | 112, 122, 124, 126  | Restart                                   | 74            |
| <b>N</b>                                             |                     | RIPE NCC                                  | 29            |
| Netmask                                              | 30, 38              | Ring manager                              | 122           |
| Network address                                      | 29                  | Ring/Network coupling (source for alarms) | 170           |
| Network Management                                   | 49                  | Router                                    | 30            |
| Network management station                           | 187                 | <b>S</b>                                  |               |
| Network topology                                     | 51                  | Segmentation                              | 166           |
| <b>O</b>                                             |                     | Service                                   | 192           |
| Object classes                                       | 218                 | Service provider                          | 29            |
| Object description                                   | 218                 | Service shell reactivation                | 215           |
| Object ID                                            | 218                 | SFP Module (source for alarms)            | 170           |
| Operation monitoring                                 | 175                 | SFP module                                | 185           |
| Option 82                                            | 28, 51, 206         | SFP status display                        | 185           |
| Out-of-band                                          | 21                  | Signal contact                            | 84, 175       |
| Overload protection                                  | 148                 | Signal contact (source for alarm)         | 170           |
| <b>P</b>                                             |                     | Signal runtime                            | 111           |
| Password                                             | 22, 66, 92, 93      | SNMP                                      | 24, 91, 166   |
| PHB                                                  | 140                 | SNTP                                      | 107, 112      |
| Polling                                              | 166                 | SNTP client                               | 112           |
| Port Configuration                                   | 83                  | Software                                  | 214           |
| Port Priority                                        | 142                 | Software release                          | 69            |
| Power over ETHERNET                                  | 84                  | Source address                            | 120           |
| PROFINET IO                                          | 11                  | Starting the graphical user interface     | 24            |
| Precedence                                           | 140                 | State on delivery                         | 62, 62, 91    |
| Precision Time Protocol                              | 115                 | Static                                    | 122           |
| Priority                                             | 137, 142            | Strict Priority                           | 143           |
|                                                      |                     | Subidentifier                             | 218           |

# Index

---

|                           |          |
|---------------------------|----------|
| Subnet                    | 38, 121  |
| Summer time               | 108      |
| Supply voltage            | 170      |
| Symbol                    | 13       |
| System Monitor            | 18       |
| System Name               | 48       |
| System requirements (GUI) | 24       |
| System time               | 111, 112 |

## T

|                                |               |
|--------------------------------|---------------|
| TAI                            | 108           |
| Target table                   | 166           |
| TCP/IP stack                   | 211           |
| Technical Questions            | 229           |
| Telnet                         | 21            |
| TFTP                           | 210           |
| TFTP Update                    | 77            |
| Time difference                | 108           |
| Time Management                | 115           |
| Time zone                      | 108           |
| Topology                       | 51            |
| ToS                            | 136, 139, 140 |
| Traffic Classes                | 136, 143, 144 |
| Training Courses               | 229           |
| Transmission reliability       | 166           |
| Trap                           | 166, 169      |
| Trap target table              | 166           |
| Trivial File Transfer Protocol | 210           |
| Trust dot1p                    | 142           |
| Trust ip-dscp                  | 142           |
| Type Field                     | 137           |
| Type of Service                | 139           |

## U

|           |     |
|-----------|-----|
| Unicast   | 124 |
| Untrusted | 142 |
| Update    | 18  |
| USB stick | 71  |
| User name | 22  |
| UTC       | 108 |

## V

|                             |               |
|-----------------------------|---------------|
| Video                       | 143           |
| VLAN                        | 137, 142, 151 |
| VLAN 0                      | 53            |
| VLAN ID (network parameter) | 52            |
| VLAN priority               | 144           |
| VLAN tag                    | 137, 151      |
| VoIP                        | 143           |
| V.24                        | 21            |

## W

|                     |     |
|---------------------|-----|
| Web-based Interface | 24  |
| Winter time         | 108 |



## D Further Support

### ■ Technical Questions

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

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

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

You can contact us

in the EMEA region at

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

in the America region at

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

in the Asia-Pacific region at

- ▶ Tel.: +65 6854 9860
- ▶ E-mail: [inet-ap@belden.com](mailto:inet-ap@belden.com)

### ■ Hirschmann Competence Center

The Hirschmann Competence Center is ahead of its competitors:

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

The current technology and product training courses can be found at <http://www.hicomcenter.com>

- ▶ Support ranges from the first installation through the standby service to maintenance concepts.

With the Hirschmann Competence Center, you have decided against making any compromises. Our client-customized package leaves you free to choose the service components you want to use.

Internet:

<http://www.hicomcenter.com>





**HIRSCHMANN**

---

A **BELDEN** BRAND



**HIRSCHMANN**

A **BELDEN** BRAND

# User Manual

**Industrial Protocols**

**Industrial ETHERNET (Gigabit-)Switch**

**MACH 100, MACH 1000, MACH 4000, MS20/MS30, OCTOPUS,  
PowerMICE, RS20/RS30/RS40, RSR20/RSR30**

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.

© 2015 Hirschmann Automation and Control GmbH

Manuals and software are protected by copyright. All rights reserved. The copying, reproduction, translation, conversion into any electronic medium or machine scannable form is not permitted, either in whole or in part. An exception is the preparation of a backup copy of the software for your own use. For devices with embedded software, the end-user license agreement on the enclosed CD/DVD applies.

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

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

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

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

# Contents

|          |                                                  |           |
|----------|--------------------------------------------------|-----------|
|          | <b>Safety Information</b>                        | <b>5</b>  |
|          | <b>About this Manual</b>                         | <b>7</b>  |
|          | <b>Key</b>                                       | <b>9</b>  |
| <b>1</b> | <b>Industry Protocols</b>                        | <b>11</b> |
| <b>2</b> | <b>EtherNet/IP</b>                               | <b>15</b> |
| 2.1      | Integration into a Control System                | 17        |
| 2.2      | EtherNet/IP Parameters                           | 21        |
| 2.2.1    | Identity Object                                  | 21        |
| 2.2.2    | TCP/IP Interface Object                          | 22        |
| 2.2.3    | Ethernet Link Object                             | 24        |
| 2.2.4    | Ethernet Switch Agent Object                     | 27        |
| 2.2.5    | I/O Data                                         | 30        |
| 2.2.6    | Assignment of the Ethernet Link Object Instances | 31        |
| 2.2.7    | Supported Services                               | 32        |
| <b>3</b> | <b>PROFINET IO</b>                               | <b>33</b> |
| 3.1      | Integration into a Control System                | 36        |
| 3.1.1    | Preparing the Switch                             | 36        |
| 3.1.2    | Configuration of the PLC                         | 37        |
| 3.1.3    | Configuring the device                           | 47        |
| 3.1.4    | Swapping devices                                 | 48        |
| 3.1.5    | Swapping modules                                 | 49        |
| 3.1.6    | Monitoring the network                           | 50        |
| 3.2      | PROFINET IO Parameters                           | 54        |
| 3.2.1    | Alarms                                           | 54        |
| 3.2.2    | Record parameters                                | 54        |
| 3.2.3    | I/O Data                                         | 58        |
| <b>4</b> | <b>IEC 61850/MMS (RSR20/RSR30/MACH1000)</b>      | <b>61</b> |
| 4.1      | Switch model for IEC 61850                       | 62        |
| 4.2      | Integration into a Control System                | 64        |
| 4.2.1    | Preparing the Switch                             | 64        |
| 4.2.2    | Offline configuration                            | 65        |
| 4.2.3    | Monitoring the device                            | 66        |

|          |                           |           |
|----------|---------------------------|-----------|
| <b>A</b> | <b>GSD File Generator</b> | <b>67</b> |
| <b>B</b> | <b>Readers' Comments</b>  | <b>68</b> |
| <b>C</b> | <b>Index</b>              | <b>71</b> |
| <b>D</b> | <b>Further Support</b>    | <b>73</b> |

# Safety Information



## **WARNING**

### **UNCONTROLLED MACHINE ACTIONS**

To avoid uncontrolled machine actions caused by data loss, configure all the data transmission devices individually.

Before you start any machine which is controlled via data transmission, be sure to complete the configuration of all data transmission devices.

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



## About this Manual

The “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 IO.

The following thematic sequence has proven itself in practice:

- ▶ Device configuration in line with the “Basic Configuration” user manual
- ▶ Check on the connection Switch <--> PLC
- ▶ Program the PLC

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

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

You will find detailed descriptions of how to operate the individual functions in the “Web-based Interface” and “Command Line Interface” reference manuals.

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

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



# Key

The designations used in this manual have the following meanings:

---

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

---

Symbols used:

---

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

---

# Key

---



Hub



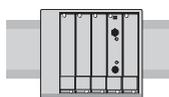
A random computer



Configuration Computer



Server



PLC -  
Programmable logic  
controller



I/O -  
Robot

---

# 1 Industry Protocols

For a long time, automation communication and office communication were on different paths. The requirements and the communication properties were too different.

Office communication moves large quantities of data with low demands with respect to the transfer time. Automation communication moves small quantities of data with high demands with respect to the transfer time and availability.

While the transmission devices in the office are usually kept in temperature-controlled, relatively clean rooms, the transmission devices used in automation are exposed to wider temperature ranges. Dirty, dusty and damp ambient conditions make additional demands on the quality of the transmission devices.

With the continued development of communication technology, the demands and the communication properties have moved closer together. The high bandwidths now available in Ethernet technology and the protocols they support enable large quantities to be transferred and exact transfer times to be defined.

With the creation of the first optical LAN to be active worldwide, at the University of Stuttgart in 1984, Hirschmann laid the foundation for industry-compatible office communication devices. Thanks to Hirschmann's initiative with the world's first rail hub in the 1990s, Ethernet transmission devices such as switches, routers and firewalls are now available for the toughest automation conditions.

The desire for uniform, continuous communication structures encouraged many manufacturers of automation devices to come together and use standards to aid the progress of communication technology in the automation sector. This is why we now have protocols that enable us to communicate via Ethernet from the office right down to the field level.

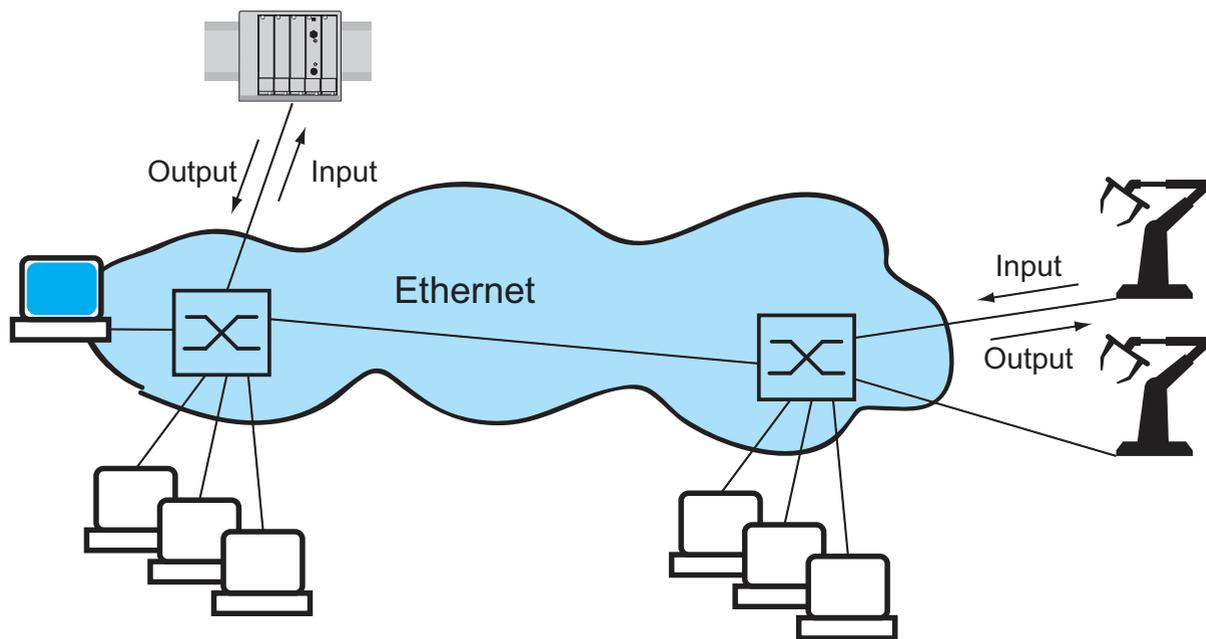


Figure 1: Example of communication.

Hirschmann switches support the following industry protocols and systems

- ▶ EtherNet/IP
- ▶ PROFINET IO

Depending on the ordered Industrial Protocol variant the Switch offers the suitable default settings:

| Settings / Variant         | Standard          | EtherNet/IP | PROFINET IO |
|----------------------------|-------------------|-------------|-------------|
| Order code                 | H                 | E           | P           |
| EtherNet/IP                | 0                 | 1           | 0           |
| IGMP Snooping              | 0                 | 1           | 0           |
| IGMP Querier               | 0                 | 1           | 0           |
| Unknown Multicast          | Send To All Ports | Discard     | Discard     |
| Address Conflict Detection | 0                 | 1           | 0           |
| RSTP                       | 1                 | 0           | 1           |
| DIP switch                 | SW-Konfig         | SW-Konfig   | SW-Konfig   |
| 100 Mbit/s TP ringports    | Autoneg           | Autoneg     | Autoneg     |

| Settings / Variant       | Standard                     | EtherNet/IP                  | PROFINET IO |
|--------------------------|------------------------------|------------------------------|-------------|
| Static Query Port        | Disable                      | Automatic                    | Automatic   |
| PROFINET IO              | 0                            | 0                            | 1           |
| Boot-Modus               | DHCP                         | DHCP                         | Lokal       |
| VLAN 0 Transparent Modus | 0                            | 0                            | 1           |
| HiDiscovery              | Read/Write                   | Read/Write                   | ReadOnly    |
| sysName                  | Product name<br>+ 3 Byte MAC | Product name<br>+ 3 Byte MAC | empty       |

If you want to configure a device with the standard configuration for PROFINET IO, you will find the corresponding dialogs of the Web-basedInterface in the following table.

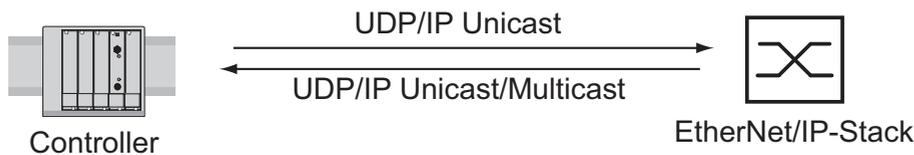
| Parameter          | Dialog                                             | Action                                                  |
|--------------------|----------------------------------------------------|---------------------------------------------------------|
| PROFINET IO        | Advanced:Industrial<br>Protocols                   | Activate PROFINET IO.                                   |
| Boot Mode          | Basic<br>Settings:Network/Mode                     | Select "Local".                                         |
| IP Address         | Basic<br>Settings:Network/Local                    | Enter the "IP address" 0.0.0.0.                         |
| Netmask            | Basic<br>Settings:Network/Local                    | Enter the "netmask" 0.0.0.0.                            |
| Gateway Address    | Basic<br>Settings:Network/Local                    | Enter the "gateway address"<br>0.0.0.0.                 |
| VLAN 0 Transparent | Switching:VLAN:Global                              | Activate the "VLAN 0 transparent<br>mode".              |
| HiDiscovery        | Basic<br>Settings:Network/HiDisco<br>very Protocol | Activate the function and select<br>"Read only" access. |
| System Name        | Basic Settings:<br>System/System data              | Delete the field content.                               |

*Table 1: Web-based interface dialogs for setting the PROFINET IO parameters*



## 2 EtherNet/IP

EtherNet/IP, which is accepted worldwide, is an industrial communication protocol standardized by the Open DeviceNet Vendor Association (ODVA) on the basis of Ethernet. It is based on the widely used transport protocols TCP/IP and UDP/IP (standard). EtherNet/IP thus provides a wide basis, supported by leading manufacturers, for effective data communication in the industry sector.



*Figure 2: Communication between the controller (PLC) and the Switch*

EtherNet/IP adds the industry protocol CIP (Common Industrial Protocol) to the Ethernet as an application level for automation applications. Ethernet is thus ideally suited to the industrial control technology sector.

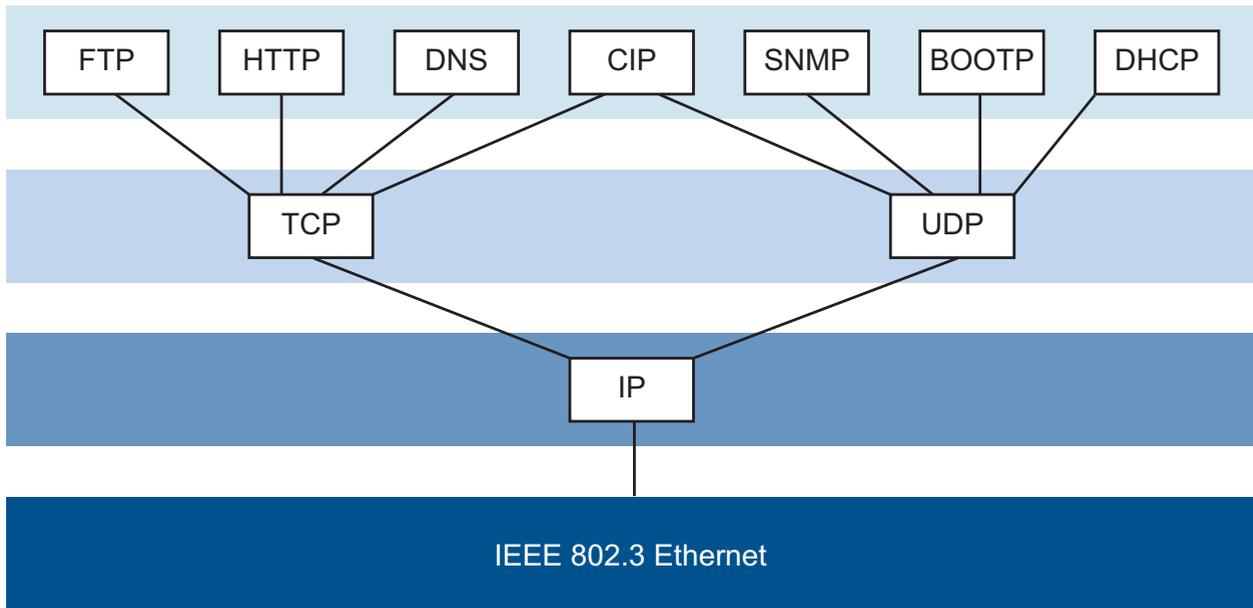


Figure 3: EtherNet/IP (CIP) in the ISO/OSI reference model

In particular, you will find EtherNet/IP in the USA and in conjunction with Rockwell controllers.

For detailed information on EtherNet/IP, see the Internet site of ODVA at [www.ethernetip.de](http://www.ethernetip.de).

## 2.1 Integration into a Control System

After installing and connecting the Switch, you configure it according to the “Basic Configuration” user manual. Then:

- Use the Web-based interface in the `Switching:Multicasts:IGMP` dialog to check whether the IGMP Snooping is activated.
- Use the Web-based interface in the `Advanced:Industry Protocols` dialog to check whether EtherNet/IP is activated.
- Use the Web-based interface in the `Advanced:Industry Protocols` dialog to download the EDS (EtherNet/IP configuration file) and the icon to your local computer.

**Note:** If EtherNet/IP and the router function are switched on at the same time, malfunctions could occur with EtherNet/IP, for example, in connection with “RS Who”. Therefore, you should switch off the router function of the device.

- ▶ Switch off the router function in the Web-based interface:  
`Routing:Global` dialog.
- ▶ Switch off the router function in the Command Line interface:  
in the configuration mode (prompt “`.. (Config) #`”) with the command  
`no ip routing`.

### ■ Configuration of a PLC using the example of Rockwell software

- Open the “EDS Hardware Installation Tool” of RSLinx.
- Use the “EDS Hardware Installation Tool” to add the EDS file.
- Restart the “RSLinx” service so that RSLinx takes over the EDS file of the Switch.
- Use RSLinx to check whether RSLinx has detected the Switch.
- Open your Logix 5000 project.
- Integrate the Switch into the Ethernet port of the controller as a new module (Generic Ethernet Module).

| Setting                         | I/O connection           | Input only               | Listen only                     |
|---------------------------------|--------------------------|--------------------------|---------------------------------|
| Comm Format:                    | Data - DINT              | Data - DINT              | Input data - DINT - Run/Program |
| IP Address                      | IP address of the Switch | IP address of the Switch | IP address of the Switch        |
| Input Assembly Instance         | 2                        | 2                        | 2                               |
| Input Size                      | 7<br>(MACH 4000: 11)     | 7<br>(MACH 4000: 11)     | 7<br>(MACH 4000: 11)            |
| Output Assembly Instance        | 1                        | 254                      | 255                             |
| Output Size                     | 1<br>(MACH 4000: 2)      | 0                        | 0                               |
| Configuration Assembly Instance | 3                        | 3                        | 3                               |
| Configuration Size              | 0                        | 0                        | 0                               |

*Table 2: Settings for integrating a Generic Ethernet Module*

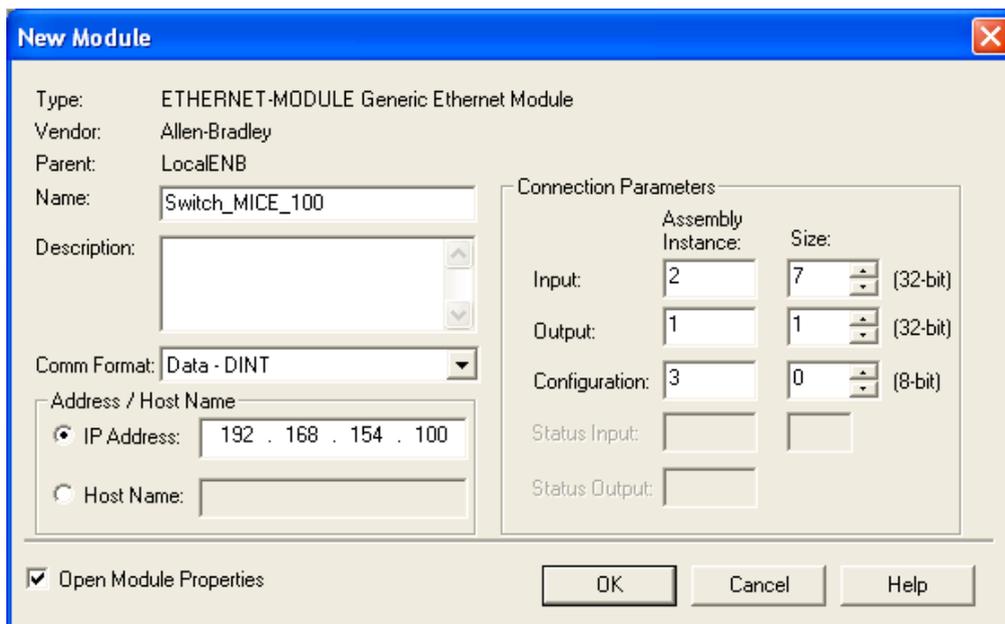


Figure 4: Integrating a new module into Logix 5000

- In the module properties, enter a value of at least 100 ms for the Request Packet Interval (RPI).

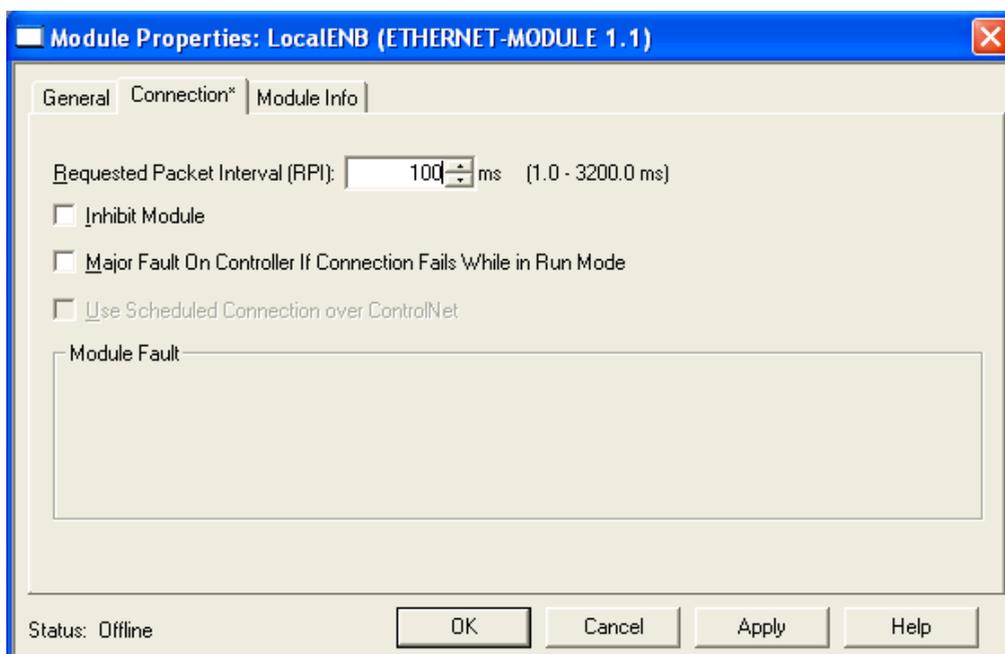


Figure 5: Module properties for the Request Packet Interval (RPI)

**Note:** If for example, a management program is occupying the Switch CPU with SNMP requests, the I/O connection between the programmable logic controller (PLC) and the Switch can be interrupted for a time. As the Switch can still transmit data packages in this case, the system can also still be ready for operation.

The monitoring of the I/O connection to the Switch CPU as a failure criterion can result in system failure and is therefore less suitable as a failure criterion.

### ■ **Example of integration from the Sample Code Library**

The Sample Code Library is a website from Rockwell. The object of the website is to provide users with a place where they can exchange their best architecture integration applications.

On the website <http://samplecode.rockwellautomation.com>, search for catalog number 9701. This is the catalog number of an example for integrating HirschmannSwitches into RS Logix 5000 rel. 16, PLC firmware release 16.

## 2.2 EtherNet/IP Parameters

### 2.2.1 Identity Object

The Switch supports the identity object (class code 01) of EtherNet/IP. The Hirschmann manufacturer ID is 634. Hirschmann uses the manufacturer-specific ID 149 (95H) to indicate the product type “Managed Ethernet Switch”.

| ID | Attribute     | Access Rule | Data Type                            | Description                                                                                  |
|----|---------------|-------------|--------------------------------------|----------------------------------------------------------------------------------------------|
| 1  | Vendor ID     | Get         | UINT                                 | Hirschmann 634                                                                               |
| 2  | Device Type   | Get         | UINT                                 | Vendor-specific Definition 149 (95H) “Managed Ethernet Switch”.                              |
| 3  | Product Code  | Get         | UINT                                 | Product Code: mapping is defined for every device type, e.g. RS20-0400T1T1SDAPHH is 16650.   |
| 4  | Revision      | Get         | STRUCT<br>USINT Major<br>USINT Minor | Revision of the Ethernet/IP implementation, currently 1.1, Major Revision and Minor Revision |
| 5  | Status        | Get         | WORD                                 | Not used                                                                                     |
| 6  | Serial Number | Get         | UDINT                                | Serial number of the device (contains last 3 bytes of MAC address).                          |
| 7  | Product Name  | Get         | Short String<br>(max. 32 bytes)      | Displayed as "Hirschmann" + order code, e.g. Hirschmann RSxxxxx.                             |

Table 3: Identity Object

## 2.2.2 TCP/IP Interface Object

The Switch supports an instance (instance 1) of the TCP/IP Interface Object (Class Code F5<sub>H</sub>, 245) of EtherNet/IP.

In the case of write access, the Switch stores the complete configuration in its flash memory. Saving can take 10 seconds. If the save process is interrupted, for example, by a power cut, the Switch may become inoperable.

**Note:** The Switch replies to the configuration change "Set Request" with a "Response" although saving of the configuration has not yet been completed.

| Id | Attribute                  | Access rule | Data type                                  | Description                                                                                                                                                                                                     |
|----|----------------------------|-------------|--------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1  | Status                     | Get         | DWORD                                      | Interface Status (0: Interface not configured, 1: Interface contains valid config).                                                                                                                             |
| 2  | Interface Capability flags | Get         | DWORD                                      | Bit 0: BOOTP Client,<br>Bit 1: DNS Client,<br>Bit 2: DHCP Client,<br>Bit 3: DHCP-DNS Update,<br>Bit 4: Configuration settable (within CIP).<br>Other bits reserved (0).                                         |
| 3  | Config Control             | Set/Get     | DWORD                                      | Bits 0 through 3:<br>Value 0: using stored config,<br>Value 1: using BOOTP,<br>Value 2: using DHCP.<br>Bit 4: 1 device uses DNS for name lookup<br>(always 0 because not supported)<br>Other bits reserved (0). |
| 4  | Physical Link Object       | Get         | Structure: UINT<br>Path size<br>EPATH Path | Path to the Physical Link Objekt, always {20H, F6H, 24H, 01H} describing instance 1 of the Ethernet Link Object.                                                                                                |

Table 4: TCP/IP Interface Object

| <b>Id</b> | <b>Attribute</b>        | <b>Access rule</b> | <b>Data type</b>                                                                                                                             | <b>Description</b>                                                                                             |
|-----------|-------------------------|--------------------|----------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------|
| 5         | Interface Configuration | Set/Get            | Structure:<br>UDINT IP address<br>UDINT Netmask<br>UDINT Gateway address<br>UDINT Name server 1<br>UDINT Name server 2<br>STRING Domain name | IP Stack Configuration (IP-Address, Netmask, Gateway, 2 Nameservers (DNS, not supported) and the domain name). |
| 6         | Host name               | Set/Get            | STRING                                                                                                                                       | Host name (for DHCP DNS Update).                                                                               |
| 8         | TTL Value               | Set/Get            | USINT                                                                                                                                        | TTL value for EtherNet/IP multicast packets                                                                    |
| 9         | Mcast Config            | Set/Get            | STRUCT of:                                                                                                                                   | IP multicast address configuration                                                                             |
|           | Alloc Control           |                    | USINT                                                                                                                                        | Multicast address allocation control word. Determines how addresses are allocated.                             |
|           | Reserved                |                    | USINT                                                                                                                                        | Reserved for future use                                                                                        |
|           | Num Mcast               |                    | UINT                                                                                                                                         | Number of IP multicast addresses to allocate for EtherNet/IP                                                   |
|           | Mcast Start Addr        |                    | UDINT                                                                                                                                        | Starting multicast address from which to begin allocation.                                                     |
| 100       | Quick Connect           | Set/Get            | DWORD                                                                                                                                        | Bitmask of 1 bit per port to enable/disable Quick Connect.                                                     |

*Table 4: TCP/IP Interface Object*

### 2.2.3 Ethernet Link Object

The Switch supports at least one instance (Instance 1; the instance of the CPU Ethernet interface) of the Ethernet Link Object (Class Code F6<sub>H</sub>, 246) of EtherNet/IP.

| Id | Attribute          | Access rule | Data type                                           | Description                                                                                                                                                                                                                                                                                                                                                                        |
|----|--------------------|-------------|-----------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1  | Interface Speed    | Get         | UDINT                                               | Used interface speed in MBits/s (10, 100, 1000, ...). 0 is used when the speed has not been determined or is invalid because of detected problems.                                                                                                                                                                                                                                 |
| 2  | Interface Flags    | Get         | DWORD                                               | Interface Status Flags:<br>Bit 0: Link State (1: Link up),<br>Bit 1: 0: Half-Duplex, 1: FullDuplex1,<br>Bits 2 through 4: Autoneg Status (0: Autoneg in Progress, 1: Autoneg unsuccessful, 2: unsuccessful but Speed detected, 3: Autoneg success, 4: No Autoneg),<br>Bit 5: manual configuration requires reset (always 0 because not needed),<br>Bit 6: detected hardware error. |
| 3  | Physical Address   | Get         | ARRAY of 6 USINTs                                   | MAC address of physical interface.                                                                                                                                                                                                                                                                                                                                                 |
| 4  | Interface Counters | Get         | Struct MIB II Counters<br>Jewels UDINT              | InOctets, InUcastPackets, InNUcastPackets, InDiscards, InErrors, InUnknownProtos, OutOctets, OutUcastPackets, OutNUcastPackets, OutDiscards, OutErrors.                                                                                                                                                                                                                            |
| 5  | Media Counters     | Get         | Struct Ethernet MIB Counters<br>Jewels UDINT        | Alignment Errors, FCS Errors, Single Collision, Multiple Collision, SQE Test Errors, Deferred Transmissions, Late Collisions, Excessive Collisions, MAC TX Errors, Carrier Sense Errors, Frame Too Long, MAC RX Errors.                                                                                                                                                            |
| 6  | Interface Control  | Get/Set     | Struct Control Bits WORD<br>Forced Iface Speed UINT | Control Bits:<br>Bit 0: Autoneg enable/disable (1: enable),<br>Bit 1: Duplex mode (1: full duplex, if Autoneg is disabled).<br>Interface speed in MBits/s: 10, 100,..., if Autoneg is disabled.                                                                                                                                                                                    |
| 7  | Interface Type     | Get         | USINT                                               | Value 0: Unknown interface type,<br>Value 1: The interface is internal,<br>Value 2: Twisted-pair,<br>Value 3: Optical fiber.                                                                                                                                                                                                                                                       |

Table 5: Ethernet Link-Objekt

| <b>Id</b> | <b>Attribute</b> | <b>Access rule</b> | <b>Data type</b> | <b>Description</b>                                                                                                                                   |
|-----------|------------------|--------------------|------------------|------------------------------------------------------------------------------------------------------------------------------------------------------|
| 8         | Interface State  | Get                | USINT            | Value 0: Unknown interface state,<br>Value 1: The interface is enabled,<br>Value 2: The interface is disabled,<br>Value 3: The interface is testing, |
| 9         | Admin State      | Set                | USINT            | Value 1: Enable the interface,<br>Value 2: Disable the interface.                                                                                    |
| 10        | Interface Label  | Get                | SHORT_STRING     | Interface name. The content of the string is vendor-specific.                                                                                        |

*Table 5: Ethernet Link-Objekt*

The Switch supports additional vendor specific attributes.

| <b>Id</b>     | <b>Attribute</b>                            | <b>Access rule</b> | <b>Data type</b> | <b>Description</b>                                                                                                                                                                   |
|---------------|---------------------------------------------|--------------------|------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 100<br>(64 H) | Ethernet Interface Index                    | Get                | UDINT            | Interface/Port Index (ifIndex from MIB II)                                                                                                                                           |
| 101<br>(65 H) | Port Control                                | Get/Set            | DWORD            | Bit 0 (RO): Link state (0: link down, 1: link up)<br>Bit 1 (R/W): Link admin state (0: disabled, 1: enabled)<br>Bit 8 (RO:): Access violation alarm<br>Bit 9 (RO): Utilization alarm |
| 102<br>(66 H) | Interface Utilization                       | Get                | UDINT            | The existing Counter from the private MIB hmlfaceUtilization is used. Utilization in percentage <sup>a</sup> . RX Interface Utilization.                                             |
| 103<br>(67 H) | Interface Utilization Alarm Upper Threshold | Get/Set            | UDINT            | Within this parameter the variable hmlfaceUtilizationAlarmUpperThreshold can be accessed. Utilization in percentage <sup>a</sup> . RX Interface Utilization Upper Limit.             |
| 104<br>(68 H) | Interface Utilization Alarm Lower Threshold | Get/Set            | UDINT            | Within this parameter the variable hmlfaceUtilizationAlarmLowerThreshold can be accessed. Utilization in percentage <sup>a</sup> . RX Interface Utilization Lower Limit.             |

*Table 6: Hirschmann-Erweiterungen des Ethernet Link-Objekts*

| <b>Id</b>        | <b>Attribute</b>                     | <b>Access rule</b> | <b>Data type</b>                                     | <b>Description</b>                                                                                                                           |
|------------------|--------------------------------------|--------------------|------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------|
| 105<br>(69<br>H) | Broadcast Limit                      | Get/Set            | UDINT                                                | Broadcast limiter Service (Egress BC-Frames limitation, 0: disabled), Frames/second                                                          |
| 106<br>(6A<br>H) | Ethernet<br>Interface<br>Description | Get                | STRING<br>[max. 64 Bytes]<br>even number of<br>Bytes | Interface/Port Description<br>(from MIB II ifDescr), e.g. "Unit: 1 Slot: 2 Port:<br>1 - 10/100 Mbit TX", or "unavailable",<br>max. 64 Bytes. |

*Table 6: Hirschmann-Erweiterungen des Ethernet Link-Objekts*

- a. Einheit: 1 Hundertstel von 1%, d.h., 100 entspricht 1%

## 2.2.4 Ethernet Switch Agent Object

The Switch supports the Hirschmann vendor specific Ethernet Switch Agent Object (Class Code 95<sub>H</sub>, 149) for the Switch configuration and information parameters with one instance (Instance 1).

For further information on these parameters and how to adjust them refer to the Reference Manual „GUI“ (Graphical User Interface / Web-based Interface).

| Attribute     | ID/Bit No. | Description                                                                          |
|---------------|------------|--------------------------------------------------------------------------------------|
| Switch Status | ID 01      | DWORD (32 bit) RO                                                                    |
|               | Bit 0      | Overall state (0: ok, 1: failed) Like the signal contact.                            |
|               | Bit 1      | Power Supply 1 (0: ok, 1: failed or does not exist)                                  |
|               | Bit 2      | Power Supply 2 (0: ok, 1: failed or does not exist)                                  |
|               | Bit 3      | Power Supply 3 (0: ok or not possible on this platform, 1: failed or does not exist) |
|               | Bit 4      | Power Supply 4 (0: ok or not possible on this platform, 1: failed or does not exist) |
|               | Bit 5      | Power Supply 5 (0: ok or not possible on this platform, 1: failed or does not exist) |
|               | Bit 6      | Power Supply 6 (0: ok or not possible on this platform, 1: failed or does not exist) |
|               | Bit 7      | Power Supply 7 (0: ok or not possible on this platform, 1: failed or does not exist) |
|               | Bit 8      | Power Supply 8 (0: ok or not possible on this platform, 1: failed or does not exist) |
|               | Bit 9      | DIP RM (ON: 1, OFF: 0)                                                               |
|               | Bit 10     | DIP Standby (ON: 1, OFF: 0)                                                          |
|               | Bit 11     | Signal Contact 1 (0: closed, 1: open)                                                |
|               | Bit 12     | Signal Contact 2 (0: closed, 1: open)                                                |
|               | Bit 13     | Quick Connect (1: ON, 0: OFF)                                                        |
|               | Bit 16     | Temperature (0: ok, 1: threshold exceeded)                                           |
|               | Bit 17     | Fan (0: ok or no fan, 1: inoperable)                                                 |
|               | Bit 21     | DIP Ring ports, 0: module 1 ports 1&2, 1: module 2, ports 1&2                        |
|               | Bit 22     | DIP Configuration (1: enabled, 0: disabled)                                          |
|               | Bit 23     | DIP HIPER-Ring state (1: ON, 0: OFF)                                                 |
|               | Bit 24     | Module removed (1: removed)                                                          |
|               | Bit 25     | ACA removed (1: removed)                                                             |
|               | Bit 28     | Hiper-Ring (1: loss of redundancy reserve)                                           |
|               | Bit 29     | Ring-/Netcoupling (1: loss of redundancy reserve)                                    |

Table 7: Hirschmann Ethernet Switch Agent Object

| Attribute                          | ID/Bit No.                                 | Description                                                                                                                                                                                |
|------------------------------------|--------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                    | Bit 30                                     | Connection Error (1: link inoperable)                                                                                                                                                      |
| Switch Temperature                 | ID 02                                      | Struct{INT RO Temperature °F, INT RO Temperature °C}                                                                                                                                       |
| Reserved                           | ID 03                                      | Always 0, attribute is reserved for future use.                                                                                                                                            |
| Switch Max Ports                   | ID 04                                      | UINT (16 bit) RO Maximum number of Ethernet Switch Ports                                                                                                                                   |
| Multicast Settings (IGMP Snooping) | ID 05                                      | WORD (16 bit) RW                                                                                                                                                                           |
|                                    | Bit 0 RW                                   | IGMP Snooping (1: enabled, 0: disabled)                                                                                                                                                    |
|                                    | Bit 1 RW                                   | IGMP Querier (1: enabled, 0: disabled)                                                                                                                                                     |
|                                    | Bit 2 RO                                   | IGMP Querier Mode (1: Querier, 0: Non-Querier)                                                                                                                                             |
|                                    | Bit 4-6 RW                                 | IGMP Querier Packet Version 1: V1, 2: V2, 3: V3, 0: Off (IGMP Querier disabled)                                                                                                            |
|                                    | Bit 8-10 RW                                | Treatment of Unknown Multicasts (Railswitch only): 0: Send To All Ports, 1: Send To Query Ports, 2: Discard                                                                                |
| Switch Existing Ports              | ID 06                                      | ARRAY OF DWORD <sup>a</sup> RO Bitmask of existing Switch Ports                                                                                                                            |
|                                    | Per Bit starting with Bit 0 (means Port 1) | 1: Port existing, 0: Port not available. Array (bit mask) size is adjusted to the size of maximum number of Switch ports (e.g. a max. no of 28 ports means that 1 DWORD is used (32 bit)). |
| Switch Port Control                | ID 07                                      | ARRAY OF DWORD <sup>a</sup> RW Bitmask Link Admin Status Switch Ports                                                                                                                      |
|                                    | Per Bit starting with Bit 0 (means Port 1) | 0: Port enabled, 1: Port disabled. Array (bit mask) size is adjusted to the size of maximum number of Switch ports (e.g. a max. no of 28 ports means that 1 DWORD is used (32 bit)).       |
| Switch Ports Mapping               | ID 08                                      | ARRAY OF USINT (BYTE, 8 bit) RO Instance number of the Ethernet Link Object                                                                                                                |
|                                    | Starting with Index 0 (means Port 1)       | All Ethernet Link Object Instances for the existing Ethernet Switch Ports (1..N (maximum number of ports)). When the entry is 0, the Ethernet Link Object for this port does not exist.    |
| Switch Action Status               | ID 09                                      | DWORD (32 bit) RO                                                                                                                                                                          |
|                                    | Bit 0                                      | Flash write in progress                                                                                                                                                                    |
|                                    | Bit 1                                      | Unable to write to flash or write incomplete                                                                                                                                               |

**Table 7:** *Hirschmann Ethernet Switch Agent Object*

- a. RS20/RS30/RS40, MS20/MS30, OCTOPUS, PowerMICE, RSR20/RSR30, MACH 100 and MACH 1000: 32 bit;  
MACH 4000: 64 bit

The Hirschmann specific Ethernet Switch Agent Object provides you with the additional vendor specific service, with the Service-Code 35<sub>H</sub> for saving the Switch configuration. The Switch replies to the request for saving the configuration, as soon as it saved the configuration in the flash memory.

## 2.2.5 I/O Data

You will find the exact meaning of the individual bits of the device status in the I/O data in [“Ethernet Switch Agent Object” on page 27](#).

| I/O Data                         | Value (data types and sizes to be defined)                                                                                                              | Direction                  |
|----------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------|
| Device Status                    | Bitmask (see Switch Agent Attribute 1)                                                                                                                  | Input, DWORD 32 Bit        |
| Link Status                      | Bitmask, 1 Bit per port<br>0: No link, 1: Link up                                                                                                       | Input, DWORD <sup>a</sup>  |
| Output Links Admin State applied | Bitmask (1 Bit per port) to acknowledge output. Link state change can be denied, e.g. for controller access port.<br>0: Port enabled, 1: Port disabled. | Input DWORD <sup>a</sup>   |
| Utilization Alarm                | Bitmask, 1 Bit per port<br>0: No alarm, 1: Alarm on port                                                                                                | Input, DWORD <sup>a</sup>  |
| Access Violation Alarm           | Bitmask, 1 Bit per port<br>0: No alarm, 1: Alarm on port                                                                                                | Input, DWORD <sup>a</sup>  |
| Multicast Connections            | Integer, number of connections                                                                                                                          | Input, 1 DINT 32 bit       |
| TCP/IP Connections               | Integer, number of connections                                                                                                                          | Input, 1 DINT 32 bit       |
| Link Admin State                 | Bitmask, one bit per port<br>0: Port enabled, 1: Port disabled                                                                                          | Output, DWORD <sup>a</sup> |

**Table 8: I/O Data**

- a. RS20/RS30/RS40, MS20/MS30, OCTOPUS, PowerMICE, RSR20/RSR30, MACH 100 and MACH 1000: 32 Bit;  
MACH 4000: 64 Bit

## 2.2.6 Assignment of the Ethernet Link Object Instances

The table shows the assignment of the Switch ports to the Ethernet Link Object Instances.

| Ethernet Link Object Instance | RS20/RS30/RS40<br>RSR20/RSR30,<br>OCTOPUS,<br>MACH 1000 | MS20/MS30,<br>PowerMICE,<br>MACH 100 | MACH 4000         |
|-------------------------------|---------------------------------------------------------|--------------------------------------|-------------------|
| 1                             | CPU                                                     | CPU                                  | CPU               |
| 2                             | 1                                                       | Module 1 / port 1                    | Module 1 / port 1 |
| 3                             | 2                                                       | Module 1 / port 2                    | Module 1 / port 2 |
| 4                             | 3                                                       | Module 1 / port 3                    | Module 1 / port 3 |
| 5                             | 4                                                       | Module 1 / port 4                    | Module 1 / port 4 |
| 6                             | 5                                                       | Module 2 / port 1                    | Module 1 / port 5 |
| 7                             | 6                                                       | Module 2 / port 2                    | Module 1 / port 6 |
| 8                             | 7                                                       | Module 2 / port 3                    | Module 1 / port 7 |
| 9                             | 8                                                       | Module 2 / port 4                    | Module 1 / port 8 |
| 10                            | 9                                                       | Module 3 / port 1                    | Module 2 / port 1 |
| 11                            | 10                                                      | Module 3 / port 2                    | Module 2 / port 2 |
| 12                            | 11                                                      | Module 3 / port 3                    | Module 2 / port 3 |
| 13                            | 12                                                      | Module 3 / port 4                    | Module 2 / port 4 |
| 14                            | 13                                                      | Module 4 / port 1                    | Module 2 / port 5 |
| ..                            | ..                                                      | ..                                   | ..                |

Table 9: Assignment of the Switch ports to the Ethernet Link Object Instances

## 2.2.7 Supported Services

The table gives you an overview of the services for the object instances supported by the EtherNet/IP implementation.

| Service code                             | Identity Object | TCP/IP Interface Object       | Ethernet Link Object                        | Switch Agent Object       |
|------------------------------------------|-----------------|-------------------------------|---------------------------------------------|---------------------------|
| Get Attribute All (01H)                  | All Attributes  | All Attributes                | All Attributes                              | All Attributes            |
| Set Attribute All (02H)                  | -               | Settable Attributes (3, 5, 6) | -                                           | -                         |
| Get Attribute Single (0EH)               | All Attributes  | All Attributes                | All Attributes                              | All Attributes            |
| Set Attribute Single (10H)               | -               | Settable Attributes (3, 5, 6) | Settable Attributes (6, 65H, 67H, 68H, 69H) | Settable Attributes (7)   |
| Reset (05H)                              | Parameter (0.1) | -                             | -                                           | -                         |
| Save Configuration (35H) Vendor-specific | Parameter (0.1) | -                             | -                                           | Save Switch Configuration |

Table 10: Supported Services

### 3 PROFINET IO

PROFINET IO is an industrial communication network based on Ethernet that is accepted worldwide. It is based on the widely used transport protocols TCP/IP and UDP/IP (standard). This is an important aspect for fulfilling the requirements for consistency from the management level down to the field level.

PROFINET IO enhances the existing Profibus technology for such applications that require fast data communication and the use of industrial IT functions.

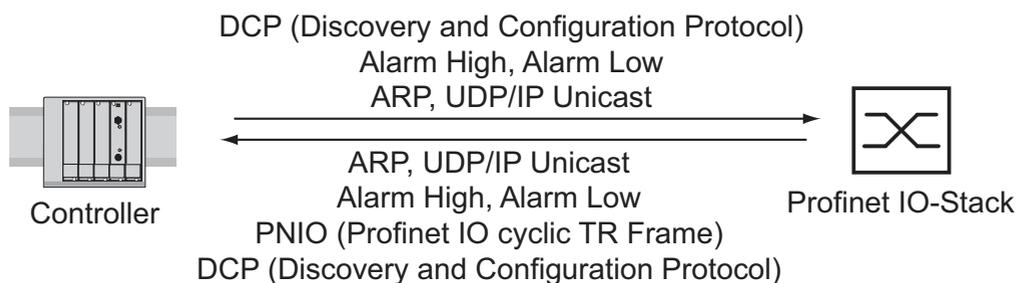


Figure 6: Communication between the Controller and the Switch

In particular, you will find PROFINET IO in Europe and in conjunction with Siemens controllers.

PROFINET IO uses the device description language GSDML (Generic Station Description Markup Language) to describe devices and their properties so that they can be processed automatically. You will find the device description in the GSD(ML) file of the device.

You will find detailed information on PROFINET on the Internet site of the PROFIBUS Organization at <http://www.profibus.com>. The devices conform to class B for PROFINET IO.

■ **Switch Models for PROFINET IO GSDML Version 2.3**

The device creates GSDML files in the GSDML V.2.3 format. Within the GSDML file, the device is modeled according to GSDML standard V.2.2.

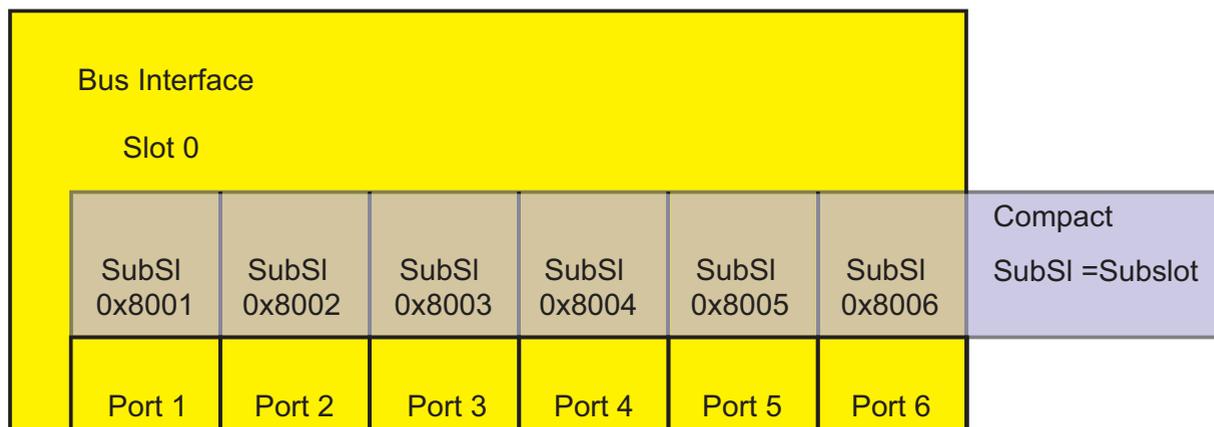


Figure 7: Compact Switch

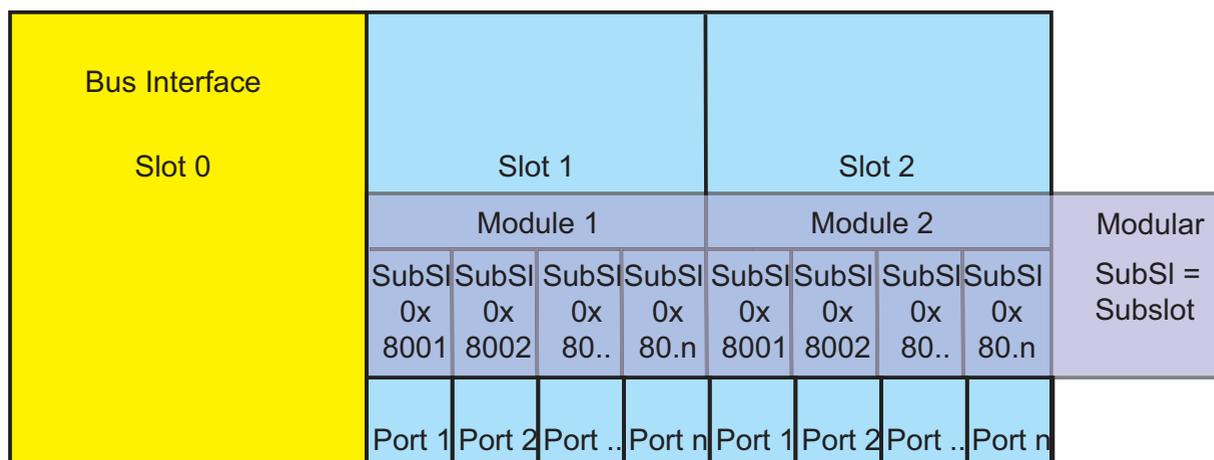


Figure 8: Modular Switch

## ■ **Graphical user interface and CLI**

In Profinet environments, the automation process establishes an application relation (AR) to the device when the device is set up successfully. As long as the application relation is established, certain device settings can not be changed by other users.

The following parameters are unchangeable via the graphical user interface, CLI, and SNMP when the application relation is established:

- ▶ IP address
- ▶ MRP
- ▶ Hiper-Ring
- ▶ DCP configuration
- ▶ HiDiscovery configuration
- ▶ Cable test
- ▶ LLDP configuration
- ▶ Port configuration

After the login of a user, the device displays a corresponding message via the graphical user interface and CLI.

# 3.1 Integration into a Control System

## 3.1.1 Preparing the Switch

After installing and connecting the Switch, you configure it according to the “Basic Configuration” user manual:

- In the `Basic Settings:System` dialog, check if a valid system name for the device is specified in the "Name" field.  
The system name can only contain alphanumeric characters, hyphens, and periods.
- Use the Web-based interface in the `Basic Settings:Network` dialog to check whether `Local` is selected in the “Mode” frame.
- Use the Web-based interface in the `Switching:VLAN:Global` dialog to check whether “VLAN 0 Transparent Mode” is selected.
- Use the Web-based interface in the `Advanced:Industry Protocols:PROFINET IO` dialog to check whether Profinet IO is activated.
- Load the GSD(ML) file and the icon onto your local computer.  
You get the GSD(ML) file and the icon
  - by using the Web-based interface in the `Advanced:Industry Protocols` dialog or
  - by using the software (Stand Alone GSDML File Generator) for creating the GSD(ML) file, which is included in the delivery.
- Configure the alarm setting and the threshold value for the alarms you want to monitor.

### 3.1.2 Configuration of the PLC

The following illustrates the configuration of the PLC using the example of the Simatic S7 software from Siemens, and assumes that you are familiar with operating the software.

The device also supports engineering stations from other manufacturers, such as PC Worx from Phönix.

**Note:** If for example, a management program is occupying the Switch CPU with SNMP requests, the I/O connection between the programmable logic controller (PLC) and the Switch can be interrupted for a time. As the Switch can still transmit data packages in this case, the system can also still be ready for operation.

The monitoring of the I/O connection to the Switch CPU as a failure criterion can result in system failure and is therefore less suitable as a failure criterion.

In the PLC default setting, the PLC sees the interruption of the I/O connection to the Switch as a failure criterion. According to the default setting, this leads to a system failure. To change this default setting, you employ Step7 programming measures.

#### ■ Providing the GDSML file

The Hirschmann provides you with the following options for generating GDSML files and icons:

- ▶ you can use the Web-based interface in the `Advanced:Industry Protocols:PROFINET IO` dialog to select `PROFINET IO` and download the GSDML file and the icon of the device.
- ▶ you can use the Web-based interface in the `Advanced:Industry Protocols:PROFINET IO` dialog to select `Other device` and download the GSDML file and the icon of another device, for which you enter the order description.
- ▶ you can use the software included in the delivery (Stand Alone GSDML File Generator) to create the GSDML file.

**■ Incorporating the Switch in the configuration**

- Open the “Simatic Manager” from Simatic S7.
- Open your project.
- Go to the hardware configuration.
- Install the GSD(ML) file using `Extras:Install GSD File`.  
Select the GSD file previously saved on your PC.  
Simatic S7 installs the file together with the icon.  
You will find the new Switch under `Profinet IO:Other Field Devices:Switching Devices:Hirschmann..` or under `Profinet IO:Other Field Devices:Network Components:Hirschmann...`
- Use Drag & Drop to pull the Switch onto the bus cable.

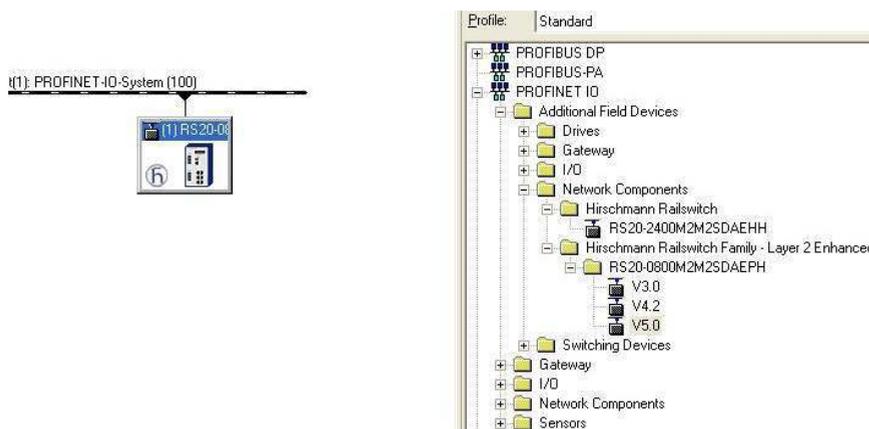


Figure 9: Adding a Switch from the Simatic S7 library

- To give the Switch its name, select the Switch and in the menu bar choose Target System:Ethernet>Edit Ethernet Participants...

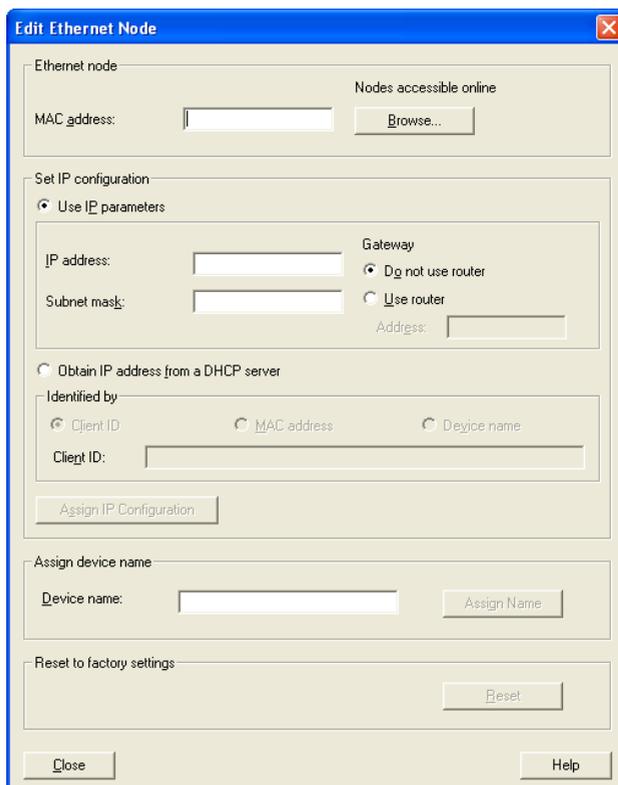
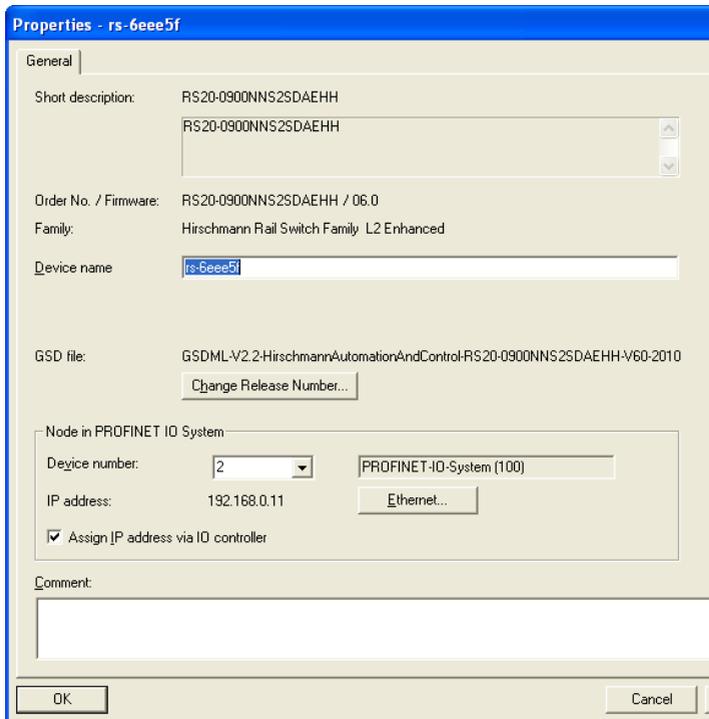


Figure 10: Dialog for entering the Switch name

- Click on "Browse".  
Select your Switch.  
Click on "OK".

- Give the Switch its name.  
Click on “Assign Name”.
- Click on “Close”.
  
- In the hardware configuration, right-click on the Switch and select Object properties.



*Figure 11: Dialog for entering the object name (= name of the Switch) and the IP parameter*

- Enter the same device name here.
- Click on “Ethernet”.  
Enter the IP parameters.  
Close the Ethernet input window.
- Click on “OK” to close the properties window.

The Switch is now included in the configuration.

## Configuring IO Cycle

- In the hardware configuration, right-click on the Switch and select Object properties.

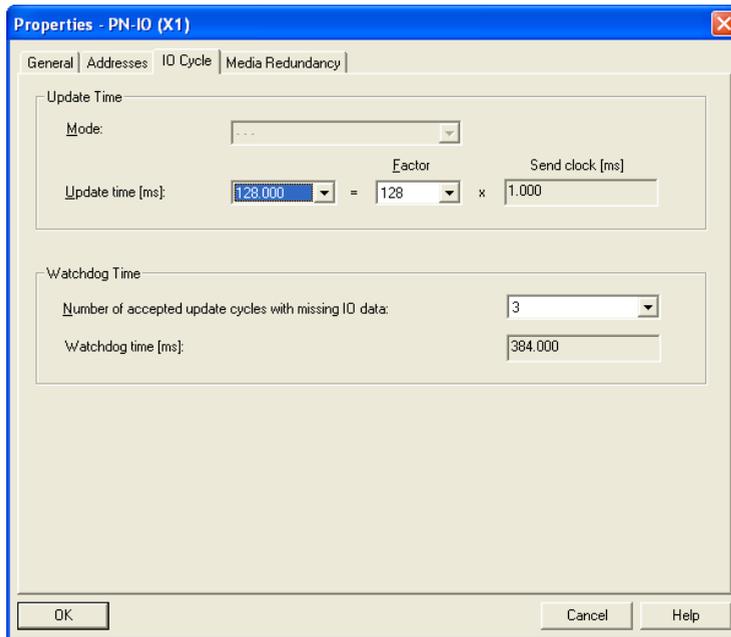


Figure 12: Dialog for entering the IO Cycle

- In the Properties window, select the “IO Cycle” tab.
- Under Update Time/Update time[ms]:, select the required update time (in ms) for the IO Cycle (see figure 12).
- Under Watchdog Time/Number of accepted update cycles with missing IO data, select the required number for the IO Cycle (see figure 12).
- Click on “OK” to close the properties window.

## Configuring Media Redundancy

- In the hardware configuration, right-click on the Switch and select Object properties.

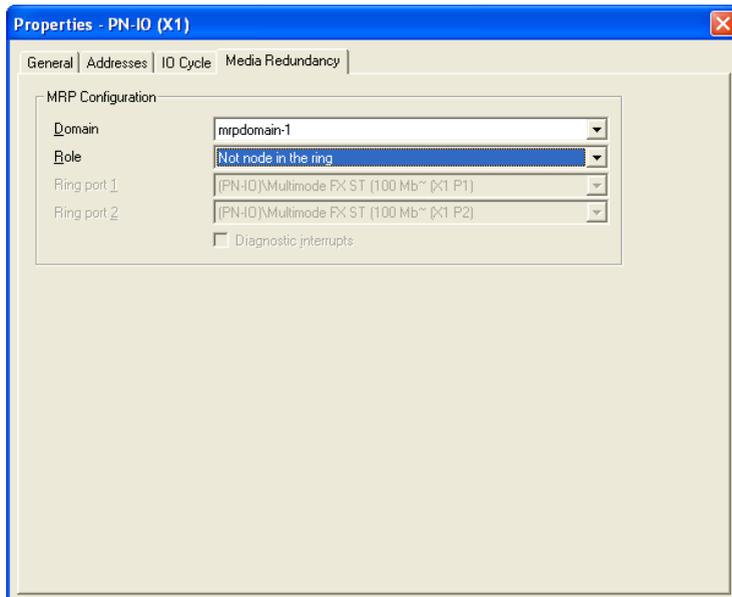


Figure 13: Dialog for entering the Media redundancy

- In the Properties window, select the “Media Redundancy” tab.
- Under MRP Configuration/Domain , select the required MRP domain for the node (see figure 13).
- Under MRP Configuration/Role , select the required role of the node in the ring (see figure 13).
- Under Ring Port 1/2 , select the active MRP Ring Ports.
- Click on “OK” to close the properties window.

## ■ Adding modules for modular devices

- Use Drag & Drop to pull a module from the library into a slot. Simatic S7 adds the ports using the Module properties.

### ■ Configuring device property

On slot 0 you enter the settings for the entire Switch.

- Select the Switch.
- Right-click on slot 0.

To configure the entire device, select `Object properties`.

- In the Properties window, select the “Parameters” tab.

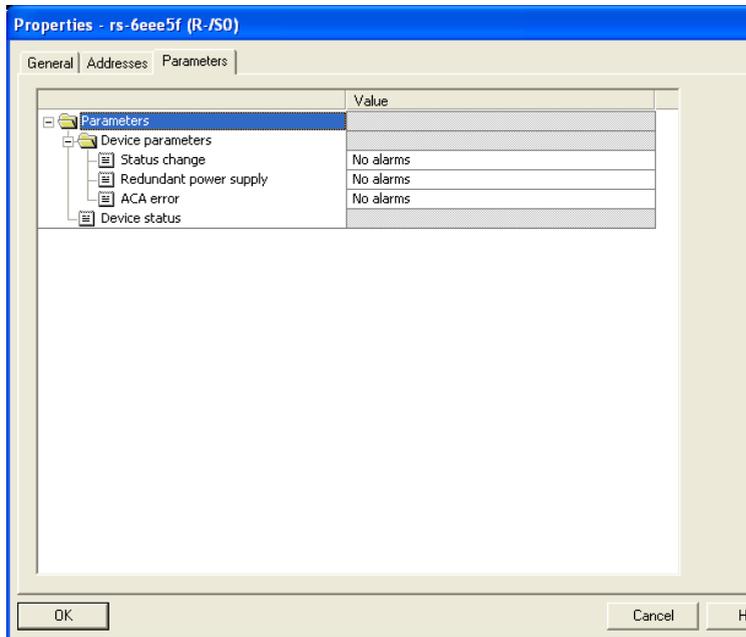


Figure 14: Configuring device alarms for e.g. RS20/RS30.

## ■ Configuring the port properties

For modular devices, slots 1 to n represent the modules. Within the slots, the ports are shown as records.

For non-modular devices, the slots 1 to n represent the ports.

### Configuring Alarms

- Right-click on one of the slots 1 to n and select `Object properties`.
- In the Properties window, select the “Parameters” tab.
- Select the desired alarms and close the window (see figure 15).

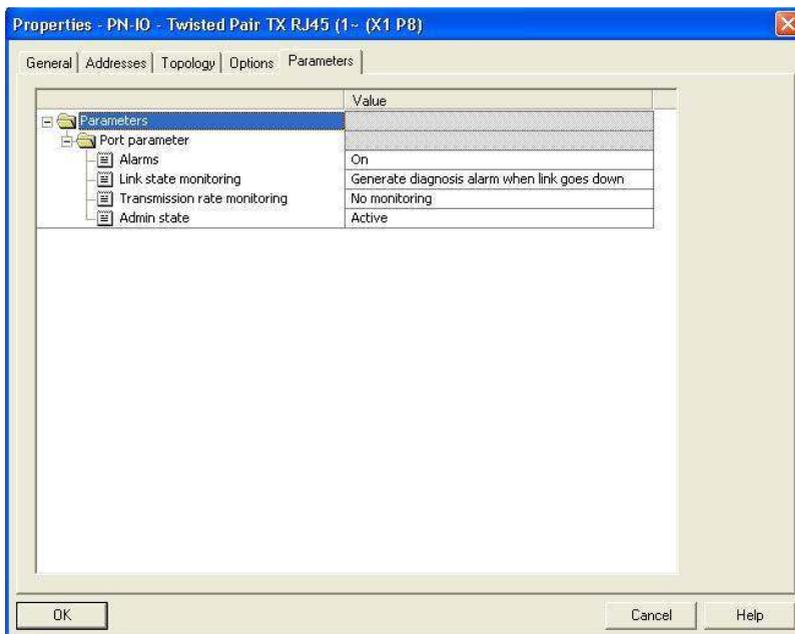


Figure 15: Port properties

Special case: “LinkDown” alarm:

The LinkDown alarm is made up of the AND-link

- of the Hirschmann-specific status for connection errors and
- of the Simatic S7-specific option for the connection.

Activating the LinkDown alarm:

- Under `Object properties`, select the `Parameter` tab (Hirschmann-specific).  
Activate “Alarms” and select the option `Generate diagnosis alarm when link goes down` under “Link state monitoring”.
- Under `Object properties`, select the `Options` tab (Simatic S7-specific).  
To activate the link monitoring, select a fixed setting for the port under `Connection/Transmission medium/Duplex`.

## ■ Configuring Connection Options

- Right-click on one of the slots 1 to n and select `Object properties`.

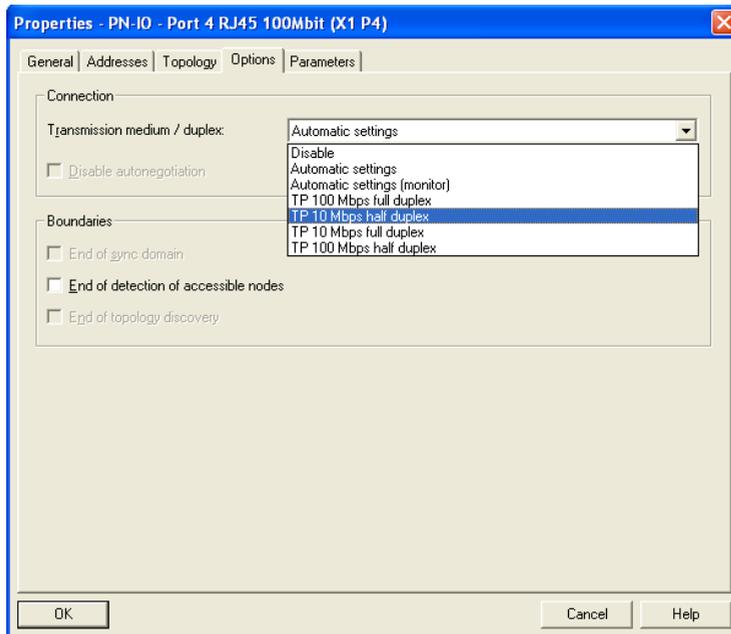


Figure 16: Dialog for entering the connection options

- In the Properties window, select the "Options" tab.
- Under "Connection/Transmission medium/duplex", select the desired setting for the port (see figure 16).

When you change the port setting to a value other than `Automatic settings`, the device disables the port for a short time. When the port is situated on the path between the I/O controller and the I/O device, the interruption possibly leads to a failure in establishing the Application Relation. Make the following provisions before changing the port setting:

- ▶ Beware of Loops! Deactivate RSTP on the ports between the I/O controller and the I/O device.
  - Open the "Redundancy:Spanning Tree:Port" dialog.
  - Unmark the "Stp active" checkbox for the relevant port.
  - Save the settings.
- ▶ Activate "Fast Start Up" on the ports between the I/O controller and the I/O device.
  - Open the "Advanced:Industrial Protocols:PROFINET" dialog.
  - For the relevant port, specify in the "Fast Start Up" field the value `enable`.

- Save the settings.
- Click "OK" to close the Properties window.

### Configuring Topology

- Right-click on one of the slots 1 to n and select `Object properties`.

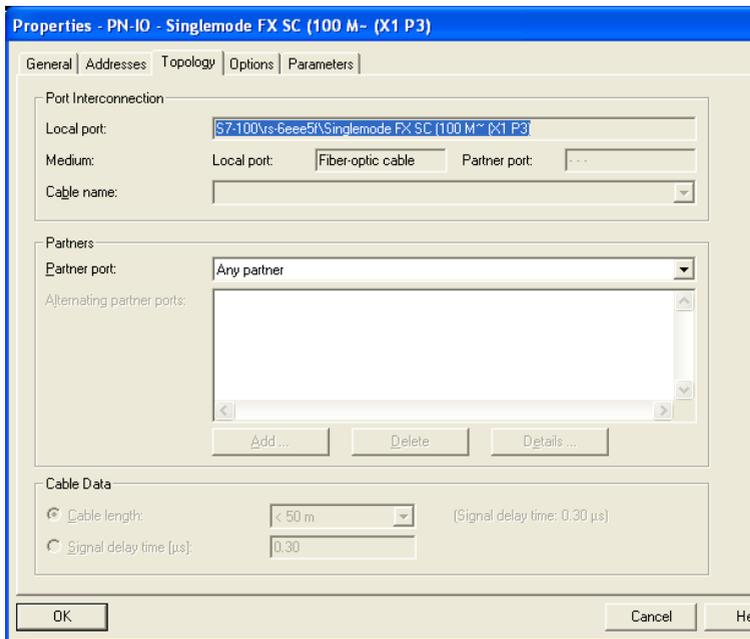


Figure 17: Dialog for entering the topology

- In the Properties window, select the "Topology" tab.
- Under `Port Interconnection/Local port`, select the required setting for the port (see figure 17).
- Under `Partner/Partner port`, select the required setting for the partner port (see figure 17).
- Click on "OK" to close the properties window.

### 3.1.3 Configuring the device

Included with the device is the program “Hirschmann Tool Calling Interface”, which you can install with the installation program

HirschmannToolCallingInterfaceXXXXXSetup.exe (XXXXX = software version, e.g. 01000).

After installing the program “Hirschmann Tool Calling Interface”, you have the option of starting two Hirschmann operating programs in Simatic S7 in order to perform more detailed device configurations.

- In Simatic S7, right-click on a device and select Web-based Interface (WWW) or Telnet in the drop-down menu.

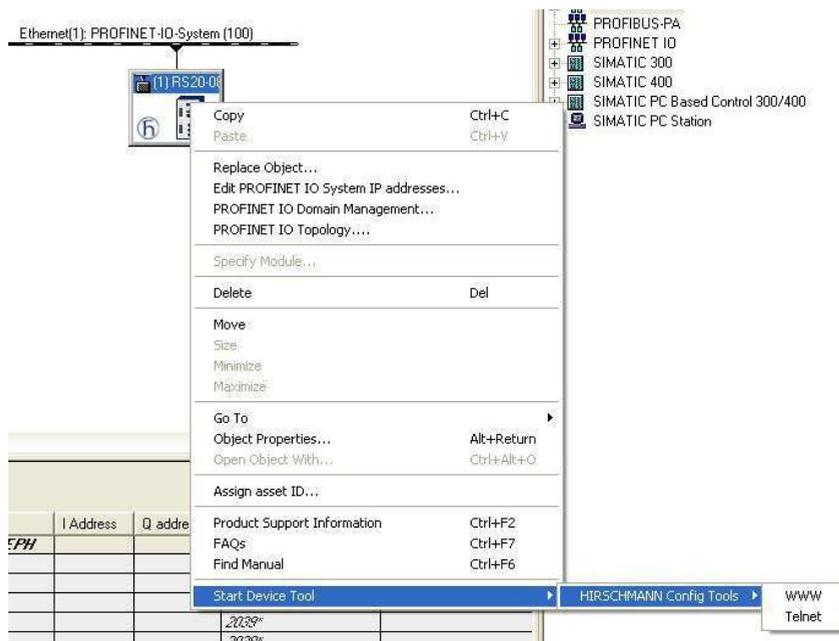


Figure 18: Call up the Hirschmann operating program

### 3.1.4 Swapping devices

Hirschmann devices support the device swapping function with an engineering station.

If identical devices are being swapped, the engineering station assigns the parameters of the original device to the new device.

The device swapping function with Simatic S7 requires the following prerequisites:

- ▶ S7 300 with SW release from V2.7 (currently available for CPU 319) or S7 400 with SW release from V5.2
- ▶ Hirschmann device SW release from 05.0.00
- ▶ Neighboring device(s) support(s) LLDP
- ▶ Topology (=neighborhood relationships) is configured and loaded onto SPS

Device swapping requires the following conditions:

- ▶ the replacement device is of exactly the same type as the device to be replaced.
- ▶ the replacement device is connected to exactly the same place in the network (same ports and neighboring devices).
- ▶ the replacement device has a Profinet default configuration. Set the device name to "" (null string).

If all these conditions are fulfilled, the engineering station automatically assigns the parameters of the original device (device name, IP parameters and configuration data) to the replacement device.

Procedure for swapping devices:

- Reset the replacement device to the state on delivery:
  - System name "" (= null string)
  - IP address = 0.0.0.0 or DHCP
  - PROFINET IO activated
- Make a note of the port assignment of the original device and remove the original device from the system.  
The PLC now detects an error.
- Now insert the replacement device at the same position in the network.  
Make sure the port assignments are the same as for the original device.  
The PLC finds the replacement device and configures it like the original device.

The PLC detects normal operation again.

If necessary, reset the PLC to "Run".

### **3.1.5 Swapping modules**

The PROFINET IO stack in the device detects a change in the modules connected and reports the change to the engineering station. If a previously configured module is removed from the device, the engineering station reports an error. If a configured module that was missing is connected, the engineering station removes the error message.

## 3.1.6 Monitoring the network

### ■ Topology Discovery

After the user initializes the Topology Discovery, the engineering station looks for connected devices.

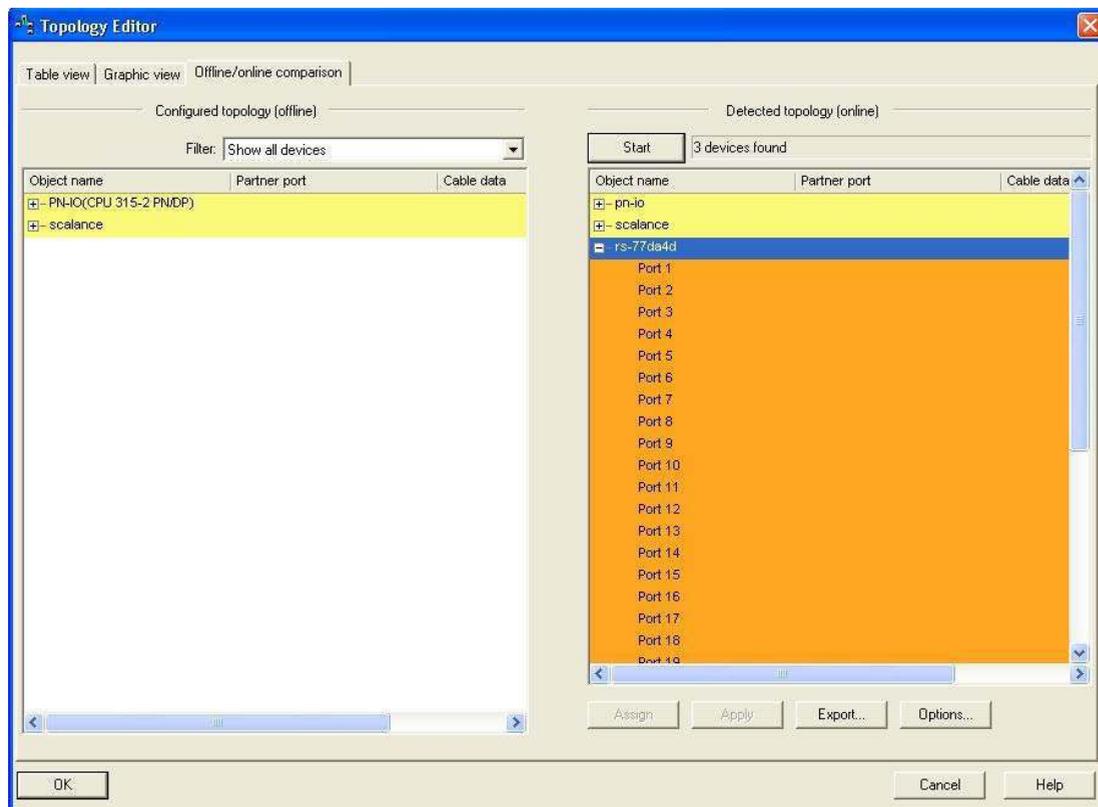


Figure 19: Topology Discovery

### ■ Configuring the topology

Simatic S7 gives the user the option to configure the topology and monitor it accordingly.

Simatic S7 displays the connection parameters (quality and settings) in a colored graphic.

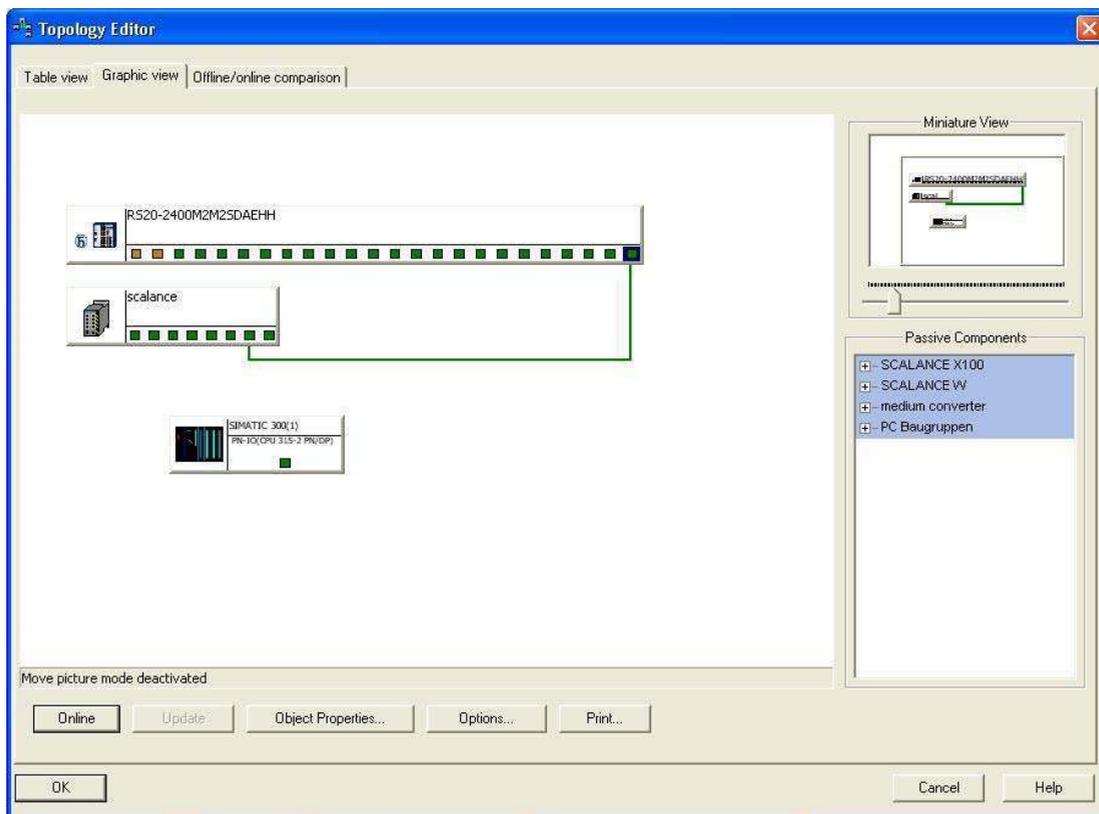


Figure 20: Configuring the topology

## ■ Communication diagnosis

Simatic S7 monitors the communication quality and outputs messages relating to communication problems.

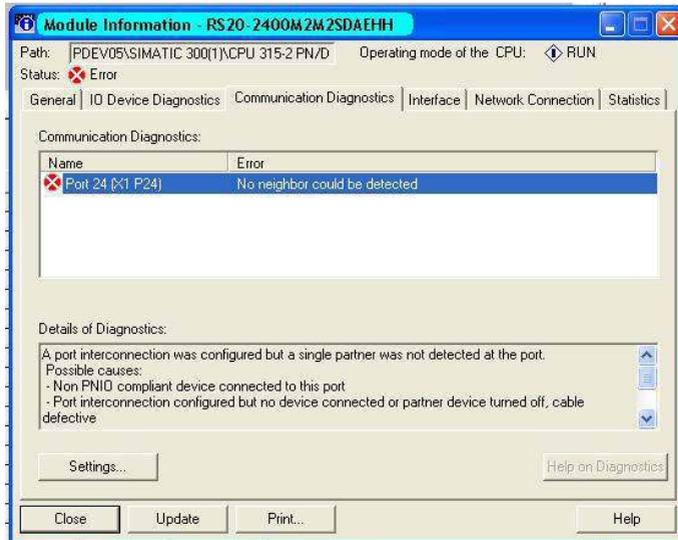
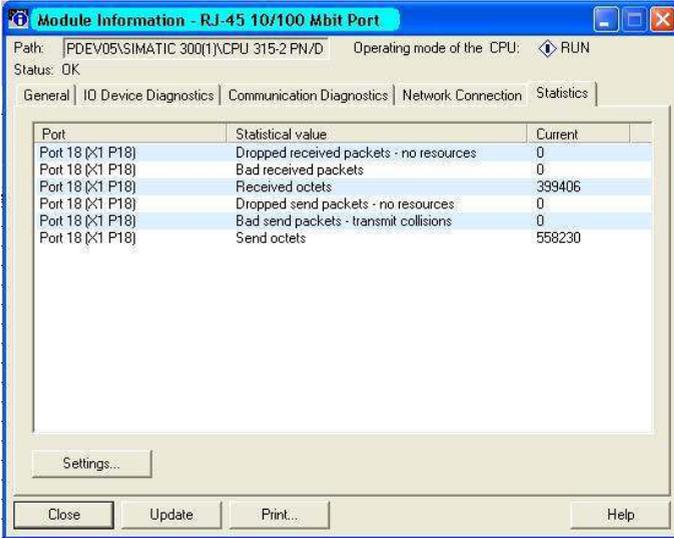


Figure 21: Diagnosis messages for the communication between the Switches and IO devices

### ■ Outputting port statistics

Simatic S7 counts for each port the number of data packets received and sent, the collisions, etc. You can view these figures in the form of statistic tables in Simatic S7.



The screenshot shows a window titled "Module Information - RJ-45 10/100 Mbit Port". The window displays the path "PDEV05\SIMATIC 300(1)\CPU 315-2 PN/D" and the operating mode of the CPU as "RUN". The status is "OK". The window has several tabs: "General", "IO Device Diagnostics", "Communication Diagnostics", "Network Connection", and "Statistics". The "Statistics" tab is active, showing a table of port statistics.

| Port             | Statistical value                       | Current |
|------------------|-----------------------------------------|---------|
| Port 18 (x1 P18) | Dropped received packets - no resources | 0       |
| Port 18 (x1 P18) | Bad received packets                    | 0       |
| Port 18 (x1 P18) | Received octets                         | 399406  |
| Port 18 (x1 P18) | Dropped send packets - no resources     | 0       |
| Port 18 (x1 P18) | Bad send packets - transmit collisions  | 0       |
| Port 18 (x1 P18) | Send octets                             | 558230  |

At the bottom of the window, there are buttons for "Settings...", "Close", "Update", "Print...", and "Help".

Figure 22: Example of a port statistic table

## 3.2 PROFINET IO Parameters

### 3.2.1 Alarms

The Switch supports alarms on the device and port levels (see „Device State“ in the Basic Configuration User Manual or the Web-based Interface Reference Manual).

|                        |                                                                                      |
|------------------------|--------------------------------------------------------------------------------------|
| Alarms on device level | Change in device status - Failure of redundant power supply - Failure/removal of ACA |
| Alarms on port level   | - Change in link status - Specified transfer rate exceeded.                          |

*Table 11: Alarms supported*

### 3.2.2 Record parameters

The Switch provides records for:

- ▶ Device parameters
- ▶ Device status
- ▶ Port status/parameters

| Byte | Content                      | Access | Value | Meaning                                                  |
|------|------------------------------|--------|-------|----------------------------------------------------------|
| 0    | Send alarm if status changes | rw     | 0     | Do not send alarms                                       |
|      |                              |        | 1     | Send alarm if one of the following alarm reasons occurs. |
| 1    | Power Alarm                  | rw     | 0     | Do not send alarm                                        |
|      |                              |        | 1     | Send alarm if a power supply fails.                      |
| 2    | ACA Alarm                    | rw     | 0     | Do not send alarm                                        |
|      |                              |        | 1     | Send alarm if the ACA is removed.                        |
| 3    | Module Alarm                 | rw     | 0     | Do not send alarm                                        |
|      |                              |        | 1     | Send alarm if the module connections are changed.        |

Table 12: Device parameters

| Byte | Content             | Access | Value | Meaning     |
|------|---------------------|--------|-------|-------------|
| 0    | Device Status       | ro     | 0     | Unavailable |
|      |                     |        | 1     | OK          |
|      |                     |        | 2     | Error       |
| 1    | Power supply unit 1 | ro     | 0     | Unavailable |
|      |                     |        | 1     | OK          |
|      |                     |        | 2     | Error       |
| 2    | Power supply unit 2 | ro     | 0     | Unavailable |
|      |                     |        | 1     | OK          |
|      |                     |        | 2     | Error       |
| 3    | Power supply unit 3 | ro     | 0     | Unavailable |
|      |                     |        | 1     | OK          |
|      |                     |        | 2     | Error       |
| 4    | Power supply unit 4 | ro     | 0     | Unavailable |
|      |                     |        | 1     | OK          |
|      |                     |        | 2     | Error       |
| 5    | Power supply unit 5 | ro     | 0     | Unavailable |
|      |                     |        | 1     | OK          |
|      |                     |        | 2     | Error       |
| 6    | Power supply unit 6 | ro     | 0     | Unavailable |
|      |                     |        | 1     | OK          |
|      |                     |        | 2     | Error       |
| 7    | Power supply unit 7 | ro     | 0     | Unavailable |
|      |                     |        | 1     | OK          |
|      |                     |        | 2     | Error       |

Table 13: Device status

| Byte | Content               | Access | Value | Meaning                                                 |
|------|-----------------------|--------|-------|---------------------------------------------------------|
| 8    | Power supply unit 8   | ro     | 0     | Unavailable                                             |
|      |                       |        | 1     | OK                                                      |
|      |                       |        | 2     | Error                                                   |
| 9    | Signal contact 1      | ro     | 0     | Unavailable                                             |
|      |                       |        | 1     | Closed                                                  |
|      |                       |        | 2     | Open                                                    |
| 10   | Signal contact 2      | ro     | 0     | Unavailable                                             |
|      |                       |        | 1     | Closed                                                  |
|      |                       |        | 2     | Open                                                    |
| 11   | Temperature           | ro     | 0     | Unavailable                                             |
|      |                       |        | 1     | OK                                                      |
|      |                       |        | 2     | Threshold value for temperature exceeded or not reached |
| 12   | Fan                   | ro     | 0     | Unavailable                                             |
|      |                       |        | 1     | OK                                                      |
|      |                       |        | 2     | Fan failure                                             |
| 13   | Module removal        | ro     | 0     | Unavailable                                             |
|      |                       |        | 1     | OK                                                      |
|      |                       |        | 2     | A module has been removed.                              |
| 14   | ACA removal           | ro     | 0     | Unavailable                                             |
|      |                       |        | 1     | OK                                                      |
|      |                       |        | 2     | The ACA has been removed.                               |
| 15   | HIPER_Ring            | ro     | 0     | Unavailable                                             |
|      |                       |        | 1     | OK                                                      |
|      |                       |        | 2     | Redundancy failure.                                     |
| 16   | Ring/Network coupling | ro     | 0     | Unavailable                                             |
|      |                       |        | 1     | OK                                                      |
|      |                       |        | 2     | Redundancy failure.                                     |
| 17   | Connection            | ro     | 0     | Unavailable                                             |
|      |                       |        | 1     | OK                                                      |
|      |                       |        | 2     | Connection failure.                                     |

Table 13: Device status

| Byte | Content           | Access | Value | Meaning                                                  |
|------|-------------------|--------|-------|----------------------------------------------------------|
| 0    | Report port error | rw     | 0     | Do not send alarms                                       |
|      |                   |        | 1     | Send alarm if one of the following alarm reasons occurs. |

Table 14: Port status/parameters

| Byte | Content                    | Access | Value | Meaning                                                                  |
|------|----------------------------|--------|-------|--------------------------------------------------------------------------|
| 1    | Report connection error    | rw     | 0     | Do not send alarm                                                        |
|      |                            |        | 1     | Send alarm if the connection has failed.                                 |
| 2    | Transmission rate too high | rw     | 0     | Do not send alarm                                                        |
|      |                            |        | 1     | Send alarm if the threshold value for the temperature has been exceeded. |
| 3    | Port on                    | rw     | 0     | Unavailable                                                              |
|      |                            |        | 1     | Switched on                                                              |
|      |                            |        | 2     | Switched off                                                             |
| 4    | Link status                | ro     | 0     | Unavailable                                                              |
|      |                            |        | 1     | Connection exists                                                        |
|      |                            |        | 2     | Connection interrupted                                                   |
| 5    | Bit rate                   | ro     | 0     | Unavailable                                                              |
|      |                            |        | 1     | Unknown                                                                  |
|      |                            |        | 2     | 10 MBit/s                                                                |
|      |                            |        | 2     | 100 MBit/s                                                               |
|      |                            |        | 2     | 1000 MBit/s                                                              |
| 6    | Duplex                     | ro     | 0     | Unavailable                                                              |
|      |                            |        | 1     | Half duplex                                                              |
|      |                            |        | 2     | Full duplex                                                              |
| 7    | Autonegotiation            | ro     | 0     | Unavailable                                                              |
|      |                            |        | 1     | Off                                                                      |
|      |                            |        | 2     | On                                                                       |

*Table 14: Port status/parameters*

### 3.2.3 I/O Data

You will find the bit assignment for the transferred I/O data in the following table.

| Direction                     | Byte | Bit | Meaning               |
|-------------------------------|------|-----|-----------------------|
| Input                         | 0    |     | General               |
|                               |      | 0   | Device status         |
|                               |      | 1   | Signal contact 1      |
|                               |      | 2   | Signal contact 2      |
|                               |      | 3   | Temperature           |
|                               |      | 4   | Fan                   |
|                               |      | 5   | Module removal        |
|                               |      | 6   | ACA removal           |
| Input                         | 1    |     | Power supply status   |
|                               |      | 0   | Power supply unit 1   |
|                               |      | 1   | Power supply unit 2   |
|                               |      | 2   | Power supply unit 3   |
|                               |      | 3   | Power supply unit 4   |
|                               |      | 4   | Power supply unit 5   |
|                               |      | 5   | Power supply unit 6   |
|                               |      | 6   | Power supply unit 7   |
| Input                         | 2    |     | Supply voltage status |
|                               |      | 0   | HIPER-Ring            |
|                               |      | 1   | Ring/Network coupling |
|                               |      | 2   | Connection error      |
|                               |      | 3   | Not used              |
|                               |      | 4   | Not used              |
|                               |      | 5   | Not used              |
|                               |      | 6   | Not used              |
| Output                        |      |     | Not defined           |
| Meaning of the bit content:   |      |     |                       |
| - 0: OK or unavailable        |      |     |                       |
| - 1: Reason for report exists |      |     |                       |

Table 15: Device I/O data

| Direction                   | Byte | Bit                | Meaning                                                 |
|-----------------------------|------|--------------------|---------------------------------------------------------|
| Input                       | 0    |                    | Connection status for ports 1 to 8                      |
|                             |      | 0                  | Port 1                                                  |
|                             |      | 1                  | Port 2                                                  |
|                             |      | 2                  | Port 3                                                  |
|                             |      | 3                  | Port 4                                                  |
|                             |      | 4                  | Port 5                                                  |
|                             |      | 5                  | Port 6                                                  |
|                             |      | 6                  | Port 7                                                  |
| Input                       | 1    |                    | Connection status for ports 9 to 16                     |
|                             |      | 0                  | Port 9                                                  |
|                             |      | 1                  | Port 10                                                 |
|                             |      | 2                  | Port 11                                                 |
|                             |      | 3                  | Port 12                                                 |
|                             |      | 4                  | Port 13                                                 |
|                             |      | 5                  | Port 14                                                 |
|                             |      | 6                  | Port 15                                                 |
| Input                       | n    |                    | Connection for port $(n * 8) + 1$ to port $(n * 8) + 8$ |
|                             |      | 0                  | Port $(n * 8) + 1$                                      |
|                             |      | 1                  | Port $(n * 8) + 2$                                      |
|                             |      | 2                  | Port $(n * 8) + 3$                                      |
|                             |      | 3                  | Port $(n * 8) + 4$                                      |
|                             |      | 4                  | Port $(n * 8) + 5$                                      |
|                             |      | 5                  | Port $(n * 8) + 6$                                      |
|                             |      | 6                  | Port $(n * 8) + 7$                                      |
|                             | 7    | Port $(n * 8) + 8$ |                                                         |
| Meaning of the bit content: |      |                    |                                                         |
| - 0: no connection          |      |                    |                                                         |
| - 1: connection active      |      |                    |                                                         |
| Output                      | 0    |                    | “Port activated” for ports 1 to 8                       |
|                             |      | 0                  | Port 1 activated                                        |
|                             |      | 1                  | Port 2 activated                                        |
|                             |      | 2                  | Port 3 activated                                        |
|                             |      | 3                  | Port 4 activated                                        |
|                             |      | 4                  | Port 5 activated                                        |
|                             |      | 5                  | Port 6 activated                                        |
|                             |      | 6                  | Port 7 activated                                        |
|                             | 7    | Port 8 activated   |                                                         |

Table 16: Port I/O data

| Direction                          | Byte | Bit                          | Meaning                                                       |
|------------------------------------|------|------------------------------|---------------------------------------------------------------|
| Output                             | 1    |                              | “Port activated” for ports 9 to 16                            |
|                                    |      | 0                            | Port 9 activated                                              |
|                                    |      | 1                            | Port 10 activated                                             |
|                                    |      | 2                            | Port 11 activated                                             |
|                                    |      | 3                            | Port 12 activated                                             |
|                                    |      | 4                            | Port 13 activated                                             |
|                                    |      | 5                            | Port 14 activated                                             |
|                                    |      | 6                            | Port 15 activated                                             |
|                                    | 7    | Port 16 activated            |                                                               |
| Output                             | n    |                              | “Port activated” for port $(n * 8) + 1$ to port $(n * 8) + 8$ |
|                                    |      | 0                            | Port $(n * 8) + 1$ activated                                  |
|                                    |      | 1                            | Port $(n * 8) + 2$ activated                                  |
|                                    |      | 2                            | Port $(n * 8) + 3$ activated                                  |
|                                    |      | 3                            | Port $(n * 8) + 4$ activated                                  |
|                                    |      | 4                            | Port $(n * 8) + 5$ activated                                  |
|                                    |      | 5                            | Port $(n * 8) + 6$ activated                                  |
|                                    |      | 6                            | Port $(n * 8) + 7$ activated                                  |
|                                    | 7    | Port $(n * 8) + 8$ activated |                                                               |
| Meaning of the output bit content: |      |                              |                                                               |
| - 0: Port activated                |      |                              |                                                               |
| - 1: Port deactivated              |      |                              |                                                               |

Table 16: Port I/O data

## **4 IEC 61850/MMS (RSR20/RSR30/MACH1000)**

IEC 61850/MMS is an industrial communication protocol standardized by the International Electrotechnical Commission (IEC). The protocol is to be found in substation automation, e.g. in the control technology of energy suppliers.

This protocol, which works in a packet-oriented way, is based on the TCP/IP transport protocol and uses the Manufacturing Messaging Specification (MMS) for the client-server communication. The protocol is object-oriented and defines a standardized configuration language that comprises, among other things, functions for SCADA, Intelligent Electronic Devices (IED) and for the network control technology.

Part 6 of the IEC 61850 standard defines the configuration language SCL (Substation Configuration Language). SCL describes the properties of the device and the system structure in an automatically processable form. The properties of the device described with SCL are stored in the ICD file on the device.

## 4.1 Switch model for IEC 61850

Technical Report IEC 61850 90-4 specifies a bridge model. The bridge model represents the functions of a switch as objects of an Intelligent Electronic Device (IED). An MMS client (e.g. the control room software) uses these objects to monitor and configure the device.

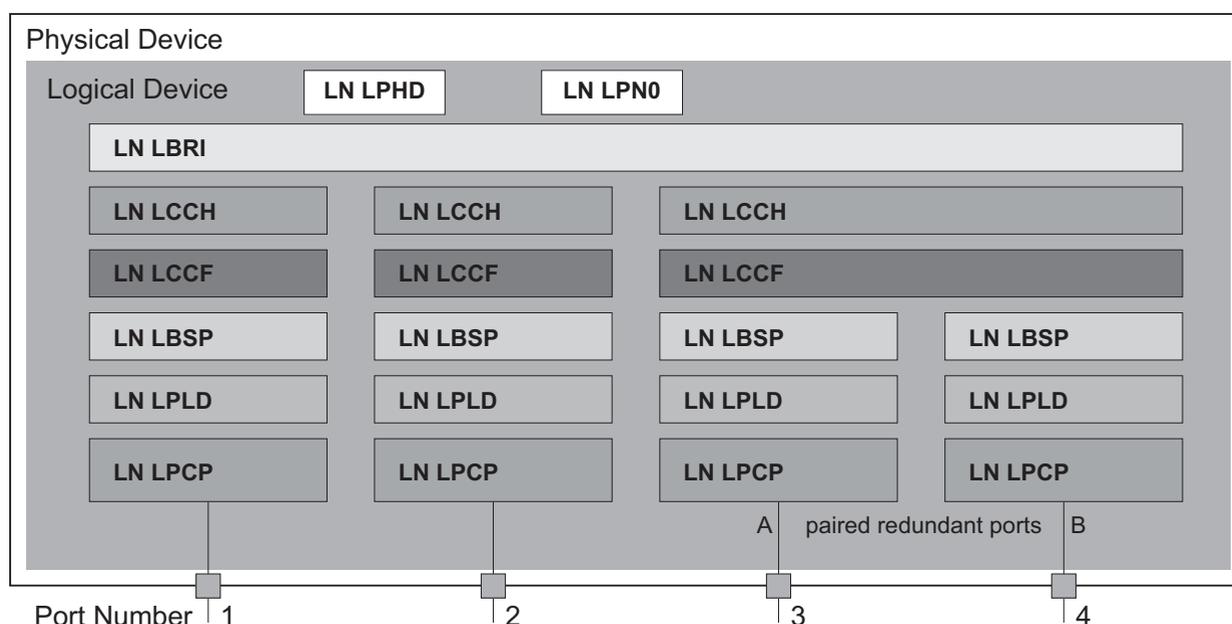


Figure 23: Bridge model based on Technical Report IEC 61850 90-4

| Class   | Description                                                                                                                              |
|---------|------------------------------------------------------------------------------------------------------------------------------------------|
| LN LLN0 | “Zero” logical node of the “Bridge” IED:<br>Defines the logical properties of the device.                                                |
| LN LPHD | “Physical Device” logical node of the “Bridge” IED:<br>Defines the physical properties of the device.                                    |
| LN LBRI | “Bridge” logical node:<br>Represents general settings of the bridge functions of the device.                                             |
| LN LCCH | “Communication Channel” logical node:<br>Defines the logical “Communication Channel” that consists of one or more physical device ports. |

Table 17: Classes of the bridge model based on TR IEC61850 90-4

| <b>Class</b> | <b>Description</b>                                                                                                                       |
|--------------|------------------------------------------------------------------------------------------------------------------------------------------|
| LN LCCF      | “Channel Communication Filtering” logical node:<br>Defines the VLAN and Multicast settings for the higher-level “Communication Channel”. |
| LN LBSP      | “Port Spanning Tree Protocol” logical node:<br>Defines the Spanning Tree statuses and settings for the respective physical device port.  |
| LN LPLD      | “Port Layer Discovery” logical node:<br>Defines the LLDP statuses and settings for the respective physical device port.                  |
| LN LPCP      | “Physical Communication Port” logical node:<br>Represents the respective physical device port.                                           |

*Table 17: Classes of the bridge model based on TR IEC61850 90-4 (cont.)*

## 4.2 Integration into a Control System

### 4.2.1 Preparing the Switch

After installing and connecting the Switch, you configure it according to the “Basic Configuration” user manual:

- Check that an IP address is assigned to the device.
- To start the MMS server, activate the function in the graphical user interface, in the `Advanced:Industry Protocols:IEC61850` dialog. Afterwards, an MMS client is able to connect to the device and to read and monitor the objects defined in the bridge model.

## **WARNING**

### **RISK OF UNAUTHORIZED ACCESS TO THE DEVICE**

IEC61850/MMS does not provide any authentication mechanisms. If the write access for IEC61850/MMS is activated, every client that can access the device using TCP/IP is capable of changing the settings of the device. This in turn can result in an incorrect configuration of the device and to failures in the network.

Only activate the write access if you have taken additional measures (e.g. Firewall, VPN, etc.) to eliminate the risk of unauthorized access.

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

- To enable the MMS client to configure the objects defined in the bridge model, you select the "Write Access" checkbox.

### **4.2.2 Offline configuration**

The device enables you to download the ICD file using the graphical user interface. This file contains the properties of the device described with SCL and enables the substation to be configured without a direct connection to the device.

- You download the ICD file by clicking the "Download ICD File" button in the `Advanced:Industry Protocols:IEC61850` dialog.

### 4.2.3 Monitoring the device

The IEC61850/MMS server integrated into the device allows you to monitor multiple statuses of the device by means of the Report Control Block (RCB). Up to 5 MMS clients can register for a Report Control Block at the same time.

The device allows the following statuses to be monitored:

| Class   | RCB object  | Description                                                                                                |
|---------|-------------|------------------------------------------------------------------------------------------------------------|
| LN LPHD | PwrSupAlm   | Changes when one of the redundant power supplies fails or starts operating again.                          |
|         | TmpAlm      | Changes when the temperature measured in the device exceeds or falls below the set temperature thresholds. |
|         | PhyHealth   | Changes when the status of the "LPHD.PwrSupAlm" or "LPHD.TmpAlm" RCB object changes.                       |
| LN LBRI | Health      | Changes when the status of the "LPHD.PwrSupAlm" or "LPHD.TmpAlm" RCB object changes.                       |
|         | RstpRoot    | Changes when the device takes over or relinquishes the role of the root bridge.                            |
|         | RstpTopoCnt | Changes when the topology changes due to a change of the root bridge.                                      |
| LN LCCH | ChLiv       | Changes when the link status of the physical port changes.                                                 |
| LN LPCP | PhyHealth   | Changes when the link status of the physical port changes.                                                 |

*Table 18: Statuses of the device that can be monitored with IEC 61850/MMS*

# A GSD File Generator

The program “Stand-alone GSD File Generator” is located on the product CD. The program allows you to generate a GSD file (PROFINET IO) and/or an EDS file (Ethernet/IP, EDS file from a later release onward) with icon from a non-existent device. You can use these files to configure devices in your engineering station that are not installed in the network yet.



Figure 24: Stand-alone GSD file generator

## B Readers' Comments

What is your opinion of this manual? We are constantly striving to provide as comprehensive a description of our product as possible, as well as important information to assist you in the operation of this product. Your comments and suggestions help us to further improve the quality of our documentation.

Your assessment of this manual:

|                     | Very Good             | Good                  | Satisfactory          | Mediocre              | Poor                  |
|---------------------|-----------------------|-----------------------|-----------------------|-----------------------|-----------------------|
| Precise description | <input type="radio"/> |
| Readability         | <input type="radio"/> |
| Understandability   | <input type="radio"/> |
| Examples            | <input type="radio"/> |
| Structure           | <input type="radio"/> |
| Comprehensive       | <input type="radio"/> |
| Graphics            | <input type="radio"/> |
| Drawings            | <input type="radio"/> |
| Tables              | <input type="radio"/> |

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

---



---



---



---



---



---



---



---

## Readers' Comments

---

Suggestions for improvement and additional information:

---

---

---

---

General comments:

---

---

---

---

Sender:

---

Company / Department:

---

Name / Telephone number:

---

Street:

---

Zip code / City:

---

E-mail:

---

Date / Signature:

---

Dear User,

Please fill out and return this page

- ▶ as a fax to the number +49 (0)7127/14-1600 or
- ▶ per mail to

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



# C Index

|                             |            |                         |        |
|-----------------------------|------------|-------------------------|--------|
| <b>A</b>                    |            | <b>R</b>                |        |
| Alarm                       | 54         | Record                  | 44, 54 |
| Alarm setting               | 36         | Redundancy              | 7      |
| <b>C</b>                    |            | Request Packet Interval | 19     |
| CIP                         | 15         | Router Function         | 17     |
| Common Industrial Protocol  | 15         | RPI                     | 19     |
| Conformity class            | 33         | RS Who                  | 17     |
| <b>D</b>                    |            | <b>S</b>                |        |
| Device description language | 33         | Simatic S7              | 37     |
| <b>E</b>                    |            | Symbol                  | 9      |
| EDS                         | 17, 67     | <b>T</b>                |        |
| Engineering Station         | 48, 49     | TCP/IP                  | 15, 33 |
| Engineering system          | 37         | Technical Questions     | 73     |
| EtherNet/IP website         | 16         | Threshold value         | 36     |
| <b>F</b>                    |            | Training Courses        | 73     |
| FAQ                         | 73         | <b>U</b>                |        |
| <b>G</b>                    |            | UDP/IP                  | 15, 33 |
| Generic Ethernet Module     | 18         |                         |        |
| GSD                         | 36, 38, 67 |                         |        |
| GSDML                       | 33         |                         |        |
| GSDML File Generator        | 36, 37     |                         |        |
| GSD file                    | 38         |                         |        |
| <b>I</b>                    |            |                         |        |
| Icon                        | 17, 36, 38 |                         |        |
| IEC 61850                   | 61         |                         |        |
| IGMP Snooping               | 17         |                         |        |
| Industrial HiVision         | 7          |                         |        |
| Industry Protocols          | 7          |                         |        |
| <b>M</b>                    |            |                         |        |
| MMS                         | 61         |                         |        |
| Module properties           | 42         |                         |        |
| <b>O</b>                    |            |                         |        |
| ODVA                        | 15         |                         |        |
| ODVA website                | 16         |                         |        |
| <b>P</b>                    |            |                         |        |
| PC Worx                     | 37         |                         |        |
| PROFIBUS Organization       | 33         |                         |        |
| PROFINET IO                 | 7          |                         |        |



## D Further Support

### ■ Technical Questions

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

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

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

You can contact us

in the EMEA region at

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

in the America region at

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

in the Asia-Pacific region at

- ▶ Tel.: +65 6854 9860
- ▶ E-mail: [inet-ap@belden.com](mailto:inet-ap@belden.com)

### ■ Hirschmann Competence Center

The Hirschmann Competence Center is ahead of its competitors:

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

The current technology and product training courses can be found at <http://www.hicomcenter.com>

- ▶ Support ranges from the first installation through the standby service to maintenance concepts.

With the Hirschmann Competence Center, you have decided against making any compromises. Our client-customized package leaves you free to choose the service components you want to use.

Internet:

<http://www.hicomcenter.com>





**HIRSCHMANN**

---

A **BELDEN** BRAND



**HIRSCHMANN**

A **BELDEN** BRAND

# User Manual

## Redundancy Configuration Industrial ETHERNET (Gigabit-)Switch RS20/RS30/RS40, MS20/MS30

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.

© 2015 Hirschmann Automation and Control GmbH

Manuals and software are protected by copyright. All rights reserved. The copying, reproduction, translation, conversion into any electronic medium or machine scannable form is not permitted, either in whole or in part. An exception is the preparation of a backup copy of the software for your own use. For devices with embedded software, the end-user license agreement on the enclosed CD/DVD applies.

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

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

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

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

# Contents

|          |                                                 |           |
|----------|-------------------------------------------------|-----------|
|          | <b>Safety Information</b>                       | <b>5</b>  |
|          | <b>About this Manual</b>                        | <b>7</b>  |
|          | <b>Key</b>                                      | <b>9</b>  |
| <b>1</b> | <b>Introduction</b>                             | <b>11</b> |
| 1.1      | Overview of Redundancy Topologies               | 12        |
| 1.2      | Overview of Redundancy Protocols                | 13        |
| <b>2</b> | <b>Ring Redundancy</b>                          | <b>15</b> |
| 2.1      | Example of a HIPER-Ring                         | 17        |
|          | 2.1.1 Setting up and configuring the HIPER-Ring | 19        |
| 2.2      | Example of a MRP-Ring                           | 23        |
| <b>3</b> | <b>Multiple Rings</b>                           | <b>29</b> |
| <b>4</b> | <b>Ring/Network Coupling</b>                    | <b>31</b> |
| 4.1      | Variants of the ring/network coupling           | 32        |
| 4.2      | Preparing a Ring/Network Coupling               | 34        |
|          | 4.2.1 STAND-BY switch                           | 34        |
|          | 4.2.2 One-Switch coupling                       | 37        |
|          | 4.2.3 Two-Switch coupling                       | 43        |
|          | 4.2.4 Two-Switch Coupling with Control Line     | 51        |
| <b>5</b> | <b>Spanning Tree</b>                            | <b>59</b> |
| 5.1      | The Spanning Tree Protocol                      | 61        |
|          | 5.1.1 The tasks of the STP                      | 61        |
|          | 5.1.2 Bridge parameters                         | 62        |
|          | 5.1.3 Bridge Identifier                         | 62        |
|          | 5.1.4 Root Path Cost                            | 63        |
|          | 5.1.5 Port Identifier                           | 65        |
| 5.2      | Rules for Creating the Tree Structure           | 66        |
|          | 5.2.1 Bridge information                        | 66        |
|          | 5.2.2 Setting up the tree structure             | 66        |

|          |                                                         |           |
|----------|---------------------------------------------------------|-----------|
| 5.3      | Example of determining the root path                    | 69        |
| 5.4      | Example of manipulating the root path                   | 71        |
| 5.5      | Example of manipulating the tree structure              | 73        |
| 5.6      | The Rapid Spanning Tree Protocol                        | 74        |
| 5.6.1    | Port roles                                              | 74        |
| 5.6.2    | Port states                                             | 77        |
| 5.6.3    | Spanning Tree Priority Vector                           | 78        |
| 5.6.4    | Fast reconfiguration                                    | 78        |
| 5.6.5    | Configuring the Rapid Spanning Tree                     | 79        |
| 5.7      | Combining RSTP and MRP                                  | 88        |
| 5.7.1    | Application example for the combination of RSTP and MRP | 90        |
| <b>A</b> | <b>Readers' Comments</b>                                | <b>93</b> |
| <b>B</b> | <b>Index</b>                                            | <b>95</b> |
| <b>C</b> | <b>Further Support</b>                                  | <b>97</b> |

# Safety Information



## **WARNING**

### **UNCONTROLLED MACHINE ACTIONS**

To avoid uncontrolled machine actions caused by data loss, configure all the data transmission devices individually.

Before you start any machine which is controlled via data transmission, be sure to complete the configuration of all data transmission devices.

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



## About this Manual

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

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

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

The “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 IO.

The “Graphical User Interface” reference manual contains detailed information on using the graphical user 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 Industrial HiVision network management software provides you with additional options for smooth configuration and monitoring:

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

# Key

The designations used in this manual have the following meanings:

---

|                                                                                   |                                                                              |
|-----------------------------------------------------------------------------------|------------------------------------------------------------------------------|
|  | List                                                                         |
|  | Work step                                                                    |
|  | Subheading                                                                   |
| <a href="#">Link</a>                                                              | Cross-reference with link                                                    |
| <b>Note:</b>                                                                      | A note emphasizes an important fact or draws your attention to a dependency. |
| <i>Courier</i>                                                                    | ASCII representation in the graphical user interface                         |
|  | Execution in the Graphical User Interface                                    |
|  | Execution in the Command Line Interface                                      |

---

Symbols used:

---

|                                                                                     |                      |
|-------------------------------------------------------------------------------------|----------------------|
|  | WLAN access point    |
|  | Router with firewall |
|  | Switch with firewall |
|  | Router               |
|  | Switch               |

---

# Key

---



Bridge



Hub



A random computer



Configuration Computer



Server



PLC -  
Programmable logic  
controller



I/O -  
Robot

# 1 Introduction

The device contains a range of redundancy functions:

- ▶ HIPER-Ring
- ▶ MRP-Ring
- ▶ Ring/Network coupling
- ▶ Rapid Spanning Tree Algorithm (RSTP)

# 1.1 Overview of Redundancy Topologies

To introduce redundancy onto layer 2 of a network, you first define which network topology you require. Depending on the network topology selected, you then choose from the redundancy protocols that can be used with this network topology.

The following topologies are possible:

| Network topology                          | Possible redundancy procedures                  | Comments                                                                                                                                                                        |
|-------------------------------------------|-------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Tree structure without loops (cycle-free) | Only possible in connection with physical loops | -                                                                                                                                                                               |
| Topology with 1 loop                      | RSTP<br>Ring Redundancy                         | Ring Redundancy procedures (HIPER-Ring, Fast HIPER-Ring or MRP) provide shorter switching times than RSTP.                                                                      |
| Topology with 2 loops                     | RSTP<br>Ring Redundancy                         | Ring redundancy: an MRP-Ring with an RSTP-Ring.                                                                                                                                 |
| Topology with 3 non-nested loops          | RSTP<br>Ring Redundancy<br>Ring coupling        | The ring coupling provides particular support when redundantly coupling a redundant ring to another redundant ring, or to any structure that only works with Hirschmann devices |

*Table 1: Overview of Redundancy Topologies*

The Ring Redundancy Protocol MRP has particular properties to offer:

- ▶ You have the option of coupling to MRP-Rings other ring structures that work with RSTP ([see on page 88 “Combining RSTP and MRP”](#)).

## 1.2 Overview of Redundancy Protocols

| Redundancy procedure | Network topology | Switch-over time                                                                                                                                                                                                                                                                    |
|----------------------|------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| RSTP                 | Random structure | typically < 1 s (STP < 30 s), up to < 30 s - depends heavily on the number of devices                                                                                                                                                                                               |
|                      |                  | <b>Note:</b> Up to 79 devices possible, depending on topology and configuration. If the default values (factory settings) are used, up to 39 devices are possible, depending on the topology ( <a href="#">see on page 59 "Spanning Tree"</a> ).                                    |
| HIPER-Ring           | Ring             | typically 80 ms, up to < 500 ms or < 300 ms (selectable) - the number of switches has a minimal effect on the switch-over time                                                                                                                                                      |
| MRP-Ring             | Ring             | typically 80 ms, up to < 500 ms or < 200 ms (selectable) - the number of switches has a minimal effect on the switch over time                                                                                                                                                      |
|                      |                  | <b>Note:</b> In combination with RSTP in MRP compatibility mode, up to 39 devices are possible, depending on the configuration. If the default values (factory settings) for RSTP are being used, up to 19 devices are possible ( <a href="#">see on page 59 "Spanning Tree"</a> ). |

Table 2: Comparison of the redundancy procedures

**Note:** When you are using a redundancy function, you deactivate the flow control on the participating device ports. If the flow control and the redundancy function are active at the same time, there is a risk that the redundancy function will not operate as intended.



## 2 Ring Redundancy

The concept of ring redundancy allows the construction of high-availability, ring-shaped network structures.

With the help of the RM (**R**ing **M**anager) function, the two ends of a backbone in a line structure can be closed to a redundant ring. The ring manager keeps the redundant line open as long as the line structure is intact. If a segment becomes inoperable, the ring manager immediately closes the redundant line, and line structure is intact again.

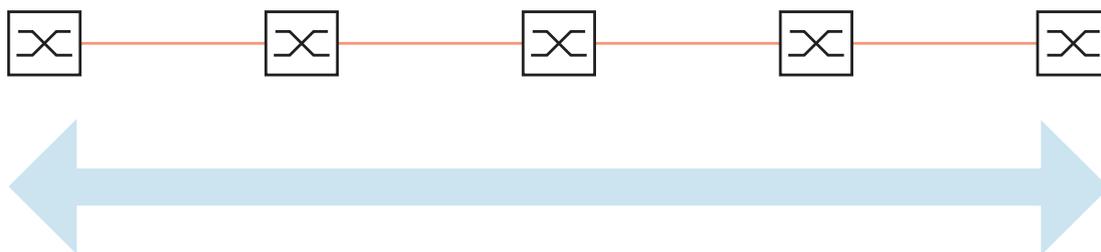


Figure 1: Line structure

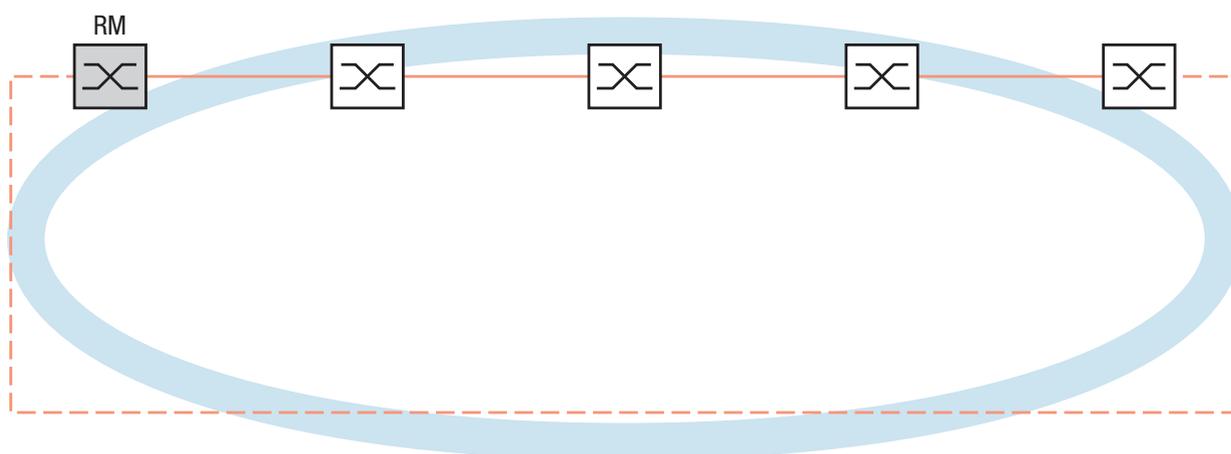


Figure 2: Redundant ring structure

RM = Ring Manager

— main line

- - - redundant line

If a section is down, the ring structure of a

- ▶ HIPER-(**HIGH PERFORMANCE REDUNDANCY**) Ring with up to 50 devices typically transforms back to a line structure within 80 ms (possible settings: standard/accelerated).
- ▶ MRP (**Media Redundancy Protocol**) Ring (IEC 62439) of up to 50 devices typically transforms back to a line structure within 80 ms (adjustable to max. 200 ms/500 ms).

Devices with HIPER-Ring function capability:

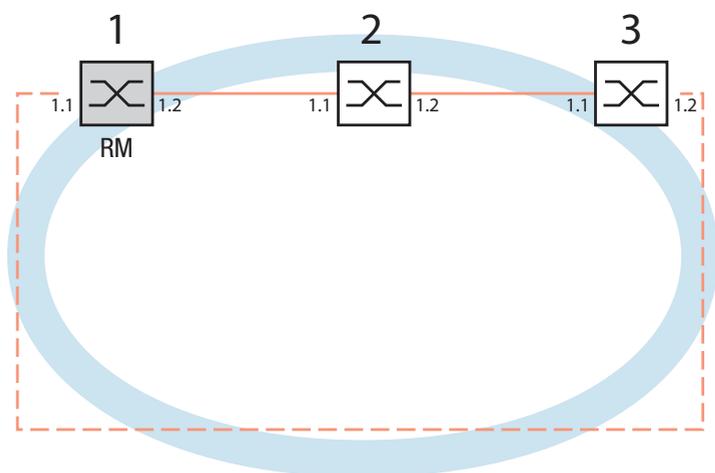
- ▶ Within a HIPER-Ring, you can use any combination of the following devices:
  - RS1
  - RS2-./.
  - RS2-16M
  - RS2-4R
  - RS20, RS30, RS40
  - RSR20, RSR30
  - OCTOPUS
  - MICE
  - MS20, MS30
  - PowerMICE
  - MACH 100
  - MACH 1000
  - MACH 1040
  - MACH 3000
  - MACH 4000
- ▶ Within an MRP-Ring, you can use devices that support the MRP protocol based on IEC62439.

**Note:** Only one Ring Redundancy method can be enabled on one device at any one time. When changing to another Ring Redundancy method, deactivate the function for the time being.

**Note:** The following usage of the term “ring manager” instead of “redundancy manager” makes the function easier to understand.

## 2.1 Example of a HIPER-Ring

A network contains a backbone in a line structure with 3 devices. To increase the redundancy reliability of the backbone, you have decided to convert the line structure to a HIPER-Ring. You use ports 1.1 and 1.2 of the devices to connect the lines<sup>1</sup>.



*Figure 3: Example of HIPER-Ring*  
*RM = Ring Manager*  
*— main line*  
*- - - redundant line*

The following example configuration describes the configuration of the ring manager device (1). The two other devices (2 to 3) are configured in the same way, but without activating the ring manager function. Select the “Standard” value for the ring recovery, or leave the field empty.

1. On modular devices the 1st number of the port designation specifies the module. The 2nd number specifies the port on the module. The specification pattern 1.x is also used on non-modular devices for consistency.

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

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

## 2.1.1 Setting up and configuring the HIPER-Ring

- Set up the network to meet your demands.
- Configure all ports so that the transmission speed and the duplex settings of the lines correspond to the following table:

| Port type | Bit rate   | Autonegotiation<br>(automatic<br>configuration) | Port setting | Duplex                       |
|-----------|------------|-------------------------------------------------|--------------|------------------------------|
| TX        | 100 Mbit/s | off                                             | on           | 100 Mbit/s full duplex (FDX) |
| TX        | 1 Gbit/s   | on                                              | on           | -                            |
| Optical   | 100 Mbit/s | off                                             | on           | 100 Mbit/s full duplex (FDX) |
| Optical   | 1 Gbit/s   | on                                              | on           | -                            |

Table 3: Port settings for ring ports

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

- Select the `Redundancy:Ring Redundancy` dialog.
- Under “Version”, select `HIPER-Ring`.
- Define the desired ring ports 1 and 2 by making the corresponding entries in the module and port fields. If it is not possible to enter a module, then there is only one module in the device that is taken over as a default.

Display in “Operation” field:

- `active`: This port is switched on and has a link.
- `inactive`: This port is switched off or it has no link.

Figure 4: Ring Redundancy dialog

- Activate the ring manager for this device. Do not activate the ring manager for any other device in the HIPER-Ring.
  - In the “Ring Recovery” frame, select the value “Standard” (default).
- Note:** Settings in the “Ring Recovery” frame are only effective for devices that you have configured as ring managers.
- Click "Set" to save the changes temporarily.

```

enable Change to the privileged EXEC mode.
configure Change to the Configuration mode.
hiper-ring mode ring-manager Select the HIPER-Ring ring redundancy and
 define the device as ring manager.

Switch's HIPER Ring mode set to ring-manager
hiper-ring port primary 1/1 Define port 1 in module 1 as ring port 1.
HIPER Ring primary port set to 1/1
hiper-ring port secondary 1/2 Define port 2 in module 1 as ring port 2.
HIPER Ring secondary port set to 1/2
exit Change to the privileged EXEC mode.

```

```

show hiper-ring Display the HIPER-Ring parameters.
HIPER Ring Mode of the Switch..... ring-manager
 configuration determined by..... management
HIPER Ring Primary Port of the Switch..... 1/1, state active
HIPER Ring Secondary Port of the Switch..... 1/2, state active
HIPER Ring Redundancy Manager State..... active
HIPER Ring Redundancy State (red. exists).. no (rm is active)
HIPER Ring Setup Info (Config. failure)..... no error
HIPER Ring Recovery Delay..... 500ms

```

- Now proceed in the same way for the other two devices.

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

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

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

**Note:** Deactivate the Spanning Tree protocol for the ports connected to the HIPER-Ring, because Spanning Tree and Ring Redundancy affect each other.

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

- Now you connect the line to the ring. To do this, you connect the 2 devices to the ends of the line using their ring ports.

The displays in the “Redundancy Manager 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.

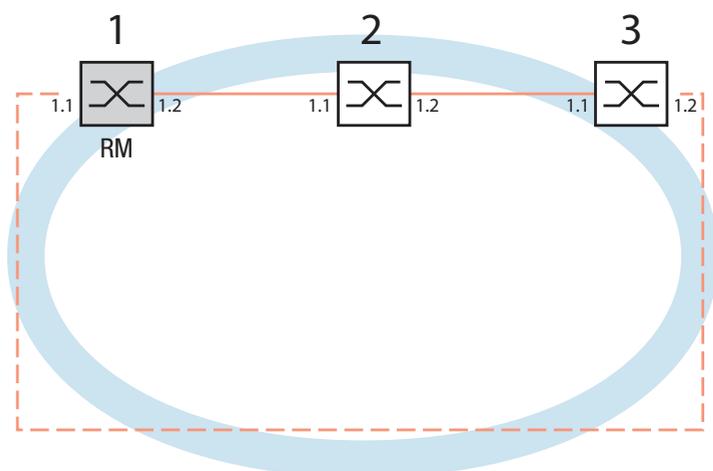
The displays in the “Information” frame mean

- “Redundancy existing”: One of the lines affected by the function may be interrupted, with the redundant line then taking over the function of the interrupted line.
- “Configuration failure”: The function is incorrectly configured or the cable connections at the ring ports are improperly configured (e.g., not plugged into the ring ports).

**Note:** If you want to use link aggregation connections in the HIPER-Ring (PowerMICE and MACH 4000), you enter the index of the desired link aggregation entry for the module and the port.

## 2.2 Example of a MRP-Ring

A network contains a backbone in a line structure with 3 devices. To increase the availability of the backbone, you decide to convert the line structure to a redundant ring. In contrast to the previous example, devices from different manufacturers are used which do not all support the HIPER-Ring protocol. However, all devices support MRP as the ring redundancy protocol, so you decide to deploy MRP. You use ports 1.1 and 2.2 of the devices to connect the lines.



*Figure 5: Example of MRP-Ring*  
*RM = Ring Manager*  
*— main line*  
*- - - redundant line*

The following example configuration describes the configuration of the ring manager device (1). You configure the 2 other devices (2 to 3) in the same way, but without activating the ring manager function. This example does not use a VLAN. You have entered 200 ms as the ring recovery time, and all the devices support the advanced mode of the ring manager.

**Note:** For devices with DIP switches, put all DIP switches to “On”. The effect of this is that you can use the software configuration to configure the redundancy function without any restrictions. You thus avoid the possibility of the software configuration being hindered by the DIP switches.

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

- Set up the network to meet your demands.
- Configure all ports so that the transmission speed and the duplex settings of the lines correspond to the following table:

| Port type | Bit rate   | Autonegotiation<br>(automatic<br>configuration) | Port setting | Duplex                       |
|-----------|------------|-------------------------------------------------|--------------|------------------------------|
| TX        | 100 Mbit/s | off                                             | on           | 100 Mbit/s full duplex (FDX) |
| TX        | 1 Gbit/s   | on                                              | on           | -                            |
| Optical   | 100 Mbit/s | off                                             | on           | 100 Mbit/s full duplex (FDX) |
| Optical   | 1 Gbit/s   | on                                              | on           | -                            |

*Table 4: Port settings for ring ports*

- Select the `Redundancy:Ring Redundancy` dialog.
- Under “Version”, select `MRP`.
- Define the desired ring ports 1 and 2 by making the corresponding entries in the module and port fields. If it is not possible to enter a module, then there is only one module in the device that is taken over as a default.

### 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 disabled
- ▶ not-connected: this port has no link

Figure 6: Ring Redundancy dialog

- In the “Ring Recovery” frame, select 200 ms.

**Note:** If selecting 200 ms for the ring recovery does not provide the ring stability necessary to meet the requirements of your network, you select 500 ms.

**Note:** Settings in the “Ring Recovery” frame are only effective for devices that you have configured as ring managers.

- Under “Configuration Redundancy Manager”, activate the advanced mode.
- Activate the ring manager for this device. Do not activate the ring manager for any other device in the MRP-Ring.
- Leave the VLAN ID as 0 in the VLAN field.
- Switch the operation of the MRP-Ring on.
- Click "Set" to save the changes temporarily.

The displays in the “Information” frame mean

- “Redundancy existing”: One of the lines affected by the function may be interrupted, with the redundant line then taking over the function of the interrupted line.
- “Configuration failure”: The function is incorrectly configured or the cable connections at the ring ports are improperly configured (e.g., not plugged into the ring ports).

The “VLAN” frame enables you to assign the MRP-Ring to a VLAN:

- If VLANs are configured, you make the following selections in the “VLAN” frame:
  - VLAN ID 0, if the MRP-Ring configuration is not to be assigned to a VLAN, as in this example.  
Select VLAN ID 1 and VLAN membership  $\cup$  (Untagged) in the static VLAN table for the ring ports.
  - A VLAN ID  $> 0$ , if the MRP-Ring configuration is to be assigned to this VLAN.  
For all devices in this MRP-Ring, enter this VLAN ID in the MRP-Ring configuration, and then choose this VLAN ID and the VLAN membership Tagged ( $\text{T}$ ) in the static VLAN table for all ring ports in this MRP-Ring.

**Note:** If you want to use the RSTP ([see on page 59 “Spanning Tree”](#)) redundancy protocol in an MRP-Ring, switch on the MRP compatibility on all devices in the MRP-Ring in the `Rapid Spanning Tree:Global` dialog as the RSTP (Spanning-Tree) and ring redundancy affect each other. If this is not possible, perhaps because individual devices do not support the MRP compatibility, you deactivate RSTP at the ports connected to the MRP-Ring.

**Note:** When you are configuring an MRP-Ring using the Command Line Interface, you define an additional parameter. When configured using CLI, an MRP-Ring is addressed via its MRP domain ID. The MRP domain ID is a sequence of 16 number blocks (8-bit values). Use the default domain of 255 255 255 255 255 255 255 255 255 255 255 255 255 255 255 for the MRP domain ID.

This default domain is also used internally for a configuration via the Web-based interface.

Configure all the devices within an MRP-Ring with the same MRP domain ID.

```

enable
configure
mrp new-domain
 default-domain

MRP domain created:
Domain ID:
255.255.255.255.255.255.255.255.255.255.255.255.255.255
(Default MRP domain)
mrp current-domain
 port primary 1/1
Primary Port set to 1/1
mrp current-domain
 port secondary 1/2
Secondary Port set to 1/2
mrp current-domain mode
manager
Mode of Switch set to manager
mrp current-domain recovery-
delay 200ms
Recovery delay set to 200ms
mrp current-domain advanced-
mode enable
Advanced Mode (react on link change) set to Enabled
mrp current-domain
 operation enable
Operation set to Enabled
exit
show mrp

Domain ID:
255.255.255.255.255.255.255.255.255.255.255.255.255
(Default MRP domain)

Configuration Settings:
Advanced Mode (react on link change)... Enabled
Manager Priority..... 32768
Mode of Switch (administrative setting). Manager
Mode of Switch (real operating state)... Manager
Domain Name..... <empty>
Recovery delay..... 200ms
Port Number, Primary..... 1/1, State: Not Connected
Port Number, Secondary..... 1/2, State: Not Connected
VLAN ID..... 0 (No VLAN)
Operation..... Enabled

```

Change to the privileged EXEC mode.

Change to the Configuration mode.

Creates a new MRP-Ring with the default domain ID  
255.255.255.255.255.255.255.255.255.255.255.255.255.255.

Define port 1 in module 1 as ring port 1 (primary).

Define port 2 in module 1 as ring port 2 (secondary)

Define this device as the ring manager.

Define 200ms as the value for the “Ring Recovery”.

Activate the “MRP Advanced Mode”.

Activate the MRP-Ring.

Go back one level.

Show the current parameters of the MRP-Ring (abbreviated display).

- Now you connect the line to the ring. To do this, you connect the 2 devices to the ends of the line using their ring ports.

## 3 Multiple Rings

The device allows you to set up multiple rings with different redundancy protocols:

- ▶ You have the option of coupling to MRP-Rings other ring structures that work with RSTP ([see on page 88 “Combining RSTP and MRP”](#)).



## 4 Ring/Network Coupling

Based on a ring, Ring/Network Coupling allows the redundant coupling of redundant rings or network segments. Ring/Network Coupling connects 2 rings/network segments via 2 separate paths.

The ring/network coupling supports the coupling of a ring (HIPER-Ring, Fast HIPER-Ring or MRP) to a second ring (also HIPER-Ring, Fast HIPER-Ring or MRP) or to a network segment of any structure, when all the devices in the coupled network are Hirschmann devices.

**Note:** Depending on the model, the devices have a DIP switch, with which you can select between the software configuration and the DIP switch configuration. Starting with software version 8.x, the device allows you to deactivate the DIP switch settings or overwrite them with the software settings. This allows you to freely specify the port settings.

The ring/network coupling supports the following devices:

- ▶ RS2-./.
- ▶ RS2-16M
- ▶ RS20, RS30, RS40
- ▶ OCTOPUS
- ▶ MICE (from rel. 3.0)
- ▶ PowerMICE
- ▶ MS20, MS30
- ▶ RSR20, RSR30
- ▶ MACH 100
- ▶ MACH 1000
- ▶ MACH 1040
- ▶ MACH 3000 (from Rel. 3.3),
- ▶ MACH 4000

## 4.1 Variants of the ring/network coupling

The redundant coupling is effected by the **one-Switch coupling** of two ports of **one** device in the first ring/network segment to one port each of two devices in the second ring/network segment (see figure 8). One of the two connections – the redundant one – is blocked for normal data traffic in normal operation.

If the main line no longer functions, the device opens the redundant line immediately. If the main line functions again, the redundant line is again blocked for normal data traffic and the main line is used again.

The ring coupling detects and handles an error within 500 ms (typically 150 ms).

The redundant coupling is effected by the **two-switch coupling** of one port each from **two** devices in the first ring/network segment to one port each of two devices in the second ring/network segment (see figure 14).

The device in the redundant line and the device in the main line use control packets to inform each other about their operating states, via the Ethernet or the control line.

If the main line no longer functions, the redundant device (slave) opens the redundant line immediately. As soon as the main line is working again, the device in the main line informs the redundant device of this. The redundant line is again blocked for normal data traffic and the main line is used again. The ring coupling detects and handles an error within 500 ms (typically 150 ms).

The type of coupling configuration is primarily determined by the topological conditions and the desired level of availability (see table 5).

|              | One-Switch coupling                                                                                                                                   | Two-Switch coupling                                                                                                       | Two-Switch coupling with control line                                                                                                                                                                                                         |
|--------------|-------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Application  | The 2 devices are in impractical topological positions. Therefore, putting a line between them would involve a lot of effort for two-Switch coupling. | The 2 devices are in practical topological positions. Installing a control line would involve a lot of effort.            | The 2 devices are in practical topological positions. Installing a control line would not involve much effort.                                                                                                                                |
| Disadvantage | If the Switch configured for the redundant coupling becomes inoperable, no connection remains between the networks.                                   | More effort for connecting the 2 devices to the network (compared with one-Switch coupling).                              | More effort for connecting the two devices to the network (compared with one-Switch and two-Switch coupling).                                                                                                                                 |
| Advantage    | Less effort involved in connecting the 2 devices to the network (compared with two-Switch coupling).                                                  | If one of the devices configured for the redundant coupling becomes inoperable, the coupled networks are still connected. | If one of the devices configured for the redundant coupling becomes inoperable, the coupled networks are still connected. The partner determination between the coupling devices occurs more secure and faster than without the control line. |

*Table 5: Selection criteria for the configuration types for redundant coupling*

**Note:** Choose a configuration based on topological conditions and the level of availability you require (see [table 5](#)).

## 4.2 Preparing a Ring/Network Coupling

### 4.2.1 STAND-BY switch

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

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

| Device type         | STAND-BY switch type                        |
|---------------------|---------------------------------------------|
| RS2-./.             | DIP switch                                  |
| RS2-16M             | DIP switch                                  |
| RS20/RS30/RS40      | Selectable: DIP switch and software setting |
| MICE/Power MICE     | Selectable: DIP switch and software setting |
| MS20/MS30           | Selectable: DIP switch and software setting |
| OCTOPUS             | Software switch                             |
| RSR20/RSR30         | Software switch                             |
| MACH 100            | Software switch                             |
| MACH 1000           | Software switch                             |
| MACH 3000/MACH 4000 | Software switch                             |

Table 6: Overview of the STAND-BY switch types

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

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

*Table 7: Setting the STAND-BY switch*

**Note:** In the following screenshots and diagrams, the following conventions are used:

- ▶ Blue indicates devices or connections of the items currently being described
- ▶ Black indicates devices or connections that connect to the items currently being described
- ▶ Thick lines indicate connections of the items currently being described
- ▶ This lines indicate connections which connect to the items currently being described
- ▶ Lines of dashes indicate a redundant connection
- ▶ Dotted lines indicate the control line.

- 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 figure 7).

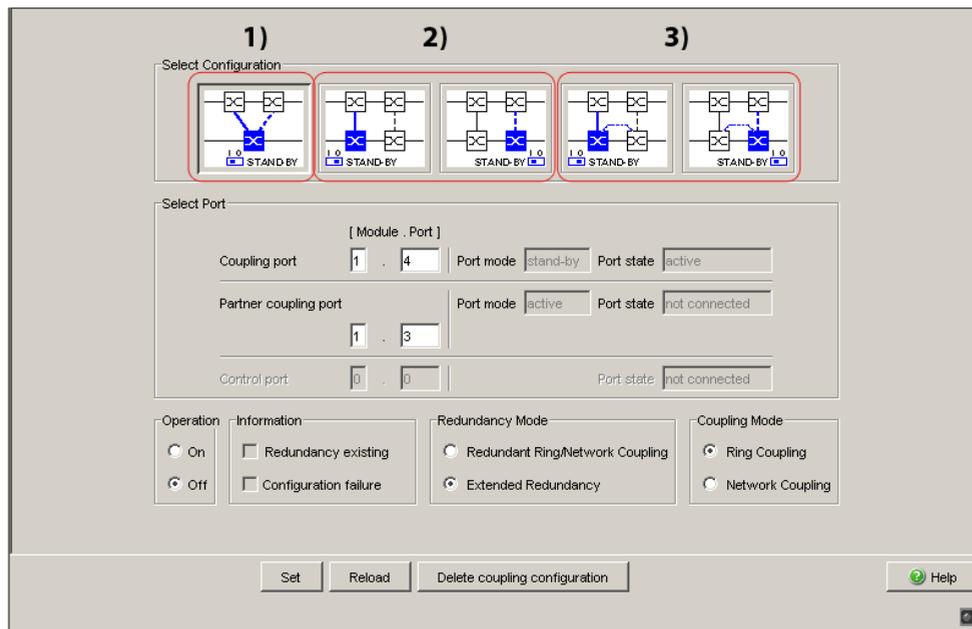


Figure 7: Choosing the ring coupling configuration (when the DIP switch is off, or for devices without a DIP switch)

For devices without DIP switches, the software settings are not restricted.

For devices **with** DIP switches, depending on the DIP switch position, the dialog displays the possible configurations in color, while those configurations that are not possible appear in gray.

The possible configurations are:

- ▶ DIP switch RM: ON or OFF, STAND-BY: OFF:  
Two-Switch coupling as master (with or without control line)
- ▶ DIP switch RM: OFF, STAND-BY: ON:  
One-Switch coupling and two-Switch coupling as slave (with or without control line)
- ▶ DIP switch RM: ON, STAND-BY: ON:  
DIP switches are deactivated, and the software settings are possible without any restrictions

If the DIP switches are activated and you want to use the software to select one of the configurations that are not possible (grayed-out), you put the DIP switches on the device into another position and reload the dialog.

**Note:** Refrain from combining Rapid Spanning Tree and Ring/Network Coupling. Competing redundancy functions are ineligible.

### 4.2.2 One-Switch coupling

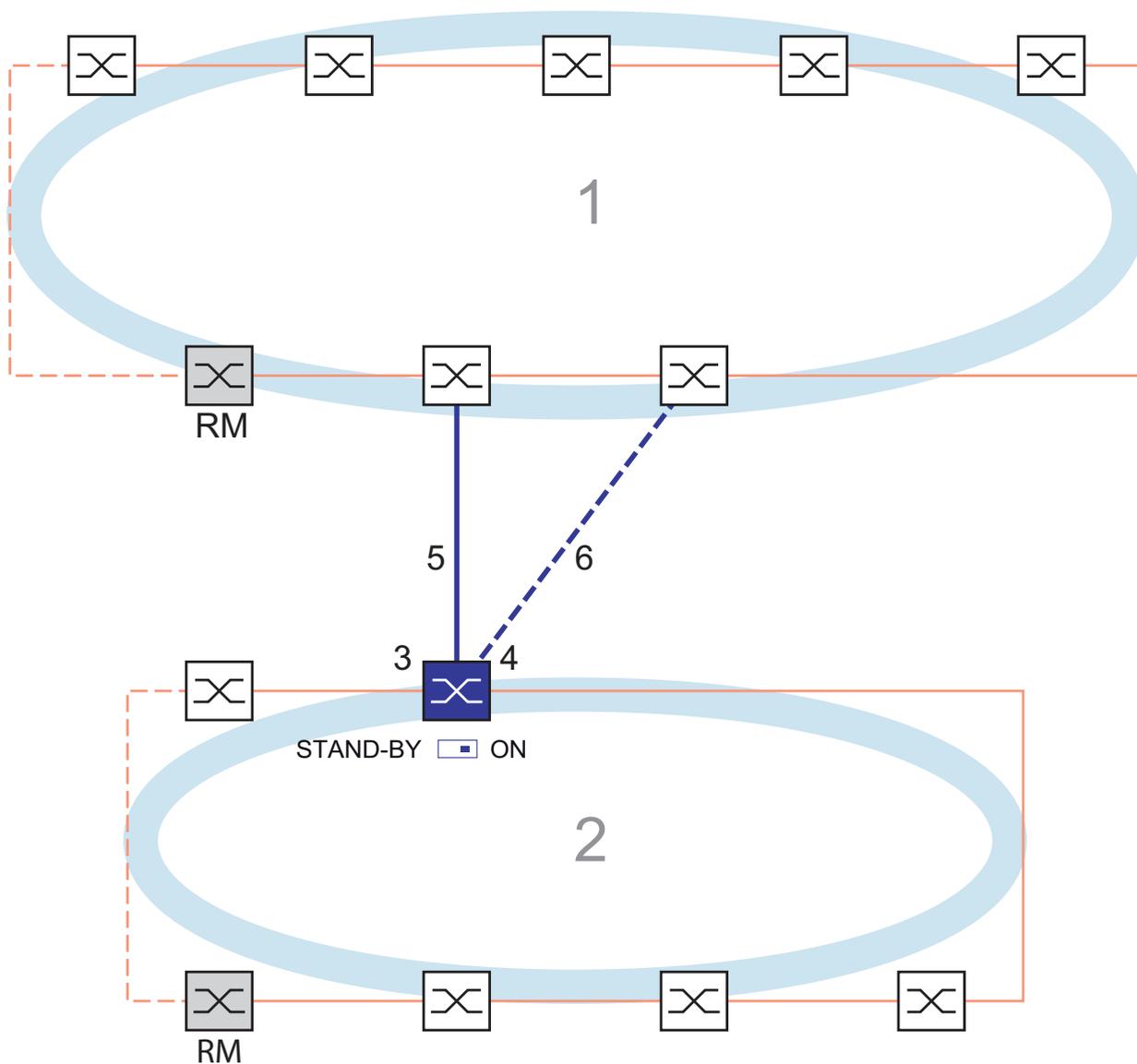
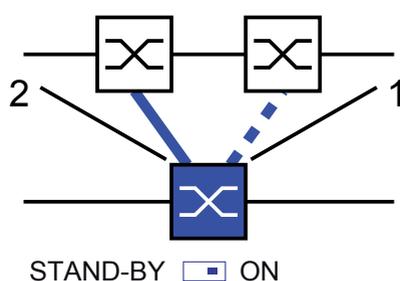


Figure 8: Example of one-Switch coupling

- 1: Backbone
- 2: Ring
- 3: Partner coupling port
- 4: Coupling port
- 5: Main Line
- 6: Redundant Line

The coupling between two networks is performed by the main line (solid blue line) in the normal mode of operation, which is connected to the partner coupling port. If the main line becomes inoperable, the redundant line (dashed blue line), which is connected to the coupling port, takes over the ring/network coupling. The coupling switch-over is performed by **one** Switch.

- Select the `Redundancy:Ring/Network Coupling` dialog.
- Select "One-Switch coupling" by means of the dialog button with the same graphic as below (see figure 9).



*Figure 9: One-Switch-coupling*  
 1: Coupling port  
 2: Partner coupling port

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

- Select the partner coupling port (see figure 10).  
 .With "Partner coupling port" you specify at which port you are connecting the control line.  
 You will find the port assignment for the redundant coupling in table 8.

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

| Device  | Partner coupling port               | Coupling port                       |
|---------|-------------------------------------|-------------------------------------|
| RS2-./. | Not possible                        | Not possible                        |
| RS2-16M | All ports (default setting: port 2) | All ports (default setting: port 1) |

*Table 8: Port assignment for one-Switch coupling*

| Device           | Partner coupling port                 | Coupling port                         |
|------------------|---------------------------------------|---------------------------------------|
| RS20, RS30, RS40 | All ports (default setting: port 1.3) | All ports (default setting: port 1.4) |
| OCTOPUS          | All ports (default setting: port 1.3) | All ports (default setting: port 1.4) |
| MICE             | All ports (default setting: port 1.3) | All ports (default setting: port 1.4) |
| PowerMICE        | All ports (default setting: port 1.3) | All ports (default setting: port 1.4) |
| MS20             | All ports (default setting: port 1.3) | All ports (default setting: port 1.4) |
| MS30             | All ports (default setting: port 2.3) | All ports (default setting: port 2.4) |
| RSR20/30         | All ports (default setting: port 1.3) | All ports (default setting: port 1.4) |
| MACH 100         | All ports (default setting: port 2.3) | All ports (default setting: port 2.4) |
| MACH 1000        | All ports (default setting: port 1.3) | All ports (default setting: port 1.4) |
| MACH 3000        | All ports                             | All ports                             |
| MACH 4000        | All ports (default setting: port 1.3) | All ports (default setting: port 1.4) |

*Table 8: Port assignment for one-Switch coupling*

**Note:** Configure the partner coupling port and the ring redundancy ports on different ports.

- Select the coupling port (see figure 10).

With “Coupling port” you specify at which port you are connecting the network segments:

You will find the port assignment for the redundant coupling in table 8.

**Note:** Configure the coupling port and the redundancy ring ports on different ports.

- Activate the function in the “Operation” frame (see figure 10)
- Now connect the redundant line.

The displays in the “Select port” frame mean:

- “Port mode”: The port is either active or in stand-by mode.
- “Port state”: The port is either active, in stand-by mode or not connected.

The displays in the “Information” frame mean:

- “Redundancy guaranteed”: The redundancy function is active.
  - The Link LED on the partner coupling port to which the main line is connected lights up permanently.
  - The Link LED on the coupling port to which the redundant line is connected blinks evenly.

If the main line no longer functions, the redundant line takes over the function of the main line.

- “Configuration failure”: The function is incomplete or incorrectly configured.

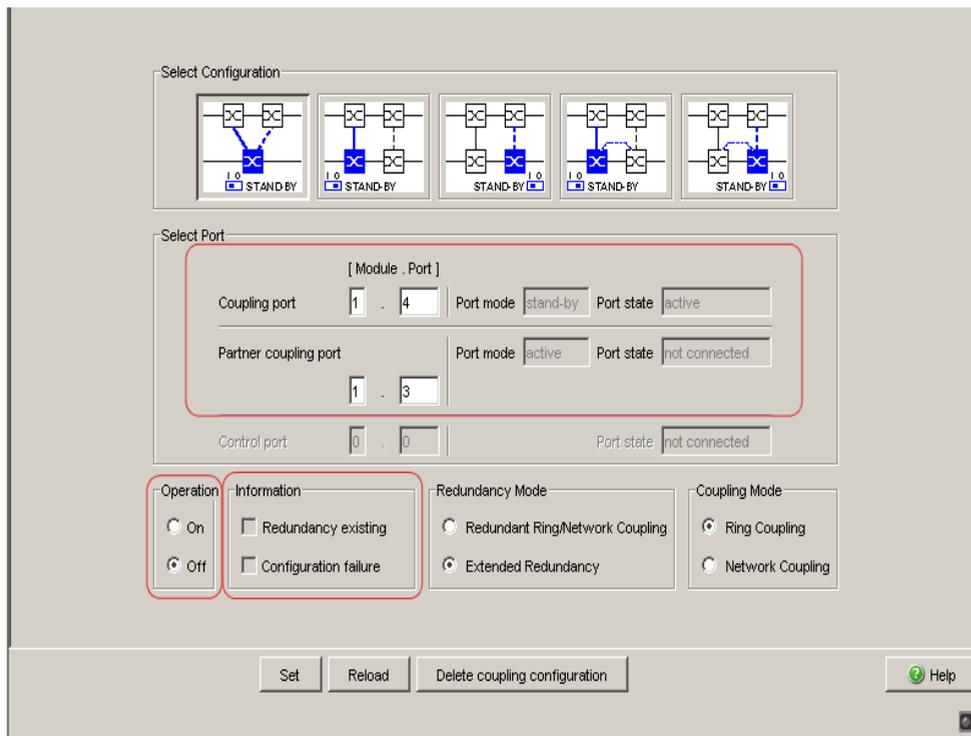


Figure 10: One-Switch coupling: Selecting the port and enabling/disabling operation

**Note:** The following settings are required for the coupling ports (you select the Basic Settings:Port Configuration dialog):  
[See table 3 on page 19.](#)

**Note:** If VLANs are configured, set the coupling and partner coupling ports' VLAN configuration as follows:

- in the Switching:VLAN:Port dialog, Port VLAN ID 1 and “Ingress Filtering” deactivated
- in the Switching:VLAN:Statisch dialog, for all redundant connections VLAN 1 and VLAN Membership T (Tagged)  
 The device sends the redundancy packets with the highest priority in VLAN 1.

## Redundancy mode

- In the “Redundancy Mode” frame, select (see figure 11)
  - “Redundant Ring/Network Coupling” or
  - “Extended Redundancy”.

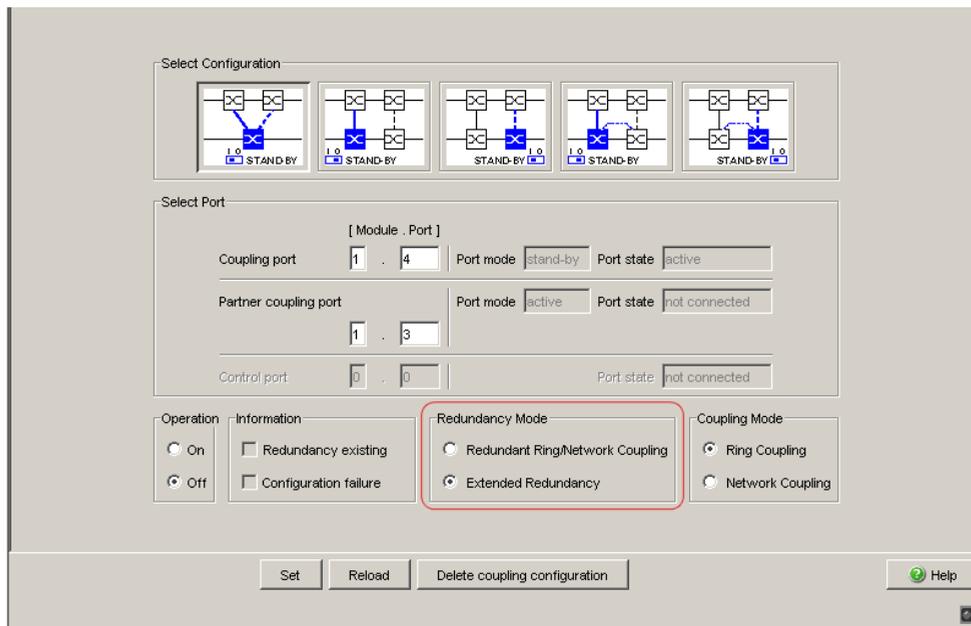


Figure 11: One-Switch coupling: Selecting the redundancy mode

With the “Redundant Ring/Network Coupling” setting, either the main line or the redundant line is active. The lines are never both active at the same time.

With the “Extended Redundancy” setting, the main line and the redundant line are simultaneously active if the connection line between the devices in the connected (i.e., remote) network becomes inoperable (see figure 12). During the reconfiguration period, packet duplications may occur. Therefore, select this setting only if your application detects package duplications.

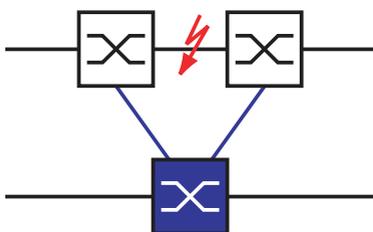


Figure 12: Extended redundancy

## Coupling mode

The coupling mode indicates the type of the connected network.

- In the “Coupling Mode” frame, select (see figure 13)
  - “Ring Coupling” or
  - “Network Coupling”

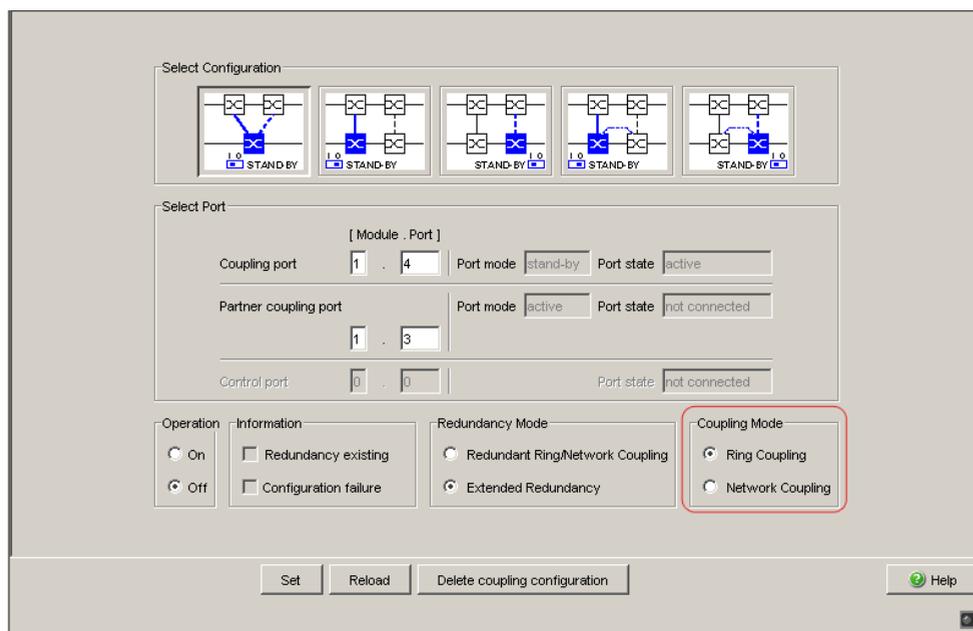


Figure 13: One-Switch coupling: Selecting the coupling mode

- Select **"Ring coupling"** if you are connecting to a redundancy ring.
- Select **"Network Coupling"** if you are connecting to a line or tree 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.

### 4.2.3 Two-Switch coupling

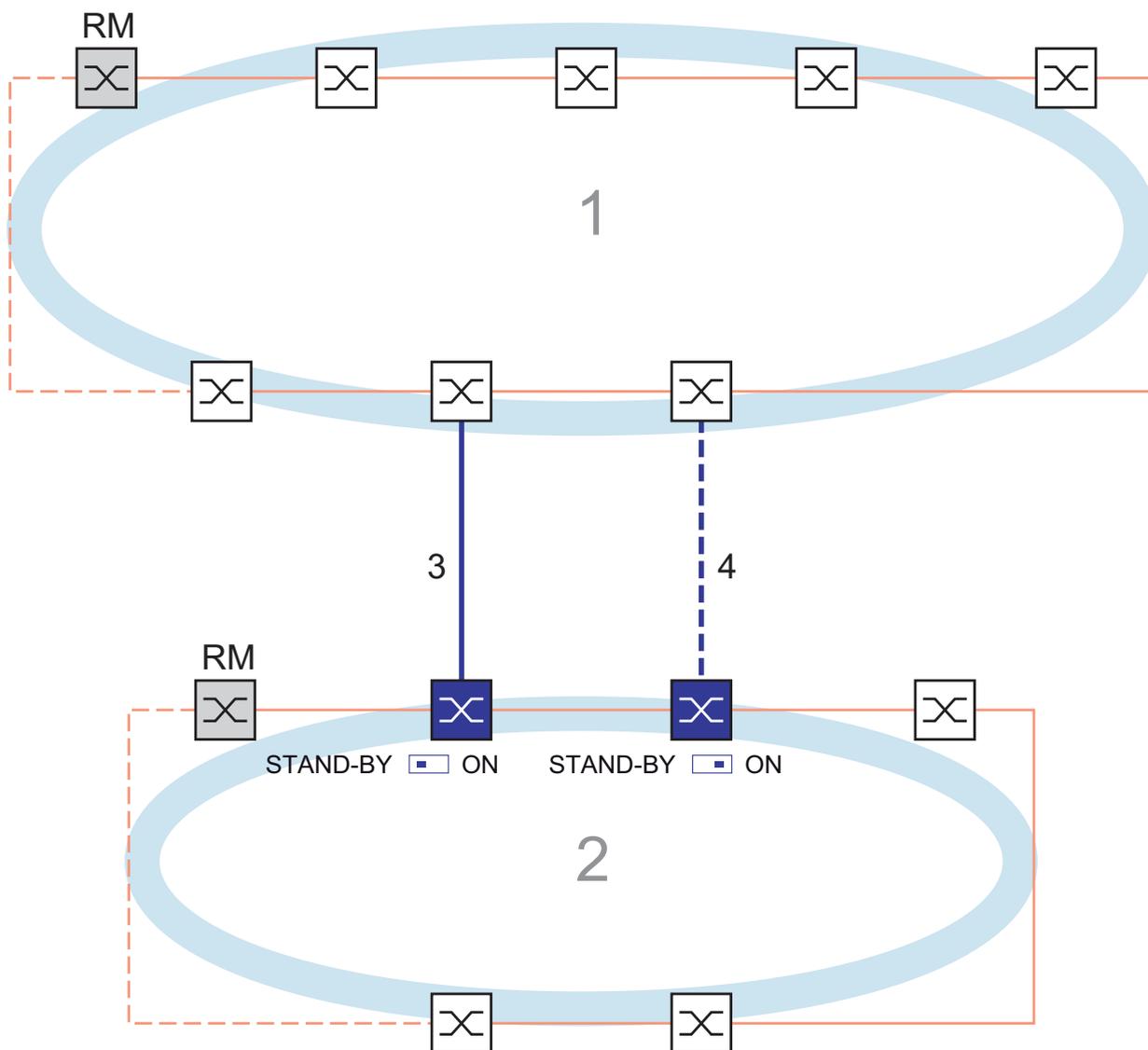


Figure 14: Example of two-Switch coupling

- 1: Backbone
- 2: Ring
- 3: Main line
- 4: Redundant line

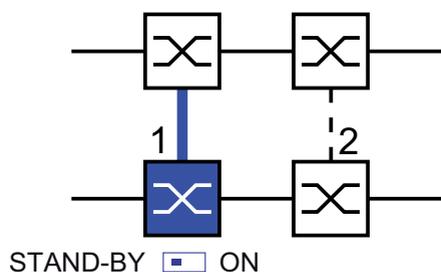
The coupling between 2 networks is performed by the main line (solid blue line). If the main line or one of the adjacent Switches becomes inoperable, the redundant line (dashed black line) takes over coupling the 2 networks. The coupling is performed by two Switches.

The switches send their control packages over the Ethernet.

The Switch connected to the main line, and the Switch connected to the redundant line are partners with regard to the coupling.

- Connect the two partners via their ring ports.

- Select the `Redundancy:Ring/Network Coupling` dialog.
- Select "Two-Switch coupling" by means of the dialog button with the same graphic as below (see figure 15).



*Figure 15: Two-Switch coupling*  
 1: Coupling port  
 2: Partner coupling port

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

- Select the coupling port (see figure 16).  
 With "Coupling port" you specify at which port you are connecting the network segments:  
 You will find the port assignment for the redundant coupling in table 9.
- For a device with DIP switches, you switch the STAND-BY switch to OFF or deactivate the DIP switches. Connect the main line to the coupling port.

| Device           | Coupling port                                        |
|------------------|------------------------------------------------------|
| RS2-./.          | Not possible                                         |
| RS2-16M          | Adjustable for all ports (default setting: port 1)   |
| RS20, RS30, RS40 | Adjustable for all ports (default setting: port 1.4) |
| OCTOPUS          | 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) |
| MS20             | Adjustable for all ports (default setting: port 1.4) |
| MS30             | Adjustable for all ports (default setting: port 2.4) |
| RSR20/30         | Adjustable for all ports (default setting: port 1.4) |
| MACH 100         | Adjustable for all ports (default setting: port 2.4) |
| 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 9: Port assignment for the redundant coupling (two-Switch coupling)*

**Note:** Configure the coupling port and the redundancy ring ports on different ports.

- Activate the function in the “Operation” frame ([see figure 16](#))
- Now connect the redundant line.

The displays in the “Select port” frame mean:

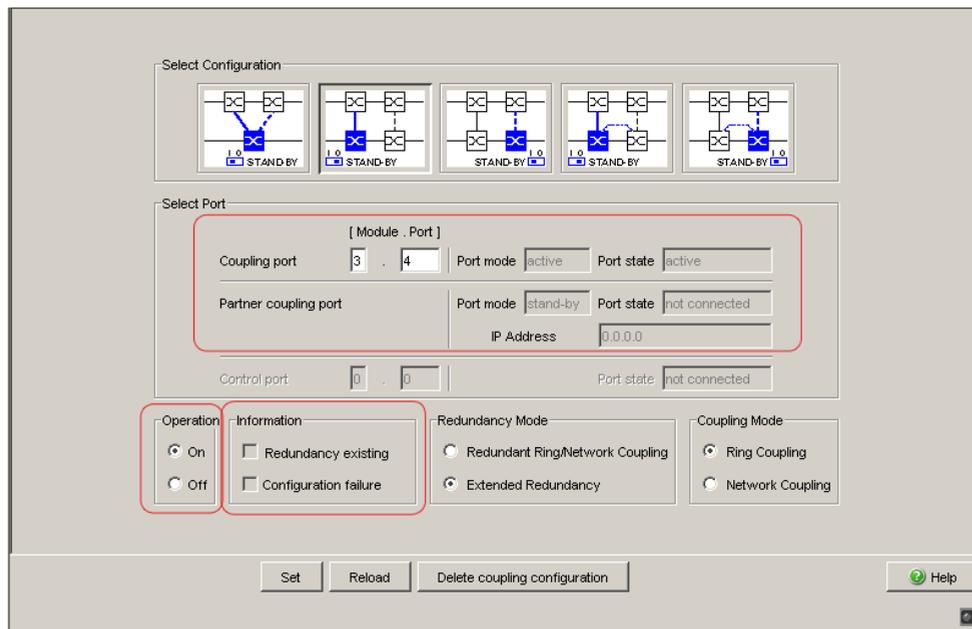
- “Port mode”: The port is either active or in stand-by mode.
- “Port state”: The port is either active, in stand-by mode or not connected.
- “IP Address”: The IP address of the partner, if the partner is already operating in the network.

The displays in the “Information” frame mean:

- “Redundancy guaranteed”: The redundancy function is active.
  - The Link LED on the partner coupling port to which the main line is connected lights up permanently.
  - The Link LED on the coupling port to which the redundant line is connected blinks evenly.

If the main line no longer functions, the redundant line takes over the function of the main line.

- “Configuration failure”: The function is incomplete or incorrectly configured.



*Figure 16: Two-Switch coupling: 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 the operation setting 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):

See [table 3 on page 19](#).

**Note:** If VLANs are configured, set the coupling and partner coupling ports' VLAN configuration as follows:

- in the `Switching:VLAN:Port` dialog, Port VLAN ID 1 and “Ingress Filtering” deactivated
- in the `Switching:VLAN:Statisch` dialog, for all redundant connections VLAN 1 and VLAN Membership T (Tagged)  
The device sends the redundancy packets with the highest priority in VLAN 1.

**Note:** If you operate the Ring Manager and Two-Switch coupling functions at the same device, there is the possibility of creating a loop.

- Select "Two-Switch coupling" by means of the dialog button with the same graphic as below (see figure 17).

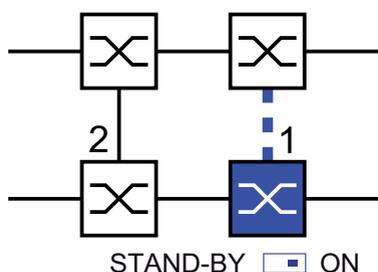


Figure 17: Two-Switch coupling

1: Coupling port

2: Partner coupling port

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

- Select the coupling port (see figure 16).  
With "Coupling port" you specify at which port you are connecting the network segments:  
You will find the port assignment for the redundant coupling in table 9.
- For a device with DIP switches, you switch the STAND-BY switch to ON or deactivate the DIP switches. You connect the redundant line to the coupling port.

**Note:** Configure the coupling port and the redundancy ring ports on different ports.

- Activate the function in the "Operation" frame (see figure 16)

The displays in the "Select port" frame mean:

- "Port mode": The port is either active or in stand-by mode.
- "Port state": The port is either active, in stand-by mode 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:

- “Redundancy guaranteed”: The redundancy function is active.
  - The Link LED on the partner coupling port to which the main line is connected lights up permanently.
  - The Link LED on the coupling port to which the redundant line is connected blinks evenly.

If the main line no longer functions, the redundant line takes over the function of the main 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):

[See table 3 on page 19.](#)

**Note:** If VLANs are configured, set the coupling and partner coupling ports’ VLAN configuration as follows:

- in the `Switching:VLAN:Port` dialog, Port VLAN ID 1 and “Ingress Filtering” deactivated
- in the `Switching:VLAN:Statisch` dialog, for all redundant connections VLAN 1 and VLAN Membership  $\mathbb{T}$  (Tagged)  
The device sends the redundancy packets with the highest priority in VLAN 1.

**Note:** If you operate the Ring Manager and Two-Switch coupling functions at the same device, there is the possibility of creating a loop.

Redundancy mode

- In the “Redundancy Mode” frame, select ([see figure 18](#))
  - “Redundant Ring/Network Coupling” or
  - “Extended Redundancy”.

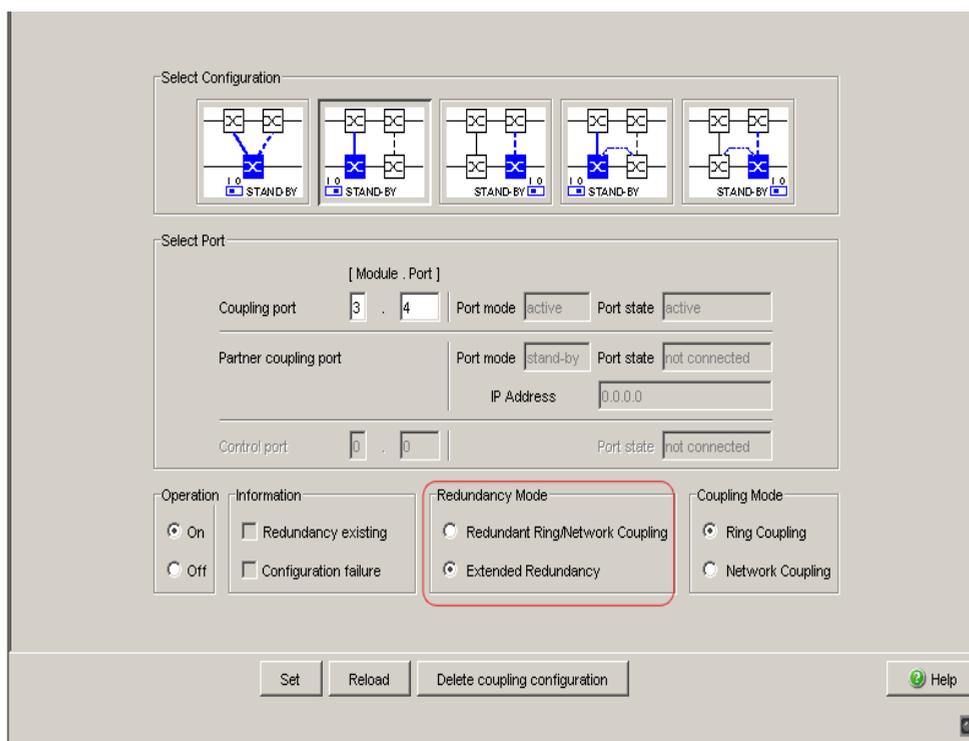


Figure 18: Two-Switch coupling: Selecting the redundancy mode

With the “Redundant Ring/Network Coupling” setting, either the main line or the redundant line is active. The lines are never both active at the same time.

With the “Extended Redundancy” setting, the main line and the redundant line are simultaneously active if the connection line between the devices in the connected (i.e. remote) network fails (see figure 12). During the reconfiguration period, package duplications may occur. Therefore, only select this setting if your application detects package duplications.

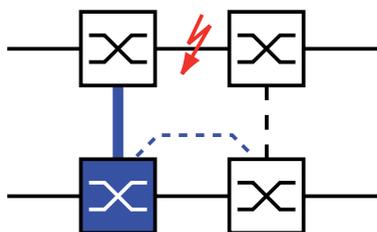


Figure 19: Extended redundancy

### Coupling mode

The coupling mode indicates the type of the connected network.

- In the “Coupling Mode” frame, select (see figure 20)
  - “Ring Coupling” or
  - “Network Coupling”

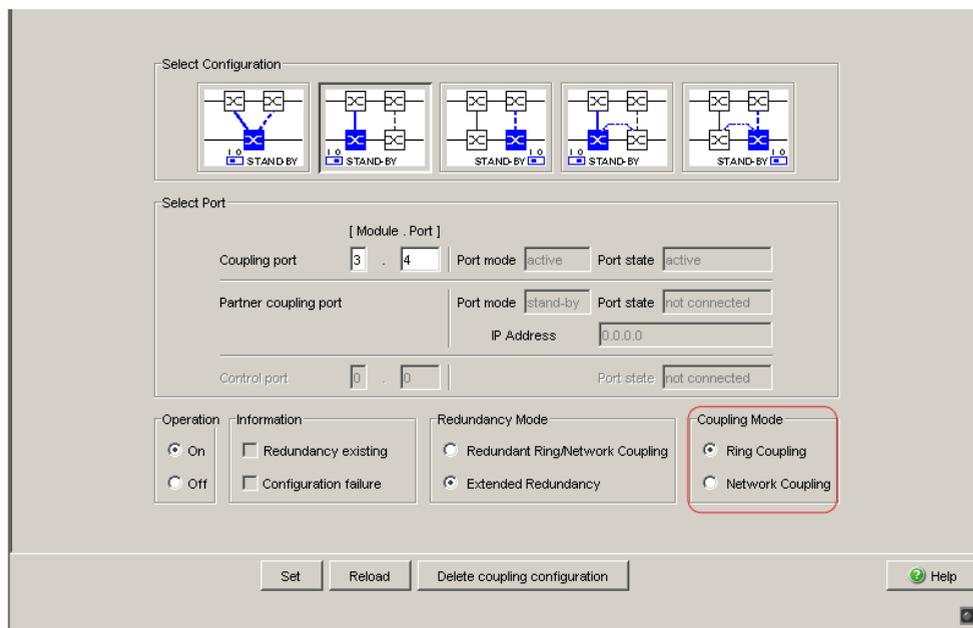


Figure 20: Two-Switch coupling: Selecting the coupling mode

- Select **"Ring coupling"** if you are connecting to a redundancy ring.
- Select **"Network Coupling"** if you are connecting to a line or tree 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.

### 4.2.4 Two-Switch Coupling with Control Line

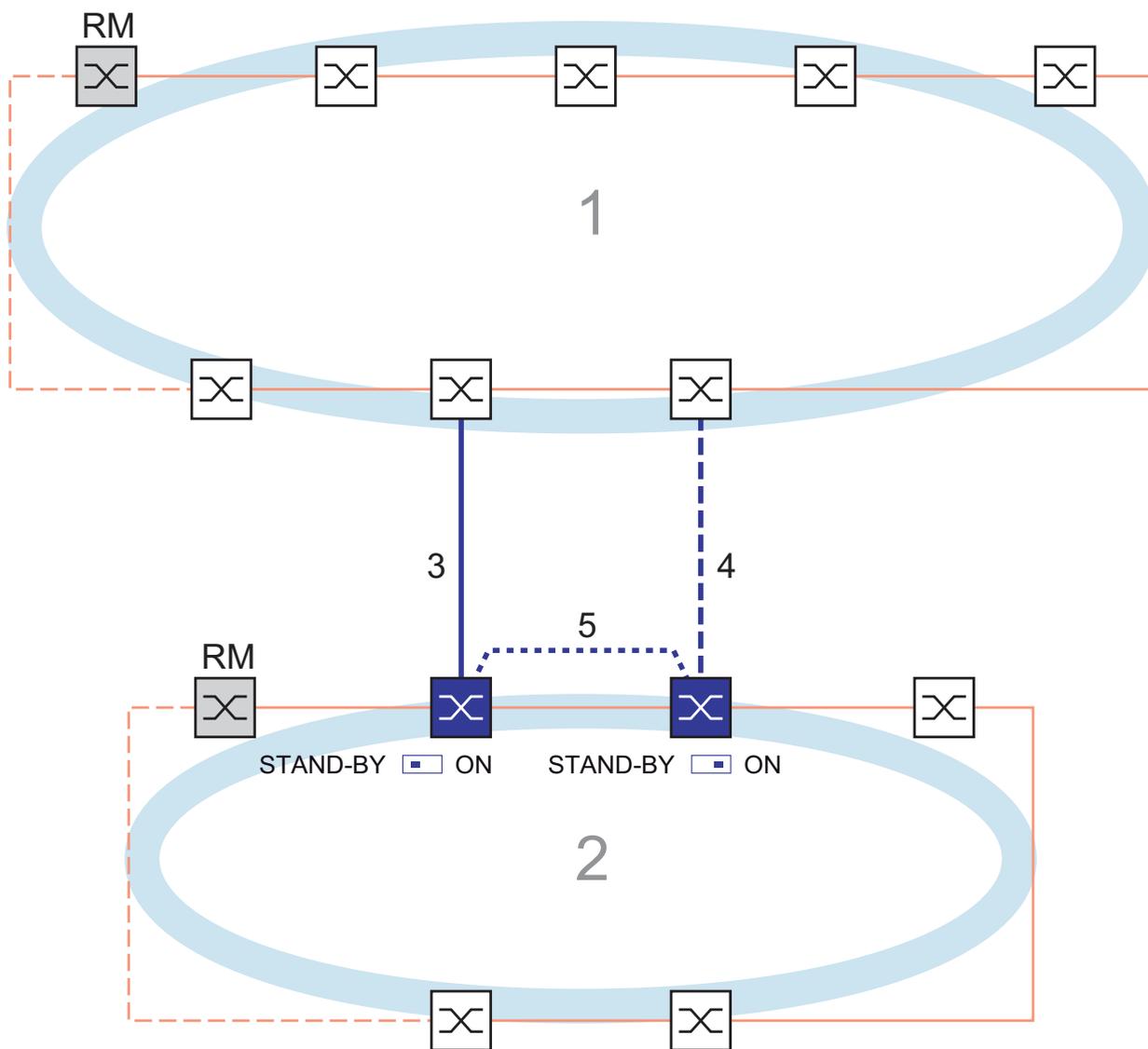


Figure 21: Example of Two-Switch coupling with control line

- 1: Backbone
- 2: Ring
- 3: Main line
- 4: Redundant line
- 5: Control line

The coupling between 2 networks is performed by the main line (solid blue line). If the main line or one of the adjacent Switches becomes inoperable, the redundant line (dashed black line) takes over coupling the 2 networks. The coupling is performed by two Switches.

The Switches send their control packets over a control line (dotted line). The Switch connected to the main line, and the Switch connected to the redundant line are partners with regard to the coupling.

- Connect the two partners via their ring ports.

- Select the `Redundancy:Ring/Network Coupling` dialog.
- Select „Two-Switch coupling with control line“ by means of the dialog button with the same graphic as below (see figure 22).

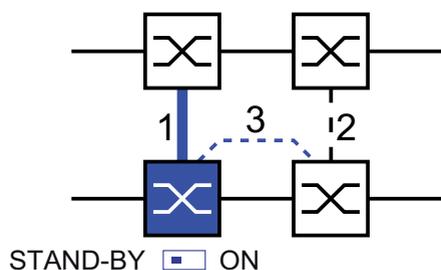


Figure 22: Two-Switch coupling with control line

- 1: Coupling port
- 2: Partner coupling port
- 3: Control line

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

- Select the coupling port (see figure 23).  
With “Coupling port” you specify at which port you are connecting the network segments:  
You will find the port assignment for the redundant coupling in table 10.
- For a device with DIP switches, you switch the STAND-BY switch to OFF or deactivate the DIP switches. Connect the main line to the coupling port.

- Select the control port (see figure 23)

With “Control port” you specify at which port you are connecting the control line.

You will find the port assignment for the redundant coupling in table 10.

| Device              | Coupling port                                           | Control port                                            |
|---------------------|---------------------------------------------------------|---------------------------------------------------------|
| RS2-./.             | Port 1                                                  | Stand-by port (can only be combined with RS2-../.. )    |
| RS2-16M             | Adjustable for all ports<br>(default setting: port 1)   | Adjustable for all ports<br>(default setting: port 2)   |
| RS20, RS30,<br>RS40 | Adjustable for all ports<br>(default setting: port 1.4) | Adjustable for all ports<br>(default setting: port 1.3) |
| OCTOPUS             | Adjustable for all ports<br>(default setting: port 1.4) | Adjustable for all ports<br>(default setting: port 1.3) |
| MICE                | Adjustable for all ports<br>(default setting: port 1.4) | Adjustable for all ports<br>(default setting: port 1.3) |
| PowerMICE           | Adjustable for all ports<br>(default setting: port 1.4) | Adjustable for all ports<br>(default setting: port 1.3) |
| MS20                | Adjustable for all ports<br>(default setting: port 1.4) | Adjustable for all ports<br>(default setting: port 1.3) |
| MS30                | Adjustable for all ports<br>(default setting: port 2.4) | Adjustable for all ports<br>(default setting: port 2.3) |
| RSR20/RSR30         | Adjustable for all ports<br>(default setting: port 1.4) | Adjustable for all ports<br>(default setting: port 1.3) |
| MACH 100            | Adjustable for all ports<br>(default setting: port 2.4) | Adjustable for all ports<br>(default setting: port 2.3) |
| MACH 1000           | Adjustable for all ports<br>(default setting: port 1.4) | Adjustable for all ports<br>(default setting: port 1.3) |
| MACH 3000           | Adjustable for all ports                                | Adjustable for all ports                                |
| MACH 4000           | Adjustable for all ports<br>(default setting: port 1.4) | Adjustable for all ports<br>(default setting: port 1.3) |

*Table 10: Port assignment for the redundant coupling (two-Switch coupling with control line)*

**Note:** Configure the coupling port and the redundancy ring ports on different ports.

- Activate the function in the “Operation” frame (see figure 23)
- Now connect the redundant line and the control line.

The displays in the “Select port” frame mean:

- “Port mode”: The port is either active or in stand-by mode.
- “Port state”: The port is either active, in stand-by mode 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:

- “Redundancy guaranteed”: The redundancy function is active.
  - The Link LED on the partner coupling port to which the main line is connected lights up permanently.
  - The Link LED on the coupling port to which the redundant line is connected blinks evenly.

If the main line no longer functions, the redundant line takes over the function of the main line.

- “Configuration failure”: The function is incomplete or incorrectly configured.

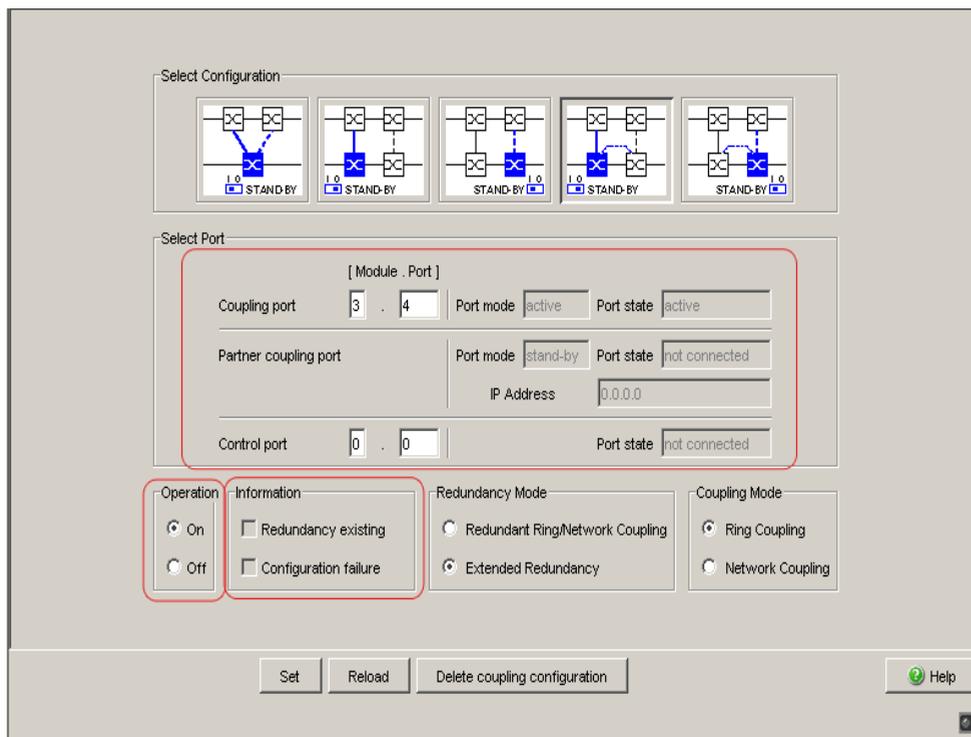


Figure 23: Two-Switch coupling with control line: Selecting the port and enabling/disabling operation

To avoid continuous loops, the Switch sets the port state of the coupling port to “off” if you:

- switch off the operation setting or
- change the configuration

while the connections are in operation at these ports.

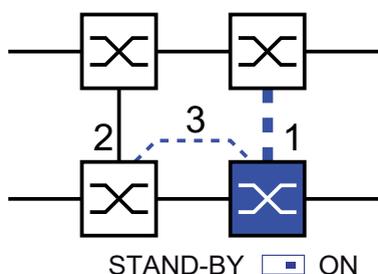
**Note:** The following settings are required for the coupling ports (you select the `Basic Settings:Port Configuration` dialog):

See [table 3 on page 19](#).

**Note:** If VLANs are configured, set the coupling and partner coupling ports' VLAN configuration as follows:

- in the `Switching:VLAN:Port` dialog, Port VLAN ID 1 and “Ingress Filtering” deactivated
- in the `Switching:VLAN:Statisch` dialog, for all redundant connections VLAN 1 and VLAN Membership  $\mathbb{T}$  (Tagged)  
The device sends the redundancy packets with the highest priority in VLAN 1.

- Select “Two-Switch coupling with control line” by means of the dialog button with the same graphic as below ([see figure 24](#)).



*Figure 24: Two-Switch coupling with control line*

- 1: Coupling port
- 2: Partner coupling port
- 3: Control line

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

- Select the coupling port ([see figure 23](#)).  
With “Coupling port” you specify at which port you are connecting the network segments:  
You will find the port assignment for the redundant coupling in [table 10](#).
- For a device with DIP switches, you switch the STAND-BY switch to ON or deactivate the DIP switches. You connect the redundant line to the coupling port.

- Select the control port (see figure 23)  
With “Control port” you specify at which port you are connecting the control line.

**Note:** Configure the coupling port and the redundancy ring ports on different ports.

- Activate the function in the “Operation” frame (see figure 23)
  - Now connect the redundant line and the control line.
- The displays in the “Select port” frame mean:
- “Port mode”: The port is either active or in stand-by mode.
  - “Port state”: The port is either active, in stand-by mode 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:

- “Redundancy guaranteed”: The redundancy function is active.
  - The Link LED on the partner coupling port to which the main line is connected lights up permanently.
  - The Link LED on the coupling port to which the redundant line is connected blinks evenly.

If the main line no longer functions, the redundant line takes over the function of the main 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 the operation setting or
- change the configuration

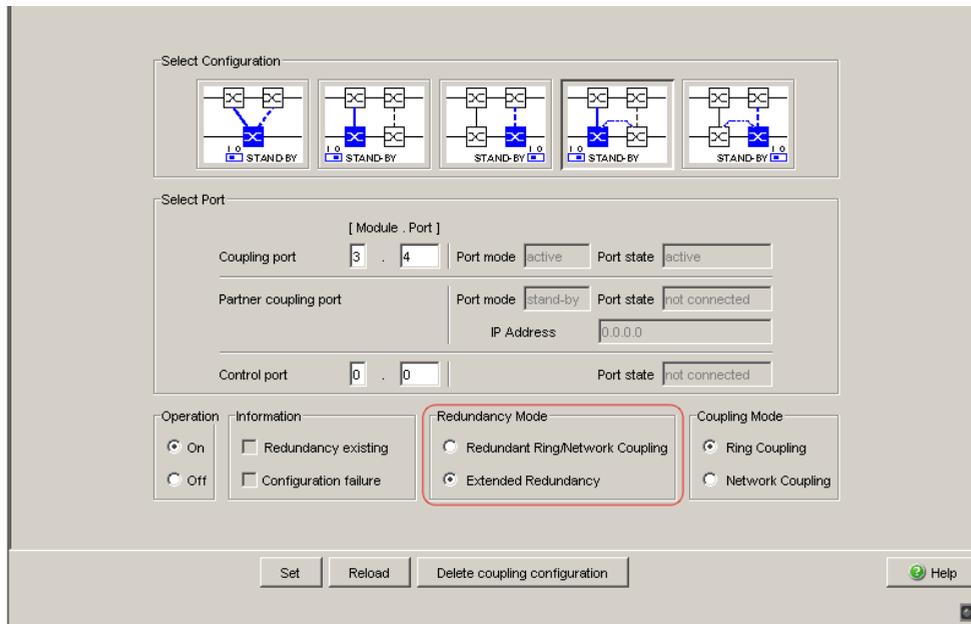
while the connections are in operation at these ports.

**Note:** If VLANs are configured, set the coupling and partner coupling ports’ VLAN configuration as follows:

- in the `Switching:VLAN:Port` dialog, Port VLAN ID 1 and “Ingress Filtering” deactivated
- in the `Switching:VLAN:Statisch` dialog, for all redundant connections VLAN 1 and VLAN Membership  $\mathbb{T}$  (Tagged)  
The device sends the redundancy packets with the highest priority in VLAN 1.

### Redundancy mode

- In the “Redundancy Mode” frame, select:
  - “Redundant Ring/Network Coupling”
  - or
  - “Extended Redundancy”.



*Figure 25: Two-Switch coupling with control line: Selecting the redundancy mode*

With the “Redundant Ring/Network Coupling” setting, either the main line or the redundant line is active. The lines are never both active at the same time.

With the “Extended Redundancy” setting, the main line and the redundant line are simultaneously active if the connection line between the devices in the connected (i.e. remote) network fails (see figure 12). During the reconfiguration period, package duplications may occur. Therefore, only select this setting if your application detects package duplications.

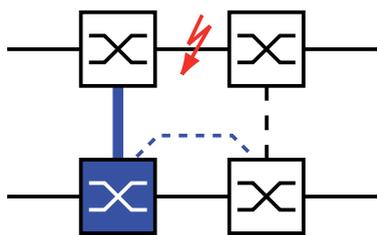


Figure 26: Extended redundancy

### Coupling mode

The coupling mode indicates the type of the connected network.

- In the “Coupling Mode” frame, select:
  - “Ring coupling”
  - or
  - “Network Coupling”

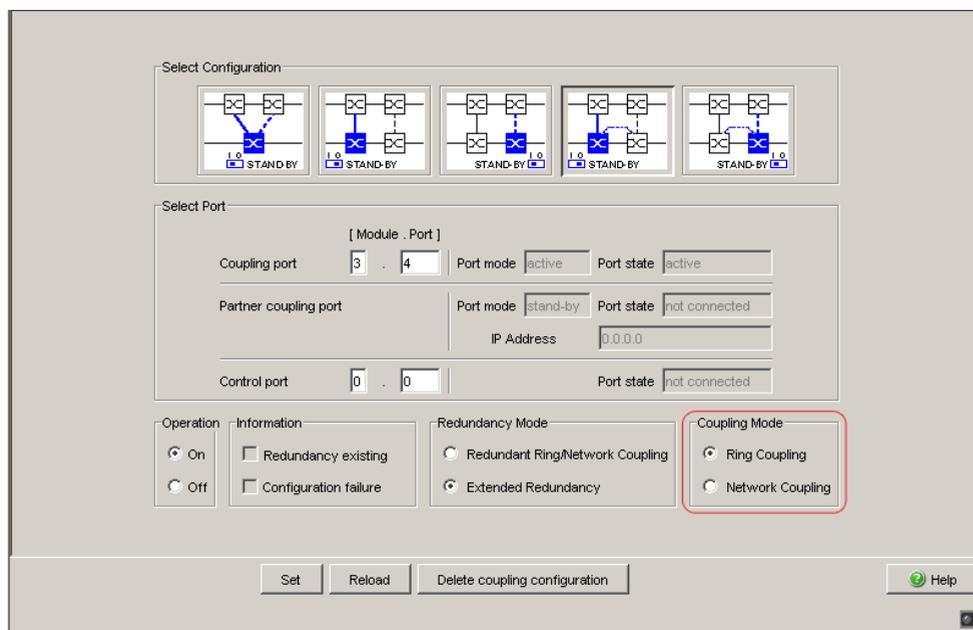


Figure 27: Two-Switch coupling with control line: Selecting the coupling mode

- Select **"Ring coupling"** if you are connecting to a redundancy ring.
- Select **"Network Coupling"** if you are connecting to a line or tree 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.

## 5 Spanning Tree

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

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

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

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

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

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

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

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

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

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

## 5.1 The Spanning Tree Protocol

Because RSTP is a further development of the STP, all the following descriptions of the STP also apply to the RSTP.

### 5.1.1 The tasks of the STP

The Spanning Tree Algorithm reduces network topologies built with bridges and containing ring structures due to redundant links to a tree structure. In doing so, STP opens ring structures according to preset rules by deactivating redundant paths. If a path is interrupted because a network component becomes inoperable, STP reactivates the previously deactivated path again. This allows redundant links to increase the availability of communication. STP determines a bridge that represents the STP tree structure's base. This bridge is called root bridge.

Features of the STP algorithm:

- ▶ automatic reconfiguration of the tree structure in the case of a bridge becoming inoperable or the interruption of a data path
- ▶ the tree structure is stabilized up to the maximum network size (up to 39 hops, depending on the setting for `Max Age`, [\(see table 13\)](#))
- ▶ stabilization of the topology within a short time period
- ▶ topology can be specified and reproduced by the administrator
- ▶ transparency for the end devices
- ▶ low network load relative to the available transmission capacity due to the tree structure created

## 5.1.2 Bridge parameters

In the context of Spanning Tree, each bridge and its connections are uniquely described by the following parameters:

- ▶ Bridge Identifier
- ▶ Root Path Cost for the bridge ports,
- ▶ Port Identifier

## 5.1.3 Bridge Identifier

The Bridge Identifier consists of 8 bytes. The 2 highest-value bytes are the priority. The default setting for the priority number is 32,768, but the Management Administrator can change this when configuring the network. The 6 lowest-value bytes of the bridge identifier are the bridge's MAC address. The MAC address allows each bridge to have unique bridge identifiers.

The bridge with the smallest number for the bridge identifier has the highest priority.



Figure 28: Bridge Identifier, Example (values in hexadecimal notation)

### 5.1.4 Root Path Cost

Each path that connects 2 bridges is assigned a cost for the transmission (path cost). The Switch determines this value based on the transmission speed (see table 11). It assigns a higher path cost to paths with lower transmission speeds.

Alternatively, the Administrator can set the path cost. Like the Switch, the Administrator assigns a higher path cost to paths with lower transmission speeds. However, since the Administrator can choose this value freely, he has a tool with which he can give a certain path an advantage among redundant paths.

The root path cost is the sum of all individual costs of those paths that a data packet has to traverse from a connected bridge's port to the root bridge.

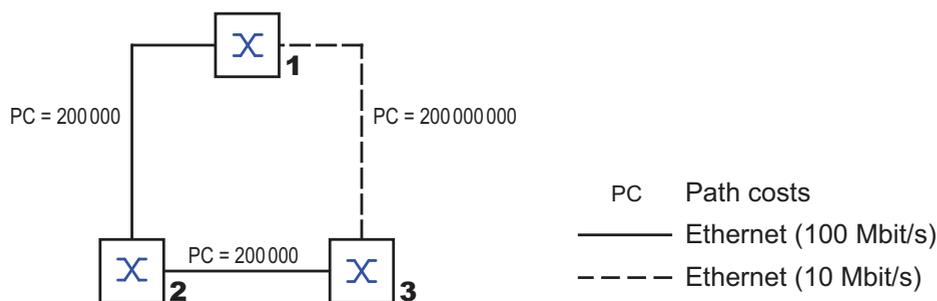


Figure 29: Path costs

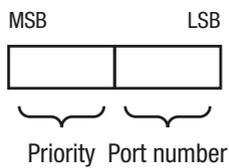
| Data rate   | Recommended value        | Recommended range      | Possible range |
|-------------|--------------------------|------------------------|----------------|
| ≤100 Kbit/s | 200,000,000 <sup>a</sup> | 20,000,000-200,000,000 | 1-200,000,000  |
| 1 Mbit/s    | 20,000,000 <sup>a</sup>  | 2,000,000-200,000,000  | 1-200,000,000  |
| 10 Mbit/s   | 2,000,000 <sup>a</sup>   | 200,000-20,000,000     | 1-200,000,000  |
| 100 Mbit/s  | 200,000 <sup>a</sup>     | 20,000-2,000,000       | 1-200,000,000  |
| 1 Gbit/s    | 20,000                   | 2,000-200,000          | 1-200,000,000  |
| 10 Gbit/s   | 2,000                    | 200-20,000             | 1-200,000,000  |
| 100 Gbit/s  | 200                      | 20-2,000               | 1-200,000,000  |
| 1 TBit/s    | 20                       | 2-200                  | 1-200,000,000  |
| 10 TBit/s   | 2                        | 1-20                   | 1-200,000,000  |

Table 11: Recommended path costs for RSTP based on the data rate.

- a. Bridges that conform with IEEE 802.1D 1998 and only support 16-bit values for the path costs should use the value 65,535 (FFFFH) for path costs when they are used in conjunction with bridges that support 32-bit values for the path costs.

### 5.1.5 Port Identifier

The port identifier consists of 2 bytes. One part, the lower-value byte, contains the physical port number. This provides a unique identifier for the port of this bridge. The second, higher-value part is the port priority, which is specified by the Administrator (default value: 128). It also applies here that the port with the smallest number for the port identifier has the highest priority.



*Figure 30: Port Identifier*

## 5.2 Rules for Creating the Tree Structure

### 5.2.1 Bridge information

To determine the tree structure, the bridges need more detailed information about the other bridges located in the network.

To obtain this information, each bridge sends a BPDU (Bridge Protocol Data Unit) to the other bridges.

The contents of a BPDU include

- ▶ bridge identifier,
- ▶ root path costs and
- ▶ port identifier

(see IEEE 802.1D).

### 5.2.2 Setting up the tree structure

- ▶ The bridge with the smallest number for the bridge identifier is called the root bridge. It is (or will become) the root of the tree structure.
- ▶ The structure of the tree depends on the root path costs. Spanning Tree selects the structure so that the path costs between each individual bridge and the root bridge become as small as possible.

- ▶ If there are multiple paths with the same root path costs, the bridge further away from the root decides which port it blocks. For this purpose, it uses the bridge identifiers of the bridge closer to the root. The bridge blocks the port that leads to the bridge with the numerically higher ID (a numerically higher ID is the logically worse one). If 2 bridges have the same priority, the bridge with the numerically larger MAC address has the numerically higher ID, which is logically the worse one.
- ▶ If multiple paths with the same root path costs lead from one bridge to the same bridge, the bridge further away from the root uses the port identifier of the other bridge as the last criterion ([see figure 30](#)). In the process, the bridge blocks the port that leads to the port with the numerically higher ID (a numerically higher ID is the logically worse one). If 2 ports have the same priority, the port with the higher port number has the numerically higher ID, which is logically the worse one.

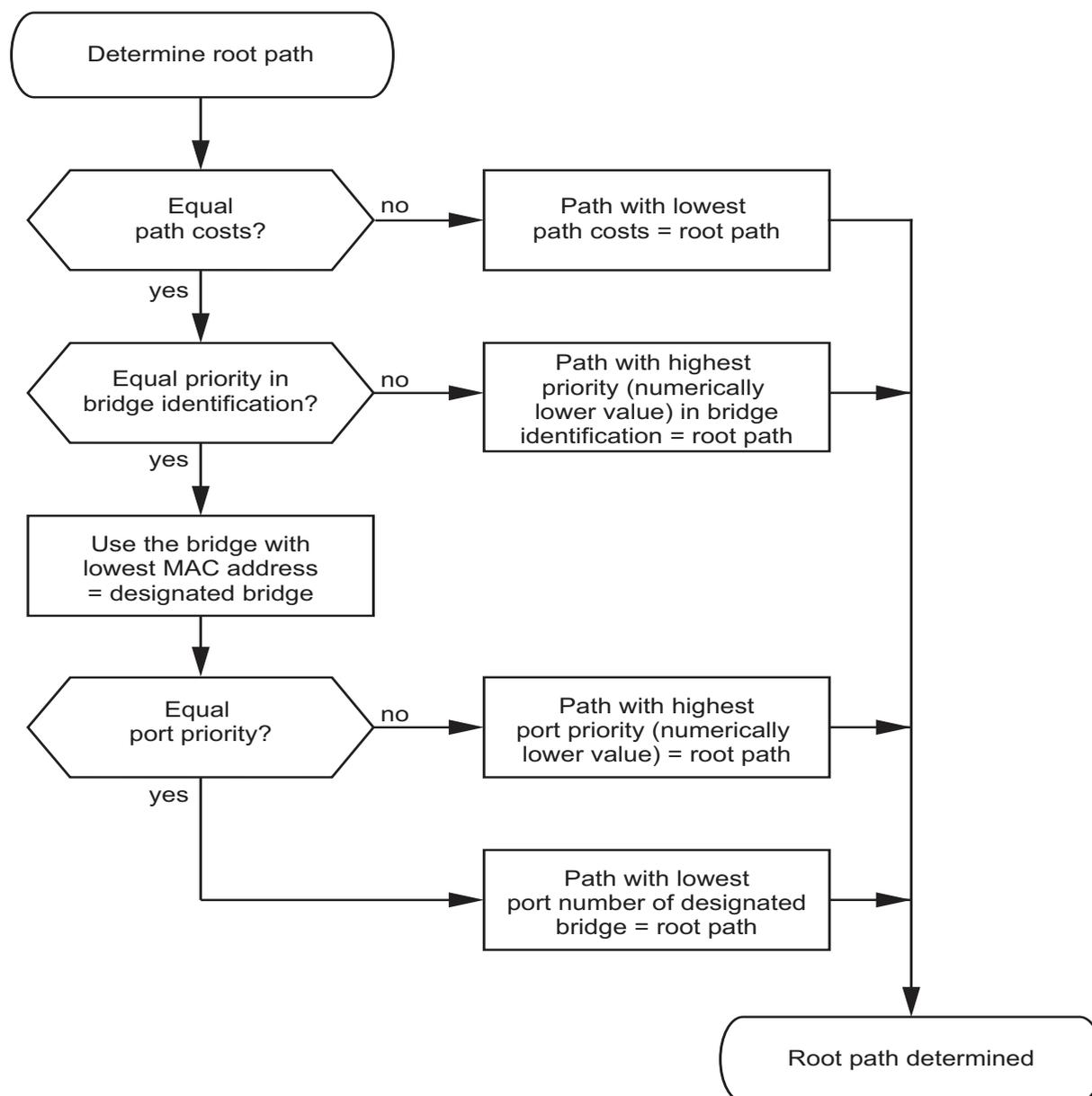


Figure 31: Flow diagram for specifying the root path

---

## 5.3 Example of determining the root path

You can use the network plan (see figure 32) to follow the flow chart (see figure 31) for determining the root path. The administrator has specified a priority in the bridge identification for each bridge. The bridge with the smallest numerical value for the bridge identification takes on the role of the root bridge, in this case, bridge 1. In the example all the sub-paths have the same path costs. The protocol blocks the path between bridge 2 and bridge 3 as a connection from bridge 3 via bridge 2 to the root bridge would result in higher path costs.

The path from bridge 6 to the root bridge is interesting:

- ▶ The path via bridge 5 and bridge 3 creates the same root path costs as the path via bridge 4 and bridge 2.
- ▶ The bridges select the path via bridge 5 because the value 28,672 for the priority in the bridge identifier is smaller than value 32,768.
- ▶ There are also 2 paths between bridge 6 and bridge 4. The port identifier is decisive here (Port 1 < Port 3).

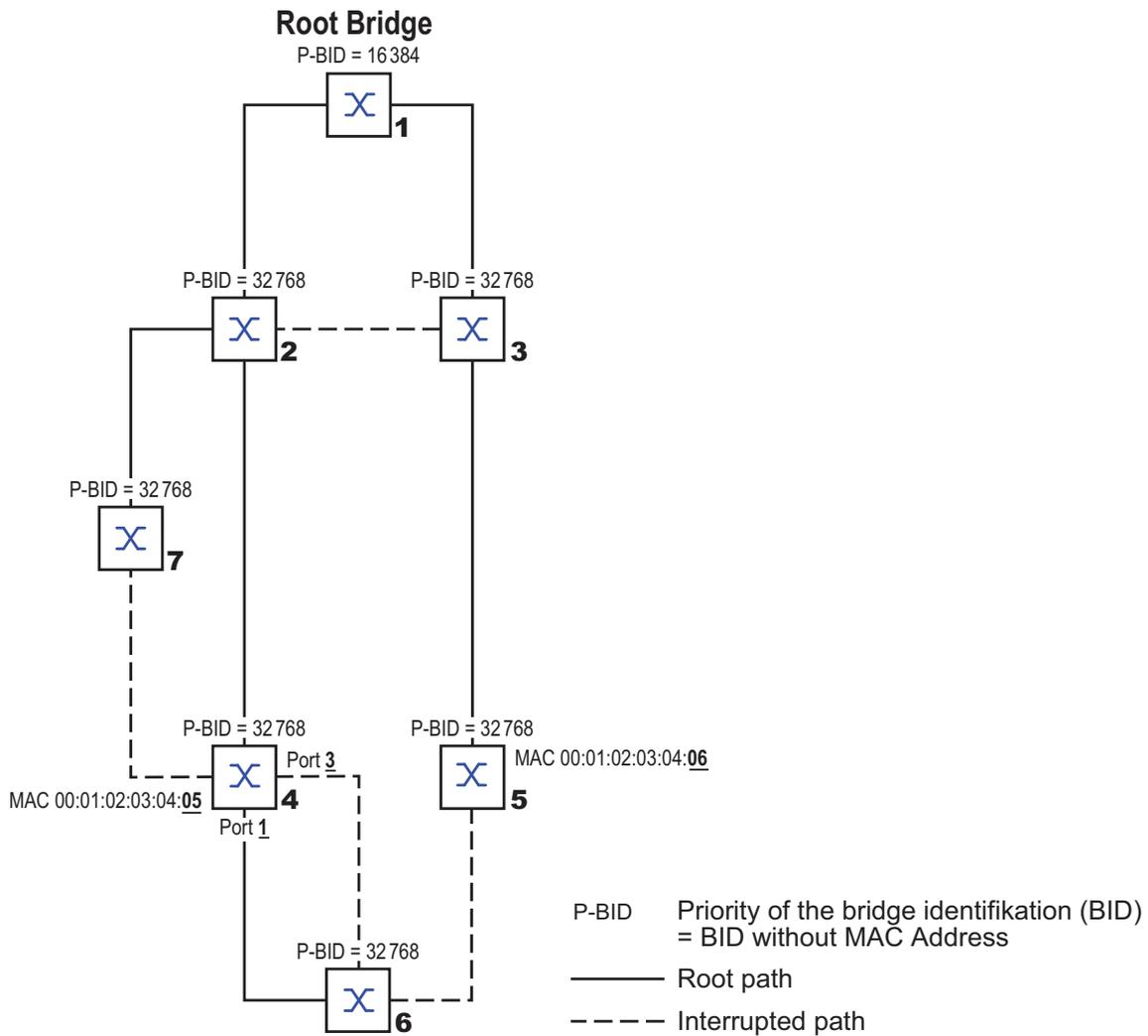


Figure 32: Example of determining the root path

## 5.4 Example of manipulating the root path

You can use the network plan (see figure 32) to follow the flow chart (see figure 31) for determining the root path. The Administrator has performed the following:

- Left the default value of 32,768 (8000H) for every bridge apart from bridge 1 and bridge 5, and
- assigned to bridge 1 the value 16,384 (4000H), thus making it the root bridge.

The protocol blocks the path between bridge 2 and bridge 3 as a connection from bridge 3 via bridge 2 to the root bridge would mean higher path costs.

The path from bridge 6 to the root bridge is interesting:

- ▶ The path via bridge 5 and bridge 3 creates the same root path costs as the path via bridge 4 and bridge 2.
- ▶ STP selects the path using the bridge that has the lowest MAC address in the bridge identification (bridge 4 in the illustration).
- ▶ There are also 2 paths between bridge 6 and bridge 4. The port identifier is decisive here.

**Note:** Because the Administrator does not change the default values for the priorities of the bridges in the bridge identifier, apart from the value for the root bridge, the MAC address in the bridge identifier alone determines which bridge becomes the new root bridge if the current root bridge goes down.

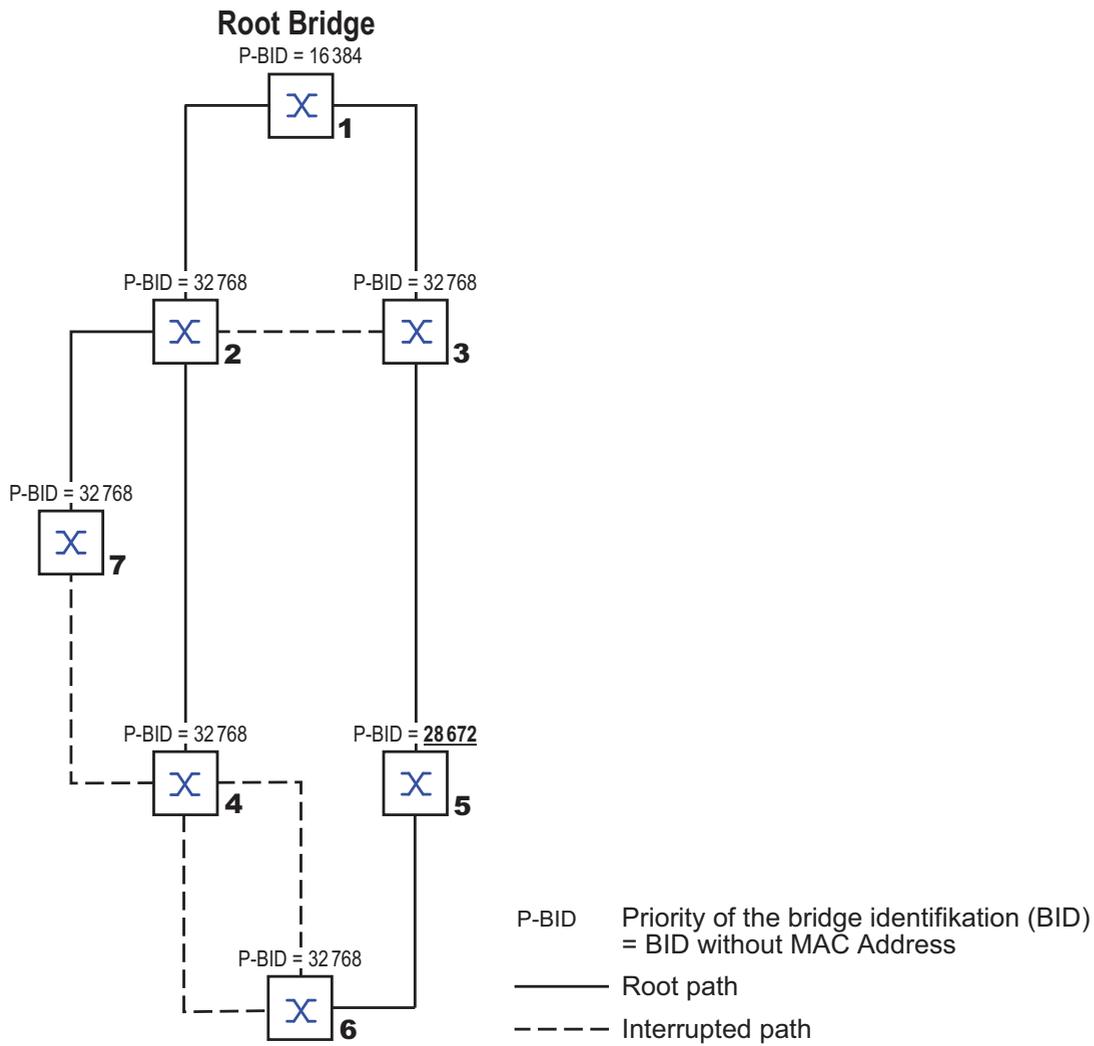


Figure 33: Example of manipulating the root path

## 5.5 Example of manipulating the tree structure

The Management Administrator soon discovers that this configuration with bridge 1 as the root bridge (see on page 69 “Example of determining the root path”) is invalid. On the paths from bridge 1 to bridge 2 and bridge 1 to bridge 3, the control packets which the root bridge sends to all other bridges add up. If the Management Administrator configures bridge 2 as the root bridge, the burden of the control packets on the subnetworks is distributed much more evenly. The result is the configuration shown here (see figure 34). The path costs for most of the bridges to the root bridge have decreased.

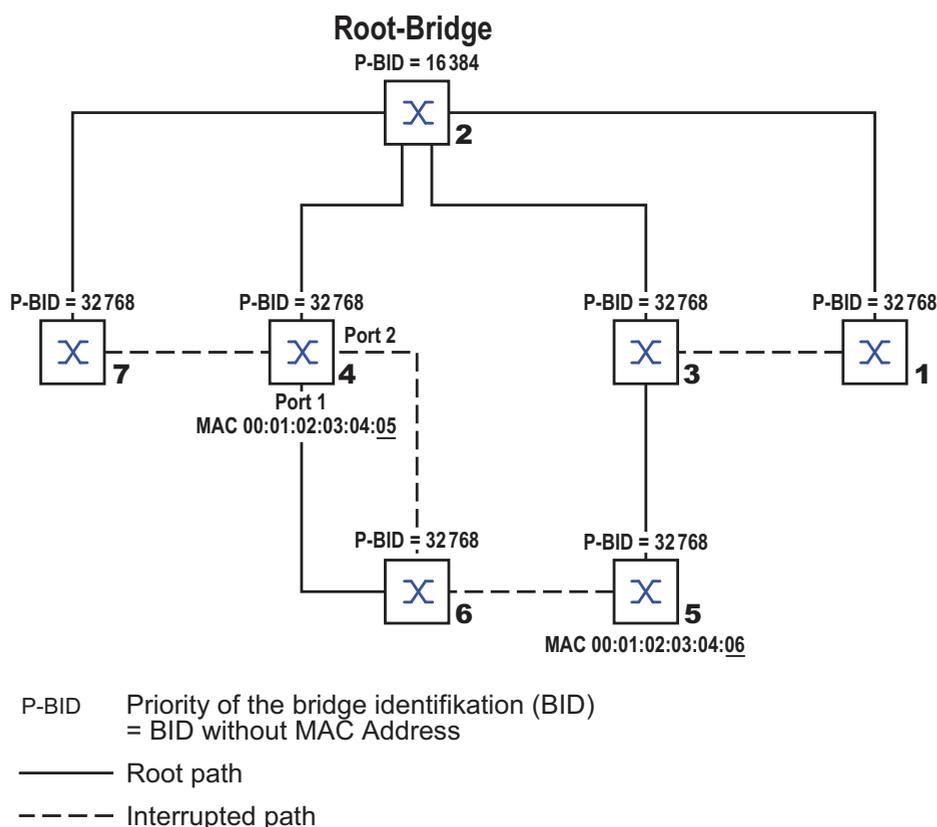


Figure 34: Example of manipulating the tree structure

## 5.6 The Rapid Spanning Tree Protocol

The RSTP uses the same algorithm for determining the tree structure as STP. RSTP merely changes parameters, and adds new parameters and mechanisms that speed up the reconfiguration if a link or bridge becomes inoperable.

The ports play a significant role in this context.

### 5.6.1 Port roles

RSTP assigns each bridge port one of the following roles ([see figure 35](#)):

► **Root Port:**

This is the port at which a bridge receives data packets with the lowest path costs from the root bridge.

If there are multiple ports with equally low path costs, the bridge ID of the bridge that leads to the root (designated bridge) decides which of its ports is given the role of the root port by the bridge further away from the root. If a bridge has multiple ports with equally low path costs to the same bridge, the bridge uses the port ID of the bridge leading to the root (designated bridge) to decide which port it selects locally as the root port ([see figure 31](#)).

The root bridge itself does not have a root port.

► **Designated port:**

The bridge in a network segment that has the lowest root path costs is the designated bridge.

If more than 1 bridge has the same root path costs, the bridge with the smallest value bridge identifier becomes the designated bridge. The designated port on this bridge is the port that connects a network segment leading away from the root bridge. If a bridge is connected to a network segment with more than one port (via a hub, for example), the bridge gives the role of the designated port to the port with the better port ID.

- ▶ **Edge port**  
Every network segment with no additional RSTP bridges is connected with exactly one designated port. In this case, this designated port is also an edge port. The distinction of an edge port is the fact that it does not receive any RST BPDUs (Rapid Spanning Tree Bridge Protocol Data Units).
- ▶ **Alternate port**  
This is a blocked port that takes over the task of the root port if the connection to the root bridge is lost. The alternate port provides a backup connection to the root bridge.
- ▶ **Backup port**  
This is a blocked port that serves as a backup in case the connection to the designated port of this network segment (without any RSTP bridges) is lost
- ▶ **Disabled port**  
This is a port that does not participate in the Spanning Tree Operation, i.e., the port is switched off or does not have any connection.

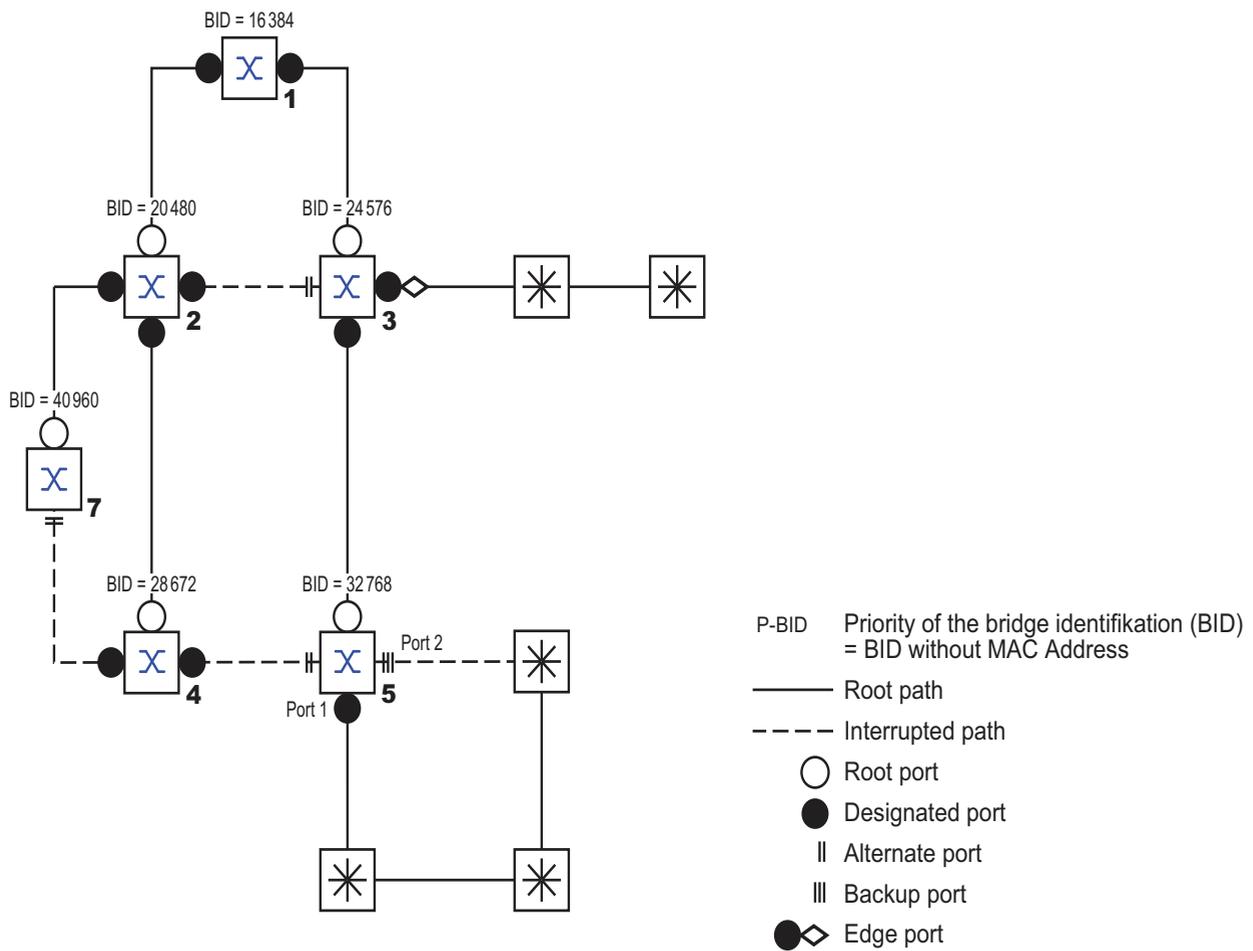


Figure 35: Port role assignment

## 5.6.2 Port states

Depending on the tree structure and the state of the selected connection paths, the RSTP assigns the ports their states.

| STP port state | Administrative bridge port state | MAC operational | RSTP Port state         | Active topology (port role)  |
|----------------|----------------------------------|-----------------|-------------------------|------------------------------|
| DISABLED       | Disabled                         | FALSE           | Discarding <sup>a</sup> | Excluded (disabled)          |
| DISABLED       | Enabled                          | FALSE           | Discarding <sup>a</sup> | Excluded (disabled)          |
| BLOCKING       | Enabled                          | TRUE            | Discarding <sup>b</sup> | Excluded (alternate, backup) |
| LISTENING      | Enabled                          | TRUE            | Discarding <sup>b</sup> | Included (root, designated)  |
| LEARNING       | Enabled                          | TRUE            | Learning                | Included (root, designated)  |
| FORWARDING     | Enabled                          | TRUE            | Forwarding              | Included (root, designated)  |

*Table 12: Relationship between port state values for STP and RSTP.*

- a. The dot1d-MIB displays "Disabled"  
 b. The dot1d-MIB displays "Blocked"

Meaning of the RSTP port states:

- ▶ Disabled: Port does not belong to the active topology
- ▶ Discarding: No address learning in FDB, no data traffic except for STP BPDUs
- ▶ Learning: Address learning active (FDB) and no data traffic except for STP BPDUs
- ▶ Forwarding: Address learning is active (FDB), sending and receipt of all frame types (not only STP BPDUs)

### 5.6.3 Spanning Tree Priority Vector

To assign roles to the ports, the RSTP bridges exchange configuration information with each other. This information is known as the Spanning Tree Priority Vector. It is part of the RSTP BPDUs and contains the following information:

- ▶ Bridge identification of the root bridge
- ▶ Root path costs of the sending bridge
- ▶ Bridge identification of the sending bridge
- ▶ Port identifiers of the ports through which the message was sent
- ▶ Port identifiers of the ports through which the message was received

Based on this information, the bridges participating in RSTP are able to determine port roles themselves and define the port states of their own ports.

### 5.6.4 Fast reconfiguration

Why can RSTP react faster than STP to an interruption of the root path?

- ▶ Introduction of edge-ports:  
During a reconfiguration, RSTP switches an edge port into the transmission mode after three seconds and then waits for the “Hello Time” (see table 13) to elapse, to be sure that no bridge sending BPDUs is connected.  
When the user determines that a terminal device is connected at this port and will remain connected, he can switch off RSTP at this port. Thus no waiting times occur at this port in the case of a reconfiguration.
- ▶ Introduction of alternate ports:  
As the port roles are already distributed in normal operation, a bridge can immediately switch from the root port to the alternative port after the connection to the root bridge is lost.
- ▶ Communication with neighboring bridges (point-to-point connections):  
Decentralized, direct communication between neighboring bridges enables reaction without wait periods to status changes in the spanning tree topology.

- ▶ **Address table:**  
With STP, the age of the entries in the FDB determines the updating of communication. RSTP immediately deletes the entries in those ports affected by a reconfiguration.
- ▶ **Reaction to events:**  
Without having to adhere to any time specifications, RSTP immediately reacts to events such as connection interruptions, connection reinstatements, etc.

**Note:** The downside of this fast reconfiguration is the possibility that data packages could be duplicated and/or arrive at the recipient in the wrong order during the reconfiguration phase of the RSTP topology. If this is unacceptable for your application, use the slower Spanning Tree Protocol or select one of the other, faster redundancy procedures described in this manual.

### 5.6.5 Configuring the Rapid Spanning Tree

- Set up the network to meet your demands.

**Note:** Before you connect the redundant lines, you must complete the configuration of the RSTP.

You thus avoid loops during the configuration phase.

- For devices with DIP switches, you switch these to “deactivated” (both to ON), so that the software configuration is not restricted.
- Select the `Redundancy:Rapid Spanning Tree:Global` dialog.
- Switch on RSTP on each device

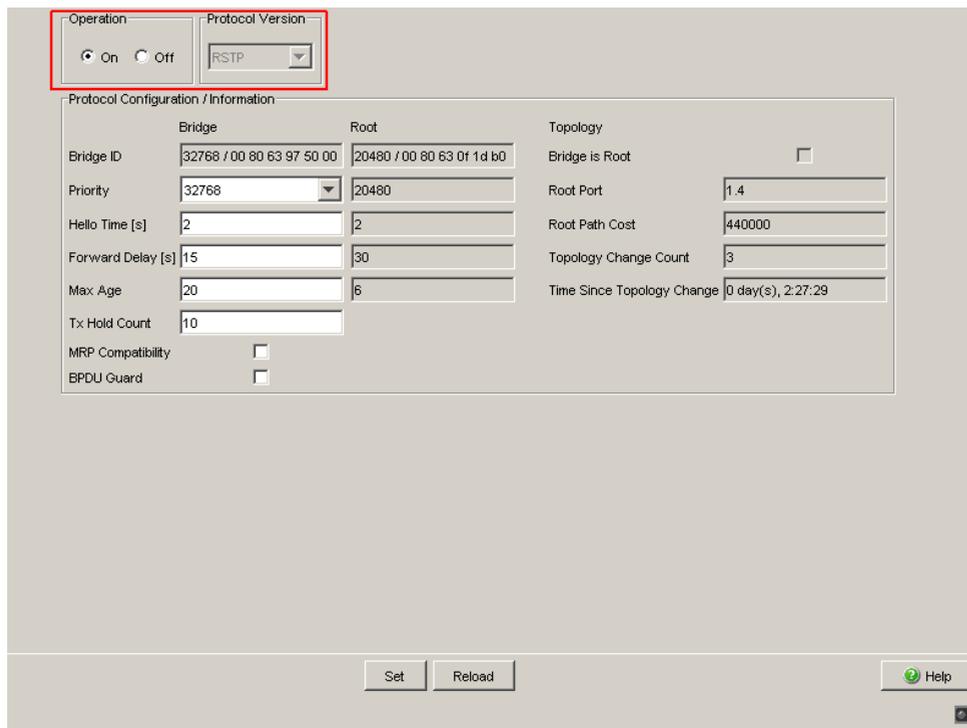


Figure 36: Operation on/off

- Define the desired Switch as the root bridge by assigning it the lowest priority in the bridge information among all the bridges in the network, in the “Protocol Configuration/Information” frame. Note that only multiples of 4,096 can be entered for this value (see table 13). In the “Root Information” frame, the dialog shows this device as the root.  
A root switch has no root port and a root cost of 0.
- If necessary, change the default priority value of 32,768 in other bridges in the network in the same way to the value you want (multiples of 4,096).  
For each of these bridges, check the display in the “Root Information” frame:
  - Root-ID: Displays the root bridge’s bridge identifier
  - Root Port: Displays the port leading to the root bridge
  - Root Cost: Displays the root cost to the root bridge
 in the “Protocol Configuration/Information” frame:
  - Priority: Displays the priority in the bridge identifier for this bridge
  - 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

- If necessary, change the values for “Hello Time”, “Forward Delay” and “Max. Age” on the rootbridge. The root bridge then transfers this data to the other bridges. The dialog displays the data received from the root bridge in the left column. In the right column you enter the values which shall apply when this bridge becomes the root bridge. For the configuration, take note of [table 13](#).

| Protocol Configuration / Information |                           |                           |
|--------------------------------------|---------------------------|---------------------------|
| Bridge                               | Root                      |                           |
| Bridge ID                            | 32768 / 00 80 63 97 50 00 | 20480 / 00 80 63 01 1d b0 |
| Priority                             | 32768                     | 20480                     |
| Hello Time [s]                       | 2                         | 2                         |
| Forward Delay [s]                    | 15                        | 30                        |
| Max. Age                             | 20                        | 16                        |
| Tx Hold Count                        | 10                        |                           |
| MRP Compatibility                    | <input type="checkbox"/>  |                           |
| BPDU Guard                           | <input type="checkbox"/>  |                           |

| Topology                   |                          |
|----------------------------|--------------------------|
| Bridge is Root             | <input type="checkbox"/> |
| Root Port                  | 1.4                      |
| Root Path Cost             | 440000                   |
| Topology Change Count      | 3                        |
| Time Since Topology Change | 0 day(s), 2:27:29        |

*Figure 37: Assigning Hello Time, Forward Delay and Max. Age*

The times entered in the RSTP dialog are in units of 1 s  
 Example: a Hello Time of 2 corresponds to 2 seconds.

- Now connect the redundant lines.

| Parameter     | Meaning                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | Possible Values                                | Default Setting |
|---------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------|-----------------|
| Priority      | The priority and the MAC address go together to make up the bridge identification.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | $0 < n * 4,096 (1000H) < 61,440 (F000H)$       | 32,768 (8000H)  |
| Hello Time    | Sets the Hello Time.<br>The local <code>Hello Time</code> is the time in seconds between the sending of two configuration messages (Hello packets).<br>If the local device has the root function, the other devices in the entire network take over this value. Otherwise the local device uses the value of the root bridge in the "Root" column on the right.                                                                                                                                                                                                                                                      | 1 - 2                                          | 2               |
| Forward Delay | Sets the Forward Delay parameter. In the previous STP protocol, the Forward Delay parameter was used to delay the status change between the statuses <code>disabled</code> , <code>discarding</code> , <code>learning</code> , and <code>forwarding</code> . Since the introduction of RSTP, this parameter has a subordinate role, because the RSTP bridges negotiate the status change without any specified delay. If the local device is the root, the other devices in the entire network take over this value. Otherwise the local device uses the value of the root bridge in the "Root" column on the right. | 4 - 30 s<br>See the note following this table. | 15 s            |
| Max Age       | Sets the Max Age parameter. In the previous STP protocol, the Max Age parameter was used to specify the validity of STP BPDUs in seconds. For RSTP, Max Age signifies the maximum permissible branch length (number of devices to the root bridge).<br>If the local device is the root, the other devices in the entire network take over this value. Otherwise the local device uses the value of the root bridge in the "Root" column on the right.                                                                                                                                                                | 6 - 40 s<br>See the note following this table. | 20 s            |

Table 13: Global RSTP settings

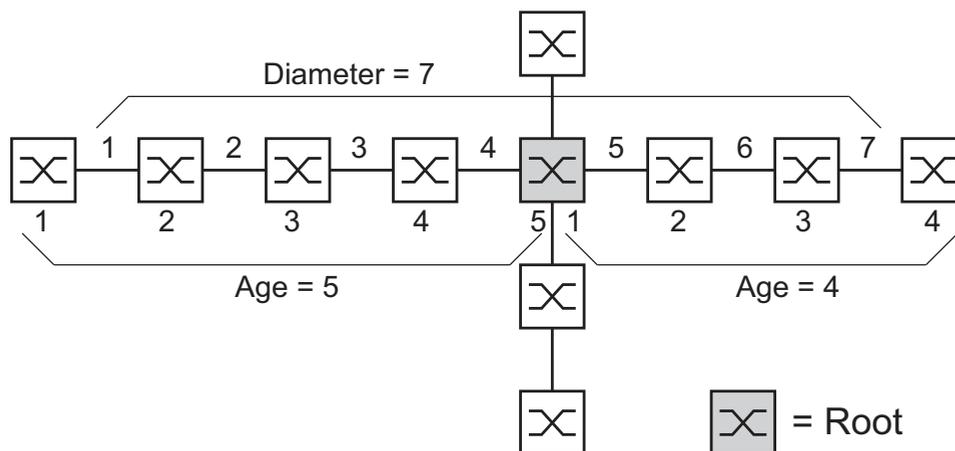


Figure 38: Definition of diameter and age

The network diameter is the number of connections between the two devices furthest away from the root bridge.

**Note:** The parameters

- Forward Delay and
- Max Age

have a relationship to each other:

**Forward Delay  $\geq$  (Max Age/2) + 1**

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

- When necessary, change and verify the settings and displays that relate to each individual port (dialog: Rapid Spanning Tree:Port).

| Module | Port | STP State Enable                    | Port State | Priority | Port Pathcost | Admin EdgePort | Oper EdgePort | Auto EdgePort | Oper PointToPoint | Designated Root (Priority/MAC Adres) |
|--------|------|-------------------------------------|------------|----------|---------------|----------------|---------------|---------------|-------------------|--------------------------------------|
| 1      | 1    | <input checked="" type="checkbox"/> | disabled   | 128      | 0             | false          | false         | true          | false             | 80 00 00 80 63 74 67                 |
| 1      | 2    | <input checked="" type="checkbox"/> | disabled   | 128      | 0             | false          | false         | true          | false             | 80 00 00 80 63 74 67                 |
| 1      | 3    | <input checked="" type="checkbox"/> | disabled   | 128      | 0             | false          | false         | true          | false             | 80 00 00 80 63 74 67                 |
| 1      | 4    | <input checked="" type="checkbox"/> | disabled   | 128      | 0             | false          | false         | true          | false             | 80 00 00 80 63 74 67                 |
| 1      | 5    | <input checked="" type="checkbox"/> | disabled   | 128      | 0             | false          | false         | true          | false             | 80 00 00 80 63 74 67                 |
| 1      | 6    | <input checked="" type="checkbox"/> | disabled   | 128      | 0             | false          | false         | true          | false             | 80 00 00 80 63 74 67                 |
| 1      | 7    | <input checked="" type="checkbox"/> | disabled   | 128      | 0             | false          | false         | true          | false             | 80 00 00 80 63 74 67                 |
| 1      | 8    | <input checked="" type="checkbox"/> | disabled   | 128      | 0             | false          | false         | true          | false             | 80 00 00 80 63 74 67                 |
| 1      | 9    | <input checked="" type="checkbox"/> | manualFwd  | 128      | 0             | false          | false         | true          | true              | 80 00 00 80 63 74 67                 |
| 1      | 10   | <input checked="" type="checkbox"/> | disabled   | 128      | 0             | false          | false         | true          | false             | 80 00 00 80 63 74 67                 |
| 1      | 11   | <input checked="" type="checkbox"/> | disabled   | 128      | 0             | false          | false         | true          | false             | 80 00 00 80 63 74 67                 |
| 1      | 12   | <input checked="" type="checkbox"/> | disabled   | 128      | 0             | false          | false         | true          | false             | 80 00 00 80 63 74 67                 |
| 1      | 13   | <input checked="" type="checkbox"/> | disabled   | 128      | 0             | false          | false         | true          | false             | 80 00 00 80 63 74 67                 |
| 1      | 14   | <input checked="" type="checkbox"/> | disabled   | 128      | 0             | false          | false         | true          | false             | 80 00 00 80 63 74 67                 |
| 1      | 15   | <input checked="" type="checkbox"/> | disabled   | 128      | 0             | false          | false         | true          | false             | 80 00 00 80 63 74 67                 |
| 1      | 16   | <input checked="" type="checkbox"/> | disabled   | 128      | 0             | false          | false         | true          | false             | 80 00 00 80 63 74 67                 |
| 1      | 17   | <input checked="" type="checkbox"/> | disabled   | 128      | 0             | false          | false         | true          | false             | 80 00 00 80 63 74 67                 |
| 1      | 18   | <input checked="" type="checkbox"/> | disabled   | 128      | 0             | false          | false         | true          | false             | 80 00 00 80 63 74 67                 |
| 1      | 19   | <input checked="" type="checkbox"/> | disabled   | 128      | 0             | false          | false         | true          | false             | 80 00 00 80 63 74 67                 |
| 1      | 20   | <input checked="" type="checkbox"/> | disabled   | 128      | 0             | false          | false         | true          | false             | 80 00 00 80 63 74 67                 |
| 1      | 21   | <input checked="" type="checkbox"/> | disabled   | 128      | 0             | false          | false         | true          | false             | 80 00 00 80 63 74 67                 |
| 1      | 22   | <input checked="" type="checkbox"/> | disabled   | 128      | 0             | false          | false         | true          | false             | 80 00 00 80 63 74 67                 |

Figure 39: Configuring RSTP for each port

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

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

| Parameter                                                                                                                                                                                                                                                                                                                             | Meaning                                                                                                                                                                                                                                   | Possible Values                                                              | Default Setting   |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------|-------------------|
| STP active                                                                                                                                                                                                                                                                                                                            | Here you can switch Spanning Tree on or off for this port. If Spanning Tree is activated globally and switched off at one port, this port does not send STP-BPDUs and drops any STP-BPDUs received.                                       | On, Off                                                                      | On                |
| <p><b>Note:</b> If you want to use other layer 2 redundancy protocols such as HIPER-Ring or Ring/Network coupling in parallel with Spanning Tree, make sure you switch off the ports participating in these protocols in this dialog for Spanning Tree. Otherwise the redundancy may not operate as intended or loops can result.</p> |                                                                                                                                                                                                                                           |                                                                              |                   |
| Port status (read only)                                                                                                                                                                                                                                                                                                               | Displays the STP port status with regard to the global MSTI (IST).                                                                                                                                                                        | discarding, learning, forwarding, disabled, manualForwarding, notParticipate | -                 |
| Port priority                                                                                                                                                                                                                                                                                                                         | Here you enter the port priority (the four highest bits of the port ID) with regard to the global MSTI (IST) as a decimal number of the highest byte of the port ID.                                                                      | $16 \leq n \cdot 16 \leq 240$                                                | 128               |
| Port path costs                                                                                                                                                                                                                                                                                                                       | Enter the path costs with regard to the global MSTI (IST) to indicate preference for redundant paths. If the value is 0, the Switch automatically calculates the path costs for the global MSTI (IST) depending on the transmission rate. | 0 - 200000000                                                                | 0 (automatically) |

Table 14: Port-related RSTP settings and displays

| Parameter       | Meaning                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | Possible Values                                                       | Default Setting       |
|-----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------|-----------------------|
| Admin Edge Port | <p>Only activate this setting when a terminal device is connected to the port (administrative: default setting). Then the port immediately has the forwarding status after a link is set up, without first going through the STP statuses. If the port still receives an STP-BPDU, the device blocks the port and clarifies its STP port role. In the process, the port can switch to a different status, e.g. forwarding, discarding, learning.</p> <p>Deactivate the setting when the port is connected to a bridge. After a link is set up, the port then goes through the STP statuses first before taking on the <code>forwarding</code> status, if applicable.</p> <p>This setting applies to all MSTIs.</p> | <code>active</code> (box selected), <code>inactive</code> (box empty) | <code>inactive</code> |
| Oper Edge Port  | <p>The device sets the “Oper Edge Port” condition to <code>true</code> if it has not received any STP-BPDUs, i.e. a terminal device is connected. It sets the condition to <code>false</code> if it has received STP-BPDUs, i.e. a bridge is connected.</p> <p>This condition applies to all MSTIs.</p>                                                                                                                                                                                                                                                                                                                                                                                                            | <code>true</code> , <code>false</code>                                | -                     |
| Auto Edge Port  | <p>The device only considers the Auto Edge Port setting when the Admin Edge Port parameter is deactivated. If Auto Edge Port is active, after a link is set up the device sets the port to the forwarding status after <math>1.5 \cdot \text{Hello Time}</math> (in the default setting 3 s).</p> <p>If Auto Edge Port is deactivated, the device waits for the <code>Max Age</code> instead (in the default setting 20 s).</p> <p>This setting applies to all MSTIs.</p>                                                                                                                                                                                                                                          | <code>active</code> (box selected), <code>inactive</code> (box empty) | <code>active</code>   |

Table 14: Port-related RSTP settings and displays

| Parameter                       | Meaning                                                                                                                                                                                                                                                                                                                                                                                                                                                     | Possible Values                                                                                                                             | Default Setting |
|---------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------|-----------------|
| Oper PointToPoint               | The device sets the “Oper point-to-point” condition to <code>true</code> if this port has a full duplex condition to an STP device. Otherwise it sets the condition to <code>false</code> (e.g. if a hub is connected).<br>The point-to-point connection makes a direct connection between 2 RSTP devices. The direct, decentralized communication between the two bridges results in a short reconfiguration time.<br>This condition applies to all MSTIs. | <code>true, false</code><br>The device determines this condition from the duplex mode:<br>FDX: <code>true</code><br>HDX: <code>false</code> |                 |
| Received bridge ID (read only)  | Displays the remote bridge ID from which this port last received an STP-BPDU. <sup>a</sup>                                                                                                                                                                                                                                                                                                                                                                  | Bridge identification (format ppppp / mm mm mm mm mm mm)                                                                                    | -               |
| Received path costs (read only) | Displays the path costs of the remote bridge from its root port to the CIST root bridge. <sup>a</sup>                                                                                                                                                                                                                                                                                                                                                       | 0-200000000                                                                                                                                 | -               |
| Received port ID (read only)    | Displays the port ID at the remote bridge from which this port last received an STP-BPDU. <sup>a</sup>                                                                                                                                                                                                                                                                                                                                                      | Port ID, format pn nn, with p: port priority / 16, nnn: port No., (both hexadecimal)                                                        | -               |

*Table 14: Port-related RSTP settings and displays*

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

## 5.7 Combining RSTP and MRP

In the MRP compatibility mode, the device allows you to combine RSTP with MRP.

With the combination of RSTP and MRP, the fast switching times of MRP are maintained.

The RSTP diameter (see figure 38) depends on the “Max Age”. It applies to the devices outside the MRP-Ring.

**Note:** The combination of RSTP and MRP presumes that both the root bridge and the backup root bridge are located within the MRP-Ring.

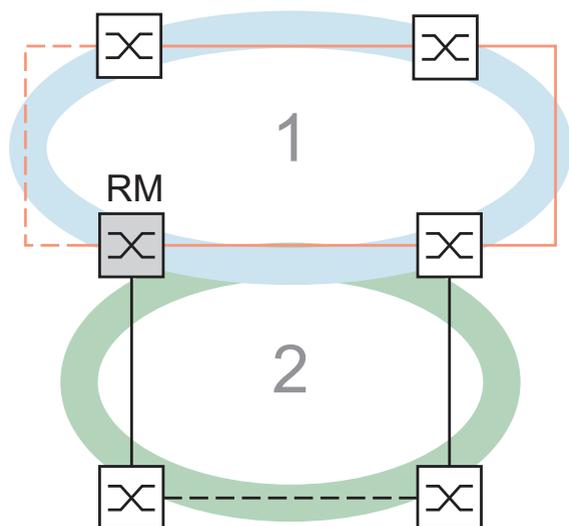


Figure 40: Combination of RSTP and MRP

1: MRP-Ring

2: RSTP-Ring

RM: Ring Manager

To combine RSTP with MRP, you perform the following steps in sequence:

- ▶ Configure MRP on all devices in the MRP-Ring.
- ▶ Close the redundant line in the MRP-Ring.
- ▶ Activate RSTP at the RSTP ports and also at the MRP-Ring ports.
- ▶ Configure the RSTP root bridge and the RSTP backup root bridge in the MRP-Ring:
  - Set their priority.
  - If you exceed the RSTP diameter specified by the preset value of  $\text{Max Age} = 20$ , modify Max Age and Forward Delay accordingly.
- ▶ Switch on RSTP globally.
- ▶ Switch on the MRP compatibility mode.
- ▶ After configuring all the participating devices, connect the redundant RSTP connection.

### 5.7.1 Application example for the combination of RSTP and MRP

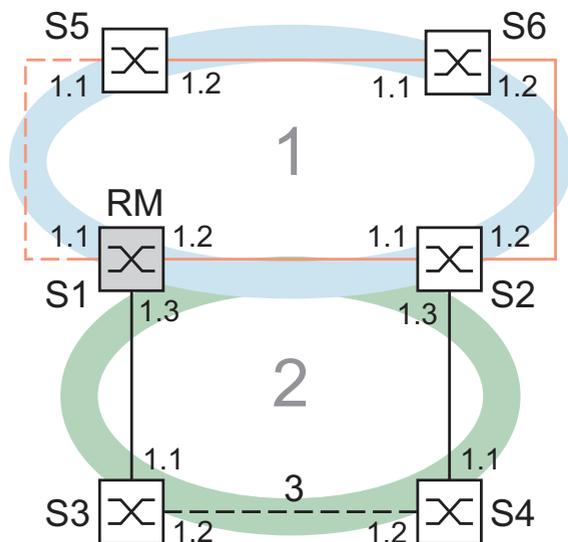
The figure (see figure 41) shows an example for the combination of RSTP and MRP.

| Parameters                                               | S1    | S2  | S3     | S4     | S5     | S6     |
|----------------------------------------------------------|-------|-----|--------|--------|--------|--------|
| MRP settings                                             |       |     |        |        |        |        |
| Ring redundancy: MRP version                             | MRP   | MRP |        |        | MRP    | MRP    |
| Ring port 1                                              | 1.1   | 1.1 |        |        | 1.1    | 1.1    |
| Ring port 2                                              | 1.2   | 1.2 |        |        | 1.2    | 1.2    |
| Port from MRP-Ring to the RSTP network                   | 1.3   | 1.3 | -      | -      | -      | -      |
| Redundancy Manager mode                                  | On    | Off | -      | -      | Off    | Off    |
| MRP operation                                            | On    | On  | Off    | Off    | On     | On     |
| RSTP settings                                            |       |     |        |        |        |        |
| For each RSTP port: STP State Enable                     | On    | On  | On     | On     | On     | On     |
| Protocol Configuration: priority (S2<S1<S3 and S2<S1<S4) | 4,096 | 0   | 32,768 | 32,768 | 32,768 | 32,768 |
| RSTP:Global: Operation                                   | On    | On  | On     | On     | On     | On     |
| RSTP:Global: MRP compatibility                           | On    | On  | -      | -      | On     | On     |

Table 15: Values for the configuration of the switches of the MRP/RSTP example

Prerequisites for further configuration:

- ▶ You have configured the MRP settings for the devices in accordance with the above table.
- ▶ The redundant line in the MRP-Ring is closed.



*Figure 41: Application example for the combination of RSTP and MRP*  
 1: MRP-Ring, 2: RSTP-Ring, 3: Redundant RSTP connection  
 RM: Ring Manager  
 S2 is RSTP Root Bridge  
 S1 is RSTP Backup Root Bridge

- Activate RSTP at the ports, using S1 as an example ([see table 15](#)).

```
enable
configure
interface 1/1

spanning-tree port mode
exit
interface 1/2

spanning-tree port mode
```

Change to the privileged EXEC mode.  
 Change to the Configuration mode.  
 Change to the Interface Configuration mode of port 1/1.  
 Activate RSTP on the port.  
 Change to the Configuration mode.  
 Change to the interface configuration mode for interface 1/2.  
 Activate RSTP on the port.

|                                      |                                                               |
|--------------------------------------|---------------------------------------------------------------|
| <code>exit</code>                    | Change to the Configuration mode.                             |
| <code>interface 1/3</code>           | Change to the interface configuration mode for interface 1/3. |
| <code>spanning-tree port mode</code> | Activate RSTP on the port.                                    |
| <code>exit</code>                    | Change to the Configuration mode.                             |

- Configure the global settings, using S1 as an example:
  - the RSTP priority
  - global operation
  - the MRP compatibility mode

|                                                    |                                                                                                              |
|----------------------------------------------------|--------------------------------------------------------------------------------------------------------------|
| <code>spanning-tree mst priority 0<br/>4096</code> | Set the RSTP priority for the MST instance 0 to the value 4,096. the MST instance 0 is the default instance. |
| <code>spanning-tree</code>                         | Activate RSTP operation globally.                                                                            |
| <code>spanning-tree stp-mrp-mode</code>            | Activate MRP compatibility.                                                                                  |

- Configure the other switches S2 though S6 with their respective values ([see table 15](#)).
- Connect the redundant RSTP connection.

# A Readers' Comments

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

Your assessment of this manual:

|                     | Very good             | Good                  | Satisfactory          | Mediocre              | Poor                  |
|---------------------|-----------------------|-----------------------|-----------------------|-----------------------|-----------------------|
| Precise description | <input type="radio"/> |
| Readability         | <input type="radio"/> |
| Understandability   | <input type="radio"/> |
| Examples            | <input type="radio"/> |
| Structure           | <input type="radio"/> |
| Completeness        | <input type="radio"/> |
| Graphics            | <input type="radio"/> |
| Drawings            | <input type="radio"/> |
| Tables              | <input type="radio"/> |

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

---



---



---



---



---



---



---



---

## Readers' Comments

---

Suggestions for improvement and additional information:

---

---

---

---

General comments:

---

---

---

---

Sender:

---

Company / Department:

---

Name / Telephone no.:

---

Street:

---

Zip code / City:

---

e-mail:

---

Date / Signature:

---

Dear User,

Please fill out and return this page

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

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

# B Index

|                           |                |                                |            |
|---------------------------|----------------|--------------------------------|------------|
| <b>A</b>                  |                | Port number                    | 65         |
| Advanced Mode             | 23             | Port priority (Spanning Tree)  | 65         |
| Age                       | 83             | Port roles (RSTP)              | 74         |
| Alternate port            | 75             | Port-State                     | 77         |
| <b>B</b>                  |                | PROFINET IO                    | 7          |
| Backup port               | 75             | <b>R</b>                       |            |
| BPDU                      | 66             | Rapid Spanning Tree            | 11, 74     |
| Bridge Identifier         | 62             | Reconfiguration                | 61         |
| Bridge Protocol Data Unit | 66             | Redundancy                     | 7, 59      |
| <b>C</b>                  |                | Redundancy existing            | 22, 26     |
| Configuration error       | 22, 26         | Redundancy functions           | 11         |
| <b>D</b>                  |                | Redundancy Manager             | 16         |
| Designated bridge         | 74             | Ring                           | 15         |
| Designated port           | 74             | Ring Manager                   | 16         |
| DIP-switch                | 18             | Ring manager                   | 15         |
| Diameter                  | 83             | Ring Redundancy                | 12, 12, 12 |
| Disabled port             | 75             | Ring structure                 | 16         |
| <b>E</b>                  |                | Ring/Network coupling          | 11         |
| Edge port                 | 75             | RM function                    | 15         |
| <b>F</b>                  |                | Root Bridge                    | 66         |
| FAQ                       | 97             | Root Path Cost                 | 62         |
| Forward Delay             | 82             | Root path                      | 69, 71     |
| <b>H</b>                  |                | Root port                      | 74         |
| Hello Time                | 82             | RSTP                           | 11         |
| HIPER-Ring                | 11, 13, 18     | RST BPDUs                      | 75, 78     |
| <b>I</b>                  |                | <b>S</b>                       |            |
| Industrial HiVision       | 8              | STP-BPDU                       | 66         |
| Industry Protocols        | 7              | Symbol                         | 9          |
| <b>L</b>                  |                | <b>T</b>                       |            |
| Loops                     | 46, 48, 55, 56 | Technical Questions            | 97         |
| <b>M</b>                  |                | Training Courses               | 97         |
| Max Age                   | 82             | Tree structure (Spanning Tree) | 66, 73     |
| MRP-Ring                  | 11, 13         | <b>V</b>                       |            |
| <b>N</b>                  |                | VLAN (HIPER-Ring)              | 21         |
| Network load              | 59, 61         | <b>P</b>                       |            |
| <b>P</b>                  |                | Path costs                     | 63, 66     |
| Port Identifier           | 62, 65         | Port Identifier                | 62, 65     |



## C Further Support

### ■ Technical Questions

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

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

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

You can contact us

in the EMEA region at

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

in the America region at

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

in the Asia-Pacific region at

- ▶ Tel.: +65 6854 9860
- ▶ E-mail: [inet-ap@belden.com](mailto:inet-ap@belden.com)

### ■ Hirschmann Competence Center

The Hirschmann Competence Center is ahead of its competitors:

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

The current technology and product training courses can be found at <http://www.hicomcenter.com>

- ▶ Support ranges from the first installation through the standby service to maintenance concepts.

With the Hirschmann Competence Center, you have decided against making any compromises. Our client-customized package leaves you free to choose the service components you want to use.

Internet:

<http://www.hicomcenter.com>





**HIRSCHMANN**

---

A **BELDEN** BRAND