



HIRSCHMANN

A **BELDEN** BRAND

Hirschmann Automation and Control GmbH

Classic L3P Rel. 09000

Reference Manuals

Graphical User Interface
Command Line Interface

User Manuals

Basic Configuration
Industry Protocols
Redundancy Configuration
Routing Configuration



HIRSCHMANN

A **BELDEN** BRAND

Reference Manual

GUI Graphical User Interface

Industrial ETHERNET (Gigabit-)Switch

PowerMICE, MACH 104, MACH 1040, MACH 4000

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
	Graphical User Interface	15
1	Basic Settings	21
1.1	System	22
1.2	Modules (MS, PowerMICE, MACH102 and MACH4000)	26
1.3	Network	29
1.4	Software	32
1.4.1	View the software versions present on the device	33
1.4.2	Restoring the Backup Version	33
1.4.3	TFTP Software Update	33
1.4.4	TFTP Bootcode Update	34
1.4.5	HTTP Software Update	35
1.4.6	Automatic software update by ACA	35
1.5	Port Configuration	36
1.6	Power over ETHERNET	39
1.7	Power over Ethernet Plus	43
1.7.1	Power over Ethernet Plus - Global	44
1.7.2	Power over Ethernet Plus - Port	47
1.8	Load/Save	51
1.8.1	Loading a Configuration	52
1.8.2	Saving the Configuration	59
1.8.3	URL	61
1.8.4	Deleting a configuration	62
1.8.5	Using the AutoConfiguration Adapter (ACA)	62
1.8.6	Cancelling a configuration change	64
1.9	Restart	66

2	Security	69
2.1	Password / SNMPv3 access	70
2.2	SNMPv1/v2 Access Settings	74
2.3	Telnet/Web/SSH Access	78
2.3.1	Description of Telnet Access	79
2.3.2	Description of Web Access (http)	80
2.3.3	Description of Web Access (https)	80
2.3.4	Description of SSH Access	81
2.4	Restricted Management Access	83
2.5	Port Security	87
2.6	802.1X Port Authentication	94
2.6.1	802.1X Global Configuration	94
2.6.2	802.1X Port Configuration	99
2.6.3	802.1X Port Clients	106
2.6.4	802.1X Port Statistics	109
2.7	RADIUS	111
2.7.1	Global	111
2.7.2	RADIUS Server	114
2.8	Login/CLI Banner	119
2.8.1	Login Banner	120
2.8.2	CLI Banner	122
2.9	Access Control Lists (ACLs)	124
3	Time	125
3.1	Basic Settings	126
3.2	SNTP configuration	129
3.3	PTP (IEEE 1588)	133
3.3.1	PTP Global (MS20/MS30, PowerMICE, MACH 104, MACH 1040)	136
3.3.2	PTP Version 1 (MS20/MS30, PowerMICE, MACH 104, MACH 1040)	140
3.3.3	PTP Version 2 (BC) (MS20/MS30, PowerMICE, MACH 104, MACH 1040)	142
3.3.4	PTP Version 2 (TC) (MS20/MS30, PowerMICE, MACH 104, MACH 1040)	149

4	Switching	155
4.1	Switching Global	156
4.2	Filter for MAC addresses	160
4.3	Rate Limiter	164
4.3.1	Rate limiter settings (PowerMICE and MACH 4000)	165
4.4	Multicasts	167
4.4.1	IGMP (Internet Group Management Protocol)	167
4.4.2	GMRP (GARP Multicast Registration Protocol)	174
4.5	VLAN	178
4.5.1	VLAN Global	178
4.5.2	Current VLAN	183
4.5.3	VLAN Static	185
4.5.4	Port	188
4.5.5	Voice VLAN	192
5	QoS/Priority	197
5.1	Global	198
5.2	Port Configuration	200
5.2.1	Entering the port priority	202
5.2.2	Selecting the Trust Mode	203
5.2.3	Displaying the untrusted traffic class	204
5.2.4	Shaping rate	204
5.3	802.1D/p mapping	205
5.4	IP DSCP mapping	207
5.5	Queue Management	210
5.5.1	Strict Priority	211
5.5.2	Weighted Fair Queuing	211
5.5.3	Maximum Bandwidth	212
6	Routing	213
6.1	Routing Global	214
6.2	Configuring Router Interfaces	215
6.2.1	Configuration	215
6.2.2	Configuring secondary addresses	218
6.3	ARP	220
6.3.1	Setting ARP parameters	220
6.3.2	ARP Statistics Display	222
6.3.3	ARP Table Display	222
6.3.4	Editing the ARP table	223

6.4	Router Discovery Configuration	225
6.5	RIP	226
6.5.1	Configuration	226
6.5.2	Route Distribution	229
6.5.3	Statistics	230
6.6	Routing table	232
6.6.1	Current	232
6.6.2	Static	234
6.6.3	Preferences	235
6.7	Tracking	237
6.7.1	Configuration	237
6.7.2	Applications	239
7	Redundancy	241
7.1	Link Aggregation	242
7.2	Ring Redundancy	246
7.2.1	Configuring the HIPER-Ring	248
7.2.2	Configuring the MRP-Ring	252
7.2.3	Configuring the Fast HIPER-Ring (MACH 1040)	259
7.3	Sub-Ring	262
7.3.1	Sub-Ring configuration	263
7.3.2	Sub-Ring – New Entry	266
7.4	Ring/Network Coupling	268
7.4.1	Preparing a Ring/Network Coupling	268
7.5	Spanning Tree	274
7.5.1	Global	276
7.5.2	MSTP (Multiple Spanning Tree)	283
7.5.3	Port	290
7.6	VRRP/HiVRRP	302
7.6.1	VRRP/HiVRRP Configuration	302
7.6.2	HiVRRP Domains	307
7.6.3	Statistics	310
7.6.4	Tracking	311
8	Diagnostics	315
8.1	Syslog	316
8.2	Trap log	320
8.3	Ports	322
8.3.1	Statistics table	322
8.3.2	Network load (Utilization)	324

8.3.3	SFP Transceiver	326
8.3.4	TP Cable Diagnosis	327
8.3.5	Port Monitor	330
8.3.6	Auto Disable	342
8.4	Configuration Check	346
8.5	Topology Discovery	349
8.5.1	LLDP Information from Neighbor Devices	349
8.5.2	LLDP-MED (Media Endpoint Discovery)	351
8.6	Port Mirroring	355
8.7	Device Status	358
8.8	Signal contact	361
8.8.1	Manual Setting	361
8.8.2	Function monitoring	362
8.8.3	Device status	363
8.8.4	Configuring Traps	364
8.9	Alarms (Traps)	366
8.10	Report	369
8.10.1	System Information	371
8.10.2	Event Log	372
8.11	IP address conflict detection	373
8.12	MAC Notification	375
8.12.1	Operation	375
8.12.2	Configuration	376
8.12.3	Table	376
8.13	Self Test	378
9	Advanced	381
9.1	DHCP Relay Agent	382
9.1.1	Global	382
9.1.2	Server	385
9.2	DHCP Server	387
9.2.1	Global	387
9.2.2	Pool	390
9.2.3	Lease Table	395
9.3	Industrial Protocols	398
9.3.1	PROFINET	398
9.3.2	EtherNet/IP	401
9.3.3	IEC61850 MMS Protocol (RSR, MACH 1000)	402
9.3.4	Digital IO Module	404

9.4	Software DIP Switch overwrite (MICE, PowerMICE and RS)	413
9.5	Command Line	415
A	Appendix	417
A.1	Technical Data	418
A.2	List of RFCs	420
A.3	Underlying IEEE Standards	422
A.4	Underlying IEC Norms	423
A.5	Underlying ANSI Norms	424
A.6	Literature references	425
A.7	Copyright of Integrated Software	426
	A.7.1 Bouncy Castle Crypto APIs (Java)	426
	A.7.2 Broadcom Corporation	427
B	Readers' Comments	428
C	Index	431
D	Further Support	435

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 “Routing Configuration User Manual” document contains the information you need to start operating the routing function. The manual enables you to configure your router by following the examples.

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

Symbols used:

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

Key



Hub



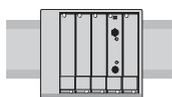
A random computer



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.

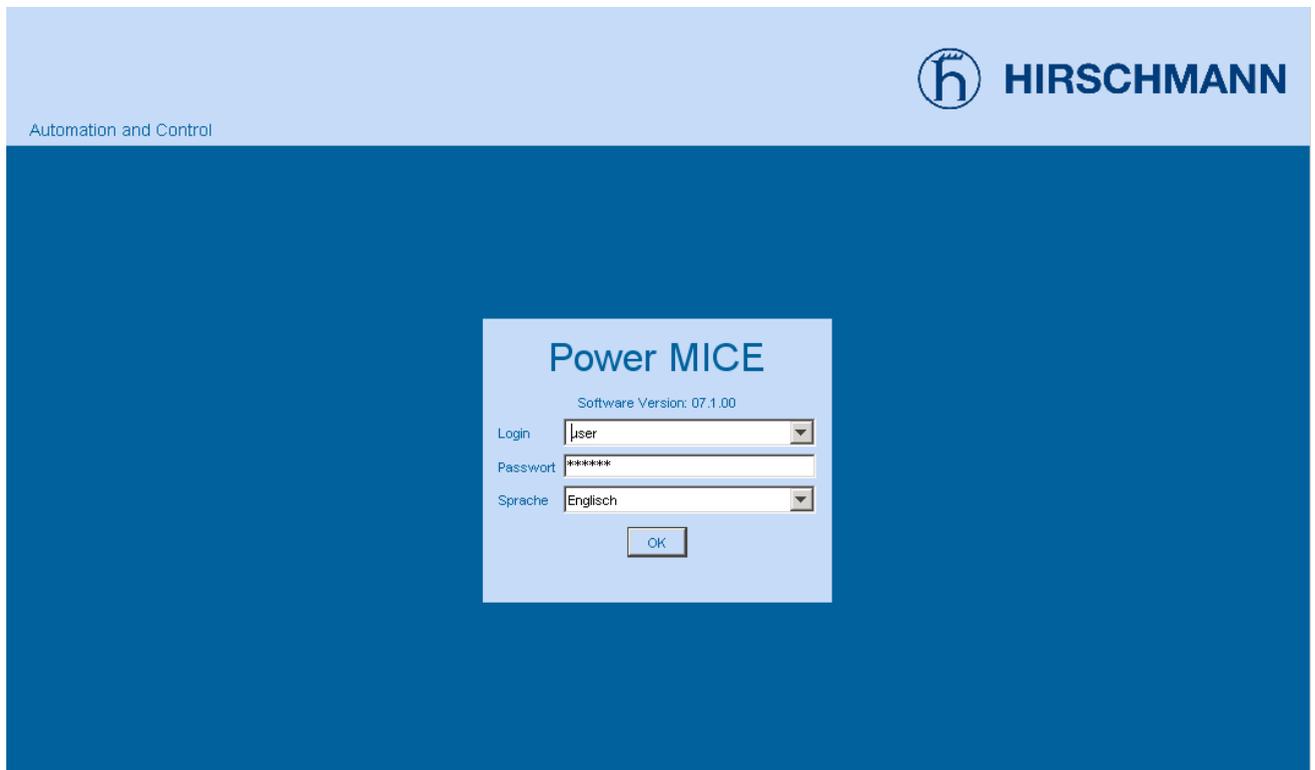


Figure 1: Login window

- 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.

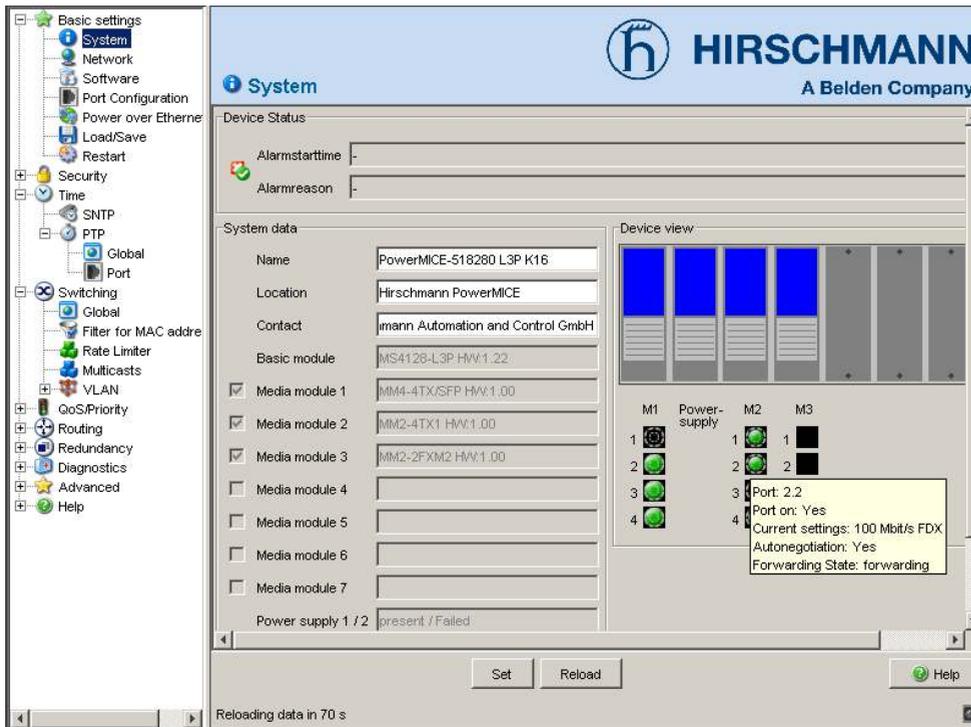
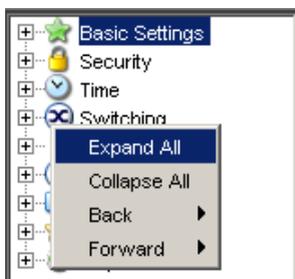


Figure 2: Web-based user interface of the device with tooltip.

■ 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 Plus
- ▶ 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

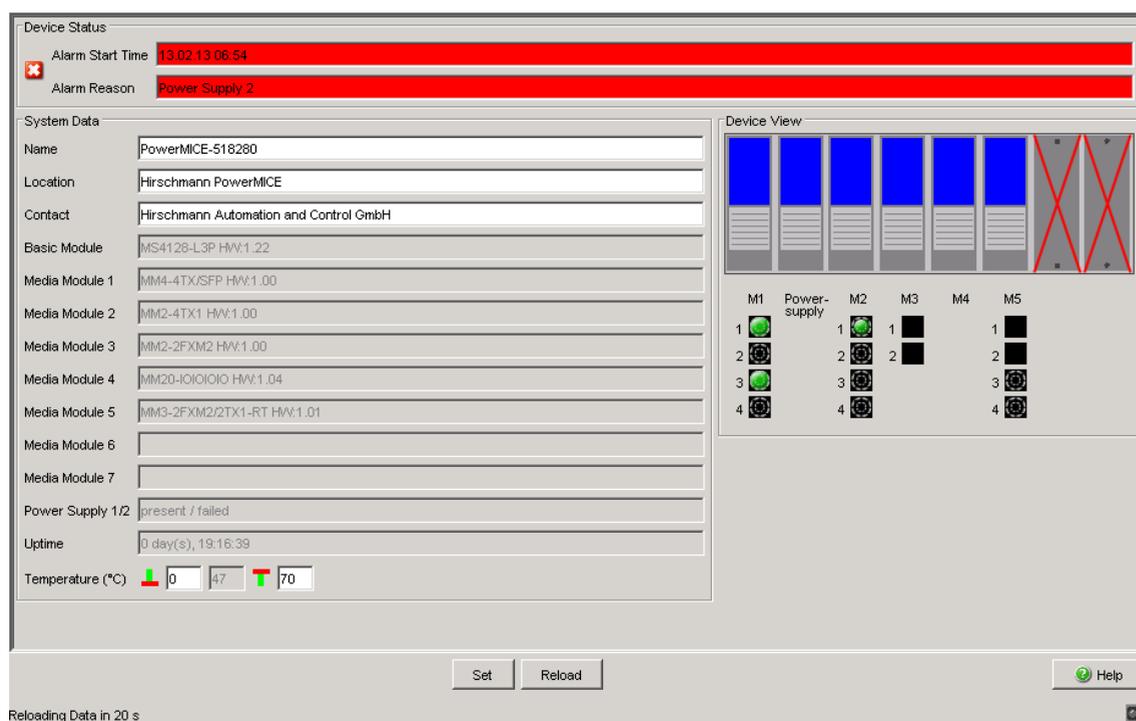


Figure 3: "System" Submenu

■ Device Status

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

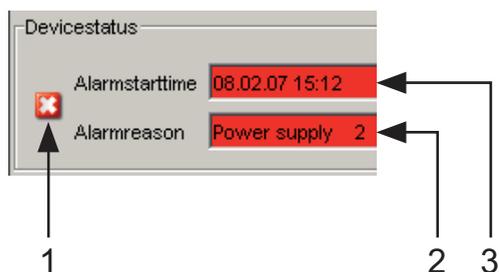


Figure 4: Device status and alarm display
 1 - The symbol displays the device state
 2 - Cause of the oldest existing alarm
 3 - Start of the oldest existing alarm

■ 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)
Power supply 3-1/3-2	Status of power units 3-1/3-2
Power supply 4-1/4-2	Status of power units 4-1/4-2

Table 2: System Data

Name	Meaning
Fan	Status of fans
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.

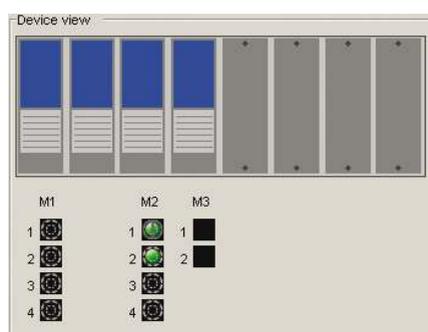


Figure 5: Device View

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.

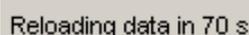


Figure 6: Time to next Reload

■ 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.

The screenshot shows a network configuration dialog box. On the left, there is a 'Mode' section with three radio buttons: 'BOOTP', 'DHCP', and 'Local'. Below it is a 'VLAN' section with a text field containing '1'. The main area is divided into four sections: 'BOOTP /DHCP' with a 'MAC Address' field containing '00:80:63:51:82:80'; 'DHCP' with a 'System name' field containing 'PowerMICE-518280'; 'Local' with three fields: 'IP Address' (10.0.1.112), 'Netmask' (255.255.255.0), and 'Gateway address' (10.0.1.1); and 'HiDiscovery Protocol v1/v2' with 'Operation' radio buttons for 'On' (selected) and 'Off', and an 'Access' dropdown menu set to 'read-write'. At the bottom, there are 'Set', 'Reload', and 'Help' buttons.

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 51 “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 51 “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

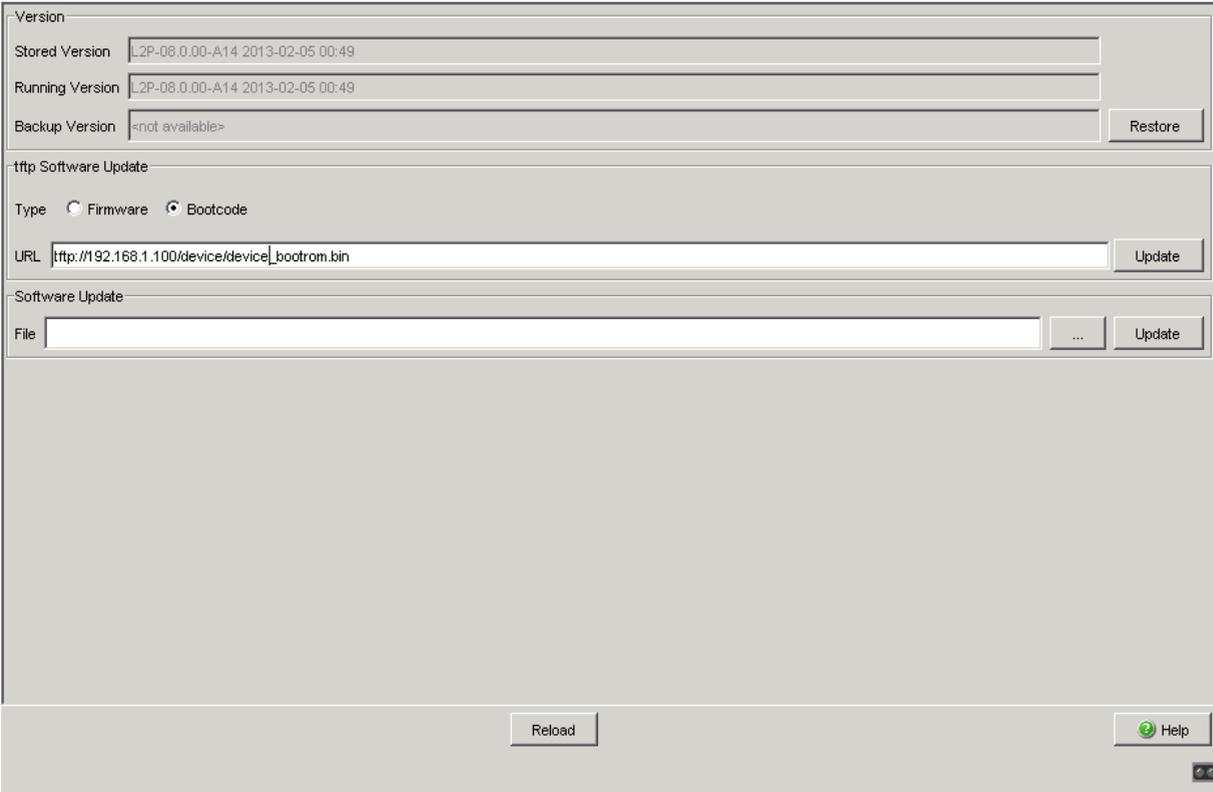
Button	Meaning
Set	Transfers the changes to the volatile memory (RAM) of the device. To permanently save the changes, open the <code>Basic Settings:Load/Save</code> dialog, select the location to save the configuration, and click "Save".
Reload	Updates the fields with the values that are saved in the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

Table 5: Buttons

1.4 Software

This dialog provides you with the following functions:

- ▶ which display the software versions in the device.
- ▶ carry out a software update of the device via http (via a file selection window), tftp or ACA.
- ▶ restore the backup version of the software saved in Flash.



The screenshot displays the 'Software Dialog' interface. It is divided into three main sections:

- Version:** Contains three text fields: 'Stored Version' (L2P-08.0.00-A14 2013-02-05 00:49), 'Running Version' (L2P-08.0.00-A14 2013-02-05 00:49), and 'Backup Version' (<not available>). A 'Restore' button is located to the right of the 'Backup Version' field.
- tftp Software Update:** Features a 'Type' section with radio buttons for 'Firmware' and 'Bootcode' (selected). Below is a 'URL' field containing 'tftp://192.168.1.100/device/device_bootrom.bin' and an 'Update' button.
- Software Update:** Includes a 'File' field with a browse button ('...') and an 'Update' button.

At the bottom of the dialog, there are 'Reload' and 'Help' buttons. A small icon is visible in the bottom right corner.

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.
- ▶ **Backup Version:**
The version of the previous software stored in the flash memory.

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.

- Click on the “Restore” button to replace the stored version of the software with the backup version.
- 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 66.](#)

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 66.](#)

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 156 “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: If you are using link aggregation, pay attention to its configuration ([see on page 242 “Link Aggregation”](#)).

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	-
Optical	100 Mbit/s	off	on	full
Optical	1 Gbit/s	on	on	-
Optical	10 Gbit/s	off	on	full

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
- ▶ MACH 4002
- ▶ MACH 1020/1030/1040

You will learn in this section how these devices operate.

Note: However the following devices are equipped with Power over Ethernet **Plus (PoE+)** ports

- ▶ MACH104-16TX-PoEP and
- ▶ MACH 102 with media module M1-8TP-RJ45 PoEP

You will learn in the “Power over Ethernet Plus” section how these devices operate.

If the device is equipped with PoE media modules, it will then allow you to supply current to devices such as IP phones via the twisted-pair cable. PoE media modules support Power over ETHERNET according to IEEE 802.3af. On delivery, the Power over ETHERNET function is activated globally and on all PoE-capable ports.

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 MACH 4000:

The device provides the nominal power for the sum of all PoE ports plus a surplus. Should the connected devices require more PoE power than is provided, the device then switches PoE off at the ports. Initially, the device switches PoE off at the ports with the lowest PoE priority. If multiple ports have the same priority, the device first switches PoE off at the ports with the higher port number.

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.
- In the "Priority" column (MACH 4000), set the PoE priority of the port to "low", "high" or "critical".

- 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.

Operation

Configuration

Send Trap Yes No

Threshold [%]

System Power

Budget [W]

Reserved [W]

Delivered [W]

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	

Set Reload Help

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 Power over Ethernet Plus

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

- ▶ MACH104-16TX-PoEP and
- ▶ MACH 102 with media module M1-8TP-RJ45 PoEP

You will learn in this section how both of these devices operate.

However the following devices are equipped with Power over Ethernet (PoE) ports:

- ▶ RS20/30
- ▶ MS20/30
- ▶ PowerMICE
- ▶ OCTOPUS
- ▶ MACH 4002
- ▶ MACH 1020/1030/1040

In the “Power over ETHERNET” section you will learn how these devices operate.

Devices with Power over Ethernet Plus (PoE+) ports enable you to supply current to terminal devices such as IP phones via the twisted-pair cable. PoE+ ports support Power over Ethernet Plus in accordance with IEEE 802.3at.

The Power over Ethernet Plus function is activated both globally and on the PoE-capable ports on delivery.

Connecting too many PoE+ Powered Devices (PD) can overload your external PoE+ power supply. It may fail as a result. The Power over Ethernet Plus dialog assists you in managing the power supply and helps you to protect your external PoE+ power supply devices from overloading.

For the devices

- ▶ MACH104-16TX-PoEP and
- ▶ MACH 102 with media module M1-8TP-RJ45 PoEP:
- ▶ Maximum power for MACH104-16TX-PoEP:
The device provides maximum power of 248 W for the aggregate of all PoE ports.
- ▶ Maximum power for MACH 102 with media module M1-8TP-RJ45 PoE:
The device provides maximum power for the aggregate of all PoE ports. Because the PoE+ media module gets its PoE voltage externally, the device cannot know the maximum power possible, so here the device uses the value of 124 watts per M1-8TP-RJ45 PoE media module as "maximum power".

Should the PDs connected require more PoE power than is provided, then the device deactivates PoE at designated ports. Initially, the device switches PoE off at the ports with the lowest PoE priority. If multiple ports have the same priority, the device first switches PoE off at the ports with the higher port number.

1.7.1 Power over Ethernet Plus - Global**Frame "Operation":**

Parameter	Meaning	Value Range	Default Setting
Operation	Switching Power over Ethernet Plus operation on/off.	On, Off	On

Table 10: PoE+ Global - Operation

Frame "Configuration":

Parameter	Meaning	Value Range	Default Setting
Send Trap	Causes the device to send a trap in the following cases: <ul style="list-style-type: none"> ▶ If a value exceeds/falls below the performance threshold. ▶ If the PoE+ supply voltage is switched on/off at at least one port. 	Yes, No	Yes
Threshold [%] (performance threshold)	Performance threshold in percent of the nominal performance: When this value is exceeded/not achieved, the device will send a trap, provided that "Send Trap" is enabled.	0 - 99%	90%

*Table 11: PoE+ Global - Configuration***Frame "System Power":**

Parameter	Meaning	Value Range	Default Setting
Budget [W]	Displays the power that the device nominally provides for the PoE+ ports.	0 - 248 W	248 W
Reserved [W]	Displays how much power the device provides at most to the connected PoE devices on the basis of their classification.	0 - 248 W	0 W
Delivered [W]	Displays how large the current power requirement is on the PoE+ ports.	0 - 248 W	-

Table 12: PoE+ Global - System Power

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

"Global" table:

Parameter	Meaning	Value Range	Default Setting
Module	<ul style="list-style-type: none"> ▶ For MACH102 media modlues M1-8TP-RJ45 PoE: Module = slot number of the PoE+ module ▶ For MACH104-16TX-PoEP devices: Module = 1 	1 - 2	-
Configured power budget [W]	Configure whichever power budget the device nominally provides for the module's PoE+ ports.	0 - 248 W	248 W
Maximum power budget [W]	Displays the power that the device nominally provides for the module's PoE+ ports.	0 - 248 W	248 W
Reserved power [W]	Displays how much power the device provides at most to the PoE devices connected to the module on the basis of their classification.	0 - 248 W	0 W
Delivered power [W]	Displays how large the current power requirement is on every PoE+ port of the module.	0 - 248 W	-
Threshold [%]	Specify the performance threshold in percent of the nominal performance; when the module exceeds or is below this value, the device will send a trap, provided that "Send Trap" is enabled.	0 - 99%	90%
Trap notification	Causes the device to send a trap in the following cases: <ul style="list-style-type: none"> ▶ If a value exceeds/falls below the performance threshold. ▶ If the PoE+ supply voltage is switched on/off on at least one port. 	On, Off	On

Table 13: Power over Ethernet Plus - Global

Module	Configured Power Budget [W]	Maximum Power Budget [W]	Reserved Power [W]	Delivered Power [W]	Threshold [%]	Trap Notification
1	248	248	0	0	90	<input checked="" type="checkbox"/>

Figure 11: Power over Ethernet Plus Dialog:Global

Note: For MACH 102 devices with media module M1-8TP-RJ45 PoE: We recommend distributing PoE+ power equally between the two port groups (ports 5 to 12 and ports 13 to 20).

1.7.2 Power over Ethernet Plus - Port

The table only shows ports that support PoE+.

Parameter	Meaning	Value range	Default setting
Port	Module and port numbers of the PoE+ port to which this entry applies. On the MACH104-16TX-PoEP device, the ports 1.5 to 1.20 support PoE+.	1, 5 - 1, 20 dB	-
PoE enable	Switching Power over Ethernet Plus operation on/off for this port.	An, Aus	An

Table 14: Power over Ethernet Plus - Port

Parameter	Meaning	Value range	Default setting
Status	Displays the PoE+ status of the port.	suche, ...	suche, ...
Priority	Specify the PoE+ priority of the port.	niedrig, hoch, kritisch	niedrig
Class	Displays the class of the connected device:Class: Maximum output power ▶ 0: 15.4 W ▶ 1: 4.0 W ▶ 2: 7.0 W ▶ 3: 15.4 W ▶ 4: 30.0 W	0 - 4	-
Consumption [W]	Displays the current power output on the particular port.	0,0 - 248,0 W	-
Power limit [mW]	Defines the maximum power in watts that the port outputs. This function allows you to distribute the power budget available among the PoE ports as required. For example, for a connected device without the "Power Class" function, the port reserves a fixed amount of 15.4 W (class 0) even if the device requires less power. The surplus power is not available to any other port. By defining the power limit, you reduce the reserved power to the actual requirement of the connected device. The unused power is available to other ports. If the exact power consumption of the connected device is unknown, see the value in the "Maximum Observed [W]" field. The power limit must be greater than the value in the "Maximum Observed [W]" field. If the maximum observed power is greater than the set power limit, the device sees the power limit as invalid. In this case, the device uses the PoE class for the calculation.	0 - 30,0	0

Table 14: Power over Ethernet Plus - Port

Parameter	Meaning	Value range	Default setting
Maximum Observed [mW]	Displays the maximum power in watts that the device has consumed so far. You reset the value when you disable PoE on the port or terminate the connection to the connected device.	0 - 30,0	-
Name	Displays the name of the port, see Grundeinstellungen:Portkonfiguration	-	-

Table 14: Power over Ethernet Plus - Port

Port	PoE enable	Status	Priority	Class	Consumption [W]	Power Limit [mW]	Maximum Observed [mW]	Name
1.5	<input checked="" type="checkbox"/>	searching	low	-	0.0			
1.6	<input checked="" type="checkbox"/>	searching	low	-	0.0			
1.7	<input checked="" type="checkbox"/>	searching	low	-	0.0			
1.8	<input checked="" type="checkbox"/>	searching	low	-	0.0			
1.9	<input checked="" type="checkbox"/>	searching	low	-	0.0			
1.10	<input checked="" type="checkbox"/>	searching	low	-	0.0			
1.11	<input checked="" type="checkbox"/>	searching	low	-	0.0			
1.12	<input checked="" type="checkbox"/>	searching	low	-	0.0			
1.13	<input checked="" type="checkbox"/>	searching	low	-	0.0			
1.14	<input checked="" type="checkbox"/>	searching	low	-	0.0			
1.15	<input checked="" type="checkbox"/>	searching	low	-	0.0			
1.16	<input checked="" type="checkbox"/>	searching	low	-	0.0			
1.17	<input checked="" type="checkbox"/>	searching	low	-	0.0			
1.18	<input checked="" type="checkbox"/>	searching	low	-	0.0			
1.19	<input checked="" type="checkbox"/>	searching	low	-	0.0			
1.20	<input checked="" type="checkbox"/>	searching	low	-	0.0			

critical
high
low

Set Reload Help

Figure 12: Power over Ethernet Plus Dialog:Port

■ 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 15: Buttons

1.8 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 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 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 for 'Status' showing '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 13: Load/Save dialog

1.8.1 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 stored on the PC as an editable and readable script or in binary form,
- ▶ 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 14: 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.

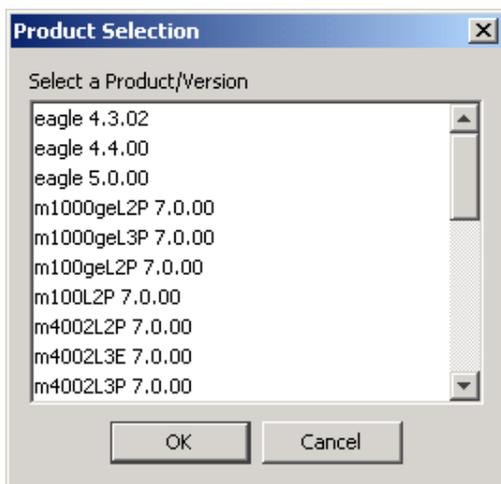


Figure 15: Creating New Script Dialog - Product Selection

- 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

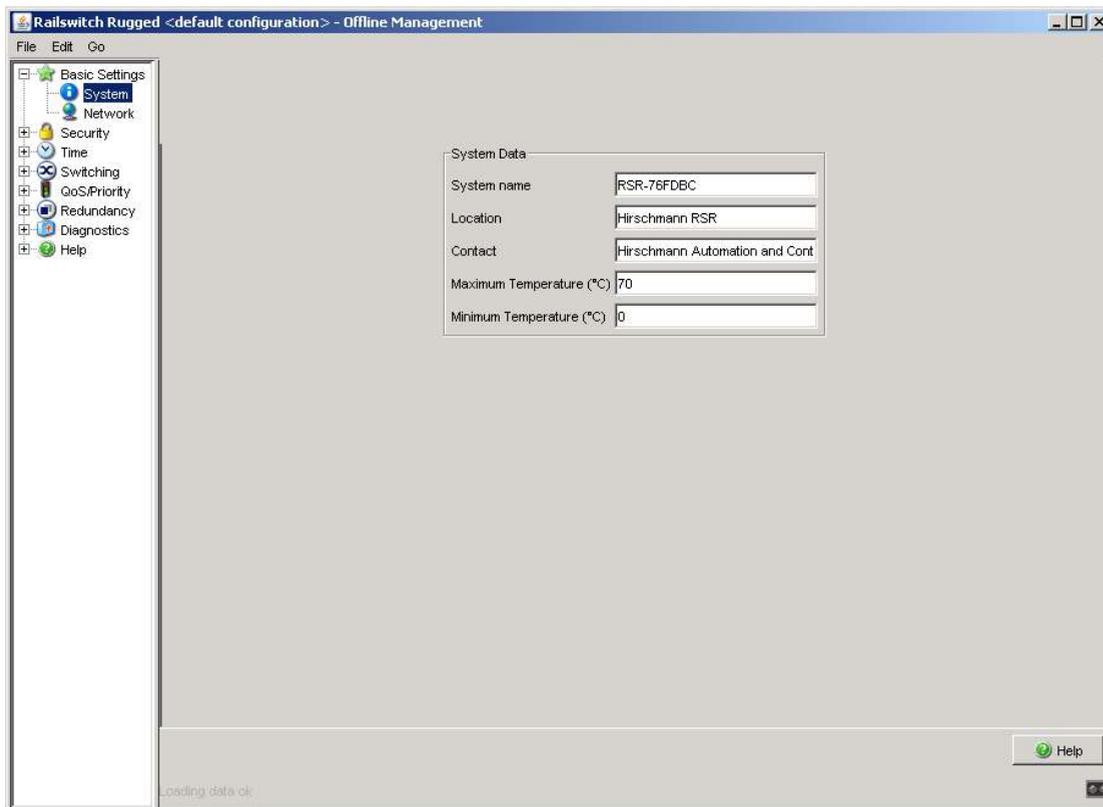


Figure 16: Basic Settings Dialog: System in the Offline Configurator

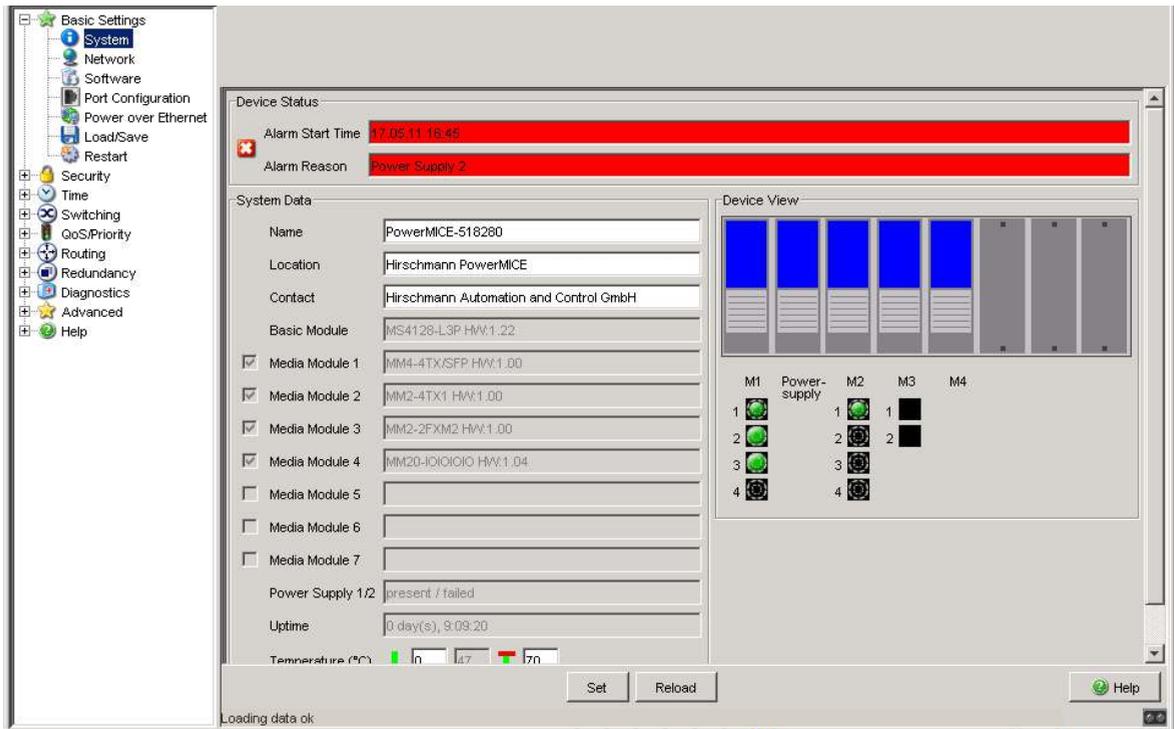


Figure 17: Basic Settings Dialog: System in the Graphical User Interface

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 22](#).

- 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 18: 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.

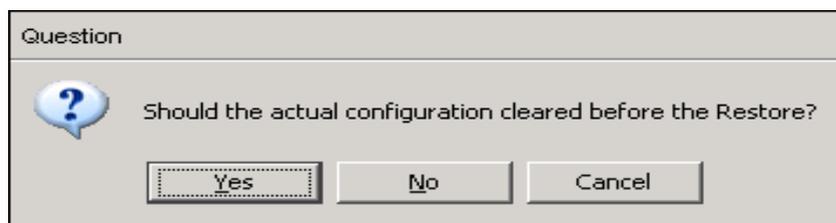


Figure 19: Query - Resetting Configuration

- 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)
hmSvsStrEnable	1	"1"	noError (0)

Figure 20: 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 16: 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 16: Information - Configuration - Tables View

Text View

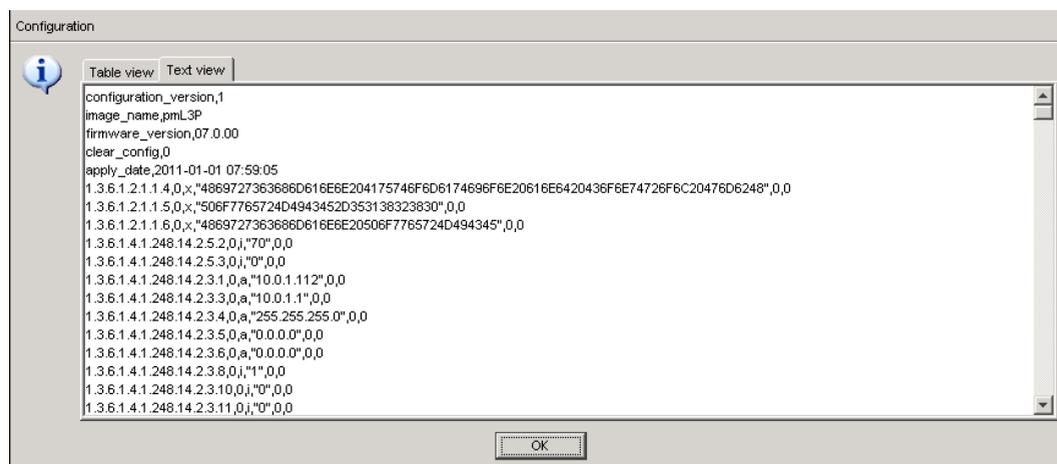


Figure 21: Information - Configuration - Text View

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 16](#), "SNMP Error" parameter)
- ▶ The last parameter has the value of 0. It is included for future expansions.

1.8.2 Saving the Configuration

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

- ▶ save the current configuration on the device,
- ▶ save the current configuration in binary form in a file under the specified URL, or as an editable and readable script,
- ▶ save the current configuration in binary form or as an editable and readable script on the PC.
- ▶ 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 62 “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 29 “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 22: 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.

1.8.3 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.

1.8.4 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.

1.8.5 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 .

Note: The device saves the configuration, with the exception of its SSH key (see on page 78 “Telnet/Web/SSH Access”). You will find instructions on how to transfer the SSH key of the old device to the new one in the document “Basic Configuration User Manual”, chapter “Replacing defective devices”.

■ 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.

Table 17: ACAstatus

Status	Meaning
notInSync	- The configuration data of the ACA and the device do not match, or only one file exists ^a , or - no configuration file is present on the ACA or on the device ^b .
outOfMemory	The local configuration data is too extensive to be stored on the ACA.
wrongMachine	The configuration data in external memory originates from a different device type and cannot be read or converted.
checksumErr	The configuration data is damaged.

Table 17: ACAstatus

- 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.
- 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.

1.8.6 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 18: Buttons

1.9 Restart

This dialog provides you with the following functions:

- ▶ initiate a cold start or delayed cold start of the device. After the time set has elapsed, 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 or delayed warm start of the device. After the time set has elapsed, the device checks the software in the volatile memory and restarts. If a warm start is not possible, a cold start is automatically performed.
- ▶ abort a delayed restart.
- ▶ 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.

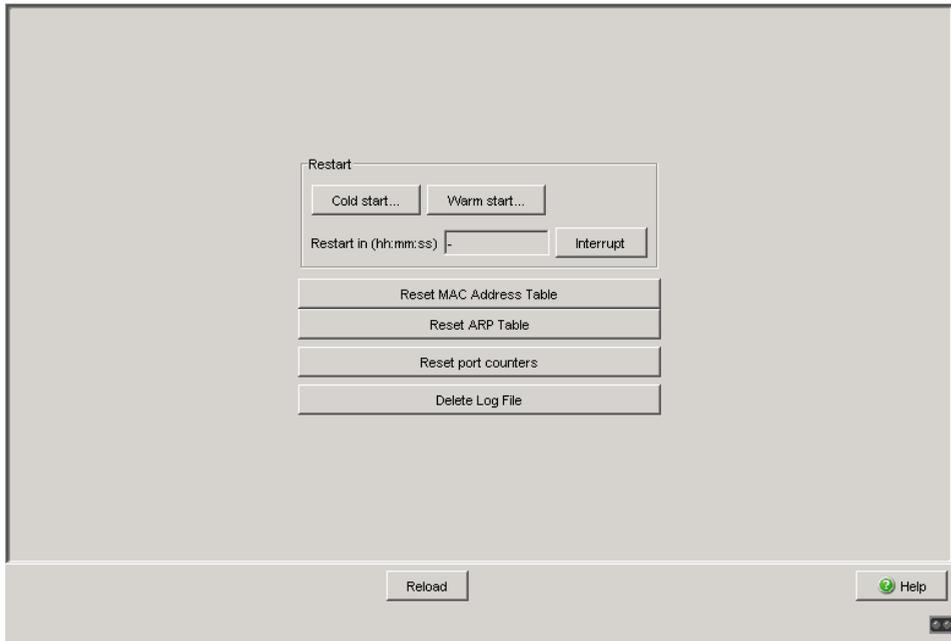


Figure 23: Restart Dialog

Note: Once you select "Cold Start" or "Warm Start", the "Restart" window appears. Here you enter the delay time after which the device performs its restart. The maximum value is 24 d, 20 h, 31 min, 23 s. In order to interrupt the restart procedure, click "Interrupt".

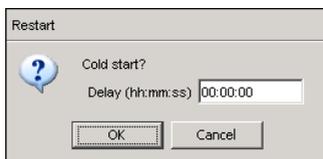


Figure 24: Delayed Restart Dialog

■ 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 19: 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/SSH access
- ▶ Restricted management access
- ▶ Port security
- ▶ 802.1X port authentication
- ▶ RADIUS
- ▶ Login Banner
- ▶ Access Control Lists (ACLs, operation via CLI only)

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.
- When you activate the "Synchronize password to v1/v2 community" function, when the password is changed the device synchronizes the corresponding community name.
- When you change the password for the read/write access, the device updates the readWrite community for the SNMPv1/v2 access to the same value.
 - When you change the password for the read access, the device updates the readOnly community for the SNMPv1/v2 access to the same value.

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

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

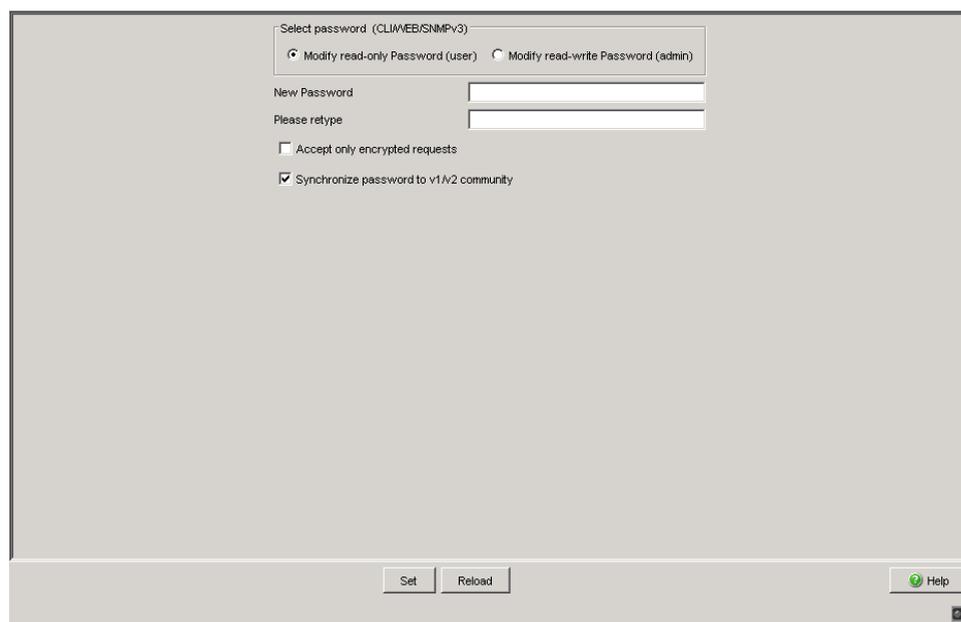


Figure 25: Dialog Password/SNMP Access

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, SSH or Telnet client in a separate dialog.

See [“Telnet/Web/SSH Access” on page 78](#).

Access at IP address level is restricted in a separate dialog.

See [“SNMPv1/v2 Access Settings” on page 74](#).

■ 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 20: 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.

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.

- When you change the readWrite community, the device updates the SNMPv3 password for the read/write access to the same value.
- When you change the readOnly community, the device updates the SNMPv3 password for the read access to the same value.
- ▶ 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.

The screenshot shows the SNMPv1/v2 Access Dialog. At the top, there is a 'Configuration' section with three checkboxes: 'SNMPv1 enabled' (checked), 'SNMPv2 enabled' (checked), and 'Synchronize community to v3 password' (unchecked). Below this is a table with the following data:

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"/>

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

Figure 26: 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 21: Buttons

2.3 Telnet/Web/SSH Access

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

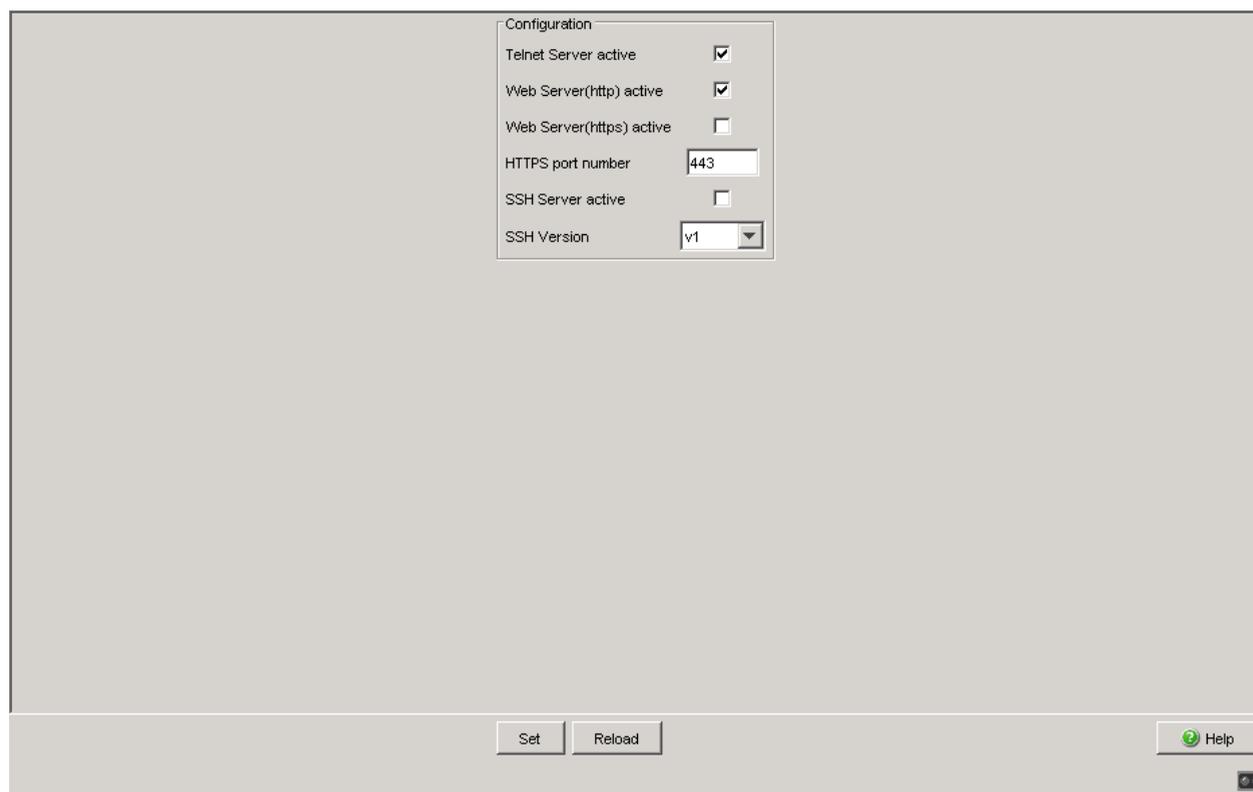


Figure 27: Telnet/Web/SSH Access dialog

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
Web server (HTTPS) active	Activates or deactivates the https service (Web server) for this device.	On Off	Off

Table 22: Telnet/Web/SSH Access

Parameters	Meaning	Possible values	Default setting
HTTPS port number	Enter the port number of the https Web server for the https access to the device.	1..65535	443
SSH server active	Activates or deactivates the SSH service (SSH access) for the device.	On Off	Off
SSH version	Defines the SSH protocol version for the device.	v1 v2 v1 & v2	v1 & v2

Table 22: Telnet/Web/SSH 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.

2.3.3 Description of Web Access (https)

The Web server of the device allows you to configure the device by using the graphical user interface via https (Hypertext Transfer Protocol Secure). In order to use the RADIUS server for authentication, activate the HTTPS function.

If you activate HTTPS and HTTP, the device redirects you to a HTTPS connection. Furthermore, if you change the HTTPS Port during an active HTTPS session, in order for the device to use the new port, deactivate and reactivate HTTPS.

You can open up to 16 http/https connections at the same time.

- To enable the https access to the device,
 - set the checkmark in the field `Web server (https) active`.
 - In the field `HTTPS Port Number`, enter the port number of the https Web server.
- To prevent https access to the device, remove the checkmark in the field `Web server (https) active`.

The HTTPS access to the Web server of the device is deactive in the default setting, and the port number of the https Web server is 443.

By deactivating the Web server you prevent a new login via a Web browser with https. The login in the open browser window remains active.

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

2.3.4 Description of SSH Access

The device's SSH server allows you to configure the device using the Command Line Interface (in-band). You can deactivate the SSH server to prevent SSH access to the device.

The server is deactivated in its default setting.

After the SSH server has been deactivated, you will no longer be able to access the device via a new SSH connection. If an SSH 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 SSH server.

Note: To be able to access the device via SSH, you require a key. If no key is present, the device generates a random key (see the "Basic Configuration 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 23: Buttons

2.4 Restricted Management Access

This dialog allows you to differentiate (restrict) the management access to the device based on IP address ranges and individual management services.

When you activate this function, you can only use the specified IP address ranges to access the management services activated for these address ranges. The device rejects all other requests. You can make up to 16 entries in the list, permit or forbid specific management access for each address range, and activate or deactivate the individual entries separately.

The following management services support restricted management access:

- ▶ http
- ▶ https
- ▶ snmp
- ▶ telnet
- ▶ ssh

Note: The CLI access via the V.24 interface is excluded from the function and cannot be restricted.

Note: You require the http or https service to start the graphical user interface in a browser.

Afterwards, you require the snmp service to access the device with the graphical user interface. When you start the graphical user interface outside the browser, you only require snmp.

In the default setting, the restricted management access is deactivated. In this case, anyone with the correct administrator logon data has access to all management services.

If you have activated the function, and if there is at least one active entry whose IP address range matches the request and for which the requested management service is allowed, the device processes the request. Otherwise the device rejects it.

In the default setting, the device provides you with a default entry with the IP address 0.0.0.0, the netmask 0.0.0.0 and all the management services. This allows access to services from any IP address. This allows you access to the device, even if a restriction is activated, for example to initially configure the function. You have the option to change or delete this entry.

When you create a new entry, this entry also has these preset properties.

Note: If you activate the function and no entry in the table permits your current access, then you can no longer access the management of the device once you write these settings to the device. If no entry allows access, nobody has access to the device management. In this case, use the CLI access via V.24 to access the management of the device.

Parameters	Meaning	Possible values	Default setting
Operation	Switches the function on and off for the device.	On Off	Off
Index	Sequential number of the entry. When you delete an entry, this leaves a gap in the numbering. When you create a new entry with the Web-based interface, the device fills the first gap.	1 - 16	1 (the preset entry).
IP Address	Together with the netmask, defines the network area for which this entry applies.	Valid IPv4 address or 0.0.0.0	0.0.0.0 (for all newly created entries)
Netmask	Together with the IP address, defines the network area for which this entry applies.	Valid IPv4 netmask or 0.0.0.0	0.0.0.0 (for all newly created entries)
HTTP	Activates or deactivates the http service (Web server) for this entry.	On Off	On (for all newly created entries)
HTTPS	Activates or deactivates the https service (Web server) for this entry.	On Off	On (for all newly created entries)

Table 24: Restricted management access

Parameters	Meaning	Possible values	Default setting
SNMP	Activates or deactivates the SNMP service (SNMP access) for this entry.	On Off	On (for all newly created entries)
Telnet	Activates or deactivates the Telnet service (Telnet access) for this entry.	On Off	On (for all newly created entries)
SSH	Activates or deactivates the SSH service (SSH access) for this entry.	On Off	On (for all newly created entries)
Active	Activates or deactivates the entire entry.	On Off	On (for all newly created entries)

Table 24: Restricted management access

Note: An entry with an IP address of 0.0.0.0 together with a netmask of 0.0.0.0 applies for all IP addresses.

Operation

On Off

Index	IP-Address	Netmask	HTTP	HTTPS	SNMP	Telnet	SSH	Active
1	0.0.0.0	0.0.0.0	<input checked="" type="checkbox"/>					

Set Reload Create Remove Help

Figure 28: Restricted Management 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 25: Buttons

2.5 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 26: 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 27: 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 27: Configuration of port security for a single port

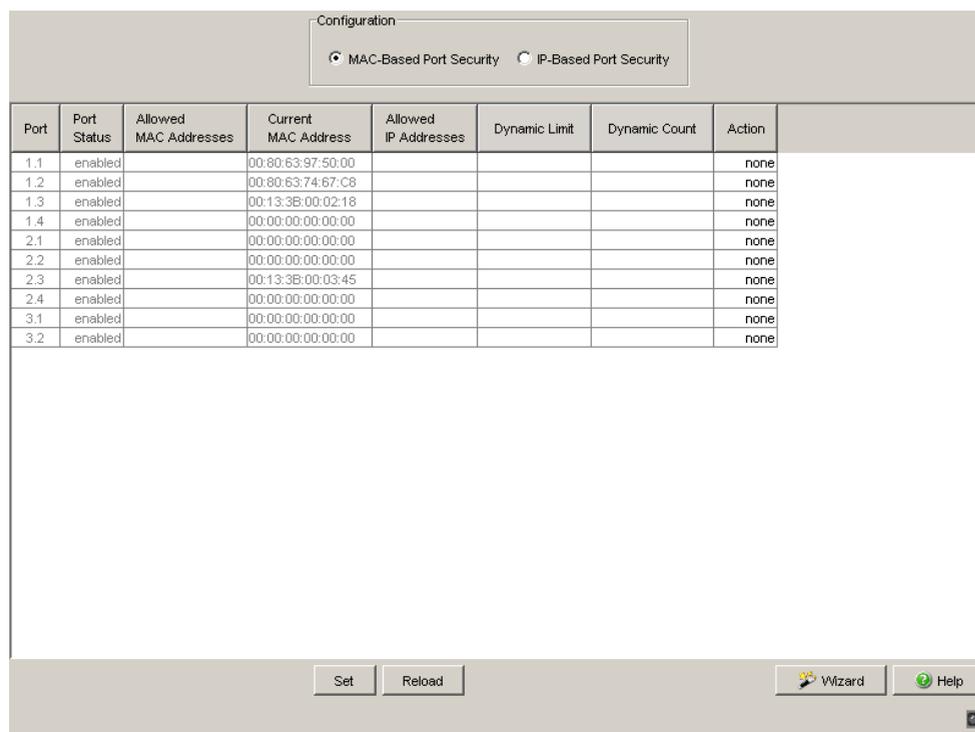


Figure 29: Port Security dialog

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 28: 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 29: 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 30: 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 31: 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 32: Buttons

2.6 802.1X Port Authentication

The 802.1X Port Authentication provides you with the following dialogs:

- ▶ [“802.1X Global Configuration”](#)
- ▶ [“802.1X Port Configuration”](#)
- ▶ [“802.1X Port Clients”](#)
- ▶ [“802.1X Port Statistics”](#)

The port-based network access control is a method described in norm IEEE 802.1X to protect IEEE 802 networks from unauthorized access. The protocol controls the access on a port by authenticating and authorizing a terminal device that is connected to this port of the device.

The 802.1X Port Authentication function requires that you configure a RADIUS Server for authentication and authorization. The authentication and authorization are carried out by the authenticator, in this case the device. The device authenticates the supplicant (the querying device, e.g. a PC), which means that it permits the access to the services it provides (e.g. access to the network to which the device is connected), or else refuses it. In the process, the device accesses an external authentication server (RADIUS server), which checks the authentication data of the supplicant. The device exchanges the authentication data with the supplicant via the Extensible Authentication Protocol over LANs (EAPOL), and with the RADIUS server via the RADIUS protocol.

2.6.1 802.1X Global Configuration

The Global dialog allows you to:

- ▶ activate or deactivate the port authentication,
- ▶ control the VLAN assignment via RADIUS.

Parameters	Meaning	Possible values	Default setting
Operation	Switches the function on or off	On, Off	Off
Activating the VLAN assignment	<p>Activates or deactivates the assigning of a VLAN ID via the RADIUS server to a port.</p> <p>If a device places a query to a port via 802.1X, the RADIUS server will optionally send along a VLAN ID when a positive response is returned. If you have activated the function, the Switch then incorporates the port as an untagged member in the VLAN specified and sets the port VLAN ID to this value.</p> <p>Note the following information about VLAN assignment.</p>	On, Off	Off

Table 33: 802.1X Port Security Dialog, Part 1

Note:

► **For the MACH 1040 device:**

► **For other devices:**

The Switch can assign untagged frames to a VLAN per port. If you:

- use the multi-client setting for a port and
- the Switch has already set up a port VLAN for the existing client, then the Switch will only accept an additional client after that:
- if the RADIUS server assigns the same VLAN ID to it.

If the VLAN ID is different for the new client, the Switch decides on the basis of the client's authentication priority which client it gives access to: A client that authenticates itself via 802.1X has a higher priority than a client with access to the guest or unauthenticated VLAN.

- If a client authenticates with a lower priority, the Switch denies access to the client with the lower priority and continues to give access to the client with the higher priority.
- If a client authenticates with a higher priority, the Switch blocks the hitherto existing access to the client with the lower priority and instead gives access to the client with the higher priority.

Parameters	Meaning	Possible values	Default setting
Activate Dynamic VLAN Creation	Assigns the Switch to create the VLAN designated by the RADIUS server, provided it does not yet exist.	On Off	Off
Activate Safe VLAN mode	<p>For the device families other than MACH 104 and MACH 1040:</p> <p>Sets whether the Switch only gives access to a safe VLAN to a client that sends untagged frames or whether it may assign to the client a different one than the VLAN specified by the RADIUS server.</p> <ul style="list-style-type: none"> ▶ On: The Switch only gives the client access to the VLAN whose ID the RADIUS server specifies. If the Switch finds a conflict between the existing port VLAN ID and the one specified by the RADIUS server, then the Switch sets the port VLAN ID that the client with the higher authentication priority requires (see above). The Switch denies access to the client with the lower priority. ▶ Off: If the Switch finds a conflict between the existing port VLAN ID and the one specified by the RADIUS server, the Switch ignores the VLAN ID specified by the RADIUS server and gives the client access to the VLAN of the port VLAN ID (native VLAN ID). 	On Off	Off

Table 34: 802.1X Port Security Dialog, Part 2

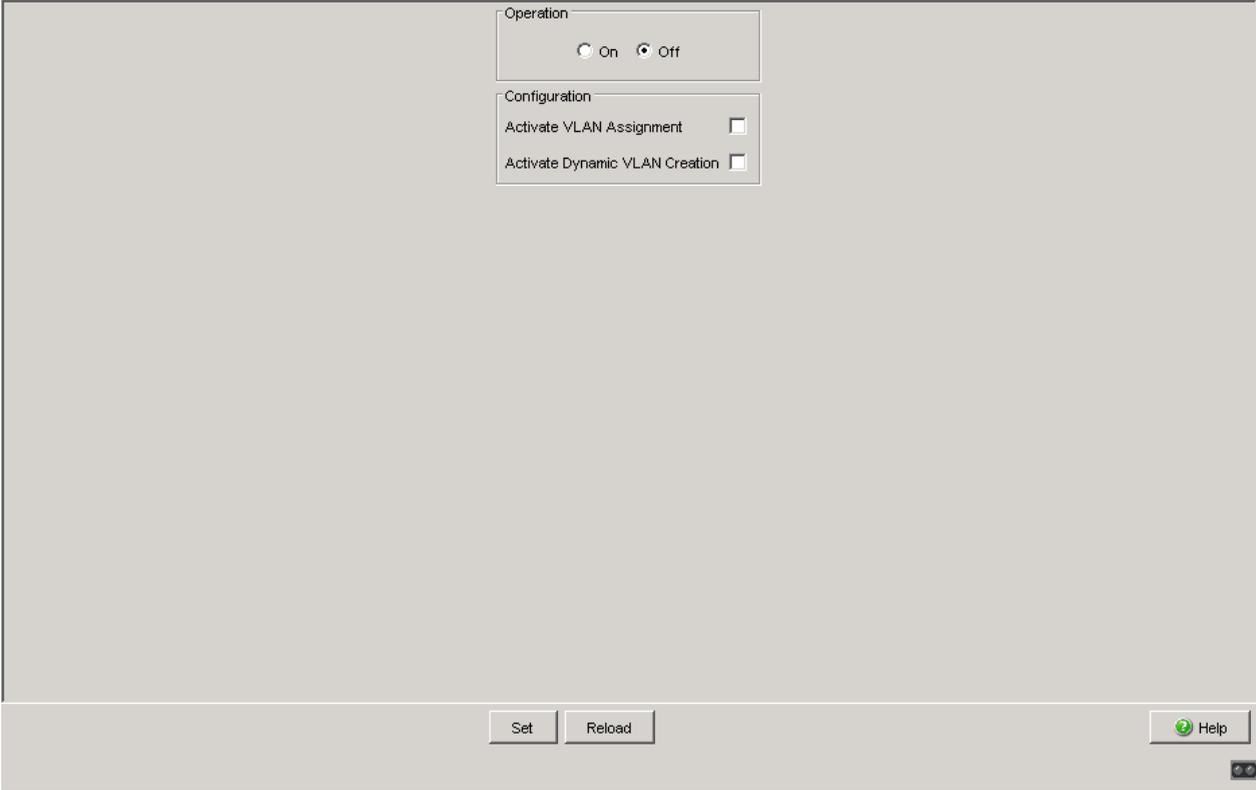


Figure 30: 802.1X Global Dialog for the MACH 104 and MACH 1040 device families

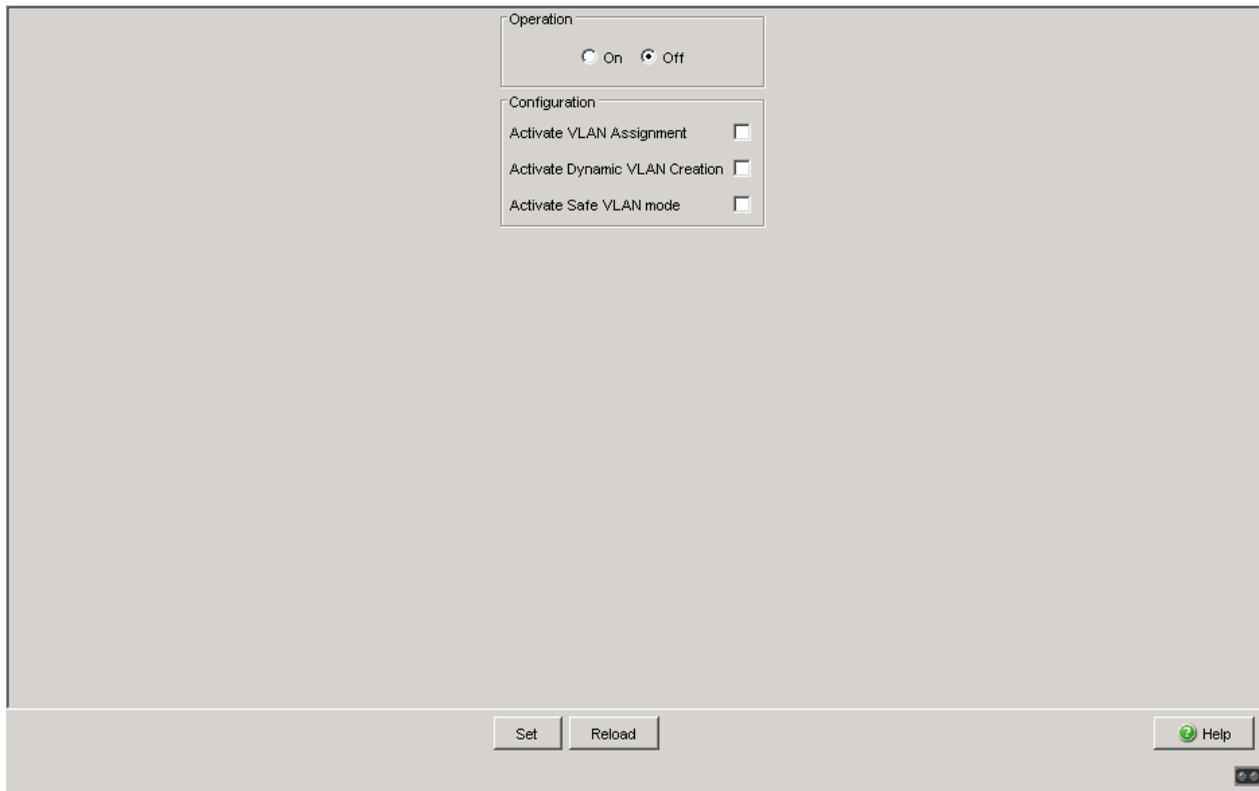


Figure 31: 802.1X Global Dialog

Preparing the device for the 802.1X port authentication:

- Configure the device's IP parameters.
- Activate the 802.1X port authentication function globally.
- Set the 802.1X "Port Control" to `auto`. The default setting is `forceAuthorized`.
- Configure a RADIUS server for authorization and authentication.

■ 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 35: Buttons

2.6.2 802.1X Port Configuration

Port	Port Initialization	Port Reauthentication	Authentication Activity	Backend Authentication State	Authentication State	Maximum Users	Port Control	Quiet Period	Transmit Period	Supplicant Timeout Period
3.2	false	false	initialize	initialize		16	forceAuthorized	60	30	30
3.1	false	false	initialize	initialize		16	forceAuthorized	60	30	30
2.4	false	false	initialize	initialize		16	forceAuthorized	60	30	30
2.3	false	false	initialize	initialize		16	forceAuthorized	60	30	30
2.2	false	false	initialize	initialize		16	forceAuthorized	60	30	30
2.1	false	false	initialize	initialize		16	forceAuthorized	60	30	30
1.4	false	false	initialize	initialize		16	forceAuthorized	60	30	30
1.3	false	false	initialize	initialize		16	forceAuthorized	60	30	30
1.2	false	false	initialize	initialize		16	forceAuthorized	60	30	30
1.1	false	false	initialize	initialize		16	forceAuthorized	60	30	30

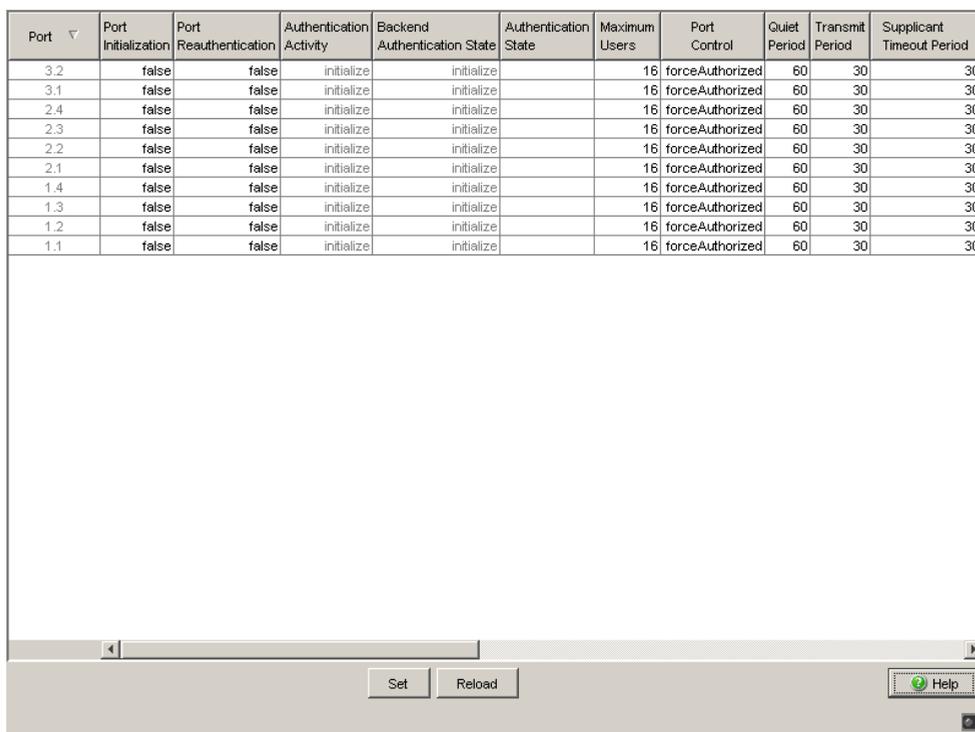


Figure 32: 802.1X Port Configuration Table

Parameter	Meaning	Possible values	Default setting
Port Initialization	Reset the initialization function. Setting this attribute to "true" causes the device to reset the function for this port. When the resetting process is concluded, the value is reset to "false".	true, false	false
Port Reauthentication	Activating and deactivating the reauthentication of the port. Setting this attribute "true" causes the device to ask the supplicant to reauthenticate itself on this port. The device resets the value to "false" following a reauthentication.	true, false	false
Authentication Activity	Displays the current status of the authentication activity.	1 = initialized 2 = disconnected 3 = connecting 4 = authenticating 5 = authenticated 6 = aborting authenticating 7 = temporarily not authenticated (held) 8 = access without authentication (force authorized) 9 = no access (force unauthorized)	
Backend Authentication State	Displays the current status of the authentication server.	1 = request 2 = response 3 = success 4 = fail 5 = timeout 6 = idle 7 = initialize	
Authentication State	Displays the current value of the authentication status for the port.	authorized = the connected subscriber is authenticated unauthorized = the connected subscriber is not authenticated	
Maximum Users	Maximum number of clients that the device authenticates on a port at the same time. This parameter is effective if you have set the port control (see below) to macBased.	1 - 16	16

Table 36: 802.1X Setting Options per Port, entries in the configuration table

Parameter	Meaning	Possible values	Default setting
Port Control	<p>Setting for the port access control.</p> <p>Note:</p> <ul style="list-style-type: none"> ▶ In the <code>ForceAuthorized</code>, <code>ForceUnauthorized</code> and <code>auto</code> modes the Switch opens or blocks the port for all clients. Use these modes if you are connecting a single client to the Switch. ▶ In the <code>macBased</code> mode the Switch authenticates the clients based on the individual MAC addresses and allows or blocks their data traffic separately. Use this mode if you want to use multi-client authentication or the “MAC Authentication Bypass” function. 	<ul style="list-style-type: none"> ▶ <code>ForceAuthorized</code>: Access is also available for all clients without authentication. ▶ <code>ForceUnauthorized</code>: Access is blocked for all clients, even for clients with authentication. ▶ <code>auto</code>: Access to the port depends on the result of the authentication. ▶ <code>macBased</code>: Behavior like for <code>auto</code>. Access is also available for clients with a MAC address which the client uses in the course of authentication. 	<code>ForceAuthorized</code>
Quiet Period	Period in seconds in which the authentication process does not expect authentication from the supplicants.	0-65535	60
Transmit Period	Wait period before the device resends an EAP packet.	1-65535	30
Supplicant Timeout Period	Excess time in seconds for the communication between the device and the supplicant.	1-65535	30
Server Timeout	Excess time in seconds for the communication between the device and the server.	1-65535	30
Max. Request Constant	Maximum number of request attempts to the supplicants before the authentication process terminates.	1-10	2

Table 36: 802.1X Setting Options per Port, entries in the configuration table

Parameter	Meaning	Possible values	Default setting
Assigned VLAN ID	<p>VLAN that the Switch assigned to the port. The port is an untagged member in this VLAN and the port VLAN ID has the same value.</p> <p>Prerequisite: The port control is set to auto.</p> <p>Note: If you are using the multi-client setting by setting “Port Control” to <code>macBased</code>, take into account:</p> <ul style="list-style-type: none"> ▶ the device-dependent resolution of possible VLAN assignment conflicts for untagged received frames; (see on page 94 “802.1X Global Configuration”) ▶ the VLANs assigned, you can find the current values in the “Port Clients” table . (see on page 106 “802.1X Port Clients”) 	0 - 4094	0
Assignment Reason	<p>Reason for assigning the VLANs to the port.</p> <p>Prerequisite: The port control is set to auto.</p> <p>Note: If you are using the multi-client setting by setting “Port Control” to <code>macBased</code>, take into account:</p> <ul style="list-style-type: none"> ▶ the device-dependent resolution of possible VLAN assignment conflicts for untagged received frames; (see on page 94 “802.1X Global Configuration”) ▶ the VLANs assigned, you can find the current values in the “Port Clients” table . (see on page 106 “802.1X Port Clients”) 	notAssigned radius unauthenticatedVLAN	notAssigned

Table 36: 802.1X Setting Options per Port, entries in the configuration table

Parameter	Meaning	Possible values	Default setting
Reauthentication Period	Time in seconds after which the device requests another authentication from the supplicant.	1-65535	3600
Reauthentication Enabled	Enabling or disabling reauthentication	Selected (on), Not selected (off)	Not selected (off)
Guest VLAN ID	<p>ID of a VLAN that the Switch assigns to the port, if:</p> <ul style="list-style-type: none"> ▶ the 802.1X protocol is active on the port and the port control is set to <code>auto</code> or <code>macBased</code>, ▶ a client wants to receive data traffic and EAPOL frames from the client fail to appear, i.e. the client does not support the 802.1X protocol. <p>The Switch:</p> <ul style="list-style-type: none"> ▶ switches the port to the authenticated state, ▶ allows data traffic, ▶ but only to the guest VLAN. <p>Specify a guest VLAN ID if you want to allow devices without 802.1X support access to a guest VLAN.</p> <p>Note:</p> <ul style="list-style-type: none"> ▶ Use only as a guest VLAN a VLAN that you have set up statically in the Switch. ▶ However, if a client connects via 802.1X and his authentication fails, then the Switch only gives him access to the unauthenticated VLAN. ▶ When you activate the MAC Authorized Bypass (MAB) function, the device automatically sets the guest VLAN ID to 0. 	0 - 4094	0
Guest VLAN Period	Time that the Switch waits for EAPOL frames after connecting a device on this port in order to determine whether it supports the 802.1X protocol. If this time elapses, the Switch only provides access to the guest VLAN for the device connected.	1 - 300 s	90 s

Table 36: 802.1X Setting Options per Port, entries in the configuration table

Parameter	Meaning	Possible values	Default setting
Unauthenticated VLAN ID	<p>ID of a VLAN that the Switch assigns to the port, if:</p> <ul style="list-style-type: none"> ▶ the 802.1X protocol is active on the port, ▶ the Switch receives EAPOL frames from the client, i.e. the client supports the 802.1X protocol, ▶ and the client's authentication fails. <p>The Switch:</p> <ul style="list-style-type: none"> ▶ switches the port to the authenticated state, ▶ allows data traffic, ▶ but only to the unauthenticated VLAN. <p>Specify a VLAN ID for unauthenticated devices, if:</p> <ul style="list-style-type: none"> ▶ you want to allow devices access to a particular VLAN, ▶ these devices do indeed support 802.1X, ▶ but their identity and authenticity are unknown to your network. 	0 - 4094	0
<p>Note:</p> <ul style="list-style-type: none"> ▶ Use only as an unauthenticated VLAN a VLAN that you have set up statically in the Switch. 			

Table 36: 802.1X Setting Options per Port, entries in the configuration table

Parameter	Meaning	Possible values	Default setting
MAC Authorized Bypass Enable	<p>The Switch makes authenticated access available via MAB, if:</p> <ul style="list-style-type: none"> ▶ You have set the “Port Control” to <code>macBased</code>, ▶ a device wants to receive data traffic employing a particular known MAC address, ▶ this device does not authenticate itself via 802.1X and ▶ the RADIUS server recognizes the MAC addresses authorized to access. <p>The Switch:</p> <ul style="list-style-type: none"> ▶ waits for the guest VLAN interval to elapse in order to do this, ▶ then sends a query to the RADIUS server and in doing so uses the MAC address as the user name and the password. <p>Activate this function, if:</p> <ul style="list-style-type: none"> ▶ you want to allow particular devices normal access, ▶ however these devices do not support 802.1X. <p>Note:</p> <ul style="list-style-type: none"> ▶ If the RADIUS server denies the MAB authentication, the Switch blocks the access for the device. ▶ When you activate the function, the device automatically deactivates guest VLAN access. 	<p>On</p> <p>Off</p>	Off

Table 36: 802.1X Setting Options per Port, entries in the configuration table

■ 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 37: Buttons

2.6.3 802.1X Port Clients

The device enables you to operate several devices on one port (e. g. via a hub) and to authenticate these devices separately (multi-client authentication).

This means that the Switch allows data traffic for an authenticated device, but at the same time denies data traffic for still unauthenticated devices attempting both to send and to receive.

This applies equally to devices whose authentication has expired and whose renewal is outstanding.

A device can also log out of the authenticated state and is then blocked by the Switch for its data traffic without this affecting other authenticated devices' data traffic. In doing so the Switch differentiates the devices based on their MAC sender address.

You can authenticate up to 16 devices separately on one port.

The dialog shows you the authenticated devices' data per port.

Port	User Name	MAC Address	Assigned VLAN ID	Assignment Reason	Session Timeout	Termination Action

Figure 33: 802.1X Port Client Table

Parameter	Meaning	Possible values	Default setting
Port	Module and port numbers to which this entry applies	-	-
User Name	The name by which the client (in the role of the IEEE 802.1X supplicant) is identified vis-à-vis the Switch	The user name of the IEEE 802.1X supplicant	-
MAC Address	The client's MAC address	Unicast MAC Address	-

Table 38: 802.1X Setting Options per Port, entries in the port client table

Parameter	Meaning	Possible values	Default setting
Assigned VLAN ID	The VLAN ID that the 802.1X protocol assigned the port after the 1st client's successful authentication	0 - 4094	-
<p>Note: If you are using the multi-client setting by setting "Port Control" to <code>macBased</code>, take into account:</p> <ul style="list-style-type: none"> ▶ the device-dependent resolution of possible VLAN assignment conflicts for untagged received frames; (see on page 94 "802.1X Global Configuration") ▶ the VLANs assigned, you can find the current values in the "Port Clients" table . (see on page 106 "802.1X Port Clients") 			
Assignment Reason	Reason for assigning the VLANs to the client.	default, radius, unauthenticatedVlan, invalid	-
Session Timeout	Duration of the client's authenticated session after authentication or reauthentication in seconds	0 - 65535 s (0: no timeout)	-
Termination Action	Action that the Switch performs when the client's session elapses	default, reauthenticate ?	-

Table 38: 802.1X Setting Options per Port, entries in the port client table

■ 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 39: Buttons

2.6.4 802.1X Port Statistics

Port	EAPOL Received Frames	EAPOL Transmitted Frames	EAPOL Start Frames	EAPOL Logoff Frames	EAPOL Response/ID Frames	EAPOL Response Frames	EAPOL Request/ID Frames
1.1	0	0	0	0	0	0	0
1.2	0	0	0	0	0	0	0
1.3	0	0	0	0	0	0	0
1.4	0	0	0	0	0	0	0
2.1	0	0	0	0	0	0	0
2.2	0	0	0	0	0	0	0
2.3	0	0	0	0	0	0	0
2.4	0	0	0	0	0	0	0
3.1	0	0	0	0	0	0	0
3.2	0	0	0	0	0	0	0

Figure 34 shows a screenshot of a web-based interface displaying the 802.1X Statistics Table. The table lists statistics for various ports (1.1 to 3.2) across eight categories: EAPOL Received Frames, EAPOL Transmitted Frames, EAPOL Start Frames, EAPOL Logoff Frames, EAPOL Response/ID Frames, EAPOL Response Frames, and EAPOL Request/ID Frames. All values in the table are 0. Below the table, there is a 'Reload' button and a 'Help' button.

Figure 34: 802.1X Statistics Table

Parameters	Meaning
EAPOL Received Frames	Number of EAPOL frames (both valid and invalid) of any type that have been received at this port.
EAPOL Transmitted Frames	Number of EAPOL frames of any type that have been received at this port.
EAPOL Start Frames	Number of EAPOL start frames that have been received at this port.
EAPOL Logoff Frames	Number of EAPOL logoff frames that have been received at this port.
EAPOL Response/ID Frames	Number of EAPOL resp/ID frames that have been received at this port.
EAPOL Response Frames	Number of valid EAP response frames (other than resp/ID frames) that have been received at this port.
EAPOL Request/ID Frames	Number of EAPOL req/ID frames that have been transmitted at this port.
EAPOL Request Frames	Number of EAPOL Request frames (other than Request/ID frames) that have been transmitted at this port.

Table 40: 802.1X Statistics Table

Parameters	Meaning
EAPOL Invalid Frames	Number of EAPOL frames with a frame type that is not recognized that have been transmitted at this port.
EAPOL Error Frames	Number of EAPOL frames with an invalid packet body length field that have been transmitted at this port.
EAPOL Frame Version	The protocol version number carried in the last EAPOL frame received at this port.
EAPOL Frame Source	The MAC source address of the last received EAPOL frames 00:00:00:00:00:00 means: no frames received yet.

Table 40: 802.1X Statistics Table

■ 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 41: Buttons

2.7 RADIUS

With its factory settings, the device authenticates users based on the local user management. However, as the size of a network increases, it becomes more difficult to keep the login data of the users consistent across the devices.

RADIUS (Remote Authentication Dial-In User Service) allows you to manage the users at a central location in the network. A RADIUS server performs the following tasks here:

- ▶ Authentication
The authentication server authenticates the users when the RADIUS client at the access point forwards the users' login data to the server.
- ▶ Authorization
The authentication server authorizes logged in users for selected services by assigning various parameters for the relevant end device to the RADIUS client at the access point.

The device forwards the users' login data to the primary authentication server. The authentication server decides whether the login data is valid and transfers the user's authorizations to the device.

The menu contains the following dialogs:

- ▶ [Global](#)
- ▶ [RADIUS Server](#)

2.7.1 Global

In this dialog you configure the device to send user requests to the RADIUS Server for service. If you configure multiple servers and requests sent to the primary server remain unanswered, then the device sends the requests to the next active RADIUS server.

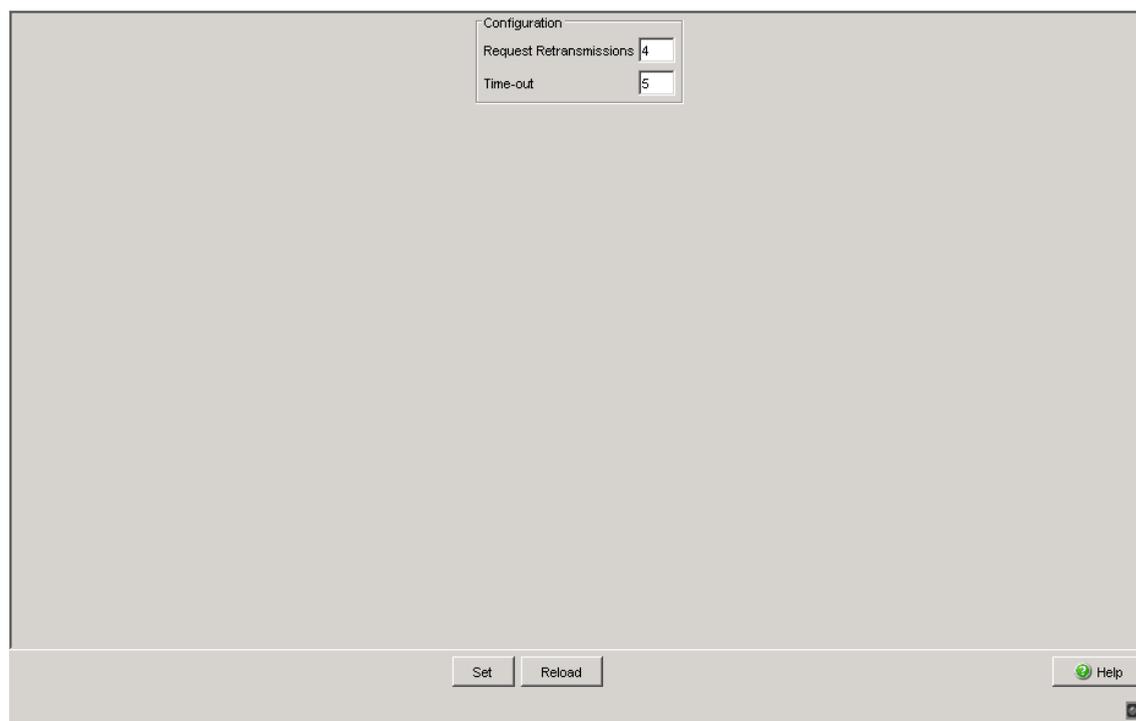


Figure 35: Security:RADIUS:Global dialog

■ Configuration

Parameters	Meaning	Possible values	Default setting
Request Retransmissions	Specify how often the Switch resubmits an unanswered request to the RADIUS server before it sends the request to another RADIUS server.	1 - 15	4
Time-out	Sets how long (in seconds) the Switch waits for a response from the RADIUS server before it resends the request.	1 - 30 s	5 s

Table 42: Security:RADIUS:RADIUS 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 43: Buttons

2.7.2 RADIUS Server

This dialog allows you to define up to 3 RADIUS servers. A RADIUS server authenticates and authorizes the users when the device forwards the login data to the server.

The device sends the login data to the specified primary server. If the server does not respond, the device contacts the next server in the table.

Address	UDP Port	Shared Secret	Primary Server	Selected Server
10.0.1.2	1812		<input type="checkbox"/>	<input checked="" type="checkbox"/>

Set Reload Create Remove Help

Figure 36: Security:RADIUS:RADIUS Server dialog for the Power MICE

Address	UDP Port	Shared Secret	Primary Server	Selected Server
10.0.1.1	1812		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
10.0.1.2	1812		<input type="checkbox"/>	<input type="checkbox"/>
10.0.1.3	1812		<input type="checkbox"/>	<input type="checkbox"/>

Buttons: Set, Reload, Create, Remove, Help

Figure 37: *Security:RADIUS:RADIUS Server dialog for the MACH 1040 family*

■ Table

Parameters	Meaning
Address	Specifies the IP address of the server. Possible values: ▶ Valid IPv4 address
UDP Port	Specifies the number of the UDP port on which the server receives requests. Possible values: ▶ 0..65535 (default setting: 1812) Exception: Port 2222 is reserved for internal functions.
Shared Secret	Defines the password with which the device logs in to the server. To change the password for a server, double click in the relevant password field. After storing the password, the device displays ***** (asterisks). Possible values: ▶ 1..20 alphanumeric characters You get the password from the RADIUS server administrator.

Table 44: *Table in the Security:RADIUS:RADIUS Server dialog*

Parameters	Meaning
Primary Server	<p>Specifies the authentication server as primary or secondary.</p> <p>Possible values:</p> <ul style="list-style-type: none"> ▶ Selected The server is specified as the primary authentication server. The device sends the login data for authenticating the users to this authentication server. If you select multiple servers, the device specifies the last server selected as the primary authentication server. ▶ Not selected (default setting) The server is specified as the secondary authentication server. The device sends the login data to the secondary authentication server if it does not receive a response from the primary authentication server.
Selected Server	<p>Shows the connection to an active server.</p> <p>Possible values:</p> <ul style="list-style-type: none"> ▶ Selected The connection is active. The device sends the login data for authenticating the users to this server if the preconditions named above are fulfilled. ▶ Not selected The connection is inactive. The device does not send any login data to this server.

Table 44: Table in the *Security:RADIUS:RADIUS Server 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 <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.
Remove	Removes the selected table entry.
Help	Opens the online help.

Table 45: Buttons

■ RADIUS Server Settings

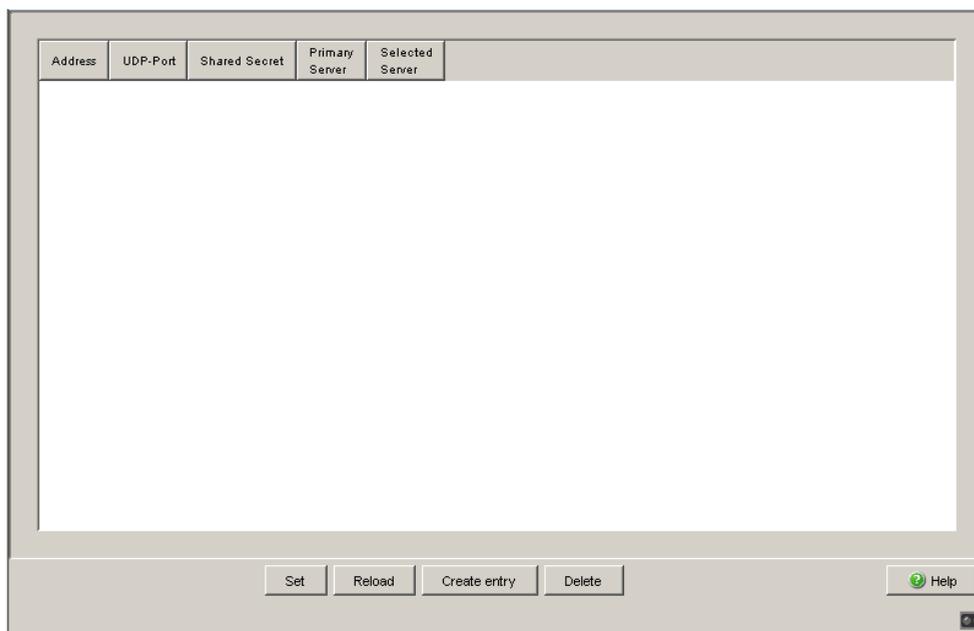


Figure 38: RADIUS Server Dialog

This dialog allows you to enter the data for up to three RADIUS servers.

- Click “Create” to display the dialog window for entering the IP address of a RADIUS server, and to enter this.
- Confirm the entered IP address with “OK”. This creates a new row in the table for this RADIUS server.
- In the “UDP Port” column you enter the UDP port for the RADIUS server (the default setting is 1812).
- In the “Shared secret” column you enter the character string which you get as a key from the administrator of your RADIUS server.
- With “Primary server” you name this server as the first server which the device should contact for port authentication queries. If this server is not available, the device contacts the next server in the table.
- “Selected server” shows the server to which the device actually sends its queries.
- With “Delete” you delete the selected row in the table.

Note: The Switch protects the password during the transfer to the RADIUS server by sending an MD5 checksum instead of the password.

2.8 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](#)

2.8.1 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.

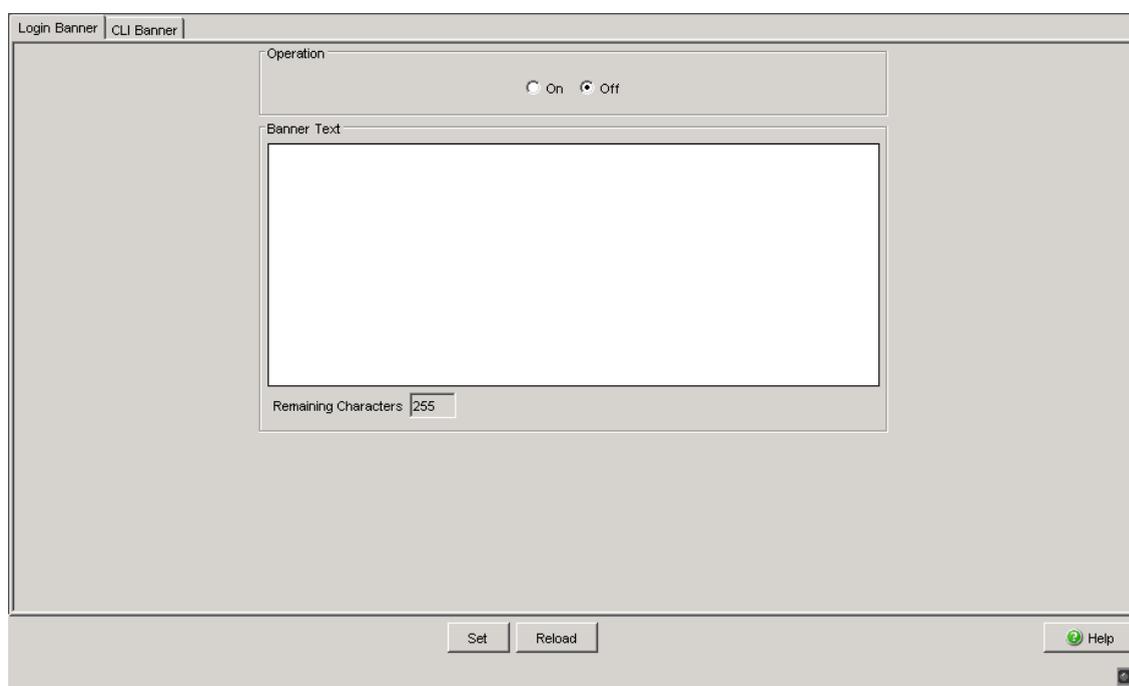


Figure 39: "Login/CLI Banner" dialog, "Login Banner" tab

■ 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

2.8.2 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.

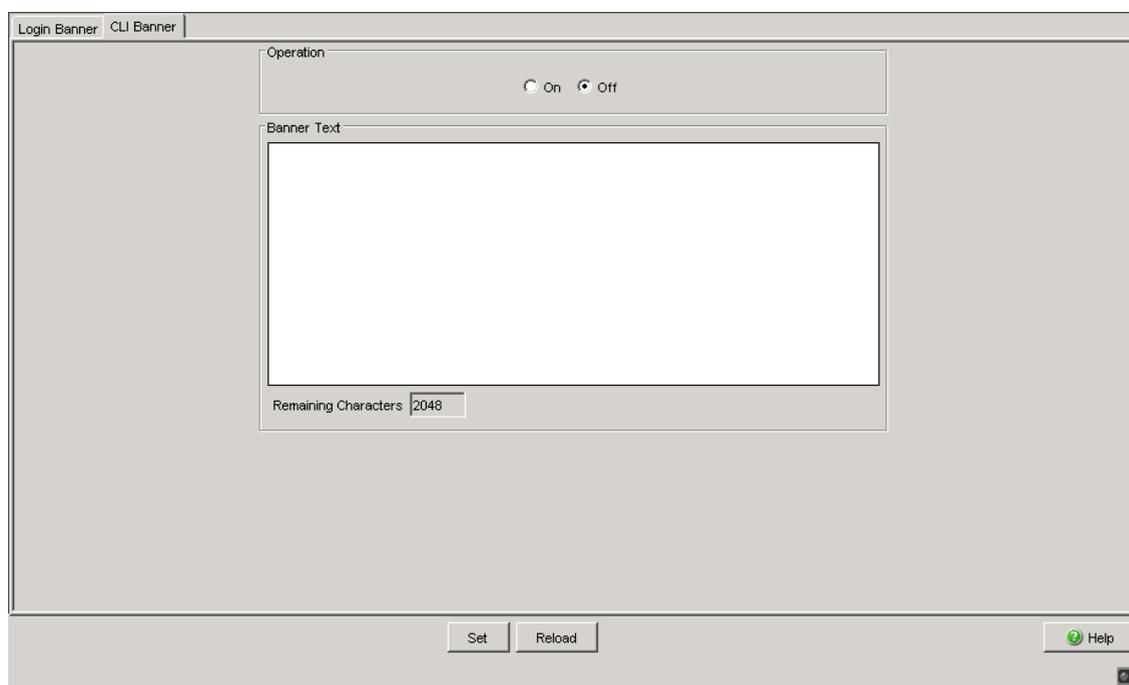


Figure 40: "Login/CLI Banner" dialog, "CLI Banner" tab

■ 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 46: Buttons

2.9 Access Control Lists (ACLs)

Access Control Lists offer the possibility to select incoming data packets based on L2 and L3 criteria and to treat them accordingly, e.g., to drop or to prioritize them.

By means of ACLs, you can realize security- as well as Quality-of-Service-(QoS-) functions in a simple manner.

You can define the conditions that the device uses to select a particular packet type in a fine-grained manner with an ACL. This also applies to the actions that the device executes if the condition matches.

You configure Access Control Lists via the Command Line Interface.

You will find details on this in the document “Reference Manual Command Line Interface”.

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.

The device is equipped with a buffered hardware clock. This keeps the current time

- ▶ if the power supply fails or
- ▶ if you disconnect the device from the power supply.

Thus the current time is available to you again, e.g. for log entries, when the device is started.

The hardware clock bridges a power supply downtime of 1 hour. The prerequisite is that the power supply of the device has been connected continually for at least 5 minutes beforehand.

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.

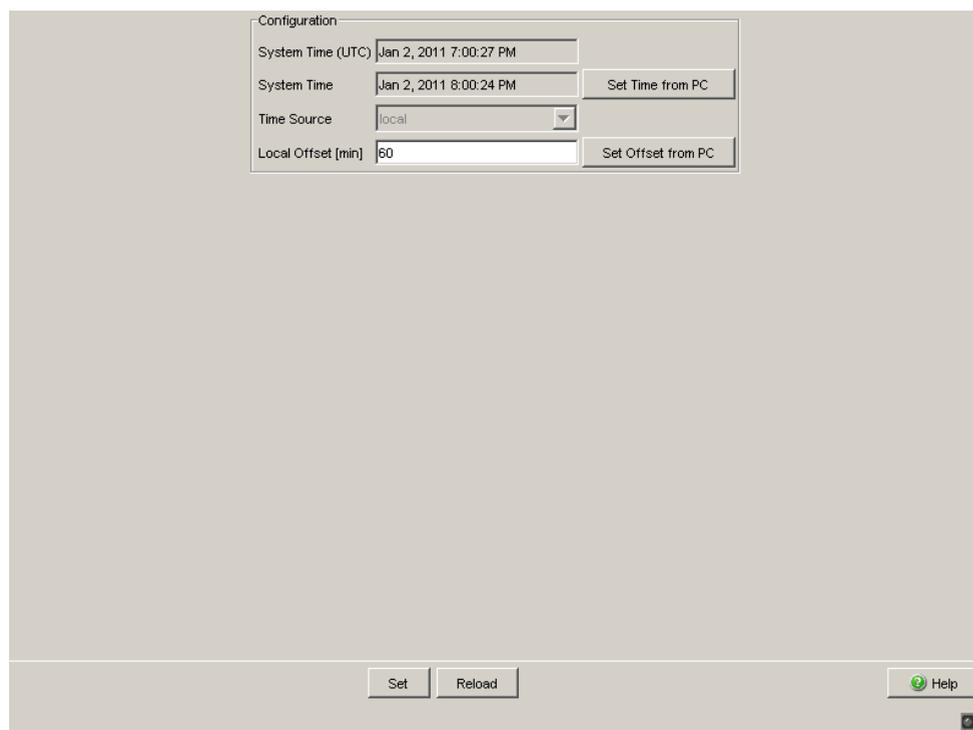


Figure 41: Time Dialog:Basic Settings

■ 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 47: 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 48: Switches SNTP on and off globally

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

Table 49: 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 50: 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 52).	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 51: 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 52: Destination address classes for SNTP and NTP packets

Figure 42: 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 53: 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

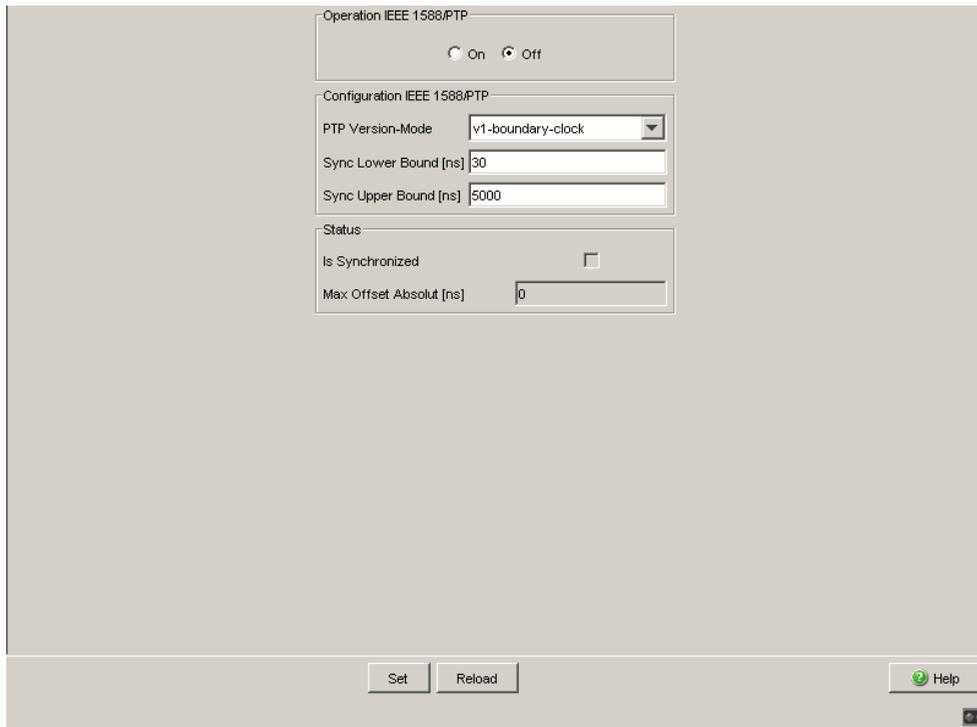
support the modes:

- 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.



The screenshot shows a configuration window titled "Operation IEEE 1588/PTP". It contains three main sections:

- Operation IEEE 1588/PTP:** A radio button interface with "On" selected and "Off" unselected.
- Configuration IEEE 1588/PTP:** A dropdown menu for "PTP Version-Mode" set to "v1-boundary-clock", and two text input fields for "Sync Lower Bound [ns]" (value: 30) and "Sync Upper Bound [ns]" (value: 5000).
- Status:** A checkbox for "Is Synchronized" (unchecked) and a text input field for "Max Offset Absolut [ns]" (value: 0).

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

Figure 43: PTP Global Dialog

Note: The MACH 104 device supports PTP only on ports for data rates of 10 Mbit/s, 100 Mbit/s and 1 Gbit/s.

Note: The MACH 104 and MACH 1040 devices support a maximum sync receive rate of 8 frames/s.

Note: The MACH 1140 and MACH 1142 devices support PTP only on front ports 1 - 16.

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 133 and [“Devices with PTP hardware support”](#) on page 134.

Table 54: 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 55: 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 56: 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 133](#) and [“Devices with PTP hardware support” on page 134](#).

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 133 and “Devices with PTP hardware support” on page 134.</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 133 and “Devices with PTP hardware support” on page 134.</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 57: 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 58: 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 59: 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 60: 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 61: 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 62: 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 63: 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. off: One synchronization run is performed in a synchronization interval.	on off	off

Table 64: 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 64: 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 65: 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 66: 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 67: IEEE 1588/PTPv2 BC Status

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

Table 68: 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 68: 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 69: 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 70: 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 70: 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 71: 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 72: 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	
Sync Interval [s]	Port is in PTP slave mode.	slave	
	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 143 "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 72: 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 72: 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 185 "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	4

Table 72: 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 73: 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 74: 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 143 “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)	
	<p>For the MACH 104 and MACH 1040 devices: Such as E2E with the following characteristics:</p> <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)	
	<p>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.</p>	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 75: 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 75: 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 185 “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	4

Table 75: 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 76: 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 77: 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 78: 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 78: 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 79: 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 ≥ 30 s.	10-630	30
Activate Flow Control	Activate/deactivate the flow control	On, Off	Off

Table 80: 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
	<p>Note: If routing is active, the device prevents the address learning from being switched off.</p> <p>When you activate routing, the device automatically activates the address learning.</p>		
Frame size	Set the maximum packet size (frame size) in bytes. Select the larger value if you want the device to transmit packets with double VLAN tagging. This allows you, for example, to operate the device in networks with MPLS switches/routers.	MACH 104, MACH 1040: 1522, 1552, 9022 PowerMICE, MACH 4000: 1522, 1552	1522
Activate Address Relearn Detection	Enable/disable whether the device detects whether it has repeatedly learned the same MAC source addresses at different ports. This process very probably indicates a loop situation in the network. If the device detects this process, it creates an entry in the log file and sends an alarm (trap).	On, Off	Off
Address Relearn Threshold	Number of 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 82).	On, Off	On

Table 81: 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
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 82: Evaluation of non-matching of the duplex mode

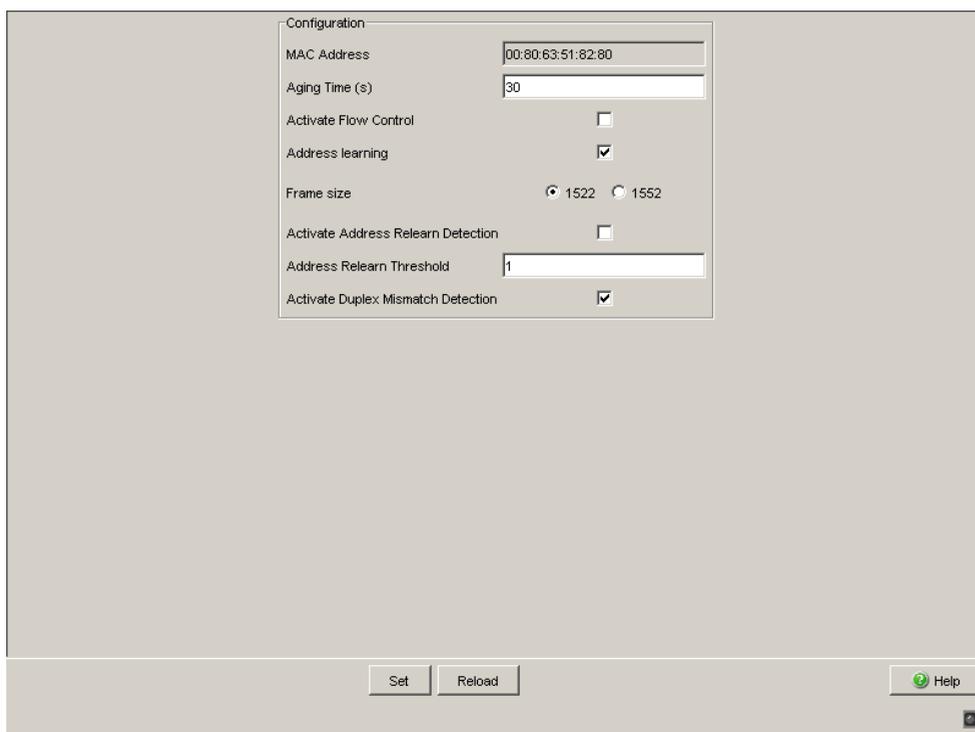


Figure 44: Dialog Switching Global

■ 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.

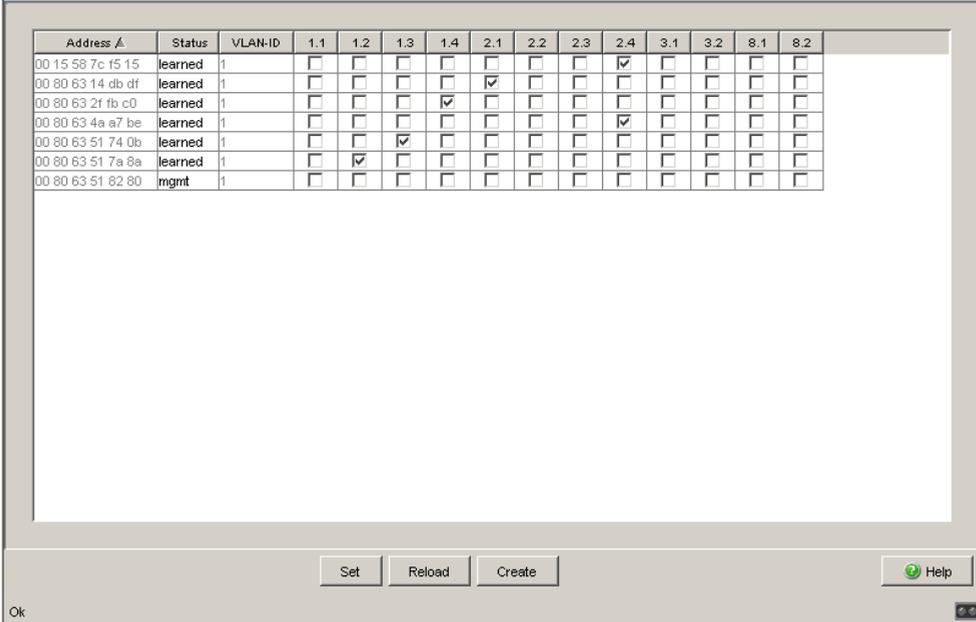
Table 83: Buttons

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 51 “Load/Save”](#)).
- ▶ `gmrp`: The filter was created by GMRP.
- ▶ `gmrp/permanent`: GMRP added further port markings to the filter after it was created by the administrator. The port markings added by the GMRP are deleted by a restart.
- ▶ `igmp`: The filter was created by IGMP 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 45: Filter Table dialog

Note: For Unicast addresses, the device allows you to include multiple ports in a filter entry. Do not include any ports if you want to create a discard filter entry.

Note: For Unicast addresses, the PowerMICE, MACH 1040 and MACH 4000 devices allow you to include multiple ports in a filter entry. Do not include any port 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 84: "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	<p>This column contains the device ports that are assigned to the table entry.</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 85: "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 <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.
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 86: 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.

Note: Ports that are included in a Link Aggregation ([see on page 242 “Link Aggregation”](#)) are excluded from the rate limitation, regardless of the entries in the “Rate Limiter” dialog.

4.3.1 Rate limiter settings (PowerMICE and MACH 4000)

- ▶ "Ingress Limiter (kbit/s)" allows you to enable or disable the ingress limiter function for all ports and to select the ingress limitation on all ports (either broadcast packets only or broadcast packets and Multicast packets).
- ▶ "Egress Limiter (Pkt/s)" allows you to enable or disable the egress limiter function for broadcasts on all ports.

Setting options per port:

- ▶ Ingress Limiter Rate for the packet type selected in the Ingress Limiter frame:
 - ▶ = 0, no ingress limit at this port.
 - ▶ > 0, maximum ingress traffic rate in kbit/s that can be sent at this port.
- ▶ Egress Limiter Rate for broadcast packets:
 - ▶ = 0, no rate limit for egress broadcast packets at this port.
 - ▶ > 0, maximum number of egress broadcasts per second sent at 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 Limiter Rate (kbit/s)	Egress Limit (Pkt/s) Packet Type: BC
1	1	0	0
1	2	0	0
1	3	0	0
1	4	0	0
2	1	0	0
2	2	0	0
2	3	0	0
2	4	0	0
3	1	0	0
3	2	0	0

Figure 46: 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 87: 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 47: 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 88: 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 89: 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 89: IGMP Querier and IGMP settings

- a. Note the connection between the parameters Max. Response Time, Transmit interval and Group Membership Interval ([see table 90.](#))

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 90: 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 91: 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 92: 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 92: 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 <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 93: Buttons

4.4.2 GMRP (GARP Multicast Registration Protocol)

With this dialog you can:

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

Port	GMRP	GMRP Service Requirement
1.1	<input checked="" type="checkbox"/>	Forward all unregistered groups
1.2	<input checked="" type="checkbox"/>	Forward all unregistered groups
1.3	<input checked="" type="checkbox"/>	Forward all unregistered groups
1.4	<input checked="" type="checkbox"/>	Forward all unregistered groups
2.1	<input checked="" type="checkbox"/>	Forward all unregistered groups
2.2	<input checked="" type="checkbox"/>	Forward all unregistered groups
2.3	<input checked="" type="checkbox"/>	Forward all unregistered groups
2.4	<input checked="" type="checkbox"/>	Forward all unregistered groups
3.1	<input checked="" type="checkbox"/>	Forward all unregistered groups
3.2	<input checked="" type="checkbox"/>	Forward all unregistered groups
5.1	<input checked="" type="checkbox"/>	Forward all unregistered groups
5.2	<input checked="" type="checkbox"/>	Forward all unregistered groups
5.3	<input checked="" type="checkbox"/>	Forward all unregistered groups
5.4	<input checked="" type="checkbox"/>	Forward all unregistered groups

Figure 48: Multicasts dialog

■ Operation

In this frame you can:

- ▶ activate/deactivate the GMRP function globally.

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

Table 94: Global setting

■ Multicasts

Note: This feature is available for the following device families: RS20/RS30/RS40, MS20/MS30, RSR20/RSR30, MACH100, MACH1000, OCTOPUS.

In this frame you specify how the device transmits packets with

- ▶ unknown MAC multicast addresses not learned with GMRP.

Prerequisite: The GMRP function is activated globally.

Parameters	Meaning	Possible values	Default setting
Unknown Multicasts	<ul style="list-style-type: none"> ▶ Send to All Ports: The device sends the packets with an unknown MAC Multicast address to all ports. ▶ Discard: The device discards the packets with an unknown MAC Multicast address. 	Send to All Ports Discard	Send to All Ports

Table 95: Unknown Multicasts

■ Settings per Port (Table)

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

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

Table 96: GMRP settings per port

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

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

■ 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 97: Buttons

4.5 VLAN

At VLAN you can find all the dialogs and views to:

- ▶ configure and monitor the VLAN functions in accordance with the IEEE 802.1Q standard.,
- ▶ for voice devices (e.g. VoIP telephones) per port:
 - define a voice VLAN network policy that the switch transmits via LLDP-MED to the devices connected,
 - bypass an active 802.1X authentication for voice devices

4.5.1 VLAN Global

With this dialog you can:

- ▶ display VLAN parameters
- ▶ activate/deactivate the VLAN 0 transparent mode
- ▶ activate/deactivate GVRP
- ▶ 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 185 “VLAN Static”)
Max. supported VLANs	Displays the maximum number of VLANs (see on page 185 “VLAN Static”).
Number of VLANs	Displays the number of VLANs configured (see on page 185 “VLAN Static”).

Table 98: 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 188 “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
GVRP active	Activate “GVRP” to ensure the distribution of VLAN information to the neighboring devices via GVRP data packets.	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 99: 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 PowerMICE, MACH 104, MACH 1040 and MACH 4000:
In “Transparent mode”, the devices ignore the VLAN tags and the priority tag on reception. Set the ports’ VLAN membership for all VLANs to "U" (Untagged).
- ▶ For MACH 4002-24/48G:
In “Transparent mode”, the devices ignore the VLAN tags but evaluate the priority tag. Set the ports’ VLAN membership for all VLANs to "U" (Untagged).

Parameters	Meaning	Possible values	Default setting
Mode	<p>Selecting the VLAN Mode.</p> <p>“Independent VLAN” subdivides the forwarding database (see on page 160 “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.</p> <p>“Shared VLAN” uses the same forwarding database for all VLANs (see on page 160 “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 66 “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 66 “Restart”) on the device, the device take the setting for the “Mode” into the status line.	Independent VLAN, Shared VLAN	

Table 100: Settings and displays in the “Learning” frame

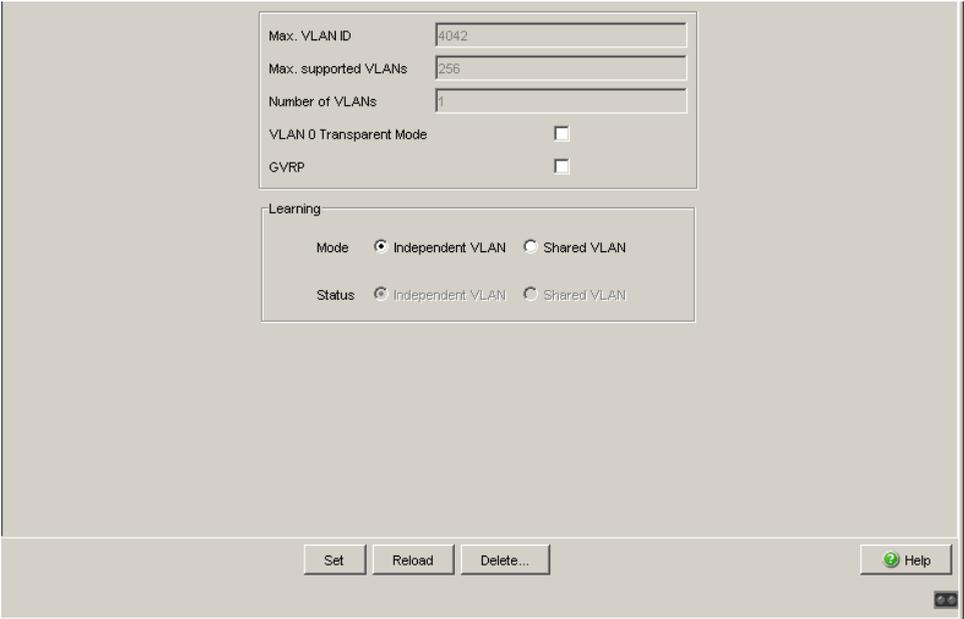


Figure 49: VLAN Global dialog

Configuration

Max. VLAN ID: 4042

Max. supported VLANs: 256

Number of VLANs: 1

VLAN 0 Transparent Mode:

GVRP active:

Double VLAN Tag Ethertype: 0x8100 (802.1q)

Learning

Mode: Independent VLAN Shared VLAN

Status: Independent VLAN Shared VLAN

Buttons: Set, Reload, Clear..., Help

Figure 50: Switching:VLAN:Global dialog (MACH4000 and MACH 1040)

■ 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 101: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
- ▶ VLANs configured via GVRP

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 185 “VLAN Static”](#)).

Note: Ports not displayed are participants in a link aggregation. You can assign these ports to a VLAN using the port assigned to the link aggregation in module 8 (display 8.X).

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 102: 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 51: 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 103: 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. (Up to 256 VLANs possible simultaneously for Power MICE, MACH 104, MACH 1040, MACH 4000.)	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 104: VLAN Static dialog

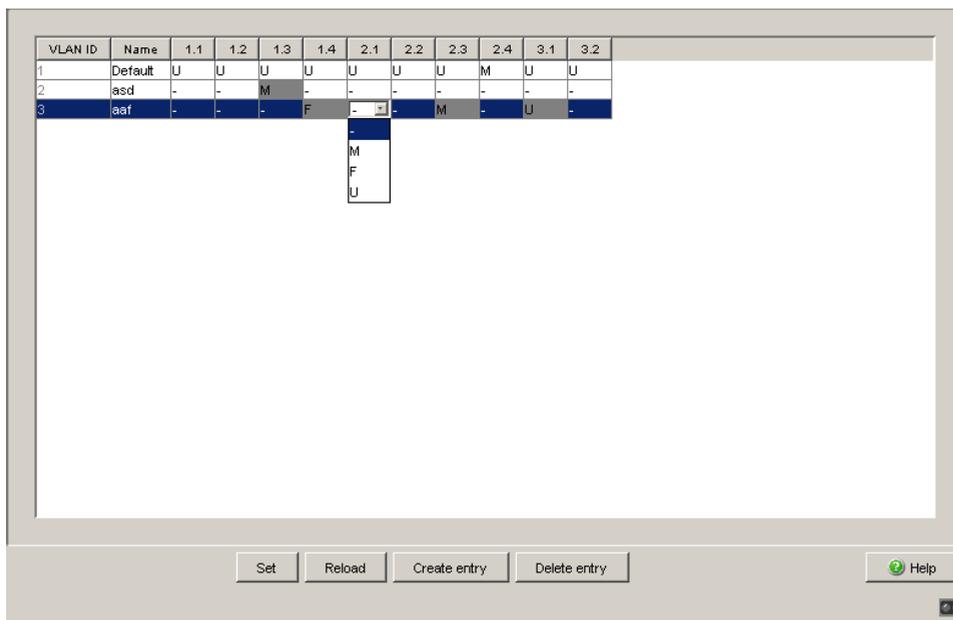


Figure 52: VLAN Static Dialog

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 105: 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 106: Buttons

4.5.4 Port

With this dialog you can:

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

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
Ingress Filtering	Specifies whether the port evaluates the received tags.	on, off	off

Table 107: Switching:VLAN:Port dialog

Parameters	Meaning	Possible values	Default setting
GVRP	<ul style="list-style-type: none"> - on: The device sends and receives GVRP data packets. The device exchanges VLAN configuration data with other devices. - off: The device does not send or receive GVRP data packets. The device does not exchange VLAN configuration data with other devices. 	On (selected), Off (not selected)	Off
DVLAN Tag Mode	<ul style="list-style-type: none"> - normal: The port is not involved in DVLAN tagging. - 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. - 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. 	normal, core, access	normal

Table 107: Switching:VLAN:Port dialog

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

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 252 “Configuring the MRP-Ring”) is not assigned to a VLAN, select the port VLAN ID 1.
 - If the MRP-Ring configuration (see on page 252 “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”.

Port	Port-VLAN-ID	Acceptable Frame Types	Ingress Filtering	GVRP
1.1	1	admitAll	<input type="checkbox"/>	<input checked="" type="checkbox"/>
1.2	1	admitAll	<input type="checkbox"/>	<input checked="" type="checkbox"/>
1.3	1	admitAll	<input type="checkbox"/>	<input checked="" type="checkbox"/>
1.4	1	admitAll	<input type="checkbox"/>	<input checked="" type="checkbox"/>
2.1	1	admitAll	<input type="checkbox"/>	<input checked="" type="checkbox"/>
2.2	1	admitAll	<input type="checkbox"/>	<input checked="" type="checkbox"/>
2.3	1	admitAll	<input type="checkbox"/>	<input checked="" type="checkbox"/>
2.4	1	admitAll	<input type="checkbox"/>	<input checked="" type="checkbox"/>
3.1	1	admitAll	<input type="checkbox"/>	<input checked="" type="checkbox"/>
3.2	1	admitAll	<input type="checkbox"/>	<input checked="" type="checkbox"/>

Figure 53: Switching:VLAN:Port dialog

Port	Port-VLAN-ID	Acceptable Frame Types	Ingress Filtering	GVRP	Double VLAN Tag Mode
1.1	1	admitAll	<input type="checkbox"/>	<input checked="" type="checkbox"/>	normal
1.2	1	admitAll	<input type="checkbox"/>	<input checked="" type="checkbox"/>	normal
1.3	1	admitAll	<input type="checkbox"/>	<input checked="" type="checkbox"/>	normal
1.4	1	admitAll	<input type="checkbox"/>	<input checked="" type="checkbox"/>	normal
1.5	1	admitAll	<input type="checkbox"/>	<input checked="" type="checkbox"/>	normal
1.6	1	admitAll	<input type="checkbox"/>	<input checked="" type="checkbox"/>	normal
1.7	1	admitAll	<input type="checkbox"/>	<input checked="" type="checkbox"/>	normal
1.8	1	admitAll	<input type="checkbox"/>	<input checked="" type="checkbox"/>	normal
1.9	1	admitAll	<input type="checkbox"/>	<input checked="" type="checkbox"/>	normal
1.10	1	admitAll	<input type="checkbox"/>	<input checked="" type="checkbox"/>	normal
1.11	1	admitAll	<input type="checkbox"/>	<input checked="" type="checkbox"/>	normal
1.12	1	admitAll	<input type="checkbox"/>	<input checked="" type="checkbox"/>	normal
1.13	1	admitAll	<input type="checkbox"/>	<input checked="" type="checkbox"/>	normal
1.14	1	admitAll	<input type="checkbox"/>	<input checked="" type="checkbox"/>	normal
1.15	1	admitAll	<input type="checkbox"/>	<input checked="" type="checkbox"/>	normal
1.16	1	admitAll	<input type="checkbox"/>	<input checked="" type="checkbox"/>	normal

Figure 54: Switching:VLAN:Port dialog (MACH4000 and MACH1040)

■ 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 108:Buttons

4.5.5 Voice VLAN

The voice VLAN function enables you to operate voice devices, e.g. VoIP telephone via plug-and-play.

For this purpose, you can use one or several VLANs configured in the Switch as voice VLANs and define voice VLAN network policy per port. The policy consists of the voice VLAN mode, the voice VLAN ID and the voice VLAN priority. The Switch sends it via LLDP-MED to the terminal devices connected.

An LLDP-MED-capable terminal device can then determine the proper settings automatically in order to receive its data traffic.

What is required for this is that you activate at the Switch both the LLDP ([see on page 349 “LLDP Information from Neighbor Devices”](#)) and the LLDP-MED ([see on page 351 “LLDP-MED \(Media Endpoint Discovery\)”](#)).

This dialog allows you to do the following:

- ▶ globally activate or deactivate the transmission of a Switch voice VLAN network policy via LLDP-MED.
- ▶ assign a voice VLAN network policy to a Switch port.
The Switch informs devices that are connected to this port about its voice VLAN network policy via LLDP-MED.
- ▶ assign a voice VLAN ID for the voice VLAN network policy to a Switch port.
The Switch informs devices on this port via LLDP-MED about its voice VLAN network policy's voice VLAN ID.
- ▶ assign a VLAN priority for the voice VLAN network policy to a Switch port.

The Switch informs devices on this port via LLDP-MED about its voice VLAN network policy's voice VLAN priority.

- ▶ explicitly deactivate an already active 802.1X authentication for an LLDP-MED-capable device (e.g. a VoIP telephone) at a Switch port.
 - For active voice authentication, the device connected must first authenticate itself via 802.1X at the Switch. Only then will the Switch allow the device's data traffic on its port.
 - For inactive voice authentication, however, the Switch will ultimately allow the data traffic for a connected device despite an active 802.1X authentication, if - the device has identified itself via LLDP-MED as a voice device, and - the device sends tagged frames with the voice VLAN ID.

Parameters	Meaning	Possible values	Default setting
Frame Operation	Globally activates or deactivates the transmission of a port-specific voice VLAN network policy via LLDP-MED.	On, Off	Off

Note: To transmit the voice VLAN network policy you must have activated both the LLDP (see on page 349 “LLDP Information from Neighbor Devices”) and the LLDP-MED (see on page 351 “LLDP-MED (Media Endpoint Discovery”).

Table 109: Global Settings for the Voice VLAN Dialog

Parameters	Meaning	Possible values	Default setting
Port	Module and port numbers to which this entry applies	-	-
Voice VLAN Mode	<p>Mode of the voice VLAN network policy which the Switch communicates via LLDP-MED to the devices connected.</p> <ul style="list-style-type: none"> ▶ disabled: The Switch does not send a voice VLAN network policy. ▶ none: The Switch sends the voice VLAN network policy of "none", i.e. that the device connected is to use its own configuration. ▶ untagged: The device connected is to send untagged frames. ▶ vlan: The device connected is to send VLAN-tagged frames. ▶ dot1p-priority: The device connected is to send priority-tagged frames (with VLAN ID 0). ▶ vlan & dot1p-priority: The device connected is to send VLAN- and priority-tagged frames. 	disabled, none, untagged, vlan, dot1p-priority, vlan & dot1p-priority	disabled
VLAN ID	VLAN ID of the voice VLAN network policy which the Switch communicates via LLDP-MED to the devices connected.	0 - 4094	0

Note: Use a VLAN ID that is already configured in the Switch. This is how you enable the plug-and-play start-up of a voice device.

Table 110: Settings for the Voice VLAN Dialog

Parameters	Meaning	Possible values	Default setting
Priority	Layer 2 (802.1p) priority of the voice VLAN network policy which the Switch communicates via LLDP-MED to the devices connected.	none, 0 - 7	none
Bypass authentication	<ul style="list-style-type: none"> ▶ On: For active 802.1X authentication, the device connected must first authenticate itself at the Switch. Only then will the Switch allow the device's data traffic on its port. ▶ Off: However, the Switch will ultimately allow the data traffic for a connected device despite an active 802.1X authentication, if <ul style="list-style-type: none"> - the device has identified itself via LLDP-MED as a voice device, and - the device sends tagged frames with the voice VLAN ID. 	On Off	On

Note:

- ▶ If you are using the authentication for a port, activate the 802.1X-based port security at this port ([see on page 99 "802.1X Port Configuration"](#)).
- ▶ If you are using the 802.1X-based port security, connecting more than one device to a port^a and are also using voice authentication, then activate the MAC-based authentication.
- ▶ If you have set MAC- or IP-based port security for this port, it remains active in any case.
- ▶ Only use IP-based port security if the voice device has a secure IP address.

Table 110: Settings for the Voice VLAN Dialog

^a For example, a VoIP telephone with integrated switch, to which you have connected a PC.

Operation
 On Off

Port	Voice VLAN Mode	VLAN-ID	Priority	Authentication active
1.1	disabled	0	none	✓
1.2	disabled	0	none	✓
1.3	disabled	0	none	✓
1.4	disabled	0	none	✓
2.1	disabled	0	none	✓
2.2	disabled	0	none	✓
2.3	disabled	0	none	✓
2.4	disabled	0	none	✓
3.1	disabled	0	none	✓
3.2	disabled	0	none	✓

Figure 55: Voice VLAN 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 111: 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
- ▶ Queue Management

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 116](#)).
 - ▶ 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 114](#)).
- 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).

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.

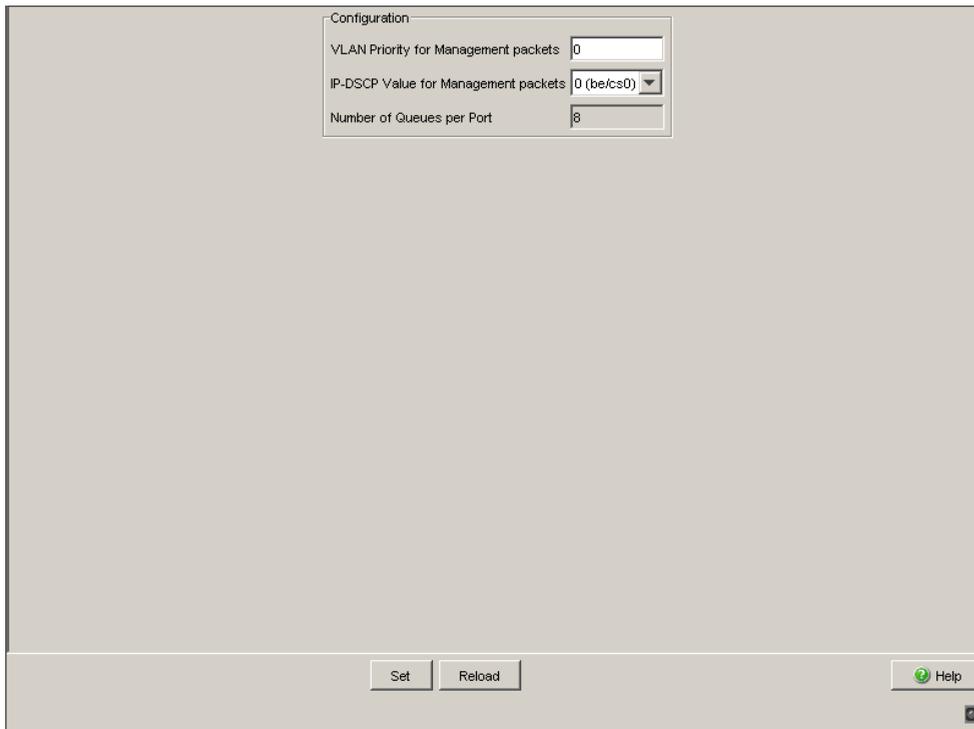


Figure 56: Global dialog

■ 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 112: Buttons

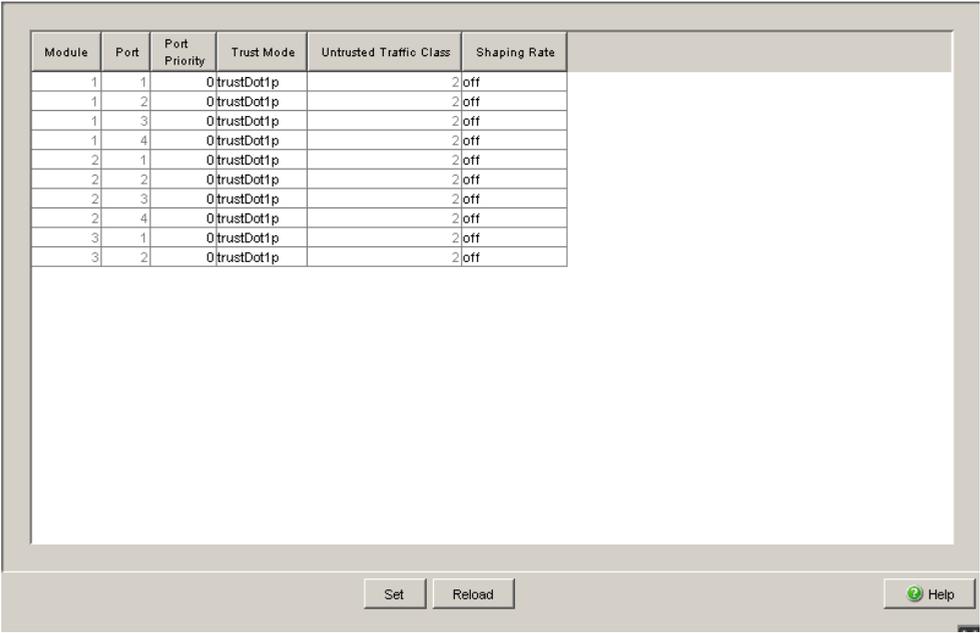
5.2 Port Configuration

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

- ▶ assign a port priority to a port.
- ▶ select the trust mode for a port,
- ▶ display the untrusted traffic class,
- ▶ assign a shaping rate 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.
Trust mode	Select the trust mode.
Untrusted traffic class	Display the traffic class used in the “untrusted” trust mode.
Shaping rate	Select the maximum bandwidth available in %. Range permitted: 0% (off) to 95% in steps of 5%.

Table 113: Port configuration table



The image shows a port configuration dialog window. It features a table with the following columns: Module, Port, Port Priority, Trust Mode, Untrusted Traffic Class, and Shaping Rate. The table contains 12 rows of data. Below the table, there are three buttons: 'Set', 'Reload', and 'Help'.

Module	Port	Port Priority	Trust Mode	Untrusted Traffic Class	Shaping Rate
1	1	0	trustDot1p		2 off
1	2	0	trustDot1p		2 off
1	3	0	trustDot1p		2 off
1	4	0	trustDot1p		2 off
2	1	0	trustDot1p		2 off
2	2	0	trustDot1p		2 off
2	3	0	trustDot1p		2 off
2	4	0	trustDot1p		2 off
3	1	0	trustDot1p		2 off
3	2	0	trustDot1p		2 off

Figure 57: 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 114).

Prerequisite:

setting in the Trust Mode column: `untrusted` or

setting in the Trust Mode column: `trustDot1p` and the data packets do not contain a VLAN tag or

setting in Trust Mode column: `trustIpDscp` and the data packets are not IP packets.

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

Table 114: Assigning the port priority to the traffic classes

5.2.2 Selecting the Trust Mode

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

- ▶ “untrusted”
The device ignores the priority information in the packet and always assigns the packets the port priority of the receiving port.
- ▶ “trustDot1p”:
The device prioritizes received packets that contain VLAN tag information according to this information (assigning them to a traffic class - see [“802.1D/p mapping”](#)).
The device prioritizes received packets that do not contain any tag information (assigning them to a traffic class - see [“Entering the port priority”](#)) according to the port priority of the receiving port .
- ▶ “trustIpDscp”:
The device prioritizes received IP packets (assigning them to a traffic class - see [“IP DSCP mapping”](#)) according to their DSCP value.
The device prioritizes received packets that are not IP packets (assigning them to a traffic class - see [“Entering the port priority”](#)) according to the port priority of the receiving port .
 - ▶ For received IP packets:
The device also performs VLAN priority remarking.
In VLAN priority remarking, the device modifies the VLAN priority of the IP packets if the packets are to be sent with a VLAN tag ([see on page 185 “VLAN Static”](#)).
 - ▶ For received IP packets:
Based on the traffic class to which the IP packet was assigned (see above), the device assigns the new VLAN priority to the IP packet in accordance with [table 118](#).
Example: A received IP packet with a DSCP value of 16 (cs2) is assigned traffic class 1 (default setting). The packet is now assigned VLAN priority 2 in accordance with [table 118](#).

5.2.3 Displaying the untrusted traffic class

“Untrusted traffic class” shows you the traffic class that is used in the “untrusted” trust mode. When you change the port priority ([see on page 202 “Entering the port priority”](#)), the untrusted traffic class also changes ([see table 118](#)).

5.2.4 Shaping rate

The device allows you to limit the maximum bandwidth of a port (traffic shaping).

Click once on a cell in the “Shaping rate” column to select one of the possible values for the bandwidth limit in the range from 5% to 95%, in steps of 5%.

- The value “off” means: no bandwidth limit (0%).
- The value “95” means that 95% of the bandwidth is available.

If the bandwidth set is temporarily exceeded, the device saves the data and sends it when the bandwidth load has decreased again. Traffic Shaping thus smooths out any overload situations.

If Traffic Shaping is active on an interface, the device ignores the bandwidths reserved for Weighted Fair Queuing.

■ 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 115: Buttons

5.3 802.1D/p mapping

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

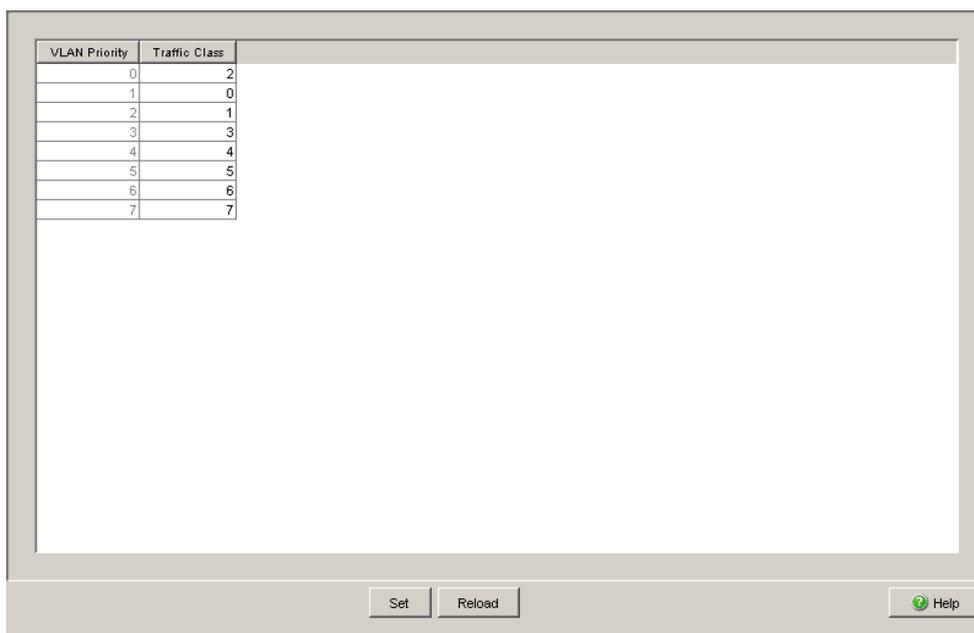


Figure 58: 802.1D/p Mapping dialog

- Enter the desired value from 0 to 7 in the Traffic Class field for every VLAN priority.

VLAN priority	Traffic class (default setting)	IEEE 802.1D traffic type
0	2	Best effort (default)
1	0	Background

Table 116: Assigning the VLAN priority to the 8 traffic classes

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

Table 116: Assigning the VLAN priority to the 8 traffic classes

Note: Network protocols and redundancy mechanisms use the highest traffic class 7. Therefore, select other traffic classes for application data.

■ Buttons

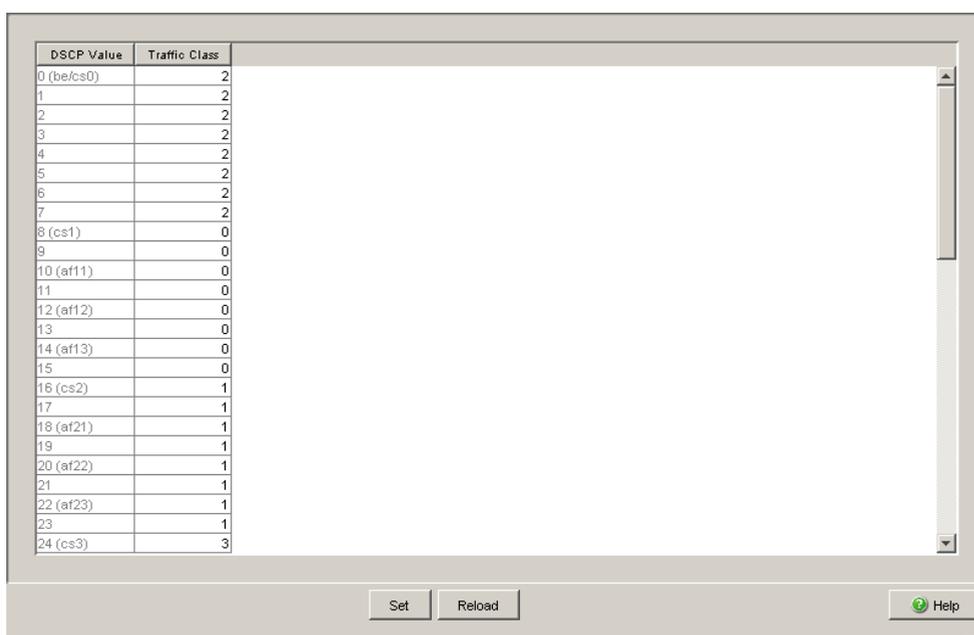
Button	Meaning
Set	Transfers the changes to the volatile memory (RAM) of the device. To permanently save the changes afterwards, you open the <code>Basic Settings:Load/Save</code> dialog and click "Save".
Reload	Updates the fields with the values that are saved in the volatile memory (RAM) of the device.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

Table 117: 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 7 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 59: 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	2
1-7		2
8	CS1	0
9,11,13,15		0
10,12,14	AF11,AF12,AF13	0
16	CS2	1
17,19,21,23		1
18,20,22	AF21,AF22,AF23	1
24	CS3	3
25,27,29,31		3
26,28,30	AF31,AF32,AF33	3
32	CS4	4
33,35,37,39		4
34,36,38	AF41,AF42,AF43	4
40	CS5	5
41,42,43,44,45,47		5
46	EF	5
48	CS6	6
49-55		6
56	CS7	7
57-63		7

Table 118: 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 119: 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 119: Buttons (cont.)

5.5 Queue Management

For every traffic class, the Queue Management table allows you to:

- ▶ enable Strict Priority (= disable Weighted Fair Queuing),
- ▶ disable Strict Priority (= enable Weighted Fair Queuing),
- ▶ enter a value for activated Weighted Fair Queuing for minimum bandwidth,
- ▶ enter a value for the maximum bandwidth,

Note: Disabling Strict Priority for a traffic class also disables Strict Priority for all traffic classes with a lower priority level. Enabling Strict Priority for a traffic class enables Strict Priority for all traffic classes with a higher priority level.

Traffic Class	Strict Priority	Min Bandwidth [%]	Max Bandwidth [%]
0	<input checked="" type="checkbox"/>	0	0
1	<input checked="" type="checkbox"/>	0	0
2	<input checked="" type="checkbox"/>	0	0
3	<input checked="" type="checkbox"/>	0	0
4	<input checked="" type="checkbox"/>	0	0
5	<input checked="" type="checkbox"/>	0	0
6	<input checked="" type="checkbox"/>	0	0
7	<input checked="" type="checkbox"/>	0	0



Figure 60: Queue Management table

5.5.1 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 applications that are time- or latency-critical, such as VoIP or video, Strict Priority enables high-priority data to be sent immediately([see on page 212 “Maximum Bandwidth”](#)).

- In the “Strict Priority” column you enable the function for the desired traffic class.

5.5.2 Weighted Fair Queuing

With Waited Fair Queuing, also called WeightedRoundRobin (WRR), the user assigns a minimum or reserved bandwidth to each traffic class. This ensures that data packets with a lower priority are also sent when the network is very busy.

If you assign Weighted Fair Queuing to every traffic class, the entire bandwidth for the corresponding port is available to you.

The weighting values range from 0% to 100% of the available bandwidth, in steps of 5%.

- ▶ A weighting of 0 is equivalent to a "no bandwidth" setting.
- ▶ The sum of the individual bandwidths may add up to 100%.
- In the “Strict Priority” column you enable the function for the desired traffic class. To do so, you disable “Strict Priority”.
- In the “Minimum Bandwidth” column you enter a value for the desired traffic class.

5.5.3 Maximum Bandwidth

By entering a maximum bandwidth you can limit the bandwidth for each traffic class to a maximum value, regardless of whether you selected "Weighted Fair Queuing" or "Strict Priority".

- ▶ Weighted Fair Queuing (see on page 211 "Weighted Fair Queuing") requires that the maximum bandwidth is at least as big as the minimum bandwidth.
- ▶ With "Strict Priority", individual high-priority packets with low latency are processed (see on page 211 "Strict Priority"). If the maximum bandwidth is configured to a value less than 100%, even data packets will lower traffic classes can be sent in periods of high-priority overloading. The weighting values range from 0% to 100% of the available bandwidth, in steps of 5%.

■ 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 120: Buttons

6 Routing

A router is a node for exchanging data on the layer 3 of the ISO/OSI layer model (network layer).

The Routing section contains the dialogs for configuring the routing function.

6.1 Routing Global

With this dialog you can:

- ▶ switch on the routing function globally.
Default setting: Routing is switched off.
- ▶ display the default TTL (Time To Live).
TTL is a value in an IP data packet. Every router that passes on a data packet reduces this value by 1. The router that receives a data packet with the TTL value 1 rejects the data packet and reports it to the sender, whose IP source address is contained in the IP packet.
If the Switch sends its own data packet, then it sets the TTL value to the default value displayed. Default value: 64.

Note: When you activate routing, the device automatically activates the learning of MAC source addresses . If routing is active, the device prevents the address learning from being switched off.

■ 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 121:Buttons

6.2 Configuring Router Interfaces

With these dialogs you can:

- ▶ Configure port-based and VLAN-based router interfaces.
- ▶ Assign a number of IP addresses for each router interface (multinetting).

6.2.1 Configuration

This dialog allows you to configure the router interfaces. You can:

- ▶ assign an IP address/netmask to a router interface. Enter additional addresses for a router interface in the “Secondary addresses” dialog (multinetting).
- ▶ set up a VLAN-based router interface.
- ▶ switch the routing function for each routing interface on/off.
- ▶ switch the proxy ARP function for each routing interface on/off.
- ▶ switch the net-directed broadcasts function for each routing interface on/off.
- ▶ **For the MACH 104 and MACH 1040 devices:**
enter an IP MTU value for a particular routing interface.

Parameters	Meaning
Module	Module of the Switch on which the port is located. The Switch uses the virtual module 9 for a VLAN-based router interface.
Port	Port to which this entry applies.
Type	Type of the router interface: – Ethernet: physical port – VLAN: VLAN-based router interface

Table 122: Router interface table

Parameters	Meaning
VLAN ID	VLAN ID of the VLAN-based router interface.
IP Address	IP address for this router interface.
Netmask	Netmask for this router interface
Routing	Switches the routing function on and off for this router interface.
Proxy ARP	Switches the proxy ARP function on and off for this router interface.
Netdirected Broadcasts	Switches the Netdirected Broadcasts function on and off for this router interface.
MTU	For the MACH 104 and MACH 1040 devices: Specifies the maximum permissible network packet size. Possible values: 128..9000. The device allows you to configure up to 8 different IP MTU values.

Table 122: Router interface 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.
Remove	Removes the selected table entry.
Wizard	Opens the "Wizard". With the "Wizard" you assign the permitted MAC addresses to a port.
Help	Opens the online help.

Table 123: Buttons

■ **Configuring the port-based router interface**

- Double-click on a cell in the “IP Address” column and enter the IP address for this router interface.
- Double-click on a cell in the “Netmask” column and enter the netmask for this router interface.
- Click once on a cell in the “Routing” column to switch on the routing function for this router interface.
- Click once on a cell in the “Proxy ARP” column to switch on the proxy ARP function for this router interface.
- Click once on a cell in the “Netdirected Broadcasts” column to switch on the Netdirected Broadcasts function for this router interface.

■ **Setting up a VLAN-based router interface**

- Click “Wizard” on the bottom right.
- In the Wizard window,
 - select a row in the table to configure an existing VLAN, or
 - enter a VLAN ID for a new VLAN to be configured.
- Click “Next”.
- In the next Wizard window, enter the name of your choice under “VLAN Name”.
- In the “Member” column select the ports you wish to assign to the VLAN.
- “Untagged”: In this column you select the ports that you want to be members of the VLAN and that will send data packets without a tag.
- “Port VLAN ID”: Double-click on a cell in this column in order to change the port VLAN ID. A tag with this port VLAN ID is added to data packets which this port receives without a tag.
- Click “Next”.
- In the “Primary IP Address” frame you enter the IP address of this router interface and the related netmask.

The “Secondary Addresses/Multinetting” frame enables you to assign additional IP addresses to this router interface. Enter the IP address and the netmask.

Click “Add” to transfer the entry to the table.

Select a row in the table to delete it from the table using “Remove”.
- Click “Finish” to transfer the configured VLAN-based router interface to the router interface table.

You then have the option of configuring additional parameters in the table for the VLAN-based router interface, like with the configuration of port-

based router interfaces.

- Click once on a cell in the “Routing” column to switch the routing function for this router interface on or off.
- Click once on a cell in the “Proxy ARP” column to switch on the proxy ARP function for this router interface.
- Click once on a cell in the “Netdirected Broadcasts” column to switch on the Netdirected Broadcasts function for this router interface.

■ Deleting a router interface

- Select a row and click "Delete". By doing this,
 - you delete the row if it is a VLAN-based entry, or
 - you reset the values in the row if it is a port-based entry.

Note: The prerequisite for resetting the values is the prior deletion of other entries (if present) in the "Secondary Addresses" dialog.

6.2.2 Configuring secondary addresses

When you want to use the multinetting function, this dialog enables you to assign secondary IP addresses to a router interface.

- Use the left mouse-button to select a row that contains the port ID in the first column. Right-click on the selected row and select “Add IP address” to add a secondary IP address/netmask to the router interface.

Note: You have the option to configure up to 31 secondary IP addresses per router interface and a total of up to 1,024 secondary IP addresses per router.

- To delete or edit an existing secondary address, select the appropriate row, right-click on this row, and select “Edit” or “Delete”.

Note: The prerequisite for deletion is that routing has been switched on for this router interface in the “Router Interfaces” dialog.

■ Buttons

Button	Meaning
Reload	Updates the fields with the values that are saved in the volatile memory (RAM) of the device.
Add IP Address	Opens the "Create" dialog. This dialog gives you the option of adding a further IP address to a router interface. Enter the desired value in the "IP Address" and "Netmask" fields. Confirm the entry by clicking on "OK".
Delete IP Address	This dialog gives you the option of deleting an IP address for a router interface. Select an IP address in the list and then click "Delete IP Address".
Help	Opens the online help.

Table 124: Buttons

6.3 ARP

The Address Resolution Protocol (ARP) determines the MAC address that belongs to an IP address.

With this dialog you can:

- ▶ set parameters for the ARP,
- ▶ view statistical values and
- ▶ view the table of the ARP entries, delete the dynamic entries in the ARP table, and configure static entries.

6.3.1 Setting ARP parameters

Parameter	Meaning	Possible Values	Default Setting
Aging Time	With "Aging Time" you specify the time for which an entry remains before being deleted from the table. If there is a data transfer with the device within this time period, then the time measuring begins from the start again.	15-21600 s	1200
Response Time	With "Response Time" you specify how long ARP waits for a response before the query is seen to have failed.	1-10	1
Retries	With "Retries" you specify how often ARP repeats a failed query before stopping the query to this address.	0-10	4

Table 125: ARP parameters

Parameter	Meaning	Possible Values	Default Setting
Cache Size	“Cache Size” enables you to limit the maximum number of entries in the table. When the maximum number is reached, ARP deletes the oldest entry.	PowerMICE: 288-2208 MACH 1040: 284-3328 MACH 4000: 308-2228 MACH 4000 24/48G: 308-2228, extendable to 3868 via CLI	Maximum
Dynamic Renew	When the “Dynamic Renew” is switched on, ARP starts a new query to a device for which the entry has exceeded the aging time. If this query is not answered, the Switch removes the entry from the table.	on/off	on
Selective Learning	In the default setting, the router learns ARP entries passively. This means that the router receives all ARP requests and automatically learns the IP/MAC address assignment of the sending device. The automatic learning of all connected devices means that time-consuming ARP queries are excluded if the router has to send a data packet to an unknown device. In this case, the ARP tables may also be filled with unnecessary ARP entries (e.g. from devices that only wish to communicate locally). If “Selective Learning” is activated, then the router only learns the source IP/MAC address assignment if the ARP request was directed to the router itself (i.e. if the router address was explicitly queried).	on/off	off

Table 125: ARP parameters

6.3.2 ARP Statistics Display

Parameter	Meaning
Total Entry Current Count	Current number of ARP entries in the ARP table
Total Entry Peak Count	Highest number of ARP entries in the ARP table
Static Entry Current Count	Current number of static ARP entries in the ARP table
Static Entry Max. Count	Maximum possible number of static ARP entries in the ARP table

Table 126: ARP Statistics

6.3.3 ARP Table Display

Parameter	Meaning
Module	Router module
Port	Port to which this entry applies.
IP Address	IP address of a device that responded to an ARP query on this port.
MAC Address	MAC address of a device that responded to an ARP query on this port.
Type	Type of entry: – static: static ARP entry that is retained even after the ARP table is deleted. – dynamic: dynamic entry that is deleted from the table after the "Aging Time" if no data is received by this device during this time. – local: IP and MAC address of the device's own port

Table 127: ARP Table

6.3.4 Editing the ARP table

■ Deleting dynamic entries

By clicking on "Reset" you delete the dynamic entries from the ARP table.

■ Editing static entries

Using an assistant, you can add, edit and delete static entries.

The prerequisites for adding static entries are:

- ▶ At least one router interface is configured, is in the network of the static entry and the routing function is switched on ([see on page 215 "Configuration"](#)).
 - ▶ The router interface has at least at one port an active connection.
 - ▶ The routing function is switched on globally ([see on page 214 "Routing Global"](#)).
- Click on "Wizard" to open the Wizard window.
 - To create a new entry, enter the IP address in the format 0.0.0.0 and the MAC address in the format 00:00:00:00:00:00 for a new entry and click on "Add".
 - Select an entry and click "Remove" to delete this entry.
 - Click "Finish" to finish the editing and transfer the changes into the ARP table.
 - Click "Cancel" to finish the editing and reject the changes.

■ 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	Removes the selected table entry.
Reset	Deletes the dynamic entries from the routing APR table.

Table 128: Buttons

Button	Meaning
Wizard	Opens the "Wizard". With the "Wizard" you assign the permitted MAC addresses to a port.
Help	Opens the online help.

Table 128: Buttons (cont.)

6.4 Router Discovery Configuration

ICMP Router Discovery is a procedure for locating possible routers in the network for data transmission. The Switch supports this procedure by transferring presence messages when the function is active.

Parameter	Meaning	Value range	Default setting
Module	Router module	Device dependent	–
Port	Port of the module	Device dependent	–
VLAN ID	VLAN membership of the port	Device dependent	
Advertise Mode	Activate/deactivate the router discovery function at this port	on/off	off
Advertise Address	Destination for sending the presence messages.	Multicast/Broadcast	Multicast

Table 129: Router discovery configuration

■ 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 130: Buttons

6.5 RIP

The Routing Information Protocol (RIP) is a routing protocol based on the distance vector algorithm. It is used for the dynamic creation of the routing table for routers.

6.5.1 Configuration

With this dialog you can enter both general settings and settings for each port for the routing information protocol.

■ General settings

- ▶ Operation: Switch the RIP function on and off. Default value: off
- ▶ Auto Summary Mode: Switch the auto summary mode on and off. When this is switched on, RIP combines a number of subnetworks together, where possible, in order to reduce the range of routing information in the routing table. Default value: selected
- ▶ Host Routes Accept Mode: Switch the host routes accept mode on and off. When this is switched on, RIP allows you to enter routes with a 32-bit network mask. Default value: selected

- ▶ Advertise default route: Switch the propagation of the default route on and off. Default value: not selected
- ▶ Update interval: the time interval at which the router transfers the entire content of the routing table to the RIP neighbors. You can set values in the range from 1 to 1,000 seconds. Values below 10 seconds cause an increased network load in larger networks. Default value: 30 s
 - The router sets the other RIP timers accordingly:
 - Timeout: 6 x update interval
 - Garbage collection: 10 x update interval

Update interval	Maximum number of routes
1 s	250
5 s	600
10 s	1,000

Table 131: Recommendation for setting the update interval.

- ▶ Split horizon: select the split horizon mode. The split horizon mode is used to avoid the count-to-infinity problem. Default value: simple
 - none: Switch off the split horizon (state on delivery).
 - simple: simple split horizon omits the entries known by a neighbor when sending the routing table to this neighbor.
 - poisonReverse: The PoisonReverse split horizon sends the routing table to a neighbor with the entries known by this neighbor, but denotes these entries with the infinity metric.
- ▶ Default metric: default metric for a route that RIP takes over from another protocol. This metric is used when no metric was configured for the corresponding protocol in the [\(see on page 229 “Route Distribution”\)](#) dialog on . Default value: 0

The value 0 means there is no specification for the default metric. In this case, RIP uses the metric 1.

■ Settings per port

Parameters	Meaning
Port	Port of the module of the Switch
VLAN ID	VLAN membership of the port. Default value: -
Admin Status	Switch the RIP function at this port on and off. Default value: not selected
Send Version	RIP version that the router uses at this port to send RIP information. Default value: ripVersion2 <ul style="list-style-type: none"> – doNotSend: RIP does not send any routing information. – ripVersion1: RIP sends information with version 1 as a broadcast. – rip1Compatible: RIP sends information with version 2 as a broadcast. – ripVersion2: RIP sends information with version 2 as a multicast.
Receive Version	RIP version that the Switch accepts on the receiver side. Default value: rip1OrRip2 <ul style="list-style-type: none"> – rip1: RIP accepts RIP V1 packets. – rip2: RIP accepts RIP V2 packets. – rip1OrRip2: RIP accepts RIP V1 and V2 packets. – doNotReceive: RIP does not allow RIP information to be received.
Authentication	Type of authentication used: <ul style="list-style-type: none"> – “noAuthentication”: RIP information is exchanged without authentication. – “simplePassword”: RIP information is exchanged with plain text password authentication. – “md5”: RIP information is exchanged with password authentication, whereby the password is transferred with md5 encryption. Default value: noAuthentication
Key	Password for authentication. For communication purposes, the port at the other end must have the same authentication settings.
Key Identifier	Password identification number for authentication. For communication purposes, the port at the other end must have the same key ID.

Table 132: RIP configuration table

■ 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 133: Buttons

6.5.2 Route Distribution

Route distribution describes how RIP propagates routes that RIP transferred from other protocols to other RIP routers.

Parameters	Meaning	Value range	Default setting
Source	Source from which RIP takes over routing information: – connected: The route points to a subnetwork that is connected directly to the interface. – static: The route is in the static routing table. – ospf: The route is from OSPF.	connected, static, ospf	
Mode	You use the mode to select whether RIP should take over routes from these sources.		
Metric	In this column you enter the metric that RIP assigned to the routes from the source. If the value 0 is entered, then RIP uses the value entered under “Default Metric” (see on page 226 “General settings”).		
Match internal	Enable: Internal OSPF routes (OSPF Intra, OSPF Inter) are adopted in RIP.	Active, Inactive	Active
Match external 1	Enable: External OSPF routes of metric type 1 (OSPF Ext T1) are adopted in RIP.	Active, Inactive	Inactive
Match external 2	Enable: External OSPF routes of metric type 2 (OSPF Ext T2) are adopted in RIP.	Active, Inactive	Inactive
Match NSSA external 1	Enable: External OSPF routes of metric type 1 from an NSSA (Not so Stubby Area) are adopted in RIP.	Active, Inactive	Inactive
Match NSSA external 2	Enable: External OSPF routes of metric type 2 from an NSSA (Not so Stubby Area) are adopted in RIP.	Active, Inactive	Inactive

Table 134: Route distribution table

■ 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 135: Buttons

6.5.3 Statistics

The RIP statistics window displays the numbers on counters that count events relevant to routing.

Parameters	Meaning
Global route changes	Number of route changes caused by RIP in the routing table
Global Queries	Number of responses sent to queries from other systems
Module	Router module
Port	Port to which this entry applies
Receive Bad Packets	Number of received routing data packets that the Switch rejected for various reasons, such as different protocol version, unknown command type.
Receive Bad Routes	Number of routing information messages received, which the router ignored because the input format was invalid.
Sent Updates	Number of routing tables sent with changed routing entries.

Table 136: RIP statistics table

■ 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 137: Buttons

6.6 Routing table

The routing table contains all the routes known by the device.

If there are a number of routes to a destination, then the device chooses the route with the lowest value in the Metric column.

Under Routing Table, you will find the following dialogs:

- ▶ Current
- ▶ Static
- ▶ Preferences

6.6.1 Current

The current routing table contains all the routes to which there is currently a valid connection.

Parameter	Meaning
Module	Module of the router
Port	Router interface
Network Address	IP address of the destination network
Netmask	Network mask for the IP address of the destination network
Next Hop IP Address	IP address of the next router on the path to the destination network.
Type	Displays the type of the entry: – local: The destination can be reached directly via this router interface. – remote: The next hop is a router.

Table 138: Current routing table

Parameter	Meaning
Protocol	Shows how the entry came about: <ul style="list-style-type: none"> – local: own router interface – netmg: static route – ospf – rip
Metric	Metric of this route. The Switch chooses the route with the smallest value for the metric for the transmission. If a number of routing entries with an identical network address/network mask, but with different next hop IP addresses, have the same metric, then the Switch enters all these entries in the routing table (ECMP - equal cost multiple path). The Switch supports up to four ECMP routes.

Table 138: Current routing table

■ 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 139: Buttons

6.6.2 Static

The static routing table allows you to enter static routes.

On delivery, the preferences are set so that the Switch gives preference to statically entered routes over dynamically entered routes ([see on page 235 “Preferences”](#)).

- Click on “Create Entry” to open a window for entering a new row in the table.

After entering

- the IP address of the destination network
 - the network mask for the IP address of the destination network, and
 - IP address of the next router on the path to the destination network,
- you click on “OK” to transfer the entry into the table.

You can change the entry for the preference directly in the table.

- To delete a row, select the row and click on “Delete entry”.

Parameter	Meaning
Destination	IP address of the destination network
Destination Mask	Network mask for the IP address of the destination network
Next Hop	IP address of the next router on the path to the destination network.
Preference	The importance of this entry, on the basis of which this route is considered in selecting the best route. As a default, the dialog takes the value from the table in the preference dialog (see on page 235 “Preferences”). A preference with the value 255 means “cannot be reached”, i.e. the route is not used.
Track ID	Identification number of the tracking object whereby if this object changes its status to <code>down</code> , the device deletes this route from the current routing table (see on page 232 “Current”).

Table 140: Table for static routes

■ 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 141: Buttons

6.6.3 Preferences

This dialog enables you to find a default setting for the importance (administrative distance) of an entry in the routing table. The smaller the value, the more important the entry. The router automatically assigns the importance that is entered in the preference list to a new entry in the routing table.

Note: You always assign "connected" to the smallest value for the administrative distance.

Source	Meaning	Default Setting
connected	Entry for routes/interfaces connected directly to the Switch.	0
static	Entry for routes from the static routing table.	1
ospf-intra	Entry for routes from OSPF within an area	8
ospf-inter	Entry for routes from OSPF between areas	10

Table 142: Preference Lists

Source	Meaning	Default Setting
ospf-ext-t1	These routes were imported from an Autonomous System Boundary Router (ASBR) into the OSPF area. These routes use the costs relating to the connection between the ASBR and this Switch as part of the route costs.	13
ospf-ext-t2	These routes were imported from an Autonomous System Boundary Router (ASBR) into the OSPF area. These routes do not use the costs relating to the connection between the ASBR and this Switch as part of the route costs.	150
rip	Entry for routes from the Routing Information Protocol.	15

Table 142: Preference Lists

■ 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 143: Buttons

6.7 Tracking

The tracking function gives you the option of monitoring certain objects, such as the availability of an interface.

A special feature of this function is that it forwards an object status change to an application, e.g. VRRP, which previously registered as an interested party for this information.

6.7.1 Configuration

This dialog allows you to create a new tracking object, or change or delete an existing tracking object.

The device provides tracking objects of the type:

- ▶ Interface
- ▶ Ping
- ▶ Logical

The device supports up to 256 tracking objects (track ID: 1 to 256).

Parameter	Meaning
Track ID	Identification number of this tracking object.
Active	Activate/deactivate this tracking object.
Module.Port	Port identification using module and port numbers of the device, e.g. 2.1 for port one of module two.
Link up delay [s]	An interface object is given the <code>up</code> status if the physical link holds for longer than the delay time.
Link down delay [s]	An interface object is given the <code>down</code> status if the physical link interruption remains for longer than the delay time.
Send change trap	Activate/deactivate the sending of an alarm when the status of this tracking object changes.

Table 144: Parameters of a tracking object of the type Interface

Parameter	Meaning
Status	Displays the status of this tracking object.
Number of changes	Displays the number of status changes.
Time since last change	Displays the time that elapsed since the last status change.

Table 144: Parameters of a tracking object of the type Interface

Parameter	Meaning
Track ID	Identification number of this tracking object.
Active	Activate/deactivate this tracking object.
IP Address	IP address of the device being monitored with ping.
Module.Port	Port identification using module and port numbers of the device, e.g. 2.1 for port one of module two. If you select "auto", the device will automatically use the interface with the best route.
Ping interval [s]	Interval between the ping requests in seconds.
Ping Replies to lose	Number of lost ping responses that will result in the status <code>down</code> .
Ping Replies to receive	Number of received consecutive ping responses that will result in the status <code>up</code> .
Ping timeout [ms]	The time for which the device waits for a ping response before it evaluates this as "No ping response".
Ping TTL	The TTL value (Time To Live) in the IP packet header that the device uses to send the ping request.
Send change trap	Activate/deactivate the sending of an alarm when the status of this tracking object changes.
Status	Displays the status of this tracking object.
Number of changes	Displays the number of status changes.
Time since last change	Displays the time that elapsed since the last status change.

Table 145: Parameters of a tracking object of the type Ping

Parameter	Meaning
Track ID	Identification number of this tracking object.
Active	Activate/deactivate this tracking object.
Operator	Operator for linking up to 8 operands (tracking objects). If the result of the link is true, then the status of this tracking object is <code>up</code> .
Operand 1 to n	Operand for the link with the operator. You select the operands from existing tracking objects.
Send change trap	Activate/deactivate the sending of an alarm when the status of this tracking object changes.

Table 146: Parameters of a tracking object of the type Logical

Parameter	Meaning
Status	Displays the status of this tracking object.
Number of changes	Displays the number of status changes.
Time since last change	Displays the time that elapsed since the last status change.

Table 146: Parameters of a tracking object of the type Logical

■ 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	Removes the selected table entry.
Wizard	Opens the "Wizard". The "Wizard" assists you in creating a new entry in the table.
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.
Help	Opens the online help.

Table 147: Buttons

6.7.2 Applications

This table displays the tracking objects for which applications are registered.

- ▶ You register VRRP for a tracking object in the `Redundancy:VRRP:Configuration` dialog (see on page 303 “VRRP instance settings”).
- ▶ You register static routes for a tracking object in the `Routing:Routing Table:Static` dialog (see on page 234 “Static”).
- ▶ The devices automatically registers logical links of tracking objects for a tracking object.

Parameter	Value
Track ID	Identification number of the tracking object.
Application	Application registered for this tracking object.
Number of changes	Number of status changes for this tracking object.
Time since last change	Time that has elapsed since the last status change for this tracking object.

Table 148: Applications registered for tracking objects

■ 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 149: Buttons

7 Redundancy

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

- ▶ Link Aggregation
- ▶ Ring Redundancy
- ▶ Ring/Network coupling
- ▶ Spanning Tree
- ▶ VRRP/HiVRRP

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

7.1 Link Aggregation

With this dialog you can:

- ▶ display an overview of all the existing link aggregations,
- ▶ create link aggregations,
- ▶ configure link aggregations,
- ▶ allow static link aggregations, and
- ▶ Delete link aggregations.

The LACP (Link Aggregation Control Protocol based on IEEE 802.3ad) is a network protocol for dynamically bundling physical network connections. The added bandwidth of all connection lines is available for data transmission. In the case of a connection breaking down, the remaining connections take over the entire data transmission (redundancy). The load distribution between the connection lines is performed automatically.

You configure a link aggregation by combining at least 2 existing parallel redundant connection lines (known as a trunk) between two devices into one logical connection. You can use link aggregation to combine up to 8 (optimally up to 4) connection lines between devices into a trunk.

Any combination of twisted pair and F/O cables can be used as the connection lines of a trunk. Configure the connections so that the data rates and the duplex settings of the related ports are matching.

A maximum of 7 trunks can exit a device.

Note: Exclude the combination of a link aggregation with the following redundancy procedures:

- ▶ Network/Ring coupling
- ▶ MRP-Ring
- ▶ Sub-Ring

Note: A link aggregation connects exactly 2 devices.

You configure the link aggregation on each of the 2 devices involved. During the configuration phase, you connect only one single connection line between the devices. This is to avoid loops.

Parameter	Meaning
Allow static link aggregation	When you connect devices using multiple lines, the Link Aggregation Control Protocol (LACP) automatically prevents loops from forming. Select <code>Allow static link aggregation</code> if the partner device does not support LACP (e.g. MACH 3000). Default value: not selected
Trunk-Port	This column shows you the index under which the device uses a link aggregation as a virtual port (8.x).
Device-Ports	List of physical ports that are members of the link aggregation.
Name	Here you can assign a name to the link aggregation.
Active	This column allows you to enable/disable a link aggregation that has been set up.
Link Trap	When you select "Link Trap", the device generates an alarm if all the connections of the link aggregation are interrupted.
STP-Mode	In the "STP Mode" column, select <code>on</code> if you have integrated the link aggregation into a Spanning Tree, or <code>off</code> if you have not.
Type	<ul style="list-style-type: none"> - <code>manual</code> The partner device does not support LACP, and you have selected "Allow static link aggregation". - <code>dynamic</code> Both devices support LACP and you have not selected "Allow static link aggregation". <p>Note: If there are multiple connections between devices that all support LACP, the device displays <code>dynamic</code> even if "Allow static link aggregation" was selected. In this case, the devices automatically switch to dynamic.</p>

Table 150: Link Aggregation

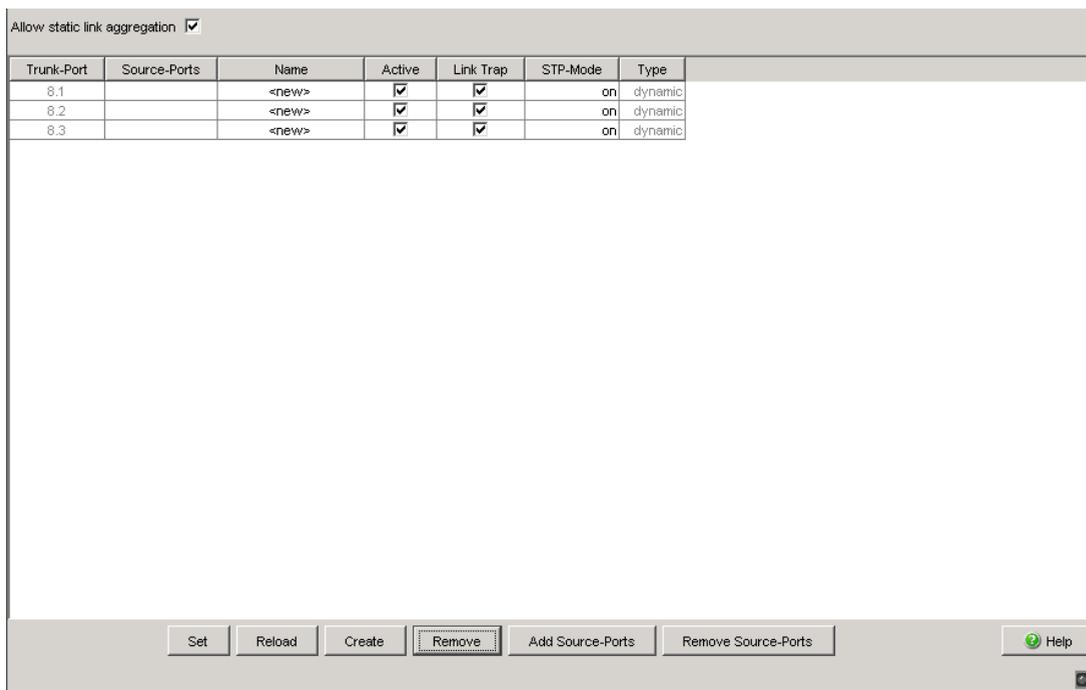


Figure 61: Setting the link aggregation

Note: For PowerMICE and MACH 4000

To increase the availability of particularly important connections, you can combine HIPER-Ring (see on page 246 “Ring Redundancy”) and link aggregation.

If you want to use a link aggregation in a HIPER-Ring, you first configure the link aggregation, then the HIPER-Ring. In the HIPER-Ring dialog, you enter the index of the desired link aggregation as the value for the module and the port (8.x). Ascertain that the respective ring port belongs to the selected link aggregation.

■ 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.
Add Device Ports	Opens "Select Ports to add" window which displays available ports. To add a port from the trunk, select it, then click "OK".
Remove Device-Ports	Opens a list of ports present on the trunk. To remove a port from the trunk, select it, then click "OK".
OK	Carries out the selected action.
Cancel	Stops the selected action.
Help	Opens the online help.

Table 151: Buttons

7.2 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.

Note: If you have configured a device as the MRP Ring Manager, the device enables you to carry out the MRP Ring Configuration automatically ([see on page 255 “Advanced Ring Configuration/Diagnostics \(ARC\)”](#)).

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 152: Ring Redundancy basic configuration

7.2.1 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	-
Optical	10 Gbit/s	-	on	10 Gbit/s full duplex (FDX)

Table 153: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 the RS20/30/40, MS20/30 and PowerMICE Switches, 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 Manager Mode	If there is exactly one device, you switch the Ring Manager function on at the ends of the line.
Ring Recovery	The settings in the "Ring Recovery" frame are only effective for devices that are ring managers. In the ring manager, select the desired value for the test packet timeout for which the ring manager waits after sending a test packet before it evaluates the test packet as lost. <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 154: HIPER-Ring configuration

The screenshot shows a configuration window for Ring Redundancy. It is divided into several sections:

- Version:** Radio buttons for HIPER-Ring and MRP.
- Ring Port 1 and Ring Port 2:** Each has fields for Module, Port, and Operation.
- Configuration Redundancy Manager:** A checkbox for Advanced Mode.
- Redundancy Manager:** Radio buttons for Mode On and Off.
- Operation:** Radio buttons for On and Off.
- Ring Recovery:** Radio buttons for 500ms and 200ms.
- VLAN:** A text field for VLAN ID.
- Information:** An empty text area.

At the bottom, there are buttons for **Set**, **Reload**, **Delete ring configuration**, and **Help**.

Figure 62: 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: 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.

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.

7.2.2 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	-
Optical	10 Gbit/s	-	on	10 Gbit/s full duplex (FDX)

Table 155: 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.	
Ring Manager Mode	If there is exactly one device, you switch the Ring Manager function on at the ends of the line.
Operation	When you have configured all the parameters for the MRP-Ring, you switch the operation on with this setting. When you have configured all the devices in the MRP-Ring, you close the redundant line.
Ring Recovery	For the device for which you have activated the ring manager, select the value 200 ms if the stability of the ring meets the requirements for your network. Otherwise select 500 ms. <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 <i>VLAN ID 1</i> and <i>VLAN membership 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 <i>VLAN membership 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 156: MRP-Ring configuration

The screenshot shows a configuration window for ring redundancy. It includes sections for selecting the version (HUPER-Ring or MRP), configuring two ring ports (Module and Port), enabling advanced mode, setting the redundancy manager mode (On/Off), operation mode (On/Off), and ring recovery time (500ms/200ms). A VLAN ID field is also present. At the bottom, there are buttons for 'Set', 'Reload', 'Delete ring configuration', and 'Help'.

Figure 63: 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.

■ **Advanced Ring Configuration/Diagnostics (ARC)**

A special feature of the Hirschmann device is completing the configuration of all the devices in an MRP Ring using the ARC protocol (Advanced Ring Configuration).

To configure an MRP Ring using ARC, all you have to do is to connect Hirschmann devices in their default state to a ring and to run the Advanced Ring Configuration/Diagnostics on a device. Only the device on which you are operating the ARC using the Web-based interface requires an IP address.

The ARC manager first sends diagnostic packets to the ring and analyzes the responses from the ring subscribers. In doing so, it determines the ring ports and the ring subscribers' current settings.

If the ARC manager determines that the requirements for the Advanced Ring Configuration/Diagnostics are met, it carries through the configuration for you automatically.

At the same time, the ARC manager sends the configuration packets to the ring. In the course of this, all the devices in the ring automatically configure their ring redundancy settings for an MRP Ring according to the ARC manager's specifications.

After this, all the devices in the ring save their new configuration non-volatily.

The prerequisites for checking and carrying out the Advanced Ring Configuration/Diagnostics automatically are:

- ▶ Preventing loops:
 - RSTP is active on all the devices and ring ports in the ring (default: globally and active on all ports).
- ▶ All the devices in the ring support Advanced Ring Configuration/Diagnostics:
 - They operate with software variant L2P, L3E or L3P,
 - They operate with software version 07.0.00 or higher.
- ▶ All the devices that you have designated as **MRP Ring Subscribers**:
 - The ring manager's configured mode is `Off` (default: `Off`).
 - Advanced Ring Configuration/Diagnostics is `Read/Write` (default: `Read/Write`).

Note: To read the settings in the Advanced Ring Configuration/Diagnostics frame, set in the Web-based interface

- the Ring Redundancy version to `MRP` and
- the function to `On`.
- The Ring Redundancy's configured version default is `MRP`. If you have selected another version, the devices automatically set your setting to `MRP` while the Advanced Ring Configuration/Diagnostics is being carried out.
- The function's default is `Off`. The devices automatically set your setting to `On` while the Advanced Ring Configuration/Diagnostics is being carried out.
- ▶ The device that you have designated as **MRP Ring Manager**:
 - Only 1 device in the ring is the MRP Ring Manager,
 - The Ring Redundancy's configured version is `MRP` (default: `MRP`),
 - The configured ring ports correlate with the ring cabling (default for both ports: 1.1),
 - The ring manager's configured mode is `On` (default: `Off`),
 - The configured function is `On` (default: `Off`),
 - Advanced Ring Configuration/Diagnostics is `On` (default: `Off`),
 - Only this device carries out the Advanced Ring Configuration/Diagnostics.
- ▶ Physical Topology:
 - You connected the devices to a physical ring.

Note: Note the following special features of the Advanced Ring Configuration/Diagnostics:

- ▶ Advanced Ring Configuration/Diagnostics configures an MRP Primary Ring only. Manually configure rings with another redundancy protocol, as well as Sub-Rings.
- ▶ When carrying out the Advanced Ring Configuration/Diagnostics configuration, deactivate all the devices in the ring at their ring ports. Exception: If the "MRP Compatibility" setting is active on a device ([see on page 276 "Global"](#)), then the device leaves RSTP activated on the ring port.
If you need RSTP, activate RSTP on the ring ports manually ([see on page 290 "Port"](#)).

If you have designated a device as a Ring **Subscriber**, it displays the “Advanced Ring Configuration/Diagnostics” frame, including 3 selection options, in the Ring Redundancy dialog.

If necessary, select the “Read/Write” option and save the setting to the device.

The screenshot shows a web-based configuration interface for Ring Redundancy. The interface is organized into several sections:

- Version:** Radio buttons for HIPER-Ring and MRP.
- Ring Port 1:** Port dropdown set to 1.1, Operation dropdown.
- Ring Port 2:** Port dropdown set to 1.2, Operation dropdown.
- Configuration Ring Manager:** Advanced Mode.
- Ring Manager:** Mode radio buttons for On and Off.
- Operation:** Radio buttons for On and Off.
- Ring Recovery:** Radio buttons for 500ms and 200ms.
- VLAN:** VLAN ID input field.
- Information:** Empty text area.
- Advanced Ring Configuration/Diagnostics:** A red-bordered box containing radio buttons for Off, Read, and Read & Write.

At the bottom, there are buttons for **Set**, **Reload**, **Delete ring configuration**, and **Help**.

Figure 64: Ring Redundancy Dialog, Advanced Ring Configuration/Diagnostics of an MRP client

If you have designated a device as a Ring **Manager**, it displays the “Advanced Ring Configuration/Diagnostics Protocol” frame in the Ring Redundancy dialog. It includes 2 selection options and the “Configuration” and “Diagnostics” buttons.

If necessary, select the “On” option and save the setting to the device.

To check whether the ARC can configure the ring automatically, click on “Diagnostics”. To configure the ring automatically using the ARC, click on “Configuration”. The device guides you through the diagnostic and configuration steps with the aid of a wizard and displays the results for you.

The screenshot displays the Ring Redundancy dialog for an MRP manager. The dialog is organized into several sections:

- Version:** Radio buttons for HIPER-Ring and MRP.
- Ring Port 1:** Port dropdown set to 1.1, Operation dropdown.
- Ring Port 2:** Port dropdown set to 1.2, Operation dropdown.
- Configuration Ring Manager:** Advanced Mode.
- Ring Manager:** Mode radio buttons for On and Off.
- Operation:** Radio buttons for On and Off.
- Ring Recovery:** Radio buttons for 500ms and 200ms.
- VLAN:** VLAN ID text input field.
- Information:** Empty text area.
- Advanced Ring Configuration/Diagnostics:** This section is highlighted with a red box. It contains radio buttons for On and Off, and two buttons: **Configuration** and **Diagnostics**.

At the bottom of the dialog, there are buttons for **Set**, **Reload**, **Delete ring configuration**, and **Help** (with a green icon).

Figure 65: Ring Redundancy Dialog, Advanced Ring Configuration/Diagnostics of an MRP manager.

7.2.3 Configuring the Fast HIPER-Ring (MACH 1040)

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

- ▶ RSR20, RSR30
- ▶ MACH 1000

To configure a Fast HIPER-Ring, you set up the network to meet your requirements. 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	-
Optical	10 Gbit/s	-	on	10 Gbit/s full duplex (FDX)

Table 157:Port settings for ring ports

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

Table 158: Fast HIPER-Ring configuration

Figure 66: Selecting and configuring Fast HIPER-Ring

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

■ 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 159: Buttons

7.3 Sub-Ring

With this dialog you can:

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

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

- RSR20/RSR30
- PowerMICE
- MACH 1000
- MACH 4000

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

Note: Configure all the devices in the Sub-Ring before you close the redundant line. In this way, you prevent loops during the configuration phase.

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

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

Note: In the Sub-Ring, you configure the devices with the Sub-Ring Manager functions switched off as participants of an MRP-Ring (see on page 252 “Configuring the MRP-Ring”).

This means:

- ▶ Define a different VLAN membership for the Primary Ring and the Sub-Ring even if the basis ring is using the MRP protocol, e.g. VLAN ID 1 for the Primary Ring and VLAN ID 2 for the Sub-Ring.
- ▶ Switch the MRP-Ring function on for all devices.
- ▶ Switch the Ring Manager function off for all devices.
- ▶ Do not configure link aggregation.
- ▶ Switch RSTP off for the MRP Ring ports used in the Sub-Ring.
- ▶ Assign the same MRP domain ID to all devices. If you are only using Hirschmann Automation and Control GmbH devices, you do not have to change the default value for the MRP domain ID.

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

7.3.1 Sub-Ring configuration

Parameter	Meaning	Possible values	Default setting
Max. Table Entries	Number of Sub-Rings that can be managed by a Sub-Ring Manager at the same time.	4 MACH1040: (16)	-
Sub Ring ID	Unique name for this Sub-Ring.	0 - 2147483647 ($2^{31}-1$)	-
Function on/off	Only switch on the Sub-Ring when the configuration is complete. Then close the Sub-Ring.	On Off	On
Configuration State	A symbol displays the current state of the Sub-Ring.		

Table 160: Sub-Ring basic configuration

Parameter	Meaning	Possible values	Default setting
Redundancy existing	A symbol displays whether the redundancy exists.		
Port	ID of the port that connects the device to the Sub-Ring.	All available ports that do not already belong to the ring redundancy of the basis ring, in the form X.X. (module.port)	
Name	Optional name for the Sub-Ring		
SRM Mode	<p>Target state: Define whether this SRM is to manage the redundant connection (<code>Redundant Manager mode</code>) or not. If you have set the same value for the SRM Mode for both SRMs, the SRM with the higher MAC address assumes the function of redundant manager. <code>SingleManager</code> describes the special state when you connect a Sub-Ring via 2 ports of a single device. In this case, the port with the higher port number manages the redundant connection.</p>	<p>Manager RedundantManager SingleManager</p>	Manager
SRM State	<p>Actual state: Shows whether this SRM manages the redundant connection (<code>Redundant Manager mode</code>) or not. If you have set the same value for the SRM Mode for both SRMs, the SRM with the higher MAC address assumes the function of redundant manager. <code>SingleManager</code> describes the special state when you connect a Sub-Ring via 2 ports of a single device. In this case, the port with the higher port number manages the redundant connection.</p>	<p>Manager RedundantManager SingleManager</p>	Manager
Port Status	Connection status of the Sub-Ring port	<p>forwarding disabled blocked not connected</p>	
VLAN	VLAN to which this Sub-Ring is assigned. If no VLAN exists under the VLAN ID entered, the device automatically creates it. If you do not want to use a separate VLAN for this Sub-Ring, you leave the entry as "0".	Corresponds to the entries in the VLAN dialog	-

Table 160: Sub-Ring basic configuration

Parameter	Meaning	Possible values	Default setting
Partner MAC	Shows the MAC address of the Sub-Ring Manager at the other end of the Sub-Ring.	Valid MAC address	00 00 00 00 00 00
MRP Domain	Assign the same MRP domain name to all the members of a Sub-Ring. If you are only using Hirschmann devices, you can use the default value for the MRP domain; otherwise adjust it if necessary. With multiple Sub-Rings, all the Sub-Rings can use the same MRP domain name.	All permitted MRP domain names	255.255.255.255. 255.255.255.255. 255.255.255.255. 255.255.255.255. 255
Protocol		standardMRP	standardMRP

Table 160: Sub-Ring basic configuration

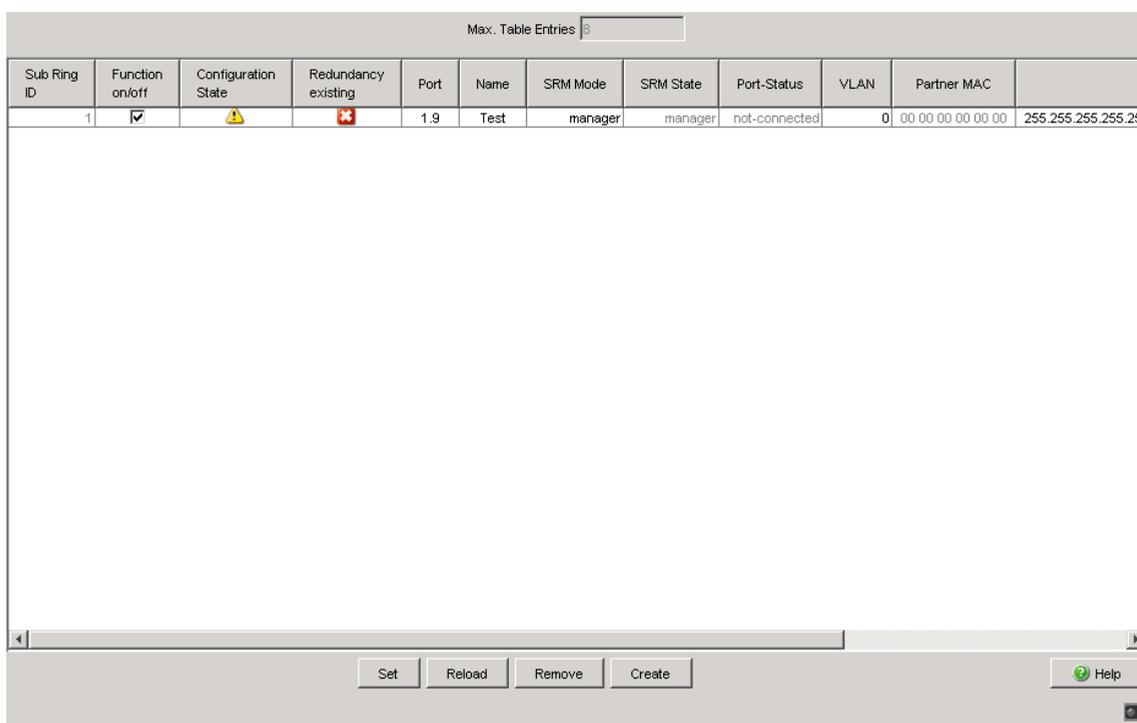


Figure 67: Sub-Ring basic configuration

7.3.2 Sub-Ring – New Entry

Parameter	Meaning	Possible values	Default setting
Sub Ring ID	Unique name for this Sub-Ring.	0 - 2147483647 ($2^{31}-1$)	-
Port	ID of the port that connects the device to the Sub-Ring.	All available ports that do not already belong to the ring redundancy of the basis ring, in the form X.X. (module.port)	
Name	Optional name for the Sub-Ring		
SRM Mode	Target state: Define whether this SRM is to manage the redundant connection (<code>RedundantManager mode</code>) or not. If you have set the same value for the SRM Mode for both SRMs, the SRM with the higher MAC address assumes the function of redundant manager. <code>SingleManager</code> describes the special state when you connect a Sub-Ring via 2 ports of a single device. In this case, the port with the higher port number manages the redundant connection.	Manager RedundantManager SingleManager	Manager
VLAN	VLAN to which this Sub-Ring is assigned. If no VLAN exists under the VLAN ID entered, the device automatically creates it. If you do not want to use a separate VLAN for this Sub-Ring, you leave the entry as "0".	Corresponds to the entries in the VLAN dialog	-
MRP Domain	Assign the same MRP domain name to all the members of a Sub-Ring. If you are only using Hirschmann devices, you can use the default value for the MRP domain; otherwise adjust it if necessary. With multiple Sub-Rings, all the Sub-Rings can use the same MRP domain name.	All permitted MRP domain names	255.255.255. 255.255.255. 255.255.255. 255.255.255. 255

Table 161: Sub-Ring - New Entry

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

The image shows a 'New Entry' dialog box with the following fields and values:

- Sub Ring ID: 1
- Port: 1.9
- Name: Test
- SRM Mode: manager
- VLAN: 0
- MRP Domain: 255.255.255.255.255.255.255

At the bottom of the dialog, there are four buttons: 'Set', 'Set and back', 'Back', and 'Help'.

Figure 68: Sub-Ring – New Entry 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.
Remove	Removes the selected table entry.
Create	Adds a new table entry.
Set and back	Transfers the changes to the volatile memory (RAM) of the device and goes back to the previous dialog.
Back	Displays the previous page again. Changes are lost.
Help	Opens the online help.

Table 162: Buttons

7.4 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

7.4.1 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
MICE/Power MICE	Selectable: DIP switch and software setting
MACH 3000/MACH 4000	Software switch

Table 163: 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 164: Setting the STAND-BY switch

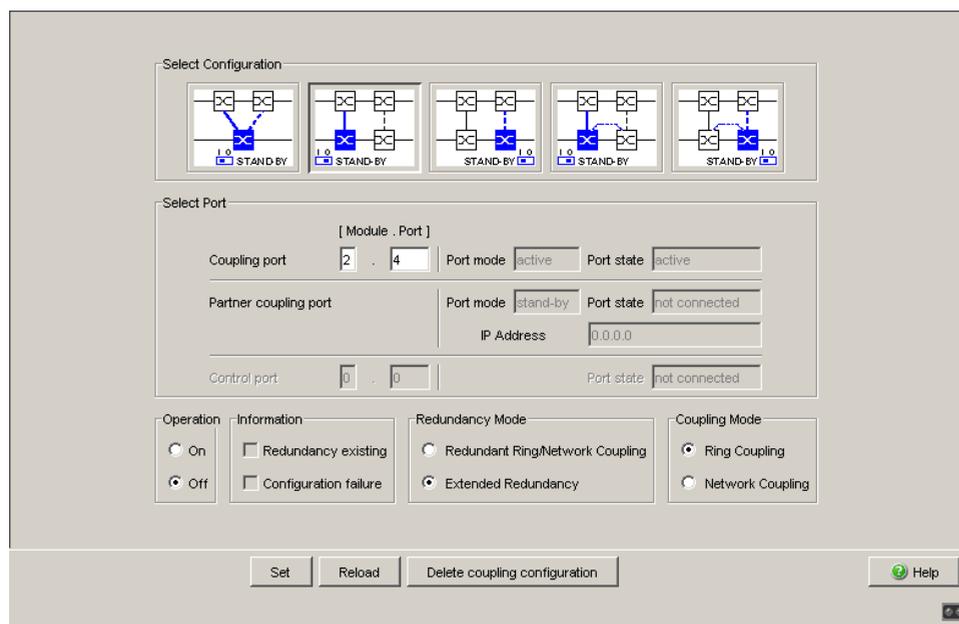


Figure 69: Software configuration of the STAND-BY switch

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 163), 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"> - active: You have switched the port on. - stand-by: The port is in stand-by mode.
Port State	<ul style="list-style-type: none"> - active: You have switched the port on. - stand-by: The port is in stand-by mode. - not connected: 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 165: 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 165: 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	-
Optical	10 Gbit/s	-	on	10 Gbit/s full duplex (FDX)

Table 166: 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 167: Buttons

7.5 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) and Multiple Spanning Tree (MSTP).

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.

Multiple Spanning Tree Protocol (MSTP)

MSTP is an extension of the Rapid Spanning Tree Protocol used to increase the benefits of VLANs. MSTP allows you to define multiple groups of VLANs, and to configure a separate Spanning Tree Instance for each group. This Spanning Tree Instance prevents loops within the related VLAN group and provides redundancy in the case of a failure.

Additionally, MSTP enables existing connections to be used more efficiently in normal operation, i.e. when all connections are being operated. For example, MSTP can set a connection between 2 bridges to the “discarding” state for a certain VLAN group, while simultaneously operating the same connection for another VLAN group in the “forwarding” state. In normal operation, MSTP thus enables you to use your resources more efficiently via load sharing.

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

7.5.1 Global

With this dialog you can:

- ▶ switch the Spanning Tree Protocol on/off and select the RSTP or MSTP protocol version
- ▶ 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 setting
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
Frame „Protocol Version“	Select the protocol version: - RSTP (IEEE 802.1Q-2005), to use the Spanning Tree jointly for all configured VLANs, - MSTP (IEEE 802.1Q-2005), to use the Spanning Tree separately for various VLAN groups.	RSTP, MSTP	RSTP

Table 168: Global Spanning Tree settings, basic function

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

In the context of MSTP, these are the settings for the Common Spanning Tree (CST).

Parameter	Meaning	Possible values	Default setting
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).		

Table 169: Global Spanning Tree settings, local bridge parameters

Parameter	Meaning	Possible values	Default setting
Priority	Sets the local bridge priority. The bridge priority and its own MAC address make up this separate Bridge ID. The device with the best (numerically lowest) priority assumes the role of the root bridge. Define the root device by assigning the device the best priority in the Bridge ID among all the devices in the network. Enter the value as a multiple of 4096.	$0 \leq n \cdot 4096 \leq 61440$	32768
Hello Time	Sets the Hello Time. The local Hello Time is the time in seconds between the sending of two configuration messages (Hello packets). If the local device has the root function, the other devices in the entire network take over this value. Otherwise the local device uses the value of the root bridge in the "Root" column on the right.	1 - 2	2
Forward Delay	Sets the Forward Delay parameter. In the previous STP protocol, the Forward Delay parameter was used to delay the status change between the statuses disabled, discarding, learning, forwarding. Since the introduction of RSTP, this parameter has a subordinate role, because the RSTP bridges negotiate the status change without any specified delay. If the local device is the root, the other devices in the entire network take over this value. Otherwise the local device uses the value of the root bridge in the "Root" column on the right.	4 - 30 s See the note following this table.	15 s
Max Age	Sets the Max Age parameter. In the previous STP protocol, the Max Age parameter was used to specify the validity of STP BPDUs in seconds. For RSTP, Max Age signifies the maximum permissible branch length (number of devices to the root bridge). If the local device is the root, the other devices in the entire network take over this value. Otherwise the local device uses the value of the root bridge in the "Root" column on the right.	6 - 40 s See the note following this table.	20 s

Table 169: Global Spanning Tree settings, local bridge parameters

Parameter	Meaning	Possible values	Default setting
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
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 180). 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 169: 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	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.	$0 \leq n \leq 4096$ 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 170: 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

Table 171: Global Spanning Tree settings, topology information

Parameters	Meaning	Possible values
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 171: 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 172: Global Spanning Tree settings, Information frame

Figure 70: 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 173: Buttons

7.5.2 MSTP (Multiple Spanning Tree)

With this dialog you can:

- ▶ manage the global Multiple Spanning Tree Instance
- ▶ create or delete a Multiple Spanning Tree Instance
- ▶ assign VLANs to a Multiple Spanning Tree Instance and manage the MSTI.

The tab for the global Multiple Spanning Tree Instance is named “MST Global (CIST)”. This instance is always available and cannot be deleted. It contains all the configured VLANs that are not explicitly assigned to an MSTI. The settings include the MST region identifier, the maximum number of Hops for the Internal Spanning Tree (IST), and information on IST and CST (known in combination as CIST).

The tabs for the MSTIs are named MSTI, followed by the number of the instance, e.g. “MSTI 2”. Here you can manage the individual Multiple Spanning Tree Instances (MSTIs). The device allows you to create up to 16 Multiple Spanning Tree Instances (MSTIs). The prerequisite for using MSTP is that all the bridges in the network that make up an MSTP region must also support MSTP.

Note: To use MSTP, disable the other redundancy protocols on this device.

Note: When combining MSTP with the management VLAN 0, note the following restriction: the DHCP client of the device only sends its DHCP Broadcasts in VLAN 1.

■ Dialog Tab MSTP Global (CIST)

This tab in the dialog allows you to configure the MST region and the global Multiple Spanning Tree Instance (IST) within the MST region, and to display information on IST and CST.

Parameters	Meaning	Possible values	Default setting
"MST Region Identifier" Frame	Information about the MST region		
Name	Name of the MSTP region to which the device belongs.	Max. 32 characters, value 0x21 (!) up to and incl. 0x7e (~)	The MAC address of the device.
Revision level	Version number of the MSTP region to which the device belongs.	0 -65535	0
Digest	The MD5 checksum of the MSTP configuration.	16 bytes in hexadecimal.	

Table 174: Dialog Multiple Spanning Tree settings, MST Global, MST region identifier

Note: Configure all the bridges of an MST region with identical values for:

- the name of the MST region,
- the Revision Level, and
- the assignment of the VLANs to the MSTP instances.

Note: Include the ports that connect the bridges of an MST region as tagged members in all the VLANs that are set up on the bridges. You thus avoid potential connection breaks when the topology is changed within the MST region.

Also include the ports that connect an MST region with other MST regions or with the CST region (known as boundary ports) as tagged members in all the VLANs that are set up on both regions. You thus avoid potential connection breaks when topology changes affecting the boundary ports are made.

Parameters	Meaning	Possible values	Default setting
Frame „Global CIST Parameters“	Detailed information on the global MST instance (IST) for the region and CST.		
Maximum Hops	Maximum number of bridges within the MST region in a branch to the root bridge.	6-40	20
Attached VLANs	List of all VLANs that are assigned only to the global MST instance and to no other MSTI.	List of all static VLANs.	1;
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).		
Root ID	The <code>Bridge ID</code> of the current root bridge of the entire layer 2 network. ^a The format is ppppp / mm mm mm mm mm mm, with: ppppp: priority (decimal) and mm: the respective byte of the MAC address (hexadecimal).		
Regional Root ID	The <code>Bridge ID</code> of the current root bridge that belongs to the global instance (IST) of the MST region to which this device belongs. ^b The format is ppppp / mm mm mm mm mm mm, with: ppppp: priority (decimal) and mm: the respective byte of the MAC address (hexadecimal).		
Root Port	The port of the device from which the current path leads to the root bridge of the entire layer 2 network (CIST root). 0: local bridge is CIST root.	Valid port ID or -	0

Table 175: Dialog Multiple Spanning Tree settings, MST Global (CIST), Global MST parameters

Parameters	Meaning	Possible values	Default setting
Root path costs	External path costs from the regional root bridge of the MST region of the device to the current root bridge of the entire layer 2 network (CIST root). ^c These are the same for all devices within an MST region. 0: Regional root bridge is simultaneously CIST root bridge	0-200000000	
Internal root path costs	Internal path costs from the root port of the device to the current regional root bridge of the MST region of the device. 0: local bridge is root.	0-200000000	-

Table 175: Dialog Multiple Spanning Tree settings, MST Global (CIST), Global MST parameters

- ^a This bridge is also known as the CIST root bridge (CIST: Common and Internal Spanning Tree). It has the best bridge ID of all bridges - both those that do not belong to any MSTP region (CST, Common Spanning Tree) and those that belong to the global instance of an MSTP region (Internal Spanning Tree, IST). All the bridges in the entire layer 2 network use the time parameters of the CIST root bridge, e.g. the Hello Time.
- ^b The IST regional root ID can be identical to the above CIST root ID for the MST region of the device if the IST regional root bridge has the best bridge ID in the entire layer 2 network.
- ^c These are identical to the root path costs from Spanning Tree or Rapid Spanning Tree if you are not using MSTP (in these cases every device sees itself as a separate region).

Figure 71: Multiple Spanning Tree dialog, MST Global (CIST)

■ MSTI (Multiple Spanning Tree Instance) dialog tab

The MSTI tabs in the dialog allow you to manage the individual Multiple Spanning Tree Instances. The tab is named MSTI, followed by the number of the instance, e.g. “MSTI 2”.

Parameters	Meaning	Possible values	Default setting
Frame „VLANs“	Manage the VLANs assigned to this Multiple Spanning Tree Instance.		
Assigned VLANs	List of all VLANs currently assigned to this MSTI.	Subset of all statically set up VLANs.	No VLANs.

Table 176: Multiple Spanning Tree settings, MST Instance, VLANs

Parameters	Meaning	Possible values	Default setting
“Add VLAN” button	Opens a dialog for selecting a VLAN ID from the statically set up VLANs of the device. Select the desired VLAN ID and click on “OK”.	One of the static VLANs.	
“Remove VLAN” button	Opens a dialog for selecting a VLAN ID. Select the desired VLAN ID and click on “OK”.	A VLAN currently assigned to the MSTI	

Table 176: Multiple Spanning Tree settings, MST Instance, VLANs

Parameters	Meaning	Possible values	Default setting
Frame „Instance Parameters“	Detailed information on the selected Multiple Spanning Tree Instance.		
Priority	The local bridge <code>Priority</code> for the selected MST Instance. The bridge priority and its own MAC address make up this separate <code>Bridge ID</code> . The device with the best (i.e. numerically lowest) priority becomes the root device of the selected MST region. Define the root device by assigning to this device the best priority in the <code>Bridge ID</code> among all the devices in the selected MST region. Enter the value as a multiple of 4096.	$0 \leq n \cdot 4096 \leq 61440$	32768
Bridge ID	The local <code>Bridge ID</code> , made up of the local <code>priority</code> + <code>MSTI</code> , following by its own MAC address. The format is <code>ppppp / mm mm mm mm mm mm</code> , with: <code>ppppp</code> : <code>priority</code> + <code>MSTI</code> (decimal) and <code>mm</code> : the respective byte of the MAC address (hexadecimal).	0 - 65534; sum of priority (0 - 61440 in steps of 4096) and <code>MSTI</code> (1 - 4094)	32768 + <code>MSTI</code>
Time since last change	Time since the last topology change for this MST Instance.		
Topology changes	Counts how often the device has put a port into the <code>Forwarding</code> status via Spanning Tree since the selected MST Instance was started.		
Root ID	The <code>Bridge ID</code> of the current root bridge of the selected MST region. The format is <code>ppppp / mm mm mm mm mm mm</code> , with: <code>ppppp</code> : <code>priority</code> (decimal) and <code>mm</code> : the respective byte of the MAC address (hexadecimal).	0 - 65534; sum of priority (0 - 61440 in steps of 4096) and <code>MSTI</code> (1 - 4094)	

Table 177: Multiple Spanning Tree settings, MST Instance, parameters

Parameters	Meaning	Possible values	Default setting
Root path costs	Path costs from the root port to the current root bridge of the selected MST region. 0: bridge is root for this MST region.	0-200000000	
Root Port	The port of the device from which the current path leads to the root bridge of the selected MST region. 0: bridge is root for this MST region.	Valid port ID or 0	

Table 177: Multiple Spanning Tree settings, MST Instance, parameters

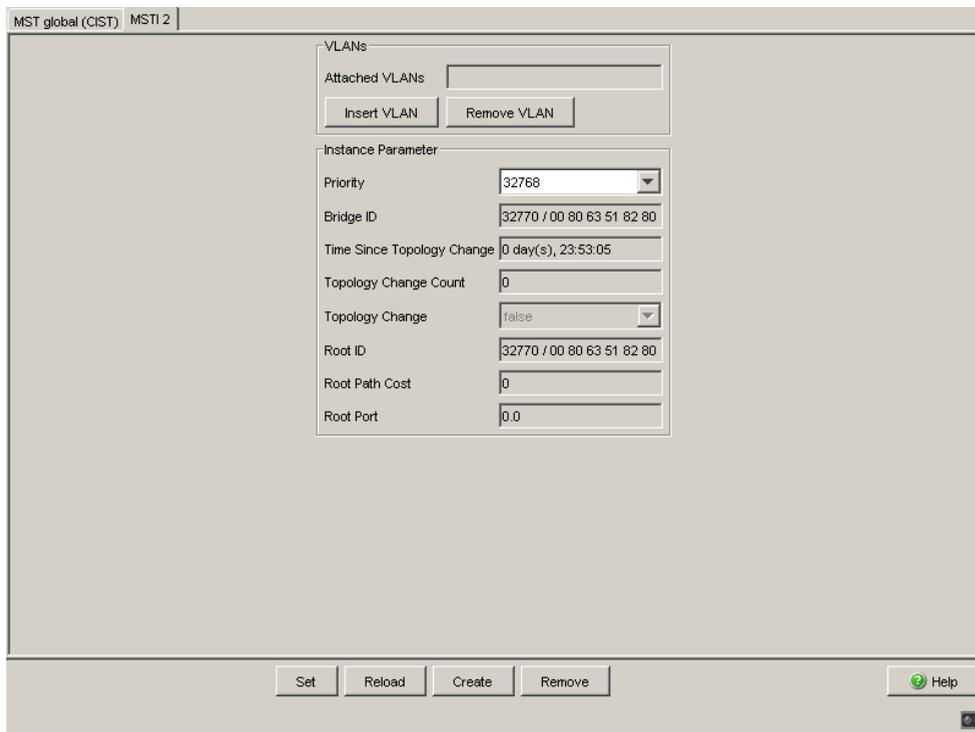


Figure 72: Multiple Spanning Tree dialog, MSTI <ID>

■ 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 MSTP instance.
Remove	Removes a MSTP instance.
Help	Opens the online help.

Table 178: Buttons

7.5.3 Port

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

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

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

The MSTI tabs in the dialog allow you to manage the individual Multiple Spanning Tree Instances. The tab is named MSTI, followed by the number of the instance, e.g. “MSTI 2”.

- ▶ switch Spanning Tree on or off at the individual ports, configure the ports for the global MST Instance (CIST), and display information on the port status,
- ▶ set various protection functions at the ports,
- ▶ configure the ports for an existing MST Instance (port path costs and port priority), read information on the port status, and display information for the selected MSTI.

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	-

Table 179: Port-related STP settings and displays, CIST

Parameters	Meaning	Possible values	Default setting
Port Role (read only)	Displays the STP port role with regard to the global MSTI (IST).	root alternate designated backup master disabled	-
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)	-
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	-

Table 179: Port-related STP settings and displays, CIST

Parameters	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 forwarding status, if applicable.</p> <p>This setting applies to all MSTIs.</p>	active (box selected), inactive (box empty)	inactive
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 $1.5 \cdot \text{Hello Time}$ (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>	active (box selected), inactive (box empty)	active

Table 179: Port-related STP settings and displays, CIST

Parameters	Meaning	Possible values	Default setting
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, 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, false</code> The device determines this condition from the duplex mode: FDX: <code>true</code> HDX: <code>false</code>	

Table 179: 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 73: 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 180: 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 <i>designated</i>. 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 <i>discarding</i>, instead of assigning the port the STP port role <i>root</i>. 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>active (box selected), inactive (box empty)</p>	<p>inactive</p>
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>active (box selected), inactive (box empty)</p>	<p>inactive</p>

Table 180: 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)	<p>Counts how often the device has set the port to the loop status (“Loop Status” column <code>true</code>).</p>	0 - 4294967295 ($2^{32}-1$)	0

Table 180: 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 169).</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 180: Port-related STP settings and displays, guards

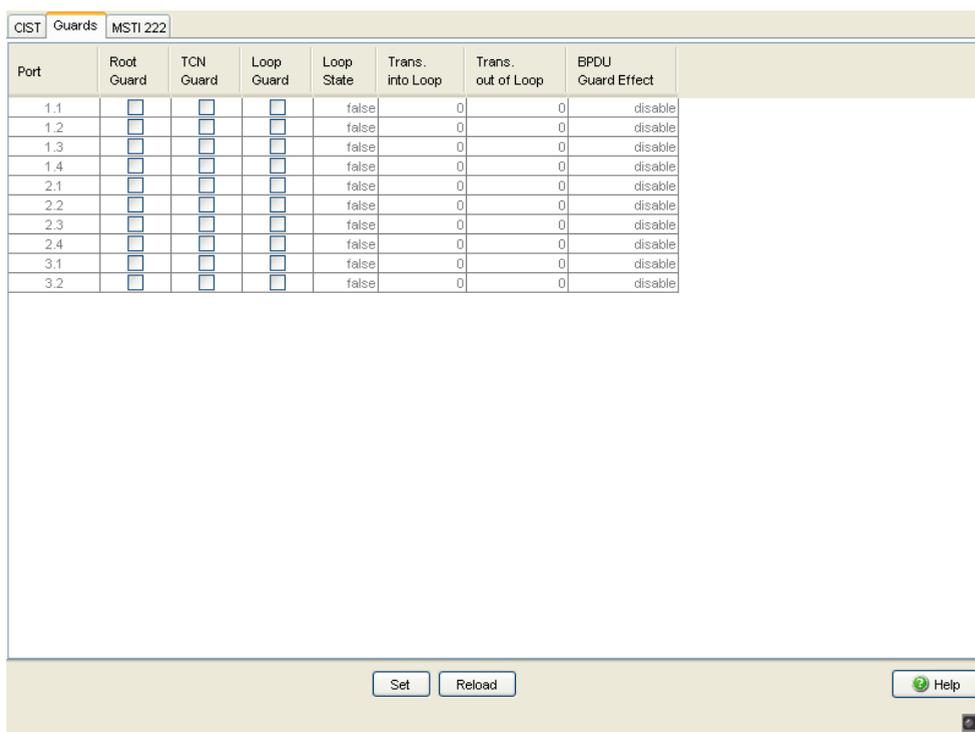


Figure 74: Multiple Spanning Tree dialog, Port, Guards tab

Parameters	Meaning	Possible values	Default setting
“MSTI <ID>” tab	Port configuration and information on the selected MSTI.		
	Note: Note: the device only displays the MSTI ... tab if you have configured at least 1 MST instance.		
Port status (read only)	Displays the STP port status with regard to the current MSTI.	discarding, learning, forwarding, disabled, manualForwarding, notParticipate	-
Port role (read only)	Displays the STP port role with regard to the current MSTI.	root, alternate, designated, backup, master, disabled	-

Table 181: Port-related STP settings and displays, per MSTI

Parameters	Meaning	Possible values	Default setting
Port path costs	Enter the path costs with regard to the current MSTI to indicate preference for redundant paths. If the value is 0, the Switch automatically calculates the path costs 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 current MSTI 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 of the current MSTI from which this port last received a BPDU. ^a	Bridge identification (format ppppp / mm mm mm mm mm mm)	-
Received port ID (read only)	Displays the port ID of the remote bridge of the current MSTI from which this port last received a 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 root bridge of the current MSTI. ^a	0-200000000	-

Table 181: Port-related STP settings and displays, per MSTI

- ^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.

Port	Port State	Port Role	Port Pathcost	Port Priority	Received Bridge ID	Received Port ID	Received Path Cost
1.1	disabled	disabled	0	128	32770 / 00 80 63 51 82 80	80 01	0
1.2	forwarding	designated	20000	128	32770 / 00 80 63 51 82 80	80 02	0
1.3	forwarding	designated	20000	128	32770 / 00 80 63 51 82 80	80 03	0
1.4	forwarding	master	20000	128	32770 / 00 80 63 51 82 80	80 04	0
2.1	forwarding	designated	200000	128	32770 / 00 80 63 51 82 80	80 05	0
2.2	forwarding	designated	200000	128	32770 / 00 80 63 51 82 80	80 06	0
2.3	disabled	disabled	0	128	32770 / 00 80 63 51 82 80	80 07	0
2.4	forwarding	designated	200000	128	32770 / 00 80 63 51 82 80	80 08	0
3.1	disabled	disabled	0	128	32770 / 00 80 63 51 82 80	80 09	0
3.2	disabled	disabled	0	128	32770 / 00 80 63 51 82 80	80 0a	0

Figure 75: Multiple Spanning Tree dialog, Port, MSTI <ID> 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 182: Buttons

7.6 VRRP/HiVRRP

The Virtual Router Redundancy Protocol (VRRP) is a procedure that enables the system to react to the failure of a router.

VRRP is used in networks with terminal devices that only support one entry for the default gateway. If the default gateway fails, VRRP ensures that the terminal devices find a redundant gateway.

The Hirschmann company has further developed the VRRP into the Hirschmann Virtual Router Redundancy Protocol (HiVRRP). With the appropriate configuration, HiVRRP provides switching times of less than 400 ms.

Note: You will find detailed information on VRRP and HiVRRP in the "Routing Configuration" user manual.

7.6.1 VRRP/HiVRRP Configuration

With this dialog you can enter general settings and settings for each port for the VRRP.

You can configure

- up to 8 virtual routers per port and
- up to 16 entries with HiVRRP per router.

■ General settings

Parameter	Meaning
Operation	Switch the VRRP function on and off
Version	Display the VRRP version

Table 183: VRRP general settings

Parameter	Meaning
Send VRRP Master Trap	As soon as the router takes over the VRRP master function, it sends a master trap
Send VRRP Authentication Failure Trap	As soon as the router receives a VRRP message with an incorrect authentication, it sends a VRRP authentication error trap.

Table 183: VRRP general settings

Port	VRID	Function	State	Priority	Current Priority	VRRP IP Address	HiVRRP Advert Interval [ms]	Preempt mode	Preempt-Delay [s]	Domain-ID	Domain-Role
2.1	1	<input type="checkbox"/>	initialize	100	100	10.0.11.1	1000	<input checked="" type="checkbox"/>	2000	0	none

Figure 76: VRRP/HiVRRP Configuration dialog

■ VRRP instance settings

Parameter	Meaning
Port	Port to which this entry applies
VRID	Virtual router ID (value 1-255)
Function	Switch the VRRP instances on and off
State	VRRP state <ul style="list-style-type: none"> - initialize: VRRP is in the initialization phase. No master has been named yet. - backup: The router sees the possibility of becoming master. - master: The router is master.

Table 184: VRRP configuration table

Parameter	Meaning
Priority	VRRP priority set (value: 1-255; default: 100). The router with the highest value takes over the master function. If the virtual router IP address is the same as the IP address of the router interface, then this router is the “owner”. If an owner exists, then VRRP assigns the owner the VRRP priority 255 and thus declares it the master.
Current Priority	VRRP priority actually used (value: 1-255). This value is usually the same as the VRRP priority set, but it can be smaller if monitored tracking objects have the “down” status.
VRRP IP address	Primary virtual router IP address.
HiVRRP Advert Interval[ms]	Interval for sending out messages (advertisements) as the master (value for VRRP: 1-255 s, value for HiVRRP: 100-255,000 ms, default setting: 1 s).
Preempt mode	This setting specifies whether this router, as a backup router, will take over the master role from a master router with a lower VRRP priority. If the preempt mode is switched off, this router only takes on the master role if the IP Multicast message from the existing master does not appear.
Preempt Delay[s]	The preempt mode, in collaboration with VRRP tracking, can enable a switch to a better router. However, dynamic routing procedures take a certain amount of time to react to changed routes and refill their routing table. To avoid the loss of packets during this time, delayed switching (preempt delay) from the master router to the backup router enables the dynamic routing procedure to fill the routing tables (value: 0-65535 s, default setting 0 s).
Domain ID	The domain ID is a number identifying the domain (see on page 307 “HiVRRP Domains”). Value: 0-8, default setting 0 = no domain.
Domain Role	<code>none</code> : not a member of a domain <code>member</code> : copies the behavior of the supervisor <code>supervisor</code> : determines the behavior of the domains
Authentication Type	Type of authentication used: – <code>noAuthentication</code> : VRRP information is exchanged without authentication. – <code>simpleTextPassword</code> : VRRP information is exchanged with plain text password authentication.
Authentication Key	Password for authentication. In order to communicate, the routers with the same virtual router IP address must have the same authentication setting.
Master IP Address	Actual router interface IP address of the master.

Table 184: VRRP configuration table

■ Setting up the VRRP router instance

- In the `Redundancy:VRRP/HiVRRP:Configuration` dialog, click “Wizard” at the bottom right.
- In the table in the Wizard dialog, select a port row and enter the virtual router ID in the VRID row. You can configure up to 8 virtual routers per interface.
- Click “Next”.
- Under “Edit entry” in the “Basic configuration” frame, enter:
 - the IP address of the virtual router
 - the VRRP priority
 - the type of authentication
 - the key for the authentication
 - the preempt delay
 - the advertisement interval.If necessary, select the preempt mode
Switch on the operation of VRRP.
If you want
 - switching times of less than 3 s,
 - the routers to use Unicasts to communicate with each other,
 - to set up domains or
 - to send link-down notifications,you activate the “HiVRRP” field.
In the “HiVRRP” frame, enter:
 - the “Advertisement Interval”
 - the “Destination Address”. The HiVRRP destination address is the IP address of the partner HiVRRP router.
 - the IP address of the second router to which the link-down notifications are sent. This function can be used when the virtual router consists of two VRRP routers.
 - the domain ID
 - the domain role
- Click “Finish” to transfer the VRRP router interface to the VRRP router interface table
or
- Click “Next” to assign tracking objects to the virtual router under “Tracking”. If a tracking object’s status changes to “down”, the VRRP priority is decremented.
Select an existing tracking entry and click “Add”. You can add up to 8 tracking objects. Ascertain that the sum of the decrements of all the assigned tracking entries is less than the VRRP priority of this VRRP interface.

Note: As the IP address owner has the fixed VRRP priority 255 by definition, the VRRP tracking function requires the IP addresses of the VRRP router interfaces to differ from the virtual router IP address.

Note: Activate the preempt mode so that, the backup router can take over the master role after the decrementation of the master's VRRP priority via the tracking function.

- Click "Finish" to transfer the VRRP router interface to the VRRP router interface table
- or
- Click "Next" if you want to enter additional IP addresses under "Associated IP Addresses" (Multinetting).
- Click "Finish" to transfer the VRRP router interface to the VRRP router interface table.

■ Configuring the VRRP router instance

- In the `Redundancy:VRRP/HiVRRP:Configuration` dialog, double-click a cell of the table and edit the entry or right-click a cell and select a value.
- As an alternative to editing directly in the table, you can mark a row in the table and use the Wizard to edit it.

■ Deleting a VRRP router instance

- In the `Redundancy:VRRP/HiVRRP:Configuration` dialog, select a row and click "Remove". You thus delete the row.

■ 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.

Table 185: Buttons

Button	Meaning
Remove	Removes the selected table entry.
Wizard	Opens the "Wizard". With the "Wizard" you assign the permitted MAC addresses to a port.
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.
Help	Opens the online help.

Table 185: Buttons (cont.)

7.6.2 HiVRRP Domains

A HiVRRP instance is a router instance configured as HiVRRP with functions that HiVRRP contains. In a HiVRRP domain you combine multiple HiVRRP instances of a router into one administrative unit. You nominate one HiVRRP instance as the supervisor of the HiVRRP domain. This supervisor regulates the behavior of all HiVRRP instances in its domain.

The router supports up to 8 domains.

■ Displaying HiVRRP domains

Parameters	Meaning
Domain ID	identification of the domains
Status	status of the supervisor of the domains noError: supervisor is active SupervisorDown: supervisor is not active noSupervisor: no supervisor defined
Supervisor Port	HiVRRP instance (module and port, written as <Slot>.<Port>) that was defined as the supervisor
Supervisor VRID	VRID of the supervisor

Table 186: Displaying HiVRRP domains

Parameters	Meaning
Supervisor Status	status of the supervisor – <code>initialize</code> : VRRP is in the initialization phase. No master has been named yet – <code>backup</code> : The router sees the possibility of becoming master – <code>master</code> : The router is master – <code>unknown</code> : no supervisor
Current Priority	current VRRP priority
Redundancy Check per Member	Activates the function for the selected domain.

Table 186: Displaying HiVRRP domains

■ HiVRRP domain instances at different ports

If domain instances (members) are divided among different physical ports, the router monitors by default only the supervisor's connection for line interruptions (“Redundancy Check per Member” deactivated).

You have the option of activating the monitoring of the other connections for line interruptions within the domain. Monitoring means that the router sends HiVRRP messages when it detects a line interruption. If there is a

low probability of a line interruption, you select a long HiVRRP message interval (see on page 303 “VRRP instance settings”) in order to minimize the network load.

- In the “Redundancy check per member” column, you can activate the function for a chosen domain as required.

Domain-Id	Status	Supervisor Port	Supervisor VRID	Supervisor Status	Current Priority	Redundancy Check per Member
1	noSupervisor	0.0	0	unknown	0	<input checked="" type="checkbox"/>
2	noSupervisor	0.0	0	unknown	0	<input checked="" type="checkbox"/>
3	noSupervisor	0.0	0	unknown	0	<input checked="" type="checkbox"/>
4	noSupervisor	0.0	0	unknown	0	<input checked="" type="checkbox"/>
5	noSupervisor	0.0	0	unknown	0	<input checked="" type="checkbox"/>
6	noSupervisor	0.0	0	unknown	0	<input checked="" type="checkbox"/>
7	noSupervisor	0.0	0	unknown	0	<input type="checkbox"/>
8	noSupervisor	0.0	0	unknown	0	<input type="checkbox"/>

Figure 77: HiVRRP domain 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 187: Buttons

7.6.3 Statistics

The VRRP statistics window displays the numbers on counters that count events relevant to VRRP.

Parameter	Meaning
Checksum Error	Number of VRRP messages received with the wrong checksum.
Version Errors	Number of VRRP messages received with an unknown or unsupported version number.
VRID Errors	Number of VRRP messages received with an invalid VRID for this virtual router.

Table 188: VRRP Statistics for All Ports

Parameter	Meaning
Port	Port of the module of the device.
VRID	Virtual router ID.
Become Master	Number of times the Switch has become the master.
Advertise received	Number of VRRP advertisements received.
Advertise interval errors	Number of VRRP advertisements received by the router outside the advertisement interval.
Authentication failures	Number of VRRP advertisements received with authentication errors.
IP TTL errors	Number of VRRP advertisements received with an IP-TTL not equal to 255.
Priority Zero packets received	Number of VRRP advertisements via a VRRP participant with priority 0.
Priority Zero packets sent	Number of VRRP advertisements that the Switch sent with priority 0.
Invalid Type packets received	Number of VRRP advertisements received with an invalid type.
Address list errors	Number of VRRP advertisements received for which the address list does not match the address list configured locally for the virtual router.
Invalid authentication type	Number of VRRP advertisements received with an invalid authentication type.
Authentication type mismatch	Number of VRRP advertisements received with an incorrect authentication type.
Packet length errors	Number of VRRP advertisements received with an incorrect packet length.

Table 189: VRRP port statistics table

Module	Port	VRID	Become master	Advertise received	Advertise Interval errors	Authentication failures	IP TTL errors	Priority
2	1	1	0	0	0	0	0	0
2	1	2	0	0	0	0	0	0
2	1	5	0	0	0	0	0	0
2	1	255	0	0	0	0	0	0

Figure 78: VRRP statistics 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 190: Buttons

7.6.4 Tracking

The VRRP Tracking window displays the status of all the tracking objects assigned to VRRP objects.

Parameter	Bedeutung
Port	Port to which this entry applies, in the form <Slot>.<Port>
VRID	Virtual router ID of the virtual route assigned.
Track ID	Identification number of the tracking object for which you are registering this entry (see on page 239 “Applications”).
Decrement	Value by which the local router reduces the current VRRP priority of the VRRP router assigned when the tracking object receives the status of “down”.
Status	Current status of the tracking object: “up” or “down”.
Active	Entry is displayed as “active” if the tracking object is completely set up and is activated. More information about active entries: (see figure 79). If the entry is not active, its status is always “up”.

Table 191: VRRP Tracking Table

Port	VRID	Track-id	Decrement	Status	Active
1.1	1	1	20	down	<input checked="" type="checkbox"/>

Buttons: Set, Reload, Delete entry, Help

Figure 79: Tracking dialog

■ Deleting a tracking object

- In the `Redundancy:VRRP:Tracking` dialog, select a row and click "Remove". You thus delete the row.

■ 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	Removes the selected table entry.
Help	Opens the online help.

Table 192: Buttons

8 Diagnostics

The diagnostics menu contains the following tables and dialogs:

- ▶ Syslog
- ▶ Trap Log
- ▶ Ports (statistics, network load, SFP modules, TP cable diagnosis, port monitor)
- ▶ Auto Disable
- ▶ Configuration Check
- ▶ Topology Discovery
- ▶ Port Mirroring
- ▶ Device Status
- ▶ Signal Contact
- ▶ Alarms (Traps)
- ▶ Report (log file, system information)
- ▶ IP Address Conflict Detection
- ▶ Self-test

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

8.1 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 320 “Trap log”](#)) and in the log file ([see on page 372 “Event Log”](#)). The device evaluates SNMP requests as events if you have activated “Log SNMP Set/Get Request” ([see table 194](#)).

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 193: 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 193: 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 194: 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 80: Syslog dialog

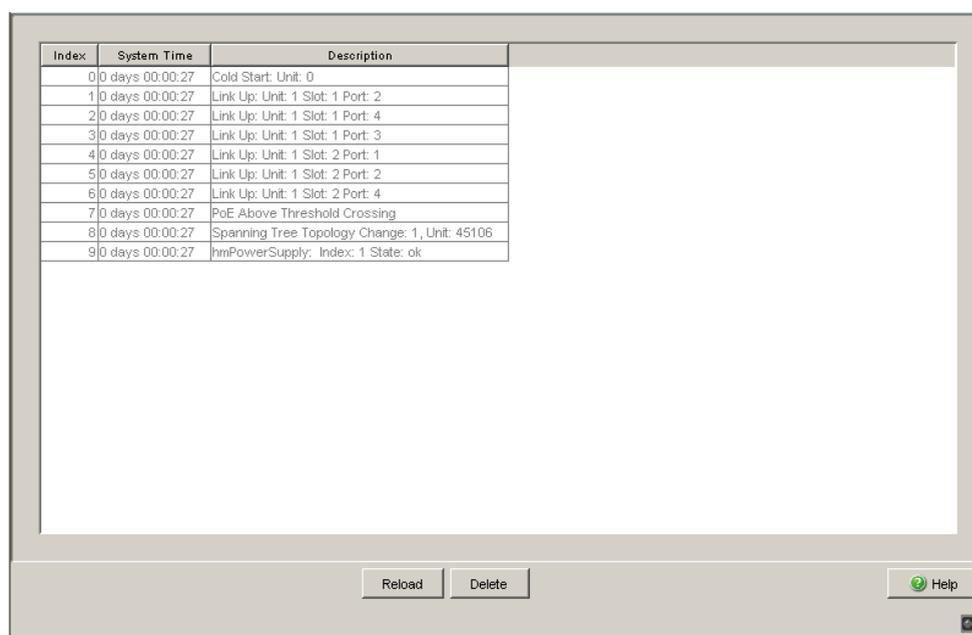
■ Buttons

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 195: Buttons

8.2 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 81: 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 196: Trap log table

You have the option to also send the logged events to one or more syslog servers ([see on page 316 “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 197: Buttons

8.3 Ports

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

- ▶ Statistics table
- ▶ Utilization
- ▶ SFP Modules
- ▶ TP cable diagnosis
- ▶ Port Monitor

8.3.1 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 82: 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 198: Buttons

8.3.2 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 83: 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 199: 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 200: Buttons

8.3.3 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 201: 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 84: 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 202: Buttons

8.3.4 TP Cable Diagnosis

The TP cable diagnosis allows you to check the connected cables for short-circuits or interruptions.

Note: While the check is running, the data traffic at this port is suspended.

- Select the TP port on which you want to perform the check.
- Click "Set" to start the check.

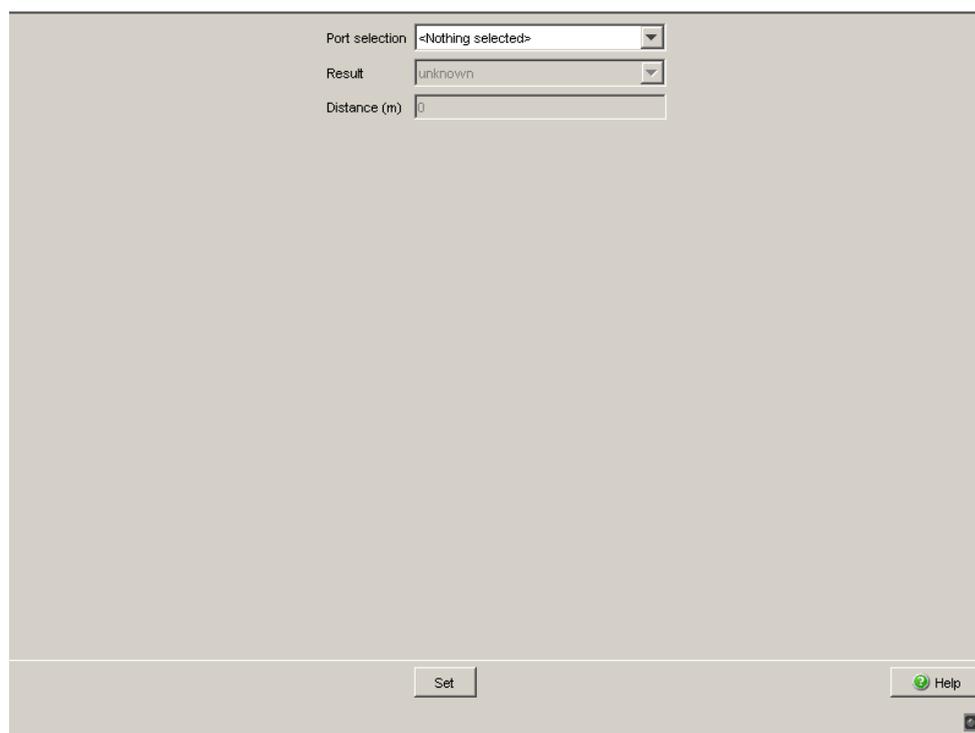


Figure 85: TP cable diagnosis dialog

The check takes a few seconds. After the check, the "Result" row contains the result of the cable diagnosis. If the result of the check shows a cable problem, then the "Distance" row contains the cable problem location's distance from the port.

Result	Meaning
normal	The cable is okay.
open	The cable is interrupted.
short circuit	There is a short-circuit in the cable.
unknown	No cable check was performed yet, or it is currently running

Table 203: Meaning of the possible results

Prerequisites for correct TP cable diagnosis:

- ▶ 1000BASE-T port, connected to a 1000BASE-T port via 8-core cable or
- ▶ 10BASE-T/100BASE-TX port, connected to a 10BASE-T/100BASE-TX port.

■ 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".
Help	Opens the online help.

Table 204: Buttons

8.3.5 Port Monitor

The Port Monitor monitors the ports of the device. When an event occurs, the device performs an action for the port, e.g. if there are too many connection breaks due to a loose contact.

■ Global

On the "Global" tab you define the triggering events and an action for the ports to be monitored:

- Switch on the function globally in the "Operation" frame.
- For every port to be monitored, mark the checkbox in the "Port Monitor on" column.
- Define the triggering event for every port to be monitored. To do this, mark the checkboxes in the "Link Flap on" to "Link Speed and Duplex Mode on" columns.
- Define the parameters for the triggering event on the related tab.
- For every port to be monitored, select the action that the device is to perform in the "Action" column.
- Save the settings.

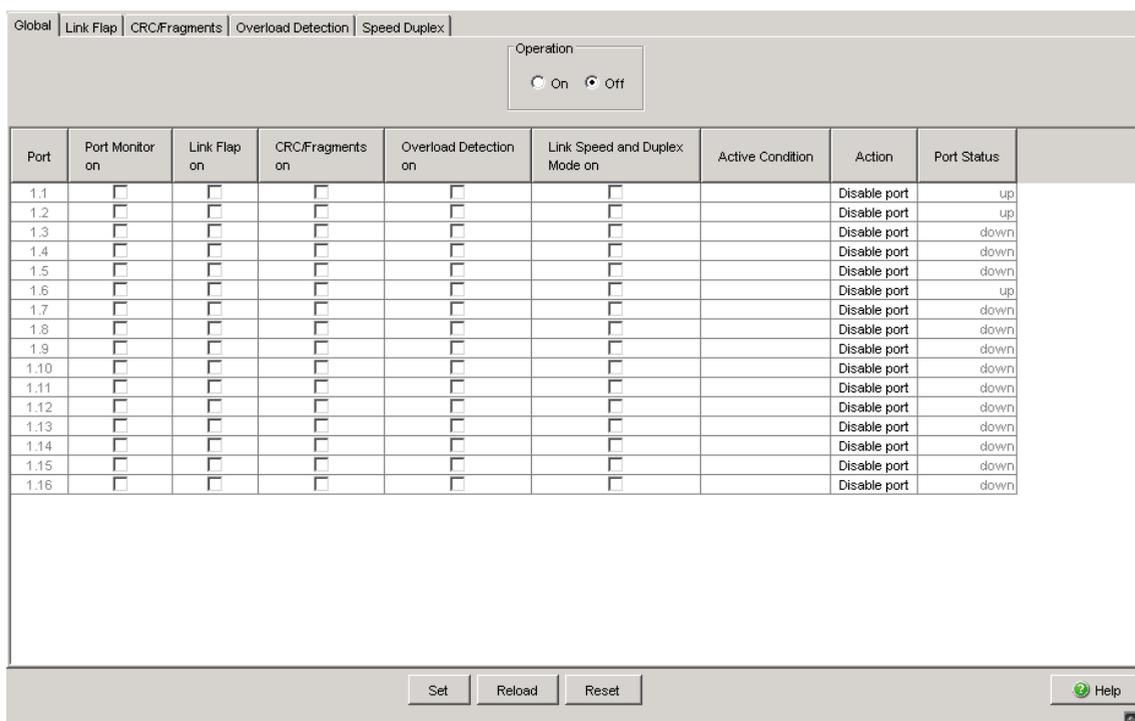


Figure 86: Global Port Monitor Dialog

Parameter	Meaning
“Operation” Frame	Switches the “Port monitor” function for the device on or off.
Port table	
Port	List of the available ports on the device.
Port Monitor on	You select the ports to be monitored here.
Link Changes on	You select here whether link changes trigger an action. Changes from the “Link down” state to “Link up” are treated as link changes.
CRC/Fragment Error on	You select here whether CRC or fragment errors that occur trigger an action.
Overload Detection on	You select here whether overload detection triggers an action.
Link Speed and Duplex Mode on	You select here whether an incorrect combination of duplex mode and transmission speed triggers an action.
Active Condition	Shows the condition on the basis of which the device performed an action on this port.

Table 205: Port Monitor Global table

Parameter	Meaning
Action	<p>You select the action here that the device performs when the triggering event occurs. The following actions are possible:</p> <ul style="list-style-type: none"> ▶ <code>Disable port</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 is marked for the triggering event that disabled the port. – The reset timer is defined >0 for the port. ▶ <code>Send trap</code> Sends an SNMP trap. The port remains enabled. ▶ <code>Auto Disable</code> Disables the port depending on the settings on 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 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 for the port is defined >0 in the <code>Diagnostics:Ports:Auto Disable</code> dialog for the port. If the device has disabled the port due to an overload, further prerequisites apply for the re-enabling of the port (see on page 336 "Overload Detection"). – The port remains enabled when the checkbox for the triggering event is unmarked.
Port Status	<p>Displays the current port status.</p> <ul style="list-style-type: none"> – <code>up</code>: data transmission via the port is possible. – <code>down</code>: data transmission via the port is interrupted. – <code>notPresent</code>: no physical port is present.

Table 205: Port Monitor Global table

■ Link Flap

On the "Link Flap" tab, define the parameters on the basis of which the device triggers an action for the relevant port if there are too many link changes:

- Open the "Link Flap" tab.
- On the "Parameter" tab, define the number of link changes and the related interval.

These parameters apply to all ports for which the checkbox is marked on the "Global" tab, "Link Flap on" column.

- Save the settings.

Port	Last Sampling Interval	Total
1.1	0	0
1.2	0	0
1.3	0	0
1.4	0	0
1.5	0	0
1.6	0	0
1.7	0	0
1.8	0	0
1.9	0	0
1.10	0	0
1.11	0	0
1.12	0	0
1.13	0	0
1.14	0	0
1.15	0	0
1.16	0	0

Figure 87: Link Flap Port Monitor Dialog

Note: For ports at which you have set the number of link changes to the value of 1, note the following particularity:

If you have selected the "Disable Port" action, the device deactivates the port as early as after the 1st link change. The "Link Up" change also relates to this in the following instances:

- ▶ on restarting the device, if a communication partner is already connected to the port,
- ▶ on the 1st connection of communication partner and
- ▶ on loading a configuration ([see on page 52 "Loading a Configuration"](#)).

If the device deactivated all the ports, you can only access the Switch via the V.24 access.

Parameters	Meaning
Link Flap Count	Number of link changes in the completed sampling interval that leads to an action by the device.
Sampling Interval [s]	Length of the sampling interval in which the device determines the number of link changes.
Port table	
Port	List of the device's available ports.
Last Sampling Interval	Number of link changes during the last sampling interval. Link changes are also still counted after the port is deactivated.
Total	Sum of all link changes having occurred up to now. Link changes are also still counted after the port is deactivated.

Table 206: Link Changes Port Monitor Table

■ CRC/Fragments

On the "CRC-/Fragments" tab, define the parameters on the basis of which the device triggers an action for the relevant port if too many faulty Ethernet packets are received:

- Open the "CRC-/Fragments" tab.
- In the "Parameter" frame, define the rate of the faulty packets (in parts per million) and the related interval.

These parameters apply to all ports for which the checkbox is marked on the "Global" tab, "CRC-/Fragments on" column.

- Save the settings.

Port	Last active Interval [ppm]	Total [ppm]
1.1	0	0
1.2	0	0
1.3	0	0
1.4	0	0
1.5	0	0
1.6	0	0
1.7	0	0
1.8	0	0
1.9	0	0
1.10	0	0
1.11	0	0
1.12	0	0
1.13	0	0
1.14	0	0
1.15	0	0
1.16	0	0

Figure 88: CRC/Fragment Error Port Monitor Dialog

Parameters	Meaning
CRC/Fragments count [ppm]	Fragment error rate in the completed sampling interval that leads to an action by the device.
Sampling Interval [s]	Length of the sampling interval in which the device determines the CRC/fragment error rate.
Port table	
Port	List of the device's available ports.

Table 207: CRC/Fragments Port Monitor Table

Parameters	Meaning
Last active Interval [ppm]	Detected error rate during the last active sampling interval that triggered the action.
Total [ppm]	Total error rate that has occurred so far in ppm (parts per million).

Table 207: CRC/Fragments Port Monitor Table

■ Overload Detection

On the "Overload Detection" tab, define the parameters on the basis of which the device triggers an action for the relevant port if there is an overload.

- Open the "Overload Detection" tab.
- Define the interval in the "Parameter" frame.
This parameter applies to all ports for which the checkbox is marked on the "Global" tab, "Overload Detection on" column.
- In the "Traffic Type" column, define which packets the device considers for the load detection.
- In the "Upper Threshold" column, define the desired value in `pps` (packets per second).
If the data rate on the port exceeds this value, the device performs the action defined on the "Global" tab for the port.
- In the "Lower Threshold" column, define the desired value in `pps` (packets per second) if you are using the `Send trap` or `Auto Disable` action on the port.
The auto-disable function re-enables a disabled port when the following prerequisites are fulfilled:
 - In the auto-disable settings, the "Reset Timer" value for the port is defined `>0`.
 - The time defined in "Reset Timer" has elapsed.
 - The load on the port is lower than the value defined in the "Lower Threshold" column.

- On the MACH104 and MACH1040 devices, you have the option to change the `pps` (packets per second) unit pre-defined in the "Threshold Type" column.
 - With the `kbps` unit you define the load in the "Upper Threshold" and "Lower Threshold" columns in the range `0..10000000` kbit/s.
 - With the `link-capacity` unit you define the load in the "Upper Threshold" and "Lower Threshold" columns in the range `0..100%`.
- Save the settings.

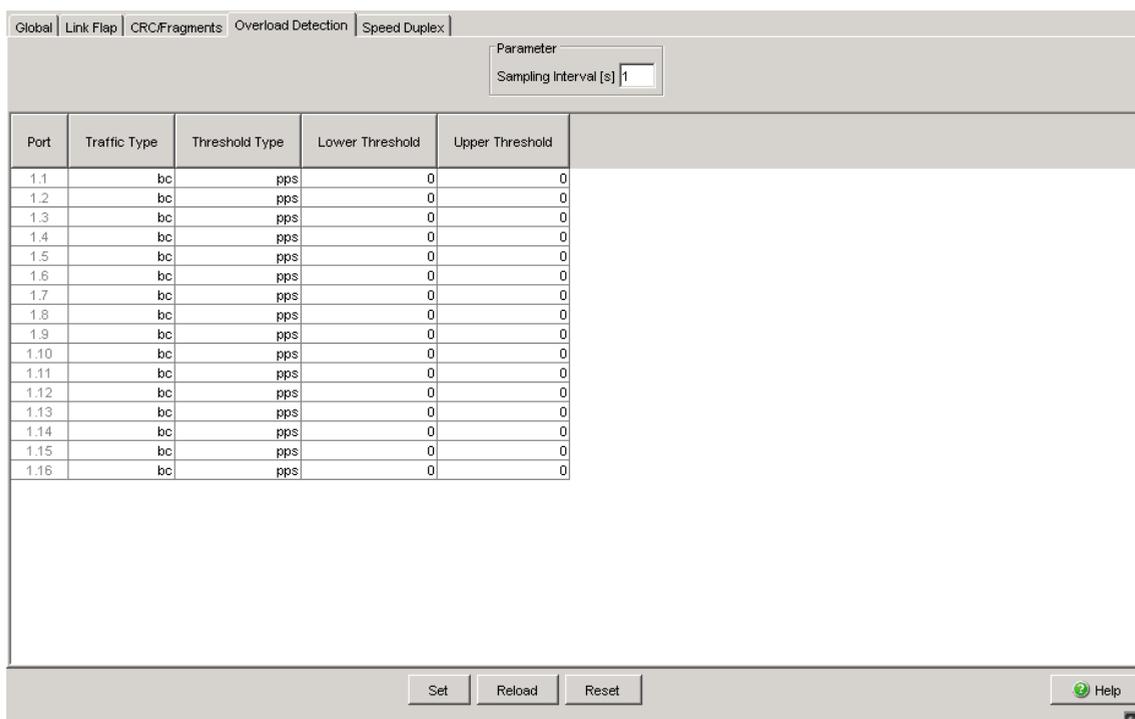


Figure 89: Overload Detection Port Monitor Dialog

Parameters	Meaning
Sampling Interval [s]	Length of the sampling interval in which the device determines the amount of values below and above the permitted thresholds.
Port table	
Port	List of the device's available ports.

Table 208: CRC/Fragments Port Monitor Table

Parameters	Meaning
Traffic Type	<p>Defines the overload detection traffic type. The following types are possible:</p> <ul style="list-style-type: none"> – all: The overload function uses unicast, broadcast and multicast traffic for threshold detection. – bc: The overload function uses broadcast traffic for threshold detection. – bc-mc: The overload function uses broadcast and multicast traffic for threshold detection.
Threshold Type	<p>Defines the overload detection threshold type. The following types are possible:</p> <ul style="list-style-type: none"> – pps - packets per second <p>Available on the MACH1040 and MACH104:</p> <ul style="list-style-type: none"> – kbps - kilobits per second – link-capacity - percent of the link capacity
Lower Threshold	Defines the value at which the device auto-enables the port.
Upper Threshold	Defines the value at which the device auto-disables the port.

Table 208: CRC/Fragments Port Monitor Table

■ Speed Duplex

On the "Speed Duplex" tab, you define the permitted combinations of speed and duplex mode. If the device detects an unpermitted combination of speed and duplex mode, it triggers an action for the relevant port:

- Open the "Speed Duplex" tab.
- You define for each port individually which duplex mode is permitted for which speed.
- Save the settings.

Note: The port monitor monitors the speed and the duplex mode exclusively on enabled physical ports.

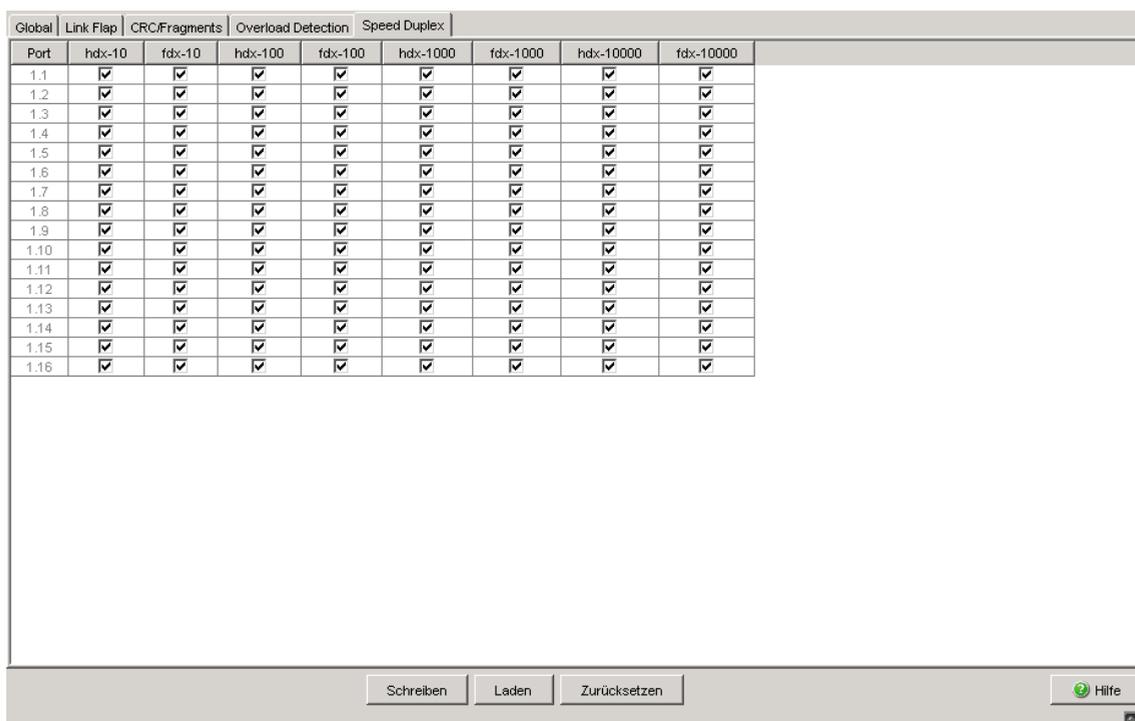


Figure 90: Port-Monitor Speed Duplex dialog

Parameters	Meaning
Port	List of the device's available ports.
hdx-10	<p>Activates/deactivates the port monitor to accept a half-duplex and 10 Mbit/s data rate combination on the port.</p> <p>Possible values:</p> <ul style="list-style-type: none"> ▶ <code>marked</code> (default setting) The port monitor allows the speed and duplex combination. ▶ <code>unmarked</code> If the port monitor detects the speed and duplex combination on the port, then the device executes the action specified in the "Global" tab.
fdx-10	<p>Activates/deactivates the port monitor to accept a full-duplex and 10 Mbit/s data rate combination on the port.</p> <p>Possible values:</p> <ul style="list-style-type: none"> ▶ <code>marked</code> (default setting) The port monitor allows the speed and duplex combination. ▶ <code>unmarked</code> If the port monitor detects the speed and duplex combination on the port, then the device executes the action specified in the "Global" tab.

Table 209: Port-Monitor Speed Duplex table

Parameters	Meaning
hdx-100	<p>Activates/deactivates the port monitor to accept a half-duplex and 100 Mbit/s data rate combination on the port.</p> <p>Possible values:</p> <ul style="list-style-type: none"> ▶ <code>marked</code> (default setting) The port monitor allows the speed and duplex combination. ▶ <code>unmarked</code> If the port monitor detects the speed and duplex combination on the port, then the device executes the action specified in the "Global" tab.
fdx-100	<p>Activates/deactivates the port monitor to accept a full-duplex and 100 Mbit/s data rate combination on the port.</p> <p>Possible values:</p> <ul style="list-style-type: none"> ▶ <code>marked</code> (default setting) The port monitor allows the speed and duplex combination. ▶ <code>unmarked</code> If the port monitor detects the speed and duplex combination on the port, then the device executes the action specified in the "Global" tab.
hdx-1000	<p>Activates/deactivates the port monitor to accept a half-duplex and 1 Gbit/s data rate combination on the port.</p> <p>Possible values:</p> <ul style="list-style-type: none"> ▶ <code>marked</code> (default setting) The port monitor allows the speed and duplex combination. ▶ <code>unmarked</code> If the port monitor detects the speed and duplex combination on the port, then the device executes the action specified in the "Global" tab.

Table 209: Port-Monitor Speed Duplex table

Parameters	Meaning
fdx-1000	<p>Activates/deactivates the port monitor to accept a full-duplex and 1 Gbit/s data rate combination on the port.</p> <p>Possible values:</p> <ul style="list-style-type: none"> ▶ <code>marked</code> (default setting) The port monitor allows the speed and duplex combination. ▶ <code>unmarked</code> If the port monitor detects the speed and duplex combination on the port, then the device executes the action specified in the "Global" tab.
fdx-10000	<p>Available on the MACH4002 24G/48G and MACH104:</p> <p>Activates/deactivates the port monitor to accept a full-duplex and 10 Gbit/s data rate combination on the port.</p> <p>Possible values:</p> <ul style="list-style-type: none"> ▶ <code>marked</code> (default setting) The port monitor allows the speed and duplex combination. ▶ <code>unmarked</code> If the port monitor detects the speed and duplex combination on the port, then the device executes the action specified in the "Global" tab.

Table 209: Port-Monitor Speed Duplex 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.
Reset	Resets the port monitor function for the selected interface and enables the port when disabled by the Port Monitor function.
Help	Opens the online help.

Table 210: Buttons

8.3.6 Auto Disable

The auto-disable function allows you to automatically re-enable ports that the port monitor has disabled after a user-defined period of time. In the process, the device allows multiple triggering events to be considered.

You define the triggering events on the basis of which the device disables the ports in the settings for the port security (see on page 87 “Port Security”) and the port monitor (see on page 330 “Port Monitor”).

When the port monitor performs the `Auto Disable` action for a port, the settings in the "Auto-Disable" dialog, "Configuration" frame, decide what happens to the port:

- ▶ The device disables the port when the checkbox for the triggering condition is marked. Then the port LED on the device blinks green 3 times per period.
The device re-enables the port if the Reset Timer value for the port is defined >0 .
- ▶ The port remains enabled when the checkbox for the triggering event is unmarked.

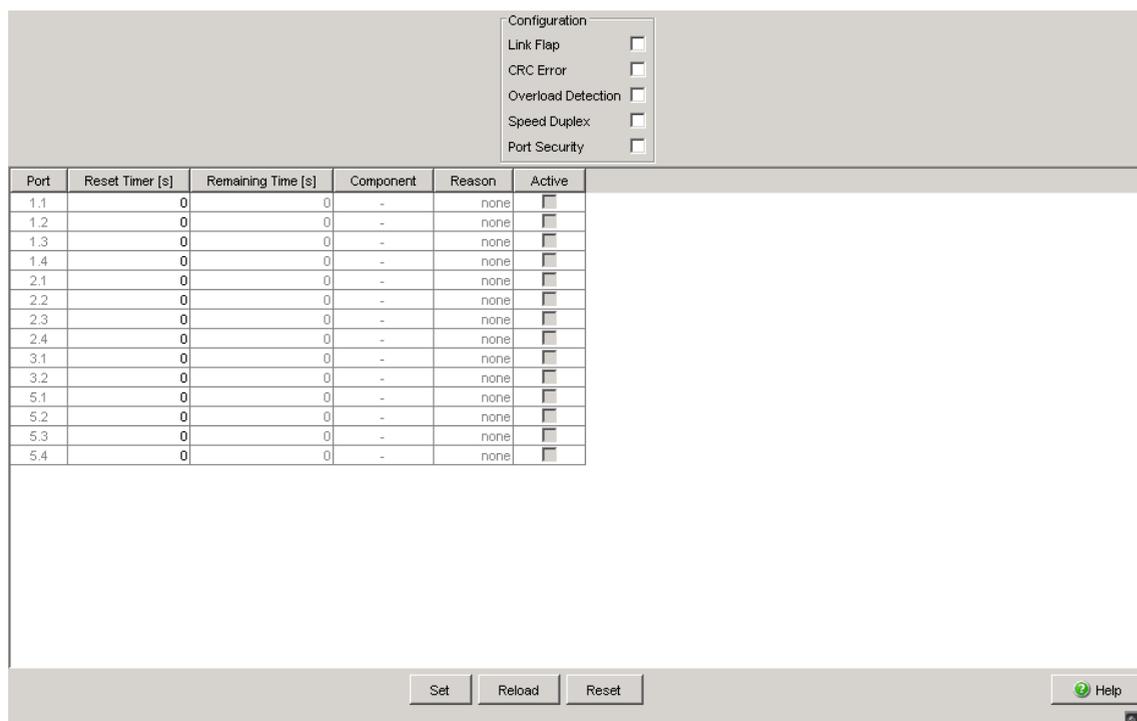


Figure 91: "Auto Disable" dialog

■ Configuration

Parameters	Meaning
Link Flap	<p>Enables/disables the monitoring of link changes on the ports.</p> <p>Possible values:</p> <ul style="list-style-type: none"> ▶ <code>marked</code> The auto-disable function monitors link changes on the ports. When the port monitor disables a port due to too many link changes, the device re-enables the port after the time defined in the “Reset Timer” field has elapsed. The prerequisite for this is that the “Reset Timer” value for the port is >0. ▶ <code>unmarked</code> (default setting) The auto-disable function ignores link changes on the ports.
CRC/Fragments	<p>Enables/disables the monitoring of CRC/fragment errors on the ports.</p> <p>Possible values:</p> <ul style="list-style-type: none"> ▶ <code>marked</code> The auto-disable function monitors CRC/fragment errors on the ports. When the port monitor disables a port due to too many CRC/fragments, the device re-enables the port after the time defined in the “Reset Timer” field has elapsed. The prerequisite for this is that the “Reset Timer” value for the port is >0. ▶ <code>unmarked</code> (default setting) The auto-disable function ignores CRC/fragment errors on the ports.
Overload Detection	<p>Enables/disables the monitoring of the load on the ports.</p> <p>Possible values:</p> <ul style="list-style-type: none"> ▶ <code>marked</code> The auto-disable function monitors the load on the ports. When the port monitor disables a port due to an overload, the device re-enables the port after the time defined in the “Reset Timer” field has elapsed. The prerequisite for this is that the “Reset Timer” value for the port is >0. For more prerequisites, see “Overload Detection” on page 336. ▶ <code>unmarked</code> (default setting) The auto-disable function ignores the load on the ports.

Table 211: "Configuration" frame in the *Diagnostics:Ports:Auto Disable dialog*

Parameters	Meaning
Speed Duplex	<p>Enables/disables the monitoring of the speed and duplex combination on the ports.</p> <p>Possible values:</p> <ul style="list-style-type: none"> ▶ <code>marked</code> The auto-disable function monitors the speed and duplex combination on the ports. When the port monitor disables a port due to an unpermitted combination of speed and duplex mode, the device re-enables the port after the time defined in the "Reset Timer" field has elapsed. The prerequisite for this is that the "Reset Timer" value for the port is >0. ▶ <code>unmarked</code> (default setting) The auto-disable function ignores the speed and duplex combination on the ports.
Port Security	<p>Enables/disables the monitoring of unauthorized accesses to the ports in combination with the "Port Security" function (see on page 87 "Port Security").</p> <p>Possible values:</p> <ul style="list-style-type: none"> ▶ <code>marked</code> The auto-disable function monitors unauthorized accesses to the ports. When the port monitor disables a port due to too many CRC/fragment errors, the device re-enables the port after the time defined in the "Reset Timer" field has elapsed. The prerequisite for this is that the "Reset Timer" value for the port is >0. ▶ <code>unmarked</code> (default setting) The auto-disable function ignores unauthorized accesses to the ports.

Table 211: "Configuration" frame in the *Diagnostics:Ports:Auto Disable* dialog

■ Table

Parameter	Meaning
Port	Shows the number of the device port to which the table entry relates.
Reset Timer [s]	<p>Defines the time in seconds after which the device automatically re-enables the port disabled by the port monitor.</p> <p>Possible values:</p> <ul style="list-style-type: none"> ▶ 0 (default setting) Timer is deactivated. The port remains disabled. ▶ 30...2147483 <p>If the port monitor has disabled the port due to an overload, further prerequisites apply for the re-enabling of the port (see on page 336 "Overload Detection").</p>
Remaining Time [s]	Remaining time in seconds until the automatic re-enabling of the port.

Table 212: Table in the *Diagnostics:Ports:Auto Disable* dialog

Parameter	Meaning
Component	Shows the name of the function that disabled the port.
Reason	Shows the triggering event due to which the port monitor disabled the port.
Active	Shows whether the auto-disable function is active on the relevant port. Possible values: <ul style="list-style-type: none"> ▶ <code>marked</code> The auto-disable function is active on the port. The port is currently disabled. After the time defined in the "Reset Timer" field has elapsed, the auto-disable function re-enables the port. ▶ <code>unmarked</code> (default setting) The auto-disable function is inactive on the port.

Table 212: Table in the *Diagnostics:Ports:Auto Disable* 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.
Reset	Enables the port when disabled by the Port Monitor or Port Security function.
Help	Opens the online help.

Table 213: Buttons

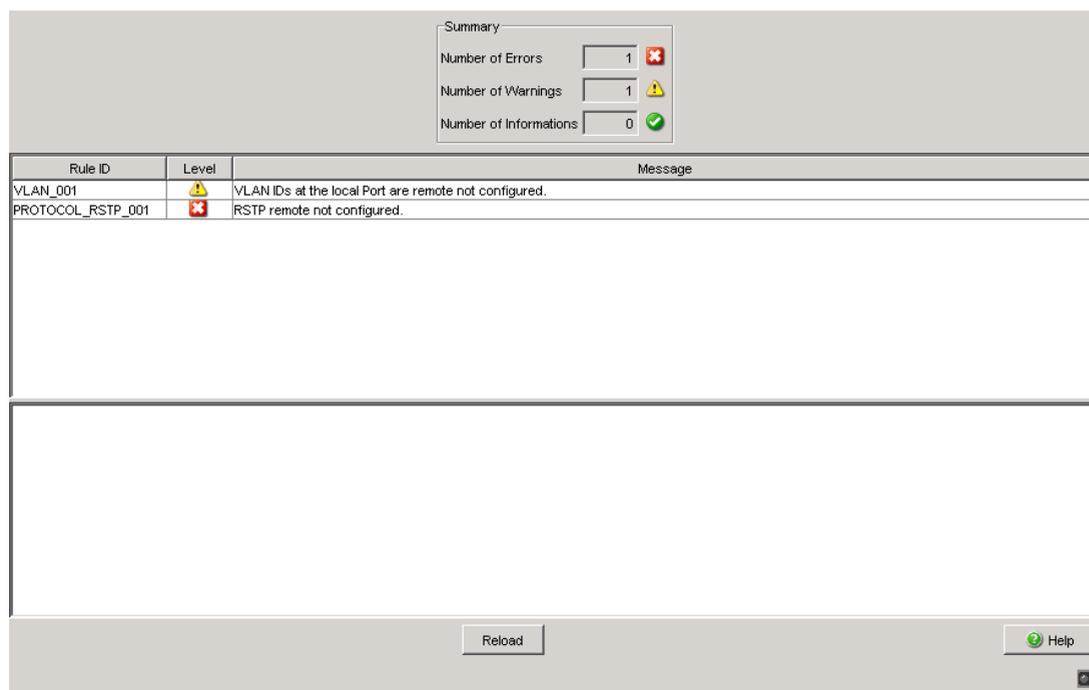
8.4 Configuration Check

The device enables you to compare its configuration with those of its neighboring devices.

For this purpose, it uses the data that it received from its neighboring devices via topology recognition (LLDP).

The dialog lists the deviations detected, which affect the performance of the communication between the device and the recognized neighboring devices.

- You update the table's content via the "Reload" button. If the table remains empty, the configuration check was successful and the device's configuration is compatible for the recognized neighboring devices.



Summary

Number of Errors	1	✖
Number of Warnings	1	⚠
Number of Informations	0	✔

Rule ID	Level	Message
VLAN_001	⚠	VLAN IDs at the local Port are remote not configured.
PROTOCOL_RSTP_001	✖	RSTP remote not configured.

Reload Help

Figure 92: Configuration Check Dialog

Parameters	Meaning
Number of Errors	Displays the number of errors that the device detected during the configuration check.
Number of Warnings	Displays the number of warnings that the device detected during the configuration check.
Amount of Information	Displays the amount of information that the device detected during the configuration check.

Table 214: Configuration Check Summary

Parameters	Meaning
Rule ID	Rule ID of the deviations having occurred. The dialog combines several deviations with the same rule ID under one rule ID.
Level	<p>Level of deviation between this device's configuration and the recognized neighboring devices. The rule level can have 3 statuses:</p> <ul style="list-style-type: none">  Information: The performance of the communication between the two devices is not impaired.  Warning: The performance of the communication between the two devices may be impaired.  Error: Communication between the two devices is impaired.
Message	The dialog specifies more precisely the information, warnings and errors having occurred.

Table 215: Configuration Check table

- If you select a line in the Configuration Check table, the device displays additional information in the window beneath it.

Note: A neighboring device without LLDP support, which forwards LLDP packets, may be the cause of equivocal messages in the dialog. This occurs if the neighboring device is a hub or a switch without management, which ignores the IEEE 802.1D-2004 standard.

In this case, the dialog displays the devices recognized and connected to the neighboring device as connected to the device itself, even though they are connected to the neighboring device.

Note: If you have more than 39 VLANs configured on the device, the dialog always displays a warning. The reason is the limited number of possible VLAN data sets in LLDP frames with a maximum length. The device compares the first 39 VLANs automatically.

If you have 40 or more VLANs configured on a device, check the congruence of the further VLANs manually, if necessary.

■ 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 216: Buttons

8.5 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 2 tables grouped according to general LLDP information and LLDP-MED information.

8.5.1 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.

Table 217: Topology discovery (LLDP information)

Parameters	Meaning
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 217: 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 93: 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 160 “Filter for MAC addresses”](#)).

8.5.2 LLDP-MED (Media Endpoint Discovery)

The card index “LLDP-MED” tabs table shows you the LLDP-MED information about neighboring devices collected. This requires that both the LLDP-MED function and the LLDP function ([see on page 349 “LLDP Information from Neighbor Devices”](#)) are activated.

The device supports the following sub-types in the network connectivity messages:

- ▶ LLDP-MED Capabilities TLV (Subtype 1)
- ▶ LLDP-MED Network Policy TLV (Subtype 2)

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.
Device Class	LLDP-MED device class of the remote device: <ul style="list-style-type: none"> – 0: undefined (properties not included in any defined class) – 1: Terminal Device Class I – 2: Terminal Device Class II – 3: Terminal Device Class III – 4: Network Device
VLAN ID	VLAN ID of the network policy for the remote device's port (0 - 4094), 0: Priority-Tagged Frames
Priority	Layer 2 (IEEE 802.1p) priority of the network policy for the remote device's port (0 - 7)
DSCP	Value of Differentiated Services Code Point (according to RFC 2474 and 2475) of the network policy for the remote device's port (0 - 63)
Unknown Bit Status	<ul style="list-style-type: none"> – <code>true</code>: The network policy for the remote device's application type is currently unknown. The values for VLAN ID, Priority and DSCP are meaningless in this instance. – <code>false</code>: The network policy for the remote device's application type is known.
Tagged Bit Status	<ul style="list-style-type: none"> – <code>true</code>: The remote device's application uses VLAN-tagged frames – <code>false</code>: The remote device's application uses untagged frames or does not support port VLAN-based operation. The values for VLAN ID and Priority are meaningless in this instance.
Hardware Revision	Manufacturer-specific string including the terminal device's hardware version (max. 32 characters)
Firmware Revision	Manufacturer-specific string including the terminal device's firmware version (max. 32 characters)
Software Revision	Manufacturer-specific string including the terminal device's software version (max. 32 characters)
Serial Number	Manufacturer-specific string including the terminal device's serial number (max. 32 characters)
Manufacturer's Name	Manufacturer-specific string including the name of terminal device's manufacturer (max. 32 characters)
Model Name	Manufacturer-specific string including the name of terminal device's model (max. 32 characters)
Asset ID	Manufacturer-specific string including the ID for the terminal device's inventory (max. 32 characters)

Table 218: Topology discovery (LLDP-MED information)

Note: When you activate the LLDP-MED function, the Switch sends out information about its properties in the form of LLDP-MED frames. Information about the voice VLANs configured in the Switch also pertain to it (see on page 192 “Voice VLAN”). As a consequence, activate the LLDP-MED function if you want to operate the Switch devices, e.g. a VoIP telephone via plug-and-play, because both devices require information about their respective neighboring devices on that account.

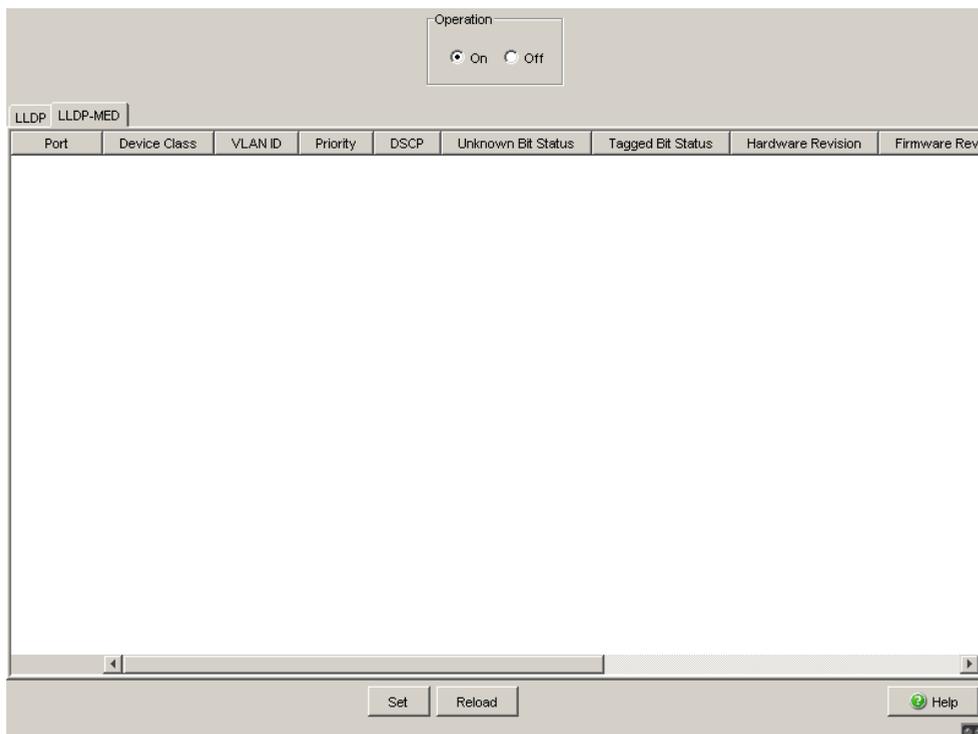


Figure 94: LLDP-MED Information

■ 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 219: 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 219: Buttons (cont.)

8.6 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 MACH4002 24/48 + 4G and the Power MICE support 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)

- Specify the monitoring traffic direction.
 - When selecting "RX", only frames received on the source port will be mirrored to the destination port (monitoring ingress).
 - When selecting "TX", only frames transmitted on the source port will be mirrored to the destination port (monitoring egress).
- To enable the function, select `On` in the "Operation" frame and click "Set".
Default setting: `Off`.

Source Port	RX	TX
1.1	<input type="checkbox"/>	<input type="checkbox"/>
1.2	<input type="checkbox"/>	<input type="checkbox"/>
1.3	<input type="checkbox"/>	<input type="checkbox"/>
1.4	<input type="checkbox"/>	<input type="checkbox"/>
2.1	<input type="checkbox"/>	<input type="checkbox"/>
2.2	<input type="checkbox"/>	<input type="checkbox"/>
2.3	<input type="checkbox"/>	<input type="checkbox"/>
2.4	<input type="checkbox"/>	<input type="checkbox"/>
3.1	<input type="checkbox"/>	<input type="checkbox"/>
3.2	<input type="checkbox"/>	<input type="checkbox"/>
5.1	<input type="checkbox"/>	<input type="checkbox"/>
5.2	<input type="checkbox"/>	<input type="checkbox"/>
5.3	<input type="checkbox"/>	<input type="checkbox"/>
5.4	<input type="checkbox"/>	<input type="checkbox"/>

Figure 95: *Diagnostics:Port Mirroring N:1 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.

Table 220: *Buttons*

Button	Meaning
Reset Config	Resets the settings in the dialog to the default settings.
Help	Opens the online help.

Table 220: Buttons (cont.)

8.7 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.

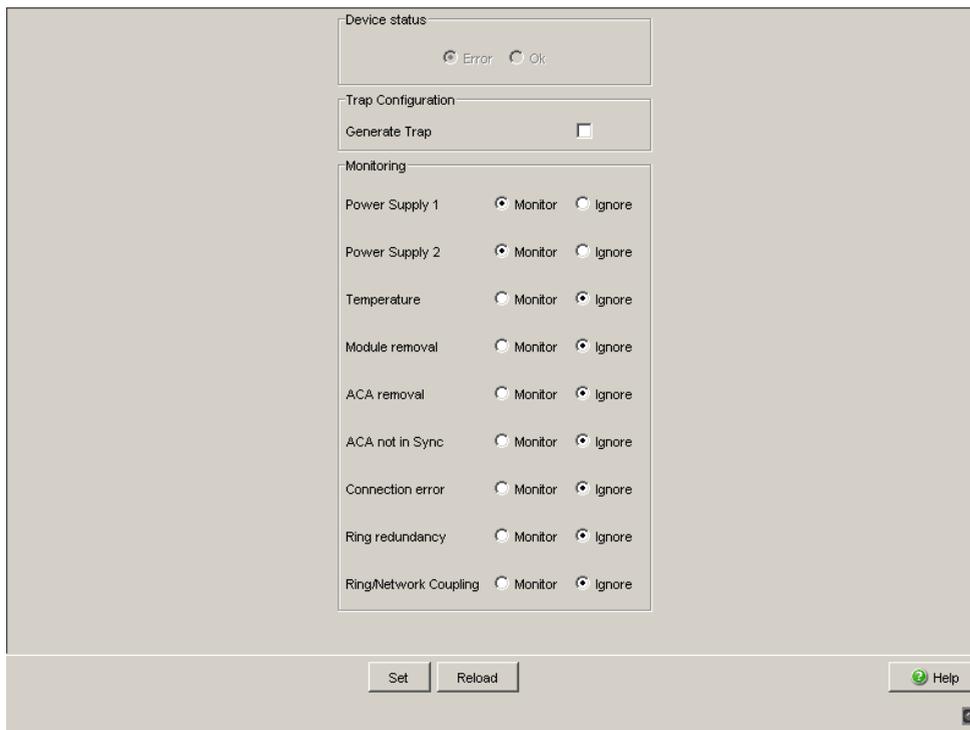


Figure 96: Device State dialog (for PowerMICE)

- 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 22 “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 36 “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.
Fan	Monitor/ignore fan function (for devices with fan).

Table 221: 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 361 “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 222: Buttons

8.8 Signal contact

The signal contacts are used for

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

8.8.1 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.

8.8.2 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 23 “System Data”). Select “Monitor” for the temperature if the signal contact should report an impermissible temperature.
- ▶ Removing a module. Select “Monitor” for removing modules if the signal contact is to report the removal of a module (for modular devices).
- ▶ Fan inoperable (for devices with a fan).
- ▶ 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 246 “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 246 “Ring Redundancy”](#)).

Default setting: no monitoring.

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

8.8.3 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 22 “Device Status”](#)) and thereby offers remote diagnosis. The device status “Error detected” ([see on page 22 “Device Status”](#)) is reported by means of a break in the contact via the potential-free signal contact (relay contact, closed circuit).

8.8.4 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.

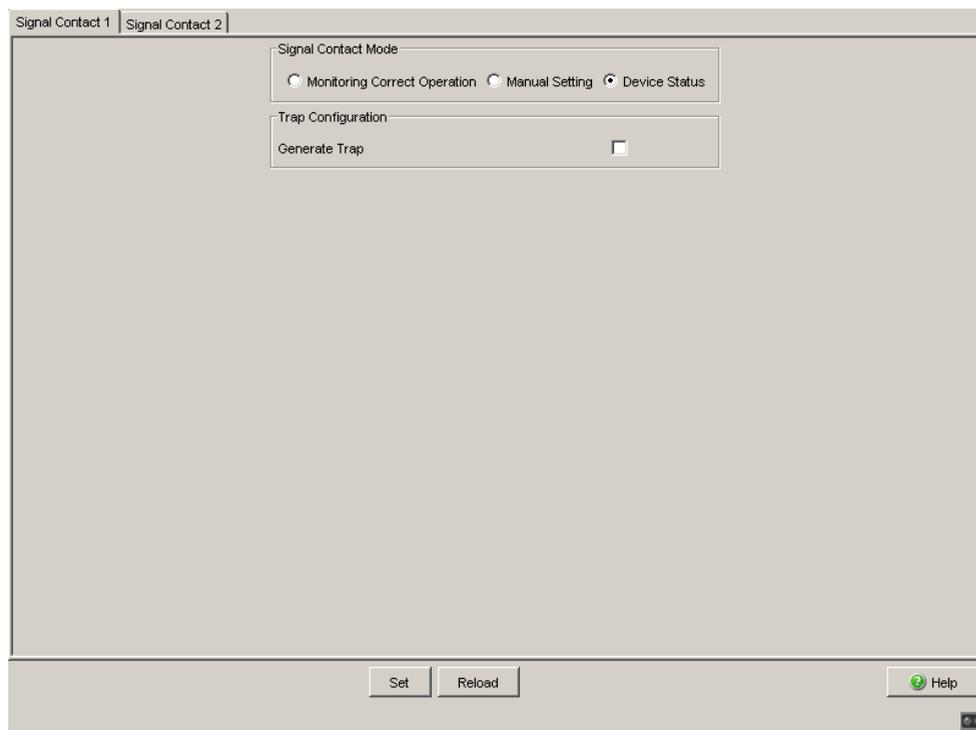


Figure 97: Signal Contact Dialog

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 223: 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 223: Buttons (cont.)

8.9 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 6 trap destinations:

- ▶ PowerMICE
- ▶ MACH 104
- ▶ MACH 1040
- ▶ MACH 4000
- 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 74 "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 224: 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 224: Trap categories

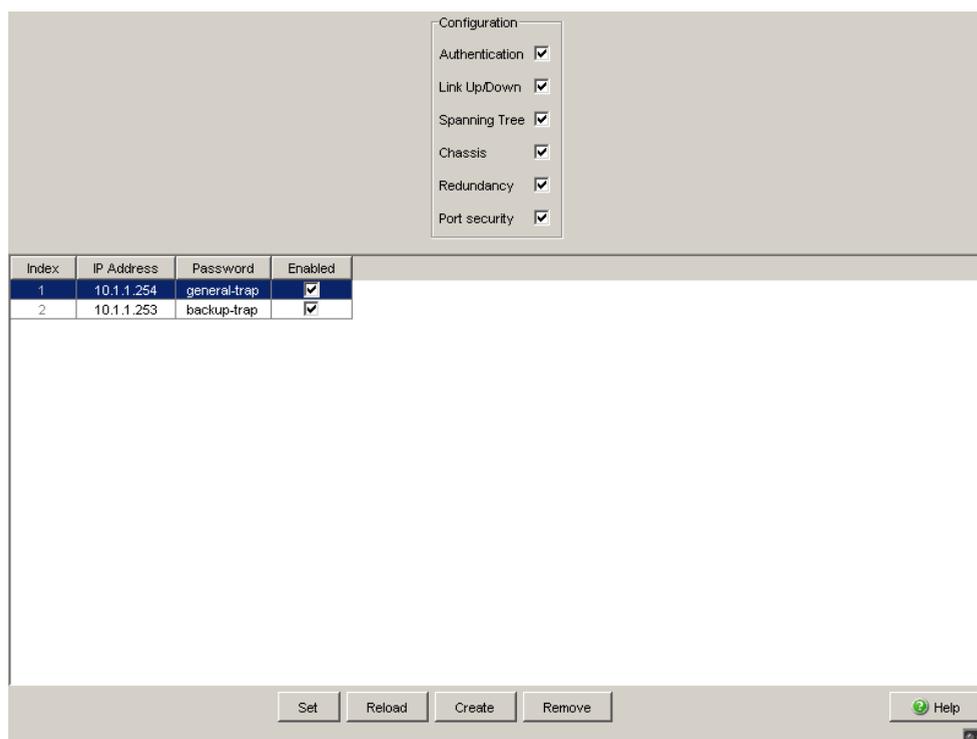


Figure 98: Alarms Dialog

■ 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 225: Buttons

8.10 Report

The following reports are available for the diagnostics:

- ▶ System Information ([see on page 371 “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 372 “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 316 “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 226](#)).
 - 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	
Device configuration (binary)	switch.cfg, powermice.cfg or .mach.cfg	Binary	File name depends on device type.
Device configuration (as script)	switch.cli, powermice.cli or mach.cli	Script	File name depends on device type.
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 226: Files in switch dump archive

a: Prerequisite: a Telnet connection is available.

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

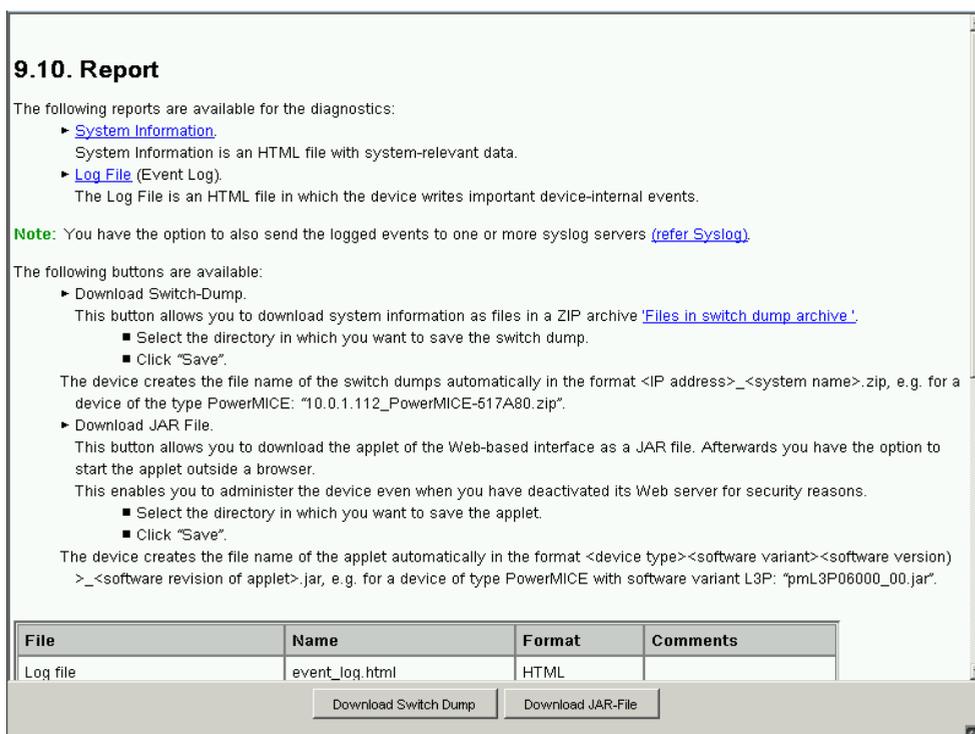


Figure 99: Report dialog

8.10.1 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 227: 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 227: Buttons (cont.)

8.10.2 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 228: Buttons

8.11 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 229). 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 229: 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.

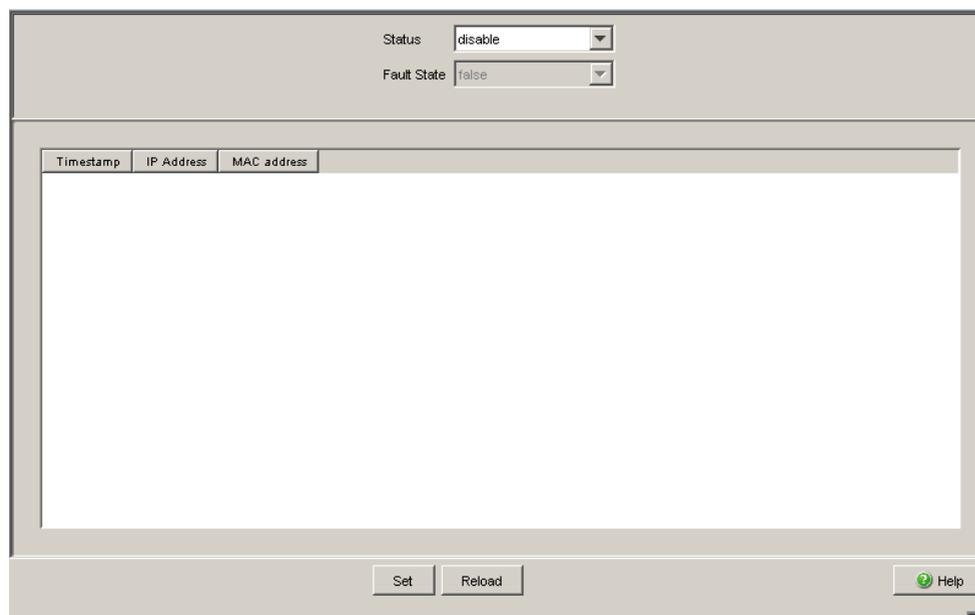


Figure 100: IP Address Conflict Detection dialog

■ 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 230: Buttons

8.12 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.

8.12.1 Operation

Parameters	Meaning
Operation	Activates/deactivates the MAC Notification function globally on the device. Possible values: <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 231: "Operation" frame in the `Diagnostics:Status Configuration:MAC Notification` dialog

8.12.2 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 232: "Configuration" frame in the `Diagnostics:Status Configuration:MAC Notification` dialog

8.12.3 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 233: 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 233: 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 234: Buttons

8.13 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.

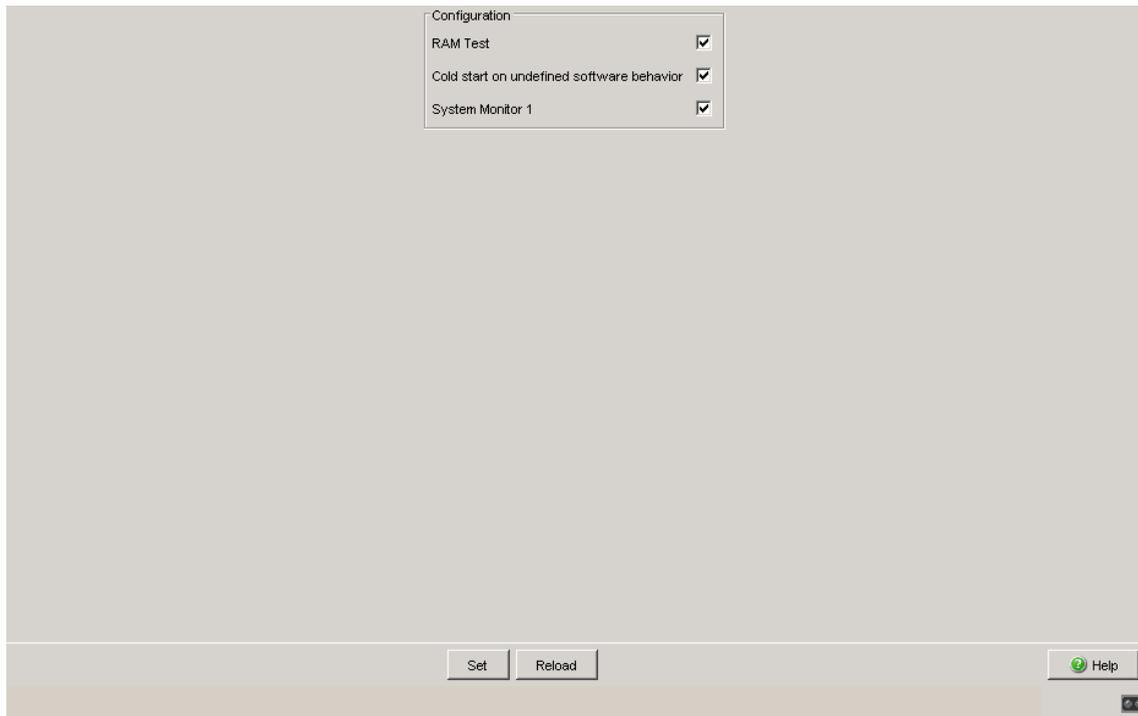


Figure 101: Self-test dialog

■ 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 235: Buttons

9 Advanced

The menu contains the dialogs, displays and tables for:

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

9.1 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.

9.1.1 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.

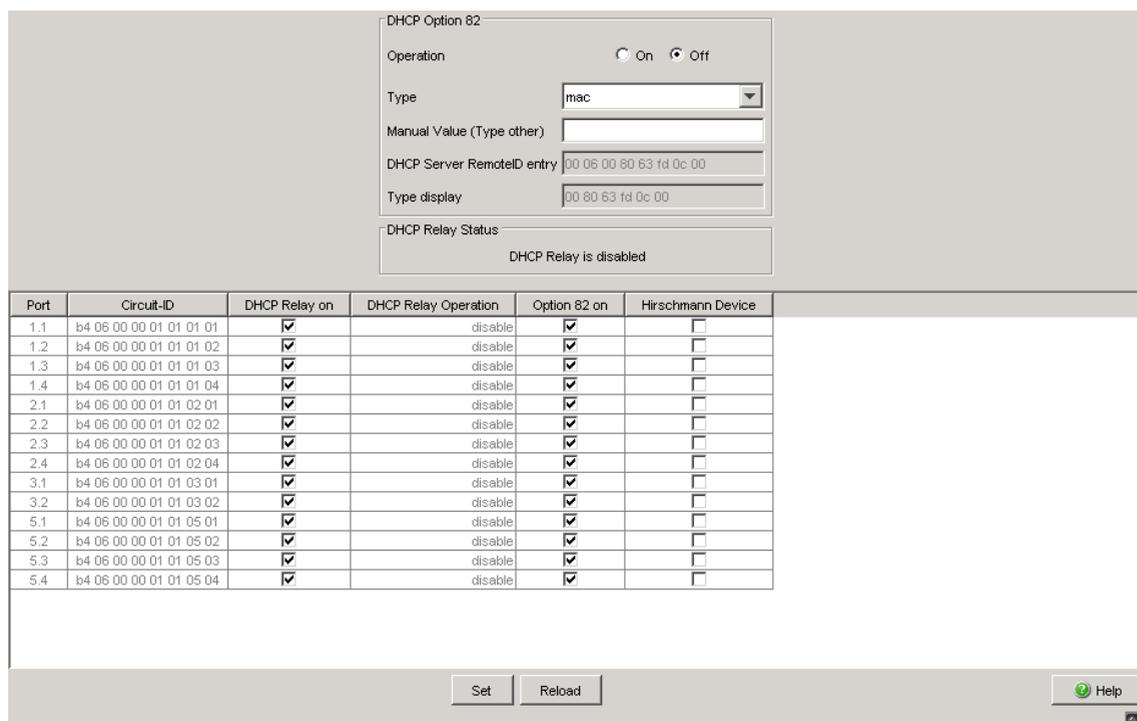


Figure 102:DHCP Relay Agent dialog

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 236:Buttons

9.1.2 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.

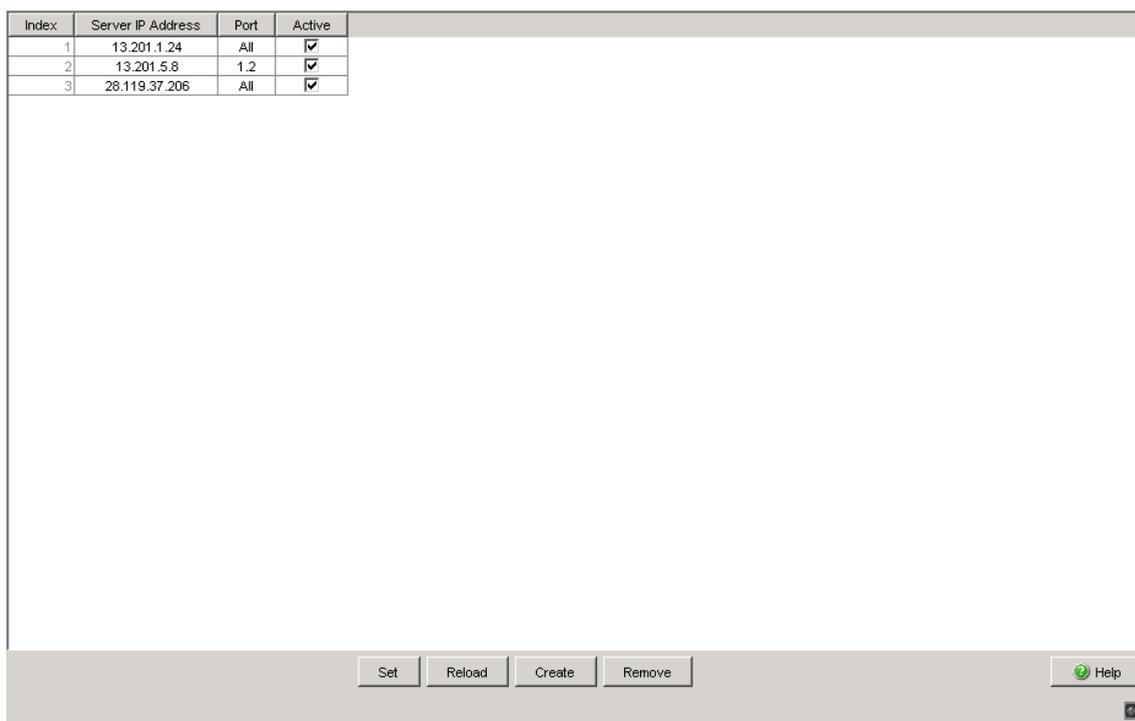


Figure 103: Advanced: DHCP Relay Agent: Port dialog

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 237: "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 237: "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 238: Buttons

9.2 DHCP Server

The DHCP Server dialogs allow you to very easily include new devices (clients) in your network or exchange them in your network: When you select DHCP as the configuration mode for the client, the client gets the configuration data from the DHCP server.

The DHCP server assigns to the client:

- a fixed IP address (static) or an address from an address range (dynamic),
- the netmask,
- the gateway address,
- the DNS server address,
- the WINS server address and
- the lease time.

You can also specify globally or for each port a URL for transferring additional configuration parameters to the client.

9.2.1 Global

This dialog allows you to switch the DHCP server of the device on and off globally and for each port.

Parameter	Meaning	Value range	Default setting
DHCP server mode	Switching the DHCP server on and off globally on the device.	On, Off	Off

Table 239: "DHCP-Server Mode" frame in the `Advanced:DHCP Server:Global` dialog

Parameter	Meaning	Value range	Default setting
IP Probe	Activates/deactivates the probing for unique IP addresses. When allocating a new address, servers verify that the offered network address is unique in the network. For example, the server probes the offered address with an ICMP Echo Request.	On, Off	On

Table 240: "Configuration" frame in the `Advanced:DHCP Server:Global` dialog

Parameter	Meaning	Value range	Default setting
Port	Module and port numbers to which this entry applies.	-	-
DHCP Server active	Switch the DHCP server on and off at this port. To activate the DHCP server at a port, also switch the DHCP server mode on globally.	On, Off	On

Table 241: Table in the `Advanced:DHCP Server:Global` dialog

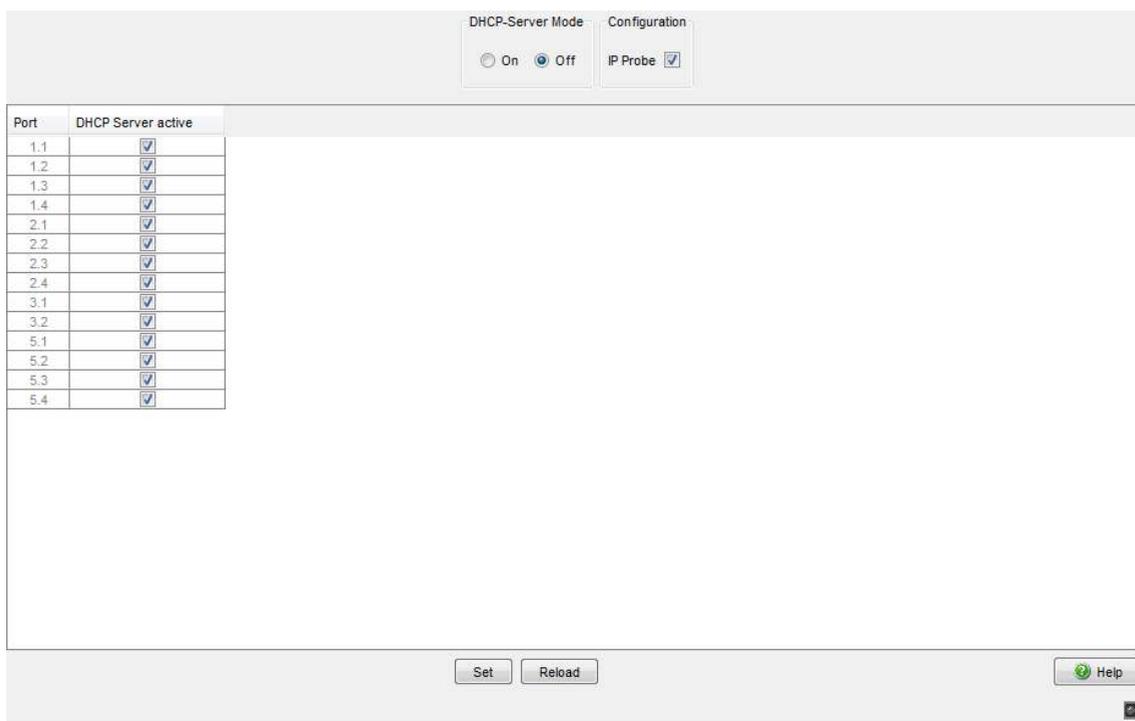


Figure 104:DHCP Server global dialog

■ Buttons

Button	Meaning
Set	Transfers the changes to the volatile memory (RAM) of the device. To permanently save the changes, open the <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 242:Buttons

9.2.2 Pool

This dialog allows you to closely control the allocation of IP addresses. You can activate or deactivate the DHCP server for each port or for each VLAN. For this purpose, the DHCP server provides what is known as an IP address pool (in short “pool”) from which it allocates IP addresses to clients. The pool consists of a list of entries. An entry can define a specific IP address or a connected IP address range.

You can choose between dynamic and static allocation.

- ▶ An entry for dynamic allocation applies to all the ports of the device for which you activate the DHCP server. If a client makes contact at a port, the DHCP server allocates a free IP address from a pool entry for this port. For dynamic allocation, create a pool entry for all ports and enter the first and last IP addresses for the IP address range. Leave the MAC Address, Client ID, Remote ID and Circuit ID fields empty.

You have the option to create multiple pool entries. You can thus create IP address ranges that contain gaps.

- ▶ With static allocation, the DHCP server always allocates the same IP address to a client. The DHCP server identifies the client using a unique hardware ID.

A static address entry can only contain 1 IP address, and it can apply for all ports or for a specific port of the device.

For static allocation, create a pool entry for all ports or one specific port, enter the IP address, and leave the “Last IP Address” field empty. Enter a hardware ID with which the DHCP server uniquely identifies the client.

This ID can be a MAC address, a client ID, a remote ID or a circuit ID. If a client makes contact with a known hardware ID, the DHCP server allocates the static IP address.

The table shows you the configured entries of the DHCP server pool. You have the option to create a new entry, edit an existing entry or delete entries. You have the option to create up to 128 pool entries.

Click “Create” to create a new entry. Fill in the fields you require, then click “Set”.

Parameter	Meaning	Value range	Default setting
Index	Shows a sequential number to which the table entry relates. The device automatically defines this number.	0, 1, 2, ...	
Active	Activates or deactivates the pool entry.	On, Off	Off
IP Address	<ul style="list-style-type: none"> ▶ For a dynamic address entry: the 1st address of the IP address pool that the DHCP server allocates to a client. ▶ For a static address entry: the IP address that the server each time allocates to the same client. 	Valid IPv4 address	-
Last IP Address	For a dynamic address entry: the last address of the IP address pool that the DHCP server allocates to a client.	Valid IPv4 address	-
Port	<p>Module and port numbers to which this entry applies.</p> <ul style="list-style-type: none"> ▶ For a dynamic address entry select <code>all</code>. ▶ For a static address entry select all or one valid module and port number. 	Valid module and port number or <code>all</code> .	<code>all</code>
VLAN	VLAN number to which this entry applies.	Valid VLAN No.	-
<p>Note: This column is available on the MS, Octopus, RS, RSR, MACH102, and MACH1020/10130 devices.</p>			
MAC Address	For a static address entry: MAC address with which the client identifies itself.	MAC address of the client that contains the static IP address	-
DHCP Relay	IP address of the DHCP relay via which the client makes its request. If the DHCP server receives a request via another DHCP relay, it ignores this. If there is no DHCP relay between the client and the DHCP server, leave these fields empty.	IPv4 address of the DHCP relay.	-
Client ID	For a static address entry: Client ID with which the client identifies itself.	Client ID of the client that contains the static IP address ^a	-

Table 243: DHCP server pool settings, IP address basic settings

Parameter	Meaning	Value range	Default setting
Remote ID	For a static address entry: Remote ID with which the client identifies itself.	Remote ID of the client that contains the static IP address ^a	-
Circuit ID	For a static address entry: Circuit ID with which the client identifies itself.	Circuit ID of the client that contains the static IP address ^a	-
Hirschmann Device	Activate this setting if the device from this entry only serves devices from Hirschmann.	On Off	Off
Configuration URL	TFTP URL, from which the client can obtain additional configuration information. Enter the URL in the form <code>tftp://server name or ip address/directory/file</code> .	Valid TFTP URL	-
Lease time [s]	Time in s for which the DHCP server allocates the address to the client. Within the lease time, the client can apply for an extension. If the client does not apply for an extension, after it has elapsed the DHCP server takes the IP address back into the pool and allocates it to any client that requires it.	1 s - 4294967295 s ($2^{32}-1$ s)	86400 s (1 day)
Default gateway	Default gateway entry for the client.	Valid IPv4 address	-
Netmask	Netmask entry for the client.	Valid IPv4 netmask	-
WINS Server	WINS (Windows Internet Name Service) entry for the client.	Valid IPv4 address	-
DNS Server	DNS server entry for the client.	Valid IPv4 address	-

Table 243: DHCP server pool settings, IP address basic settings

Parameter	Meaning	Value range	Default setting
Host name	Host name for the client. If this name is entered, it overwrites the system name of the client (see on page 23 "System Data").	Max. 64 ASCII characters in the range 0x21 (!) - 0x7e (~).	- (no host name)
Vendor specific	Defines vendor-specific information entered as a hex string in a TLV (Type Length Value) format.	Valid hex string.	-

Note: For example: Vendor Specific Information, "f1 08 0a 7e 7e 02 0a 7f 7f 02". Represents a specific type of vendor f1, with a field length of 08. The next 8 octets contain the actual vendor data. If present, the device treats the next 2 octets as type and length fields. Therefore, enter a valid hex string containing the correct length values.

Table 243: DHCP server pool settings, IP address basic settings

^a A client, remote or circuit ID consists of 1 - 255 bytes in hexadecimal form (00 - ff), separated by spaces.

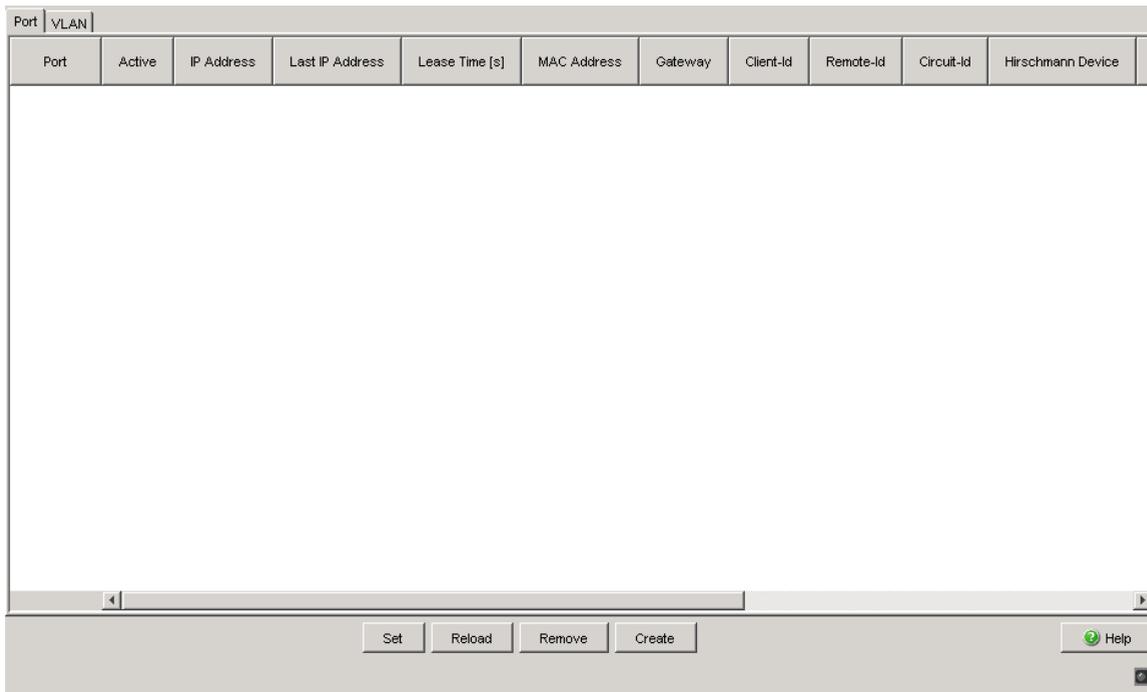


Figure 105:DHCP Server Pool per Port dialog

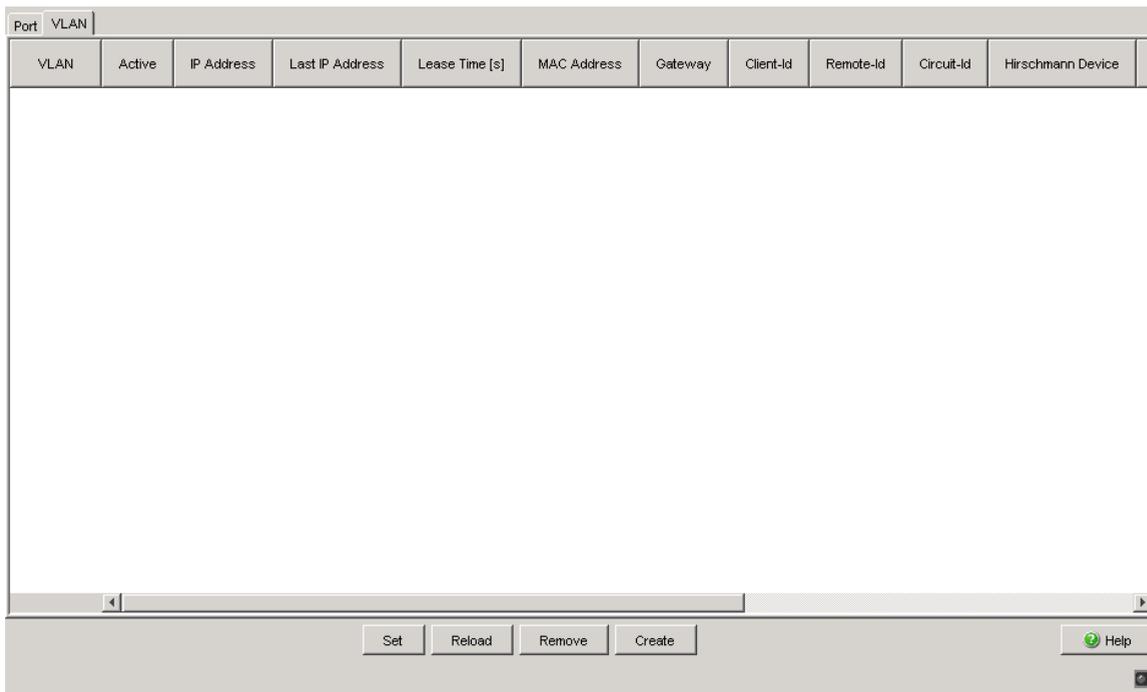


Figure 106:DHCP Server Pool per VLAN dialog

■ 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 244: Buttons

9.2.3 Lease Table

The lease table shows you the IP addresses that the DHCP server has currently allocated.

The device displays the related details for every IP address allocated.

Parameters	Meaning	Possible values
Port	Module and port numbers to which this entry applies.	-
IP Address	IP address that the DHCP server has allocated to the device with the specified MAC address.	An IPv4 address from the pool.
Status	Status of the DHCP address allocation according to the Dynamic Host Configuration Protocol.	bootp, offering, requesting, bound, renewing, rebinding, declined, released
Remaining Lifetime	Time remaining in seconds until the validity of the IP address elapses, unless the client applies for an extension.	-
Leased MAC Address	MAC address of the client that is currently leasing the IP address.	Format xx:xx:xx:xx:xx

Table 245: DHCP lease table

Parameters	Meaning	Possible values
DHCP Relay	IP address of the DHCP relay via which the client has made the request.	IPv4 address or empty
Client ID	The client ID that the client submitted for the DHCP request.	^a
Remote ID	The remote ID that the client submitted for the DHCP request.	^a
Circuit ID	The circuit ID that the client submitted for the DHCP request.	^a

Table 245: DHCP lease table

- ^a A client, remote or circuit ID consists of 1 - 255 bytes in hexadecimal form (00 - ff), separated by spaces.

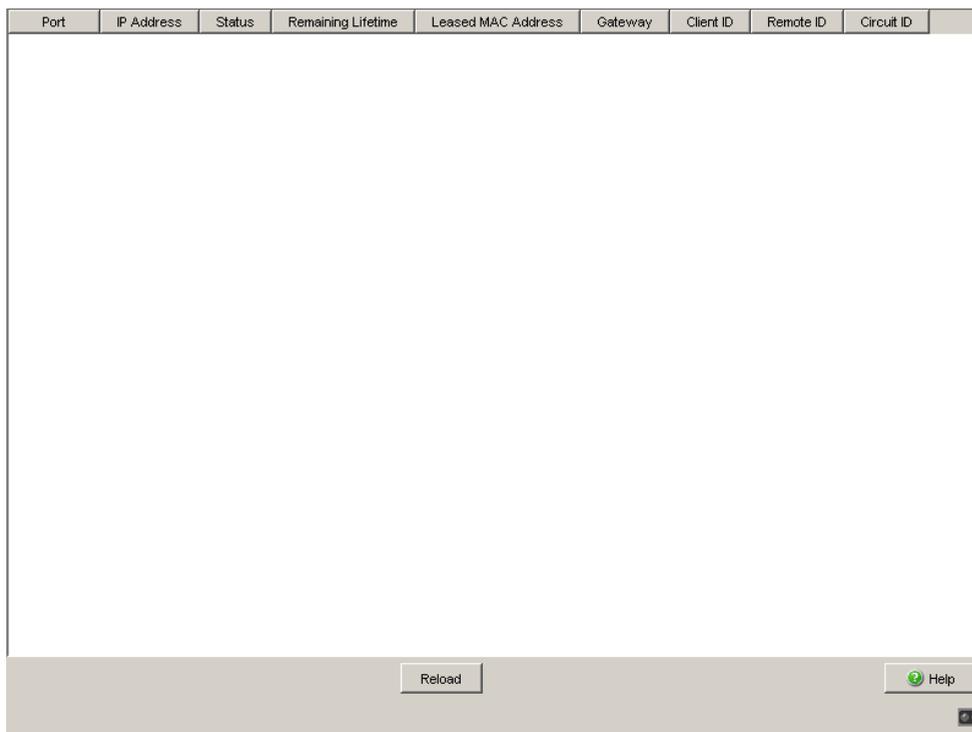


Figure 107: DHCP Server Lease Table dialog

■ 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 246: Buttons

9.3 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”.

9.3.1 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 29 “Network”](#)).
- In the `Switching:VLAN:Global` dialog, check whether “VLAN 0 Transparent Mode” is selected ([see on page 178 “VLAN Global”](#)).

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

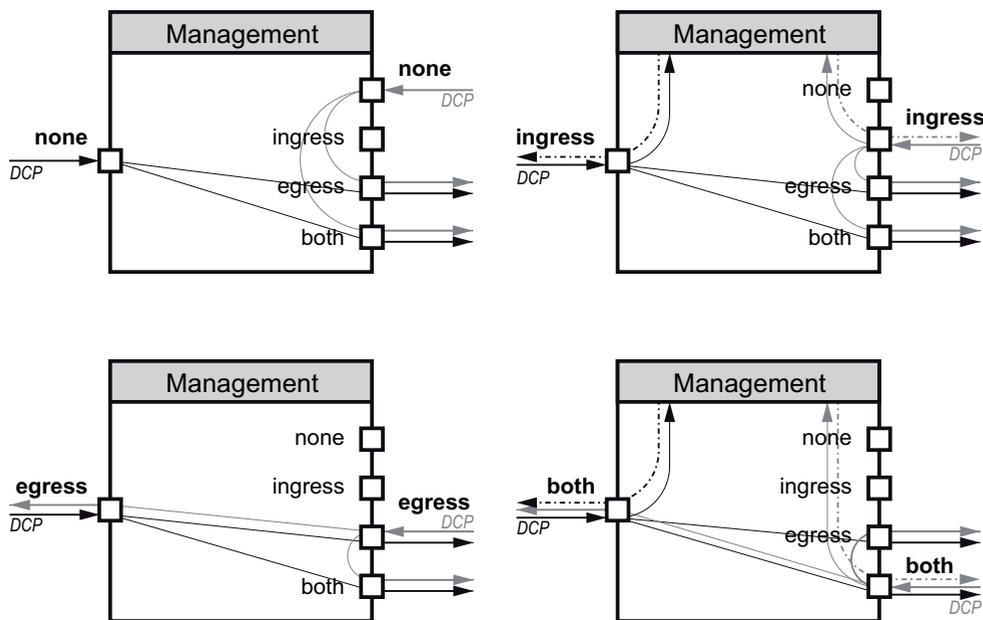
- Configure the alarm settings and the threshold values for the alarms you want to monitor ([see on page 358 “Device Status”](#)).

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 36 “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 247: Buttons

9.3.2 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 167 “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 248: Buttons

9.3.3 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 249: "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 250: "Configuration" frame in the *Advanced:Industrial Protocols:IEC61850* dialog

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

Table 251: "Download" frame in the Advanced:Industrial Protocols:IEC61850 dialog

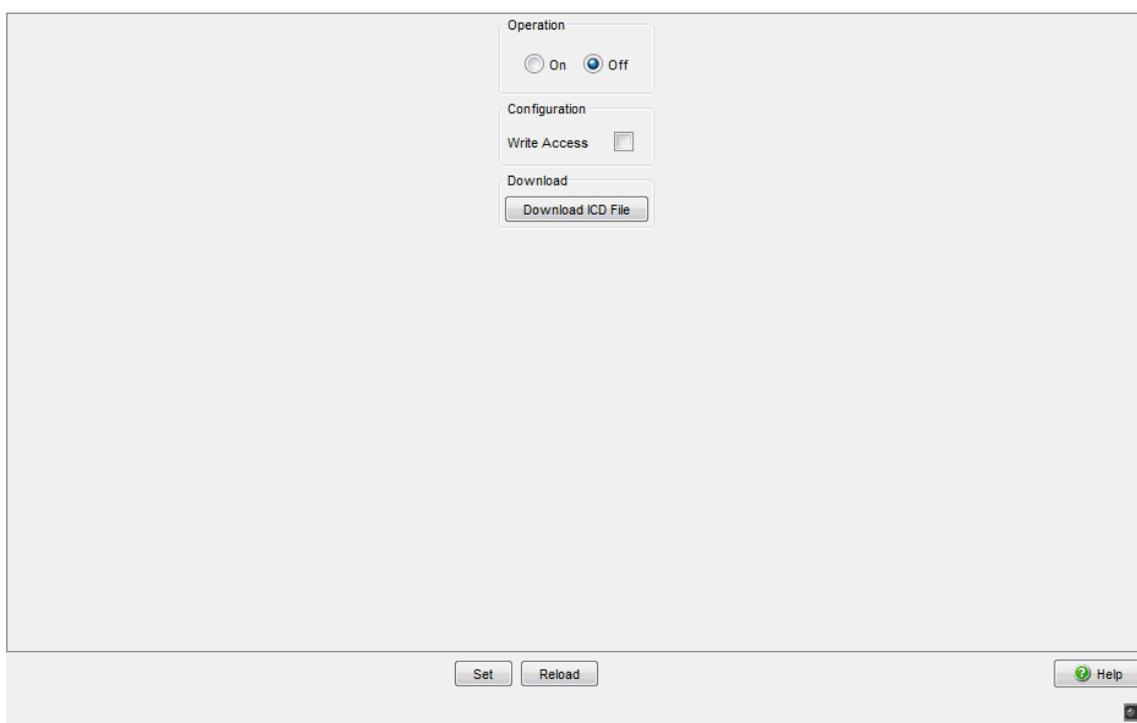


Figure 108:Advanced:Industrial Protocols:IEC61850 dialog

■ Buttons

Button	Meaning
Set	Transfers the changes to the volatile memory (RAM) of the device. To permanently save the changes, open the <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 252:Buttons

9.3.4 Digital IO Module

The Digital I/O MICE Media module MM24-IOIOIOIO enables you to easily transfer status messages from one place in your network to another place. You install this module on (Power)MICE basic devices at the place designated in your network.

The Digital I/O MICE Media module's 4 digital inputs enable you to capture and to forward digital sensors signals.

The Digital I/O MICE Media module's 4 digital outputs enable you to apply actors.

The Digital I/O MICE Media module's 24 VDC output voltage enables you to operate actors or indicator lights, for example.

The software supports the logical function 1 for n. You can query a digital input of a Digital I/O MICE Media module and set practically any number (n) of outputs as a result. The outputs can be located in the following places:

- ▶ on the same Digital I/O MICE Media module on the same (Power)MICE basic device,
- ▶ on another Digital I/O MICE Media module on the same (Power)MICE basic device,
- ▶ on a Digital I/O MICE Media module on another (Power)MICE basic device.

In the "Description and Operation Instructions for Industrial ETHERNET Digital I/O MICE Media module MM24-IOIOIOIO" you will find:

- ▶ safety instructions
- ▶ a description of the device
- ▶ information about assigning the Digital I/O MICE Media module connection terminals
- ▶ a description of the display elements
- ▶ and other information that you need for installing the device prior to your configuring it

The "Digital IO Modules" menu contains the dialogs, displays and tables for configuring Digital I/O MICE Media modules:

- ▶ IO Input
 - ▶ Function (Activate/Deactivate)
 - ▶ Configuration (Configuring the update interval)
 - ▶ Displaying the input ID and value
 - ▶ Configuring the Log Event and SNMP Trap
- ▶ IO Output
 - ▶ Function (Activate/Deactivate)
 - ▶ Configuration (Configuring the update interval and number of retries)
 - ▶ Displaying the output ID and value
 - ▶ Configuring the Source IP Address, Input ID, Log Event and SNMP Trap

■ IO Input

This menu enables you to configure the 4 digital inputs of a Digital I/O MICE Media module MM24-IOIOIOIO.

The screenshot shows the 'IO Input' dialog box. At the top, there are two tabs: 'IO Input' (selected) and 'IO Output'. Below the tabs, there are two sections: 'Operation' with radio buttons for 'On' and 'Off', and 'Configuration' with a text box for 'Refresh Interval [s]' containing the value '1'. Below these sections is a table with the following data:

Input ID	Value	Log Event	SNMP Trap
4.1	low	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
4.2	low	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
4.3	high	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
4.4	low	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

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

Figure 109:IO Input Dialog

Function

Parameter	Meaning	Value Range	Default Setting
Function	Activates or deactivates the cyclical queries from the digital inputs (IO Input).	On, Off	Off

Table 253: IO Input - Function

Configuration

Parameter	Meaning	Value Range	Default Setting
Update Interval [s]	Configure the interval for updating the IO input status. With this specification you define the intervals at which the device queries the values of the Digital I/O MICE Media module's digital inputs.	1 - 10 seconds	1 second

Table 254: IO Input - Configuration

IO Input

The "IO Input" table enables you to:

- ▶ display the input ID and value.
- ▶ configure the Log Event and SNMP Trap for this entry.

Once you have configured the Digital I/O MICE Media module's digital inputs, the dialog lists the values of the digital inputs configured.

Parameter	Meaning	Value Range	Default Setting
Input ID	Slot number of the Digital I/O MICE Media module and number of the digital input (i) that this entry applies to. Notation: x.i	x = 1 - 7 i = 1 - 4	-
Value	Digital input level <ul style="list-style-type: none"> - low: "0" state, input voltage at the digital input 0 V - high: "1" state, input voltage at the digital input +24 VDC - not-available: "undefined" state. Input voltage at the digital input corresponds to neither the high nor the low level. Possible cause: The digital inputs' cyclical query is deactivated. 	low, high, not-available	not-available

Table 255: IO Input Table

Parameter	Meaning	Value Range	Default Setting
Log Event	<p>Activates/deactivates the logging function for input status changes.</p> <ul style="list-style-type: none"> On: The device checks the status of the Digital I/O MICE Media module's digital inputs at regular intervals according to your setting in the "Update Interval [s]" input field. If the device detects a change in one of these IO input values, it writes an entry in its event log. The <code>Diagnostics:Report:EventLog</code> dialog displays these entries. Off: The device does not write an entry in its event log in the course of an input status change. 	On, Off	Off
SNMP Trap	<p>Activates or deactivates the transmission of SNMP traps in the course of an input status changes.</p> <ul style="list-style-type: none"> On: The device checks the status of the Digital I/O MICE Media module's digital inputs at regular intervals according to your setting in the "Update Interval [s]" input field. If the device detects a change in one of these IO input values, it sends an SNMP trap. The <code>Diagnostics:Trap Log</code> dialog displays these traps. Off: The device does not send an SNMP trap in the course of an input status change. 	On, Off	Off

Table 255: IO Input Table

■ IO Output

This menu enables you to set the 4 digital outputs of a Digital I/O MICE Media module MM24-IOIOIOIO to the value of "High" (+24 VDC) or "Low" (0 VDC) ([see table 258](#)).

Output ID	Value	Source IP	Input ID	Log Event	SNMP Trap
4.1	high	10.0.1.112	4.3	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
4.2	high	10.0.1.112	4.3	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
4.3	high	10.0.1.112	4.3	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
4.4	high	10.0.1.112	4.3	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Figure 110:IO Output Dialog

Function

Parameters	Meaning	Possible values	Default setting
Operation	Activates or deactivates the cyclical setting of the digital outputs (IO Output).	On Off	Off

Table 256:IO Output - Function

Configuration

Note: If after the number of retries configured the device does not receive a response to its queries, it sets the digital output to the default value (low). This applies to all digital outputs that you have configured input monitoring for.

Parameter	Meaning	Value Range	Default Setting
Update Interval [s]	Configure the interval for updating the IO output status. With this specification you define the intervals at which the device sets the values of the Digital I/O MICE Media module's digital outputs.	1 - 10 seconds	1 second
Number of Retries	Specify the number of retry attempts the device will undertake to set the Digital I/O MICE Media module's digital outputs.	1 - 10	3

Table 257: IO Output - Configuration

IO Output

The "IO Output" table enables you to:

- ▶ display the output ID and value.
 - ▶ configure the Source IP Address, Input ID, Log Event and SNMP Trap for this entry.
- In the "Source IP" field, enter the IP address of the (Power)MICE device that you installed the Digital I/O MICE Media module on, whose digital inputs you want to use for setting digital outputs.
 - In the "Input ID" field, select the Digital I/O MICE Media module's slot number and the number of the digital input, whose status you want to use for setting the digital outputs.
 - By clicking on the "Log Event" field, set a checkmark in order to activate the event log function for this digital output on the device.
 - By clicking on the "SNMP Trap" field, set a checkmark in order to activate the transmission of SNMP traps for this digital output on the device.
 - Click on "Set" to save your settings.
 - Click on "Reload" in order to display in the table the current values at the device's digital outputs.

Parameter	Meaning	Value range	Default setting
Output ID	Slot number of the Digital I/O MICE Media module (x) and number of the digital output (o) that this entry applies to. Notation: x.o	x = 1 - 7 o = 1 - 4	-
Value	Digital output level. <ul style="list-style-type: none"> - low: State "0", relay on digital output is in position 2 (center contact is connected to de-energized contact). - high: State "1", relay on digital output is in position 1 (center contact is connected to operating contact). - not-available: "undefined" state. Voltage at the digital output corresponds to neither the high nor the low level. Possible cause: The digital outputs' cyclical setting is deactivated. 	low, high, not-available	not-available
Source IP	IP address of the (Power)MICE device with a Digital I/O MICE Media module from which you want to analyze a digital input for setting the digital output.	Valid IPv4 address	0.0.0.0
Input ID	Slot number of the Digital I/O MICE Media module (x) and number of the digital input (i) that you use for setting the digital output. Notation: x.i	x = 1 - 7 i = 1 - 4	1.1

Table 258: IO Output Table

Parameter	Meaning	Value range	Default setting
Log Event	<p>Activates/deactivates the logging function for output status changes.</p> <ul style="list-style-type: none"> – On: The device checks the status of the Digital I/O MICE Media module's digital inputs at regular intervals according to the setting in the "Update Interval [s]" input field. If the device detects a change in one of these IO output values, it writes an entry in its event log. The <code>Diagnostics:Report:EventLog</code> dialog displays these entries. – Off: The device does not write an entry in its event log in the course of an output status change. 	On, Off	Off
SNMP Trap	<p>Activates or deactivates the transmission of SNMP traps in the course of an output status changes.</p> <ul style="list-style-type: none"> – On: The device checks the status of the Digital I/O MICE Media module's digital inputs at regular intervals according to the setting in the "Update Interval [s]" input field. If the device detects a change in one of these IO output values, it sends an SNMP trap. – Off: The device does not send an SNMP trap in the course of an output status change. 	On, Off	Off

Table 258: IO Output Table

Note: If the device cannot read the Digital I/O MICE Media module's digital input, it writes an entry in its event log. Possible cause: The device is unreachable or the configuration is incorrect.

9.4 Software DIP Switch overwrite (PowerMICE)

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><i>On</i>: The device uses the settings specified with the DIP switches. The prerequisite is that "DIP Switch On" is active.</p> <p><i>Off</i>: The device ignores the settings of the DIP switches.</p>	On, Off	On

Table 259: "Operation" frame in the *Advanced:DIP-Switch* dialog

Parameter	Meaning	Value range	Default setting
Conflict with hardware settings	<p>Displays the conflicts between the settings of the DIP switches on the device and the software settings.</p> <p><i>Active</i>: Conflict between the settings of the DIP switches on the device and the software settings.</p> <p><i>Inactive</i>: No conflict.</p>	Active, inactive	-

Table 260: "DIP-Switch Status" frame in the *Advanced:DIP-Switch* dialog

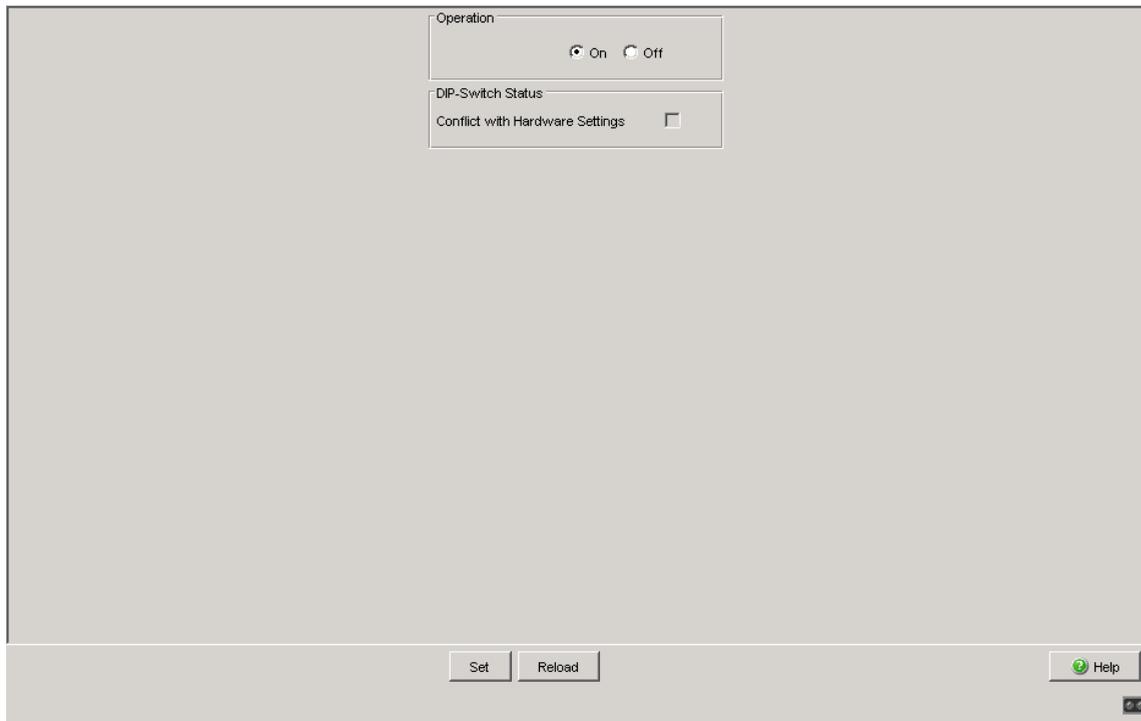


Figure 111: Advanced: DIP-Switch dialog

■ 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 261: Buttons

9.5 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 262: 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	1,000
Max. length of over-long packets	1,552 bytes
Latency, depending on the port data rate	
10,000 Mbit/s	Layer 2: typically 3.0 μ s; Layer 3: typically 3.0 μ s
1,000 Mbit/s	Layer 2: typically 3.5 μ s; Layer 3: typically 4.5 μ s
100 Mbit/s	Layer 2: typically 4.5 μ s; Layer 3: typically 5.5 μ s
10 Mbit/s	Layer 2: typically 19 μ s; Layer 3: typically 20 μ s
Max. number of static address entries	100 (in RM mode: 0 Unicast entries)

VLAN	
VLAN ID	1 to 4,042
Number of VLANs	max. 256 simultaneously per device max. 256 simultaneously per port
Number of VLANs in GMRP in VLAN 1	max. 256 simultaneously per device max. 256 simultaneously per port

Access Control Lists (ACLs)	
Number of ACL entries	100
Number of possible rules	1,000
Number of rules per ACL entry	10
Number of rules per interface	100
Number of Switch queues	8
Port priorities that can be set	0-7

Router	
ARP entries	up to 2,000
Routing entries	up to 4,000 (1,500 for MACH 4002 24G/48G)
Number of VLAN interfaces	up to 128
Static routes	256
Static ARP entries	64
Multicast routes	512
Number of tracking objects	256

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
RFC 3580	(802.1X RADIUS Usage Guidelines)
RFC 4188	(Definitions of Managed Objects for Bridges)

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-1998	Virtual Bridged Local Area Networks (VLAN Tagging, Port-Based VLANs, GVRP)
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 802.3ad	Link Aggregation with Static LAG and LACP Support
IEEE 802.3af-2003	Power over Ethernet (PoE)
IEEE 802.3x	Flow Control

A.4 Underlying IEC Norms

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

A.5 Underlying ANSI Norms

ANSI/TIA-1057 Link Layer Discovery Protocol for Media Endpoint Devices, April 2006

A.6 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.7 Copyright of Integrated Software

A.7.1 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.7.2 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	205	Diagnostics	315
802.1X	94	DiffServ	197
802.1X authentication (Voice VLAN)	193	Discovery	225
		Distance vector	226
		DSCP	197
A		E	
ACA (AutoConfiguration Adapter)	51, 367	EF	207
Acceptable Frame Types	188	EtherNet/IP	401
Access Control Lists (ACL)	124	Event Log	372
Address Conflict Detection (ACD)	373	Event log	320
Address Resolution Protocol (ARP)	220	Expedited Forwarding	207
Administrative Distance	235		
Advanced	381	F	
AF	208	FAQ	435
Aging Time	156	Fast HIPER-Ring	259
Alarm	366	Filters for MAC addresses	160
ARP parameters	220	Forward Delay	278, 280
ARP Statistics	222		
ARP Table	222	G	
Assured Forwarding	208	Grandmaster	144
Authentication	305	Graphical User Interface (GUI)	15
AutoConfiguration Adapter (ACA)	367		
Auto summary	226	H	
		Hardware clock (buffered)	126
B		Hello Time	278, 280
Basic Settings	21	HIPER-Ring	187, 248, 248
BPDU Guard	279	HIPER-Ring (source for alarms)	367
Broadcast Limiter	165	HiView	15
		HiVRRP	241, 302
C		HiVRRP domains	307
Cable crossing	37	HiVRRP (configuration)	302
CLI	415	Host routes accept	226
Class Selector	207		
Clock	133	I	
Cold Start	66	ICMP	225
Cold start (after software update)	34, 34	IGMP querier	168
Command Line Interface	415	IGMP settings	168
Configuration Check	346	IGMP snooping	168
Count-to-infinity	227	Independent VLAN	180
Current VLAN Dialog	183	Industrial HiVision	12
		Industry protocols	11, 398
D		Ingress Filtering	188
DHCP Relay Agent	382	IP DSCP mapping	197, 207
DHCP server	387	IP DSCP value	198
DHCP server pool	390		
DHCP server (lease table)	395		
DIP switch	248		

J		Q	
Java Runtime Environment	21	QoS/Priority	197
L		Queue	211
LACP Link Aggregation Control Protocol	242	Queue Management	197, 210
Link Aggregation	241, 244	R	
Link State (Port)	36	RADIUS	111
LLDP	346, 349	RAM test	378
LLDP-MED (Voice VLAN)	192	Rapid Spanning Tree (RSTP)	274, 290
Login Banner	119, 120	Rate Limiter	164
Login window	17	Rate Limiter Settings	165
M		Reboot	66
Maximum Bandwidth	212	Receiver power status	367
Max Age	278, 280	Redundancy	11, 241, 274
Media module (for modular devices)	23	Reference clock	144
MRP Domain	265, 266	Report	369
MRP-Ring	187, 242, 252, 252	Request Interval (SNTP)	130
Multicasts	167	Restart	66
Multinetting	215	Restore default settings	51
Multiple Spanning Tree (MSTP)	274	Restore state on delivery	51
N		Restricted management access	83
Netdirected Broadcasts	215, 217, 218	RFC	420
Network load	274, 324	RIP	226
Network management station	349	RIP Statistics	230
O		RIP (configuration)	226
One-Switch coupling	270	Ring	246
Operating instructions (GUI)	18	Ring Manager	246
OSPF routes	229	Ring port	248
P		Ring Redundancy	241
Password	70, 72	Ring structure	246
Per-Hop-Behavior (PHB)	207	Ring/Network coupling	187, 241, 268, 359
PHY Fast Startup per Port	400	Ring/Network coupling (source for alarms)	367
Ports	322	RMON probe	355
Port configuration	36, 200	RM Function	246
Port configuration (QoS/priority)	200	Root bridge	275
Port Mirroring	355	Router	11, 213
Port Monitor	330	Router Discovery	225
Port priority	200, 202	Route Distribution	229, 229
Port State (Link)	36	Routing Function	215
Port security (802.1X-based)	94	Routing Information Protocol (RIP)	226
Port security (IP-/MAC-based)	87	Routing table	232
Port security (source for alarms)	89, 93	Routing (global settings)	214
Port statistics table	322	Routing (interface settings)	215
Port VLAN ID	188	S	
PROFINET IO	11, 398	Saving a configuration profile (GUI)	19
Precedence	207	Security	69
Precision Time Protocol	133	Self-test	378
Pre-login Banner	119	SFP Module	326
Priority queue	198	SFP Status Display	326
Proxy ARP	217, 218	Shaping rate	200, 204
PTP	133	Shared VLAN	180
		Signal contact	361
		Signal contact (source for alarm)	367

SNMPv1/v2 access settings	74	U	
SNMP logging	316	Untrusted traffic class	200, 204
SNTP Broadcasts	130	Untrusted (global trust mode)	203
SNTP server	385	V	
Software Update	32	Video	211
Spanning Tree (STP)	274	Virtual Router Redundancy Protocol	302
Split horizon	227	VLAN	178
SSH Access	78	VLAN 0	31
Starting the graphical user interface	15	VLAN and GOOSE Protocol	179
Static routing table	234	VLAN and GVRP	189
Statistics table	322	VLAN and redundancy rings	190
Status line via menu	18	VLAN Global dialog	178
Strict Priority	211	VLAN ID (network parameter)	29
Sub-Ring	262, 263, 266	VLAN Mapping	197
Supply voltage	367	VLAN Mode	180
Switching	155	VLAN Port dialog	188
Symbol	13	VLAN priority	198
Syslog	316	VLAN Static dialog	185
System Information	371	VLAN (HIPER-Ring)	250
System requirements (GUI)	15	VLAN (Router Interface)	215
System time	130	VoIP	211
T		Voice VLAN	192
Technical Questions	435	VRRP	241, 302
Telnet Access	78	VRRP advertisement interval	305
Temperature (device)	23	VRRP instance	303
Temperature (SFPs)	326	VRRP router instance	305
Time	125, 126	VRRP statistics	310
Time Management	133	VRRP Tracking	237, 239, 311, 311
Time Stamp Unit	134	VRRP (configuration)	302
Time To Live	214	W	
Topology	349	Web Access	78
Topology Recognition	346	Weighted Fair Queuing	204, 211, 211
ToS	197	Weighted Round Robin	211
TP cable diagnosis	327		
Tracking	234, 237		
Tracking Applications	239		
Tracking Configuration	237		
Tracking (VRRP)	237, 311		
Traffic class	210		
Training Courses	435		
Trap	366		
Trunk	242		
TrustDot1p (global trust mode)	203		
TrustIpdscp	203		
Trust mode	200, 203		
TTL	214		
Two-switch coupling	270		
TX Hold Count	279		
Type of Service	197		

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

PowerMICE, MACH 104, MACH 1040, MACH 4000

L3P 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	27
Maintenance	29
Service Shell	31
Permanently disabling the Service Shell	31
1 Command Structure	33
1.1 Format	34
1.1.1 Command	35
1.1.2 Parameters	35
1.1.3 Values	36
1.1.4 Conventions	38
1.1.5 Annotations	39
1.1.6 Special keys	40
1.1.7 Special characters in scripts	41
1.1.8 Secrets in scripts	43
1.1.9 Slot-Port Naming Convention	45
2 Quick Start up	47
2.1 Quick Starting the Switch	48
2.2 System Info and System Setup	49
3 Mode-based CLI	55
3.1 Mode-based Topology	57
3.2 Mode-based Command Hierarchy	58
3.3 Flow of Operation	61
3.4 “No” Form of a Command	63
3.4.1 Support for “No” Form	63
3.4.2 Behavior of Command Help (“?”)	63

4	CLI Commands: Base	65
4.1	System Information and Statistics	66
4.1.1	show	66
4.1.2	show address-conflict	66
4.1.3	show arp switch	67
4.1.4	show bridge address-learning	67
4.1.5	show bridge address-relearn-detect	68
4.1.6	show bridge aging-time	68
4.1.7	show bridge duplex-mismatch-detect	69
4.1.8	show bridge fast-link-detection	69
4.1.9	show bridge framesize	69
4.1.10	show bridge vlan-learning	70
4.1.11	bridge framesize	70
4.1.12	show config-watchdog	71
4.1.13	show device-status	71
4.1.14	show authentication	72
4.1.15	show eventlog	73
4.1.16	show interface	74
4.1.17	show interface ethernet	76
4.1.18	show interface switchport	83
4.1.19	show interface utilization	84
4.1.20	show logging	85
4.1.21	show mac-address-conflict	86
4.1.22	show mac-addr-table	87
4.1.23	show signal-contact	88
4.1.24	show slot	90
4.1.25	show running-config	91
4.1.26	show sysinfo	92
4.1.27	show temperature	95
4.1.28	utilization alarm-threshold	95
4.2	Debug Commands	96
4.2.1	debug tcpdump help	96
4.2.2	debug tcpdump start cpu	96
4.2.3	debug tcpdump start cpu filter	97
4.2.4	debug tcpdump stop	97
4.2.5	debug tcpdump filter show	98
4.2.6	debug tcpdump filter list	98
4.2.7	debug tcpdump filter delete	99
4.3	Management VLAN Commands	100

4.3.1	network mgmt_vlan	100
4.4	Class of Service (CoS) Commands	101
4.4.1	classofservice dot1p-mapping	102
4.4.2	classofservice ip-dscp-mapping	103
4.4.3	classofservice trust	104
4.4.4	show classofservice dot1p-mapping	105
4.4.5	show classofservice ip-dscp-mapping	106
4.4.6	show classofservice trust	107
4.4.7	vlan port priority all	107
4.4.8	vlan priority	108
4.4.9	dvlan-tunnel ethertype	108
4.4.10	mode dvlan-tunnel	110
4.4.11	show dvlan-tunnel	111
4.5	Link Aggregation(802.3ad) Commands	112
4.5.1	link-aggregation staticcapability	112
4.5.2	show link-aggregation brief	113
4.6	Management Commands	114
4.6.1	telnet	114
4.6.2	transport input telnet	115
4.6.3	transport output telnet	116
4.6.4	session-limit	117
4.6.5	session-timeout	118
4.6.6	bridge address-learning	118
4.6.7	bridge address-relearn detect operation	119
4.6.8	bridge address-relearn detect threshold	119
4.6.9	bridge aging-time	120
4.6.10	bridge fast-link-detection	121
4.6.11	bridge duplex-mismatch-detect operation	121
4.6.12	bridge vlan-learning	122
4.6.13	digital-input	122
4.6.14	digital-output	124
4.6.15	show digital-input	127
4.6.16	show digital-input config	128
4.6.17	show digital-input all	129
4.6.18	show digital-input <slot/input>	130
4.6.19	show digital-output	131
4.6.20	show digital-output config	132
4.6.21	show digital-output all	133
4.6.22	show digital-output <slot/output>	134

4.6.23	ethernet-ip	135
4.6.24	network mgmt-access add	136
4.6.25	network mgmt-access delete	136
4.6.26	network mgmt-access modify	137
4.6.27	network mgmt-access operation	138
4.6.28	network mgmt-access status	139
4.6.29	network parms	139
4.6.30	network protocol	140
4.6.31	network priority	141
4.6.32	profinetio	142
4.6.33	serial timeout	143
4.6.34	set prompt	143
4.6.35	show ethernet-ip	144
4.6.36	show network	144
4.6.37	show network mgmt-access	146
4.6.38	show profinetio	147
4.6.39	show serial	147
4.6.40	show snmp-access	148
4.6.41	show snmpcommunity	149
4.6.42	show snmp sync	150
4.6.43	show snmptrap	151
4.6.44	show telnet	152
4.6.45	show telnetcon	153
4.6.46	show trapflags	154
4.6.47	snmp-access global	155
4.6.48	snmp-access version	156
4.6.49	snmp-access version v3-encryption	157
4.6.50	snmp-server	158
4.6.51	snmp-server community	159
4.6.52	snmp-server contact	160
4.6.53	snmp-server community ipaddr	161
4.6.54	snmp-server community ipmask	162
4.6.55	snmp-server community mode	163
4.6.56	snmp-server community ro	164
4.6.57	snmp-server community rw	164
4.6.58	snmp-server location	164
4.6.59	snmp-server sysname	165
4.6.60	snmp-server enable traps	165
4.6.61	snmp-server enable traps chassis	166
4.6.62	snmp-server enable traps l2redundancy	167
4.6.63	snmp-server enable traps linkmode	168

4.6.64	snmp-server enable traps multiusers	169
4.6.65	snmp-server enable traps port-sec	170
4.6.66	snmp-server enable traps stpmode	171
4.6.67	snmptrap	172
4.6.68	snmptrap ipaddr	173
4.6.69	snmptrap mode	174
4.6.70	snmptrap snmpversion	175
4.6.71	telnetcon maxsessions	176
4.6.72	telnetcon timeout	177
4.7	Syslog Commands	178
4.7.1	logging buffered	178
4.7.2	logging buffered wrap	179
4.7.3	logging cli-command	180
4.7.4	logging console	181
4.7.5	logging host	182
4.7.6	logging host reconfigure	183
4.7.7	logging host remove	183
4.7.8	logging snmp-requests get operation	183
4.7.9	logging snmp-requests set operation	184
4.7.10	logging snmp-requests get severity	184
4.7.11	logging snmp-requests set severity	185
4.7.12	logging syslog	186
4.7.13	logging syslog port	186
4.8	Scripting Commands	187
4.8.1	script apply	187
4.8.2	script delete	188
4.8.3	script list	188
4.8.4	script show	189
4.8.5	script validate	189
4.9	Device Configuration Commands	191
4.9.1	addport	191
4.9.2	adminmode	192
4.9.3	auto-disable reason	193
4.9.4	auto-disable reset	195
4.9.5	auto-disable timer	195
4.9.6	auto-negotiate	196
4.9.7	auto-negotiate all	197
4.9.8	cable-crossing	198
4.9.9	media-module	199

4.9.10	deleteport	200
4.9.11	deleteport all	200
4.9.12	dip-switch operation	201
4.9.13	macfilter	202
4.9.14	macfilter adddest	203
4.9.15	macfilter adddest all	204
4.9.16	mac notification (Global Config)	205
4.9.17	mac notification (Interface Config)	206
4.9.18	monitor session <session-id>	207
4.9.19	monitor session <session-id> mode	209
4.9.20	monitor session <session-id> source/destination	210
4.9.21	link-aggregation	211
4.9.22	link-aggregation adminmode	212
4.9.23	link-aggregation linktrap	213
4.9.24	link-aggregation name	214
4.9.25	rmon-alarm add	214
4.9.26	rmon-alarm delete	215
4.9.27	rmon-alarm enable	215
4.9.28	rmon-alarm disable	216
4.9.29	rmon-alarm modify mib-variable	216
4.9.30	rmon-alarm modify thresholds	217
4.9.31	rmon-alarm modify interval	217
4.9.32	rmon-alarm modify sample-type	218
4.9.33	rmon-alarm modify startup-alarm	218
4.9.34	rmon-alarm modify rising-event	219
4.9.35	rmon-alarm modify falling-event	219
4.9.36	set garp timer join	220
4.9.37	set garp timer leave	221
4.9.38	set garp timer leaveall	222
4.9.39	set gmrp adminmode	223
4.9.40	set gmrp interfacemode	224
4.9.41	set gmrp interfacemode	225
4.9.42	set gmrp forward-all-groups	226
4.9.43	set gmrp forward-unknown	227
4.9.44	set igmp	228
4.9.45	set igmp	229
4.9.46	set igmp aging-time-unknown	229
4.9.47	set igmp automatic-mode	230
4.9.48	set igmp forward-all	231
4.9.49	set igmp static-query-port	232
4.9.50	set igmp groupmembershipinterval	233

4.9.51	set igmp interfacemode	234
4.9.52	set igmp lookup-interval-unknown	235
4.9.53	set igmp lookup-resp-time-unknown	235
4.9.54	set igmp maxresponse	236
4.9.55	set igmp querier max-response-time	237
4.9.56	set igmp querier protocol-version	237
4.9.57	set igmp querier status	238
4.9.58	set igmp querier tx-interval	238
4.9.59	set igmp query-ports-to-filter	239
4.9.60	selftest ramtest	239
4.9.61	selftest reboot-on-error	240
4.9.62	serviceshell	241
4.9.63	update module-configuration	241
4.9.64	show auto-disable brief	242
4.9.65	show auto-disable reasons	243
4.9.66	show dip-switch	244
4.9.67	show garp	245
4.9.68	show gmrp configuration	245
4.9.69	show igmpsnooping	246
4.9.70	show mac-filter-table gmrp	248
4.9.71	show mac-filter-table igmpsnooping	249
4.9.72	show mac-filter-table multicast	250
4.9.73	show mac-filter-table static	251
4.9.74	show mac-filter-table staticfiltering	252
4.9.75	show mac-filter-table stats	253
4.9.76	show mac notification	253
4.9.77	show monitor session	255
4.9.78	show port	256
4.9.79	show link-aggregation	257
4.9.80	show rmon-alarm	258
4.9.81	show selftest	259
4.9.82	show serviceshell	259
4.9.83	show storm-control	260
4.9.84	show storm-control limiters port	260
4.9.85	show vlan	261
4.9.86	show vlan brief	263
4.9.87	show vlan port	264
4.9.88	show voice vlan	265
4.9.89	show voice vlan interface	266
4.9.90	shutdown	267
4.9.91	shutdown all	268

4.9.92	snmp sync community-to-v3	269
4.9.93	snmp sync v3-to-community	270
4.9.94	snmp trap link-status	270
4.9.95	snmp trap link-status all	271
4.9.96	spanning-tree bpdumigrationcheck	272
4.9.97	speed	273
4.9.98	storm-control broadcast	274
4.9.99	storm-control egress-limiting	274
4.9.100	storm-control ingress-limiting	275
4.9.101	storm-control ingress-mode	275
4.9.102	storm-control broadcast (port-related)	276
4.9.103	storm-control egress-limit	276
4.9.104	storm-control ingress-limit	277
4.9.105	storm-control ingress-mode	277
4.9.106	storm-control flowcontrol	278
4.9.107	storm-control flowcontrol per port	279
4.9.108	vlan	280
4.9.109	vlan0-transparent-mode	281
4.9.110	vlan acceptframe	282
4.9.111	vlan database	283
4.9.112	vlan ingressfilter	284
4.9.113	vlan name	285
4.9.114	vlan participation	286
4.9.115	vlan participation all	287
4.9.116	vlan port acceptframe all	288
4.9.117	vlan port ingressfilter all	289
4.9.118	vlan port pvid all	290
4.9.119	vlan port tagging all	291
4.9.120	vlan pvid	292
4.9.121	vlan tagging	293
4.9.122	voice vlan (Global Config Mode)	294
4.9.123	voice vlan <id>	295
4.9.124	voice vlan dot1p	296
4.9.125	voice vlan none	296
4.9.126	voice vlan untagged	297
4.9.127	voice vlan auth	297
4.10	User Account Management Commands	298
4.10.1	disconnect	298
4.10.2	show loginsession	299
4.10.3	show users	300

4.10.4	users defaultlogin	301
4.10.5	users login <user>	302
4.10.6	users access	303
4.10.7	users name	304
4.10.8	users passwd	305
4.10.9	users snmpv3 accessmode	306
4.10.10	users snmpv3 authentication	307
4.10.11	users snmpv3 encryption	308
4.11	System Utilities	309
4.11.1	address-conflict	309
4.11.2	boot skip-aca-on-boot	310
4.11.3	show boot skip-aca-on-boot	310
4.11.4	cablestatus	311
4.11.5	clear eventlog	311
4.11.6	traceroute	312
4.11.7	clear arp-table-switch	312
4.11.8	clear config	313
4.11.9	clear config factory	313
4.11.10	clear counters	313
4.11.11	clear hiper-ring	314
4.11.12	clear igmpsnooping	314
4.11.13	clear mac-addr-table	315
4.11.14	clear pass	315
4.11.15	clear link-aggregation	316
4.11.16	clear signal-contact	316
4.11.17	clear traplog	317
4.11.18	clear ring-coupling	317
4.11.19	clear vlan	317
4.11.20	config-watchdog	318
4.11.21	copy	318
4.11.22	device-status connection-error	327
4.11.23	device-status monitor	328
4.11.24	logout	329
4.11.25	mac-address conflict operation	329
4.11.26	ping	330
4.11.27	signal-contact connection-error	330
4.11.28	signal-contact	331
4.11.29	temperature	332
4.11.30	reboot	333
4.11.31	show reboot	334

4.11.32 reload	335
4.11.33 show reload	336
4.11.34 set clibanner	337
4.11.35 set pre-login-banner	339
4.12 LLDP - Link Layer Discovery Protocol	341
4.12.1 show lldp	341
4.12.2 show lldp config	341
4.12.3 show lldp config chassis	342
4.12.4 show lldp config chassis admin-state	342
4.12.5 show lldp config chassis notification-interval	342
4.12.6 show lldp config chassis re-init-delay	343
4.12.7 show lldp config chassis tx-delay	343
4.12.8 show lldp config chassis tx-hold-mult	343
4.12.9 show lldp config chassis tx-interval	344
4.12.10 show lldp config port	345
4.12.11 show lldp config port tlv	346
4.12.12 show lldp med	347
4.12.13 show lldp med interface	348
4.12.14 show lldp med local-device detail	349
4.12.15 show lldp med remote-device	350
4.12.16 show lldp med remote-device detail	351
4.12.17 show lldp remote-data	351
4.12.18 lldp	353
4.12.19 lldp config chassis admin-state	354
4.12.20 lldp config chassis notification-interval	354
4.12.21 lldp config chassis re-init-delay	355
4.12.22 lldp config chassis tx-delay	355
4.12.23 lldp config chassis tx-hold-mult	356
4.12.24 lldp chassis tx-interval	356
4.12.25 clear lldp config all	357
4.12.26 lldp admin-state	357
4.12.27 lldp fdb-mode	358
4.12.28 lldp hm-mode	358
4.12.29 lldp max-neighbors	359
4.12.30 lldp med	360
4.12.31 lldp med all	361
4.12.32 lldp med confignotification	361
4.12.33 lldp med confignotification all	362
4.12.34 lldp med faststartrepeatcount	363
4.12.35 lldp med transmit-tlv	364

4.12.36	lldp med transmit-tlv all	365
4.12.37	lldp notification	366
4.12.38	lldp tlv link-aggregation	366
4.12.39	lldp tlv mac-phy-config-state	366
4.12.40	lldp tlv max-frame-size	367
4.12.41	lldp tlv mgmt-addr	367
4.12.42	lldp tlv pnio	367
4.12.43	lldp tlv pnio-alias	368
4.12.44	lldp tlv pnio-mrp	368
4.12.45	lldp tlv port-desc	368
4.12.46	lldp tlv port-vlan	369
4.12.47	lldp tlv gmrp	369
4.12.48	lldp tlv igmp	369
4.12.49	lldp tlv portsec	370
4.12.50	lldp tlv ptp	370
4.12.51	lldp tlv protocol	370
4.12.52	lldp tlv sys-cap	371
4.12.53	lldp tlv sys-desc	371
4.12.54	lldp tlv sys-name	371
4.12.55	lldp tlv vlan-name	372
4.12.56	name	372
4.13	SNTP - Simple Network Time Protocol	373
4.13.1	show sntp	373
4.13.2	show sntp anycast	375
4.13.3	show sntp client	375
4.13.4	show sntp operation	376
4.13.5	show sntp server	377
4.13.6	show sntp status	377
4.13.7	show sntp time	378
4.13.8	no sntp	378
4.13.9	sntp anycast address	379
4.13.10	sntp anycast transmit-interval	379
4.13.11	sntp anycast vlan	380
4.13.12	sntp client accept-broadcast	380
4.13.13	sntp client disable-after-sync	381
4.13.14	sntp client offset	381
4.13.15	sntp client request-interval	382
4.13.16	no sntp client server	382
4.13.17	sntp client server primary	383
4.13.18	sntp client server secondary	384

4.13.19	sntp client threshold	385
4.13.20	sntp operation	386
4.13.21	sntp server disable-if-local	387
4.13.22	sntp time system	387
4.14	PTP - Precision Time Protocol	388
4.14.1	show ptp	388
4.14.2	show ptp configuration	391
4.14.3	show ptp operation	391
4.14.4	show ptp port	392
4.14.5	show ptp status	393
4.14.6	ptp clock-mode	394
4.14.7	ptp operation	395
4.14.8	ptp sync-lower-bound	395
4.14.9	ptp sync-upper-bound	396
4.14.10	ptp v1 preferred-master	396
4.14.11	ptp v1 re-initialize	397
4.14.12	ptp v1 subdomain-name	397
4.14.13	ptp v1 sync-interval	398
4.14.14	ptp v2bc priority1	399
4.14.15	ptp v2bc priority2	399
4.14.16	ptp v2bc domain	400
4.14.17	ptp v2bc utc-offset	400
4.14.18	ptp v2bc utc-offset-valid	400
4.14.19	ptp v2bc vlan	401
4.14.20	ptp v2bc vlan-priority	401
4.14.21	ptp v1 burst	402
4.14.22	ptp v1 operation	402
4.14.23	ptp v2bc operation	403
4.14.24	ptp v2bc announce-interval	403
4.14.25	ptp v2bc announce-timeout	404
4.14.26	ptp v2bc sync-interval	404
4.14.27	ptp v2bc delay-mechanism	404
4.14.28	ptp v2bc pdelay-interval	405
4.14.29	ptp v2bc network-protocol	405
4.14.30	ptp v2bc v1-compatibility-mode	405
4.14.31	ptp v2bc asymmetry	406
4.14.32	ptp v2tc asymmetry	406
4.14.33	ptp v2tc delay-mechanism	406
4.14.34	ptp v2tc management	407
4.14.35	ptp v2tc multi-domain-mode	407

4.14.36	ptp v2tc network-protocol	408
4.14.37	ptp v2tc operation	408
4.14.38	ptp v2tc pdelay-interval	409
4.14.39	ptp v2tc primary-domain	409
4.14.40	ptp v2tc profile	410
4.14.41	ptp v2tc syntonization	410
4.14.42	ptp v2tc vlan	411
4.14.43	ptp v2tc power-tlv-check	411
4.14.44	ptp v2tc vlan-priority	412
4.14.45	ptp v2tc sync-local-clock	412
4.15	PoE - Power over Ethernet	413
4.15.1	show inlinepower	413
4.15.2	show inlinepower port	414
4.15.3	inlinepower (Global Config)	417
4.15.4	inlinepower (Interface Config)	418
4.15.5	clear inlinepower	419
4.16	PoE+ - Power over Ethernet Plus	420
4.16.1	show inlinepower slot	420
4.16.2	inlinepower budget slot	421
4.16.3	inlinepower threshold slot	422
4.16.4	inlinepower trap slot	422
4.17	Port monitor	423
4.17.1	show port-monitor	424
4.17.2	show port-monitor <slot/port>	424
4.17.3	show port-monitor brief	426
4.17.4	show port-monitor crc-fragment	427
4.17.5	show port-monitor link-flap	427
4.17.6	show port-monitor overload-detection	428
4.17.7	show port-monitor speed-duplex	429
4.17.8	port-monitor (Global Config)	430
4.17.9	port-monitor (Interface Config)	430
4.17.10	port-monitor action	431
4.17.11	port-monitor condition link-flap (Global Config)	432
4.17.12	port-monitor condition link-flap (Interface Config)	432
4.17.13	port-monitor condition crc-fragment (Global Config)	433
4.17.14	port-monitor condition crc-fragment (Interface Config)	434
4.17.15	port-monitor condition speed-duplex-monitor (Interface Config)	434

4.17.16	port-monitor condition speed-duplex-monitor speed (Interface Config)	435
4.17.17	port-monitor condition speed-duplex-monitor clear (Interface Config)	435
5	CLI Commands: Switching	437
5.1	Spanning Tree Commands	439
5.1.1	show spanning-tree	439
5.1.2	show spanning-tree interface	442
5.1.3	show spanning-tree mst detailed	443
5.1.4	show spanning-tree mst port detailed	444
5.1.5	show spanning-tree mst port summary	447
5.1.6	show spanning-tree mst summary	448
5.1.7	show spanning-tree summary	449
5.1.8	show spanning-tree vlan	450
5.1.9	spanning-tree	451
5.1.10	spanning-tree auto-edgeport	452
5.1.11	spanning-tree bpduguard	453
5.1.12	spanning-tree configuration name	454
5.1.13	spanning-tree configuration revision	455
5.1.14	spanning-tree edgeport	456
5.1.15	spanning-tree forceversion	457
5.1.16	spanning-tree forward-time	458
5.1.17	spanning-tree guard loop	459
5.1.18	spanning-tree guard none	460
5.1.19	spanning-tree guard root	461
5.1.20	spanning-tree hello-time	462
5.1.21	spanning-tree hold-count	462
5.1.22	spanning-tree max-age	463
5.1.23	spanning-tree max-hops	464
5.1.24	spanning-tree mst	465
5.1.25	spanning-tree mst priority	467
5.1.26	spanning-tree mst vlan	468
5.1.27	spanning-tree mst instance	469
5.1.28	spanning-tree port mode	470
5.1.29	spanning-tree port mode all	471
5.1.30	spanning-tree stp-mrp-mode	472
5.1.31	spanning-tree tcnguard	473
5.2	MRP	474
5.2.1	show mrp	474

5.2.2	show mrp current-domain	475
5.2.3	mrp current-domain	476
5.2.4	mrp delete-domain	478
5.2.5	mrp new-domain	478
5.2.6	arc	479
5.2.7	show arc	480
5.3	HIPER-Ring	482
5.3.1	show hiper-ring	483
5.3.2	hiper-ring	484
5.3.3	hiper-ring mode	484
5.3.4	hiper-ring port primary	485
5.3.5	hiper-ring port secondary	485
5.3.6	hiper-ring recovery-delay	486
5.4	Fast-HIPER-Ring	487
5.4.1	fast-hiper-ring	490
5.5	Redundant Coupling	492
5.5.1	show ring-coupling	493
5.5.2	ring-coupling	495
5.5.3	ring-coupling config	496
5.5.4	ring-coupling net-coupling	497
5.5.5	ring-coupling operation	497
5.5.6	ring-coupling port	498
5.5.7	ring-coupling redundancy-mode	498
5.6	Port Security	499
5.6.1	show port-sec dynamic	499
5.6.2	show port-sec mode	500
5.6.3	show port-sec port	501
5.6.4	port-sec mode	501
5.6.5	port-sec action	502
5.6.6	port-sec allowed-ip	503
5.6.7	port-sec allowed-ip add	503
5.6.8	port-sec allowed-ip remove	504
5.6.9	port-sec allowed-mac	504
5.6.10	port-sec allowed-mac add	505
5.6.11	port-sec allowed-mac remove	505
5.6.12	port-sec dynamic	506
5.6.13	clear port-sec	506
5.7	DHCP Relay Commands	507
5.7.1	dhcp-relay	508

5.7.2	dhcp-relay	509
5.7.3	show dhcp-relay	510
5.8	DHCP Server Commands	512
5.8.1	DHCP server configuration example	512
5.8.2	show dhcp-server	514
5.8.3	show dhcp-server operation	515
5.8.4	show dhcp-server port	515
5.8.5	show dhcp-server pool	516
5.8.6	dhcp-server addr-probe	516
5.8.7	dhcp-server operation	517
5.8.8	dhcp-server pool add <id>	517
5.8.9	dhcp-server pool modify <id> mode	518
5.8.10	dhcp-server pool modify <id> option	520
5.8.11	dhcp-server pool modify leasetime	521
5.8.12	dhcp-server pool modify <id> hirschmann-device	521
5.8.13	dhcp-server pool enable	522
5.8.14	dhcp-server pool disable	522
5.8.15	dhcp-server pool delete	522
5.9	Sub-Ring Commands	523
5.9.1	show sub-ring	523
5.9.2	sub-ring <id> mode	525
5.9.3	sub-ring <id> operation	526
5.9.4	sub-ring <id> protocol	526
5.9.5	sub-ring <id> port	527
5.9.6	sub-ring <id> ring-name	527
5.9.7	sub-ring <id> vlan	528
5.9.8	sub-ring <id> mrp-domainID	529
5.9.9	sub-ring delete-ring	530
5.9.10	sub-ring new-ring	530
6	CLI Commands: Security	531
6.1	Security Commands	533
6.1.1	authentication login	533
6.1.2	authorization network radius	535
6.1.3	clear dot1x statistics	535
6.1.4	clear radius statistics	536
6.1.5	dot1x defaultlogin	536
6.1.6	dot1x dynamic-vlan enable	537
6.1.7	dot1x guest-vlan	538

6.1.8	dot1x initialize	539
6.1.9	dot1x login	539
6.1.10	dot1x mac-auth-bypass	540
6.1.11	dot1x max-req	541
6.1.12	dot1x max-users	542
6.1.13	dot1x port-control	543
6.1.14	dot1x port-control all	544
6.1.15	dot1x re-authenticate	545
6.1.16	dot1x re-authentication	545
6.1.17	dot1x safe-vlan	546
6.1.18	dot1x system-auth-control	547
6.1.19	dot1x timeout	547
6.1.20	dot1x timeout guest-vlan-period	549
6.1.21	dot1x unauthenticated-vlan	550
6.1.22	dot1x user	551
6.1.23	ip ssh protocol	552
6.1.24	radius accounting mode	553
6.1.25	radius server host	553
6.1.26	radius server key	555
6.1.27	radius server msgauth	555
6.1.28	radius server primary	556
6.1.29	radius server retransmit	557
6.1.30	radius server timeout	558
6.1.31	show radius accounting	558
6.1.32	show authentication	561
6.1.33	show authentication users	562
6.1.34	show dot1x	562
6.1.35	show dot1x users	567
6.1.36	show dot1x clients	568
6.1.37	show ip ssh	569
6.1.38	show radius	570
6.1.39	show radius statistics	571
6.1.40	show users authentication	573
6.1.41	users login	574
6.2	HTTP Commands	575
6.2.1	ip http server	575
6.2.2	show ip http	576
6.2.3	ip https server	577
6.2.4	ip https port	578
6.2.5	ip https certgen	578

6.2.6	show ip https	579
7	Appendix- VLAN Example	581
7.1	SOLUTION 1	583
7.2	SOLUTION 2	585
8	Routing Commands	587
8.1	ARP Commands	589
8.1.1	arp	590
8.1.2	ip proxy-arp	591
8.1.3	arp cachesize	592
8.1.4	arp dynamicrenew	593
8.1.5	arp purge	593
8.1.6	arp resptime	594
8.1.7	arp retries	595
8.1.8	arp selective-learning	596
8.1.9	arp timeout	597
8.1.10	clear arp-cache	597
8.1.11	show arp	598
8.1.12	show arp brief	600
8.1.13	show arp switch	601
8.2	IP Routing	602
8.2.1	routing	603
8.2.2	ip routing	604
8.2.3	ip address	605
8.2.4	ip mtu	606
8.2.5	ip netdirbcast	607
8.2.6	ip route	608
8.2.7	ip route default	610
8.2.8	ip route distance	611
8.2.9	ip forwarding	612
8.2.10	ip vlan-single-mac	613
8.2.11	show ip brief	614
8.2.12	ip table-sizes	615
8.2.13	ip table-sizes arp-entries	616
8.2.14	ip table-sizes unicast-routes	617
8.2.15	ip table-sizes multicast-routes	618
8.2.16	show ip interface	619
8.2.17	show ip interface brief	621

8.2.18	show ip route	622
8.2.19	show ip route bestroutes	623
8.2.20	show ip route entry	624
8.2.21	show ip route preferences	625
8.2.22	show ip route static	626
8.2.23	show ip stats	627
8.3	Router Discovery Protocol Commands	633
8.3.1	ip irdp	634
8.3.2	ip irdp address	635
8.3.3	ip irdp holdtime	636
8.3.4	ip irdp maxadvertinterval	637
8.3.5	ip irdp minadvertinterval	638
8.3.6	ip irdp preference	639
8.3.7	show ip irdp	639
8.4	Virtual LAN Routing Commands	641
8.4.1	vlan routing	642
8.4.2	show ip vlan	643
8.5	Tracking Commands	644
8.5.1	track interface	644
8.5.2	track logical	645
8.5.3	track mode	645
8.5.4	track ping	646
8.5.5	track trap	647
8.5.6	show track	647
8.5.7	show track <id>	649
8.5.8	show track applications	651
8.6	VRRP Commands	652
8.6.1	ip vrrp	653
8.6.2	ip vrrp domain send-member-advertisements	654
8.6.3	ip vrrp trap	655
8.6.4	ip vrrp	656
8.6.5	ip vrrp mode	657
8.6.6	ip vrrp ip	658
8.6.7	ip vrrp authentication	659
8.6.8	ip vrrp preempt	660
8.6.9	ip vrrp delay-preemption	661
8.6.10	ip vrrp priority	662
8.6.11	ip vrrp timers advertise	663
8.6.12	ip vrrp advertisement-address	664

8.6.13	ip vrrp link-down-notification	665
8.6.14	ip vrrp track	666
8.6.15	ip vrrp domain	667
8.6.16	show ip vrrp interface stats	668
8.6.17	show ip vrrp	670
8.6.18	show ip vrrp domain	671
8.6.19	show ip vrrp interface	672
8.6.20	show ip vrrp interface brief	674
8.7	OSPF Commands	675
8.7.1	enable (OSPF)	676
8.7.2	ip ospf	677
8.7.3	1583compatibility	678
8.7.4	area default-cost	678
8.7.5	area nssa	679
8.7.6	area nssa default-info-originate	679
8.7.7	area nssa no-redistribute (OSPF)	680
8.7.8	area nssa no-summary (OSPF)	680
8.7.9	area nssa translator-role (OSPF)	680
8.7.10	area nssa translator-stab-intv	681
8.7.11	area range	681
8.7.12	area stub	682
8.7.13	area stub summarylsa	683
8.7.14	area virtual-link	684
8.7.15	area virtual-link authentication	685
8.7.16	area virtual-link dead-interval	686
8.7.17	area virtual-link hello-interval	687
8.7.18	area virtual-link retransmit-interval	688
8.7.19	area virtual-link transmit-delay	689
8.7.20	default-information originate (OSPF)	690
8.7.21	default-metric (OSPF)	691
8.7.22	distance ospf	692
8.7.23	distribute-list out	693
8.7.24	exit-overflow-interval	694
8.7.25	external-lsdb-limit	695
8.7.26	ip ospf areaid	696
8.7.27	ip ospf authentication	697
8.7.28	ip ospf cost	698
8.7.29	ip ospf dead-interval	699
8.7.30	ip ospf hello-interval	700
8.7.31	ip ospf priority	701

8.7.32	ip ospf retransmit-interval	702
8.7.33	ip ospf transmit-delay	703
8.7.34	ip ospf mtu-ignore	704
8.7.35	router-id	704
8.7.36	redistribute	705
8.7.37	maximum-paths	706
8.7.38	trapflags	707
8.7.39	show ip ospf	707
8.7.40	show ip ospf area	710
8.7.41	show ip ospf database	711
8.7.42	show ip ospf interface	713
8.7.43	show ip ospf interface brief	715
8.7.44	show ip ospf interface stats	716
8.7.45	show ip ospf neighbor	717
8.7.46	show ip ospf neighbor brief	720
8.7.47	show ip ospf range	721
8.7.48	show ip ospf stub table	722
8.7.49	show ip ospf virtual-link	723
8.7.50	show ip ospf virtual-link brief	724
8.8	RIP Commands	725
8.8.1	enable (RIP)	725
8.8.2	ip rip	726
8.8.3	auto-summary	727
8.8.4	default-information originate (RIP)	728
8.8.5	default-metric (RIP)	729
8.8.6	distance rip	730
8.8.7	distribute-list out	731
8.8.8	ip rip authentication	732
8.8.9	ip rip receive version	733
8.8.10	ip rip send version	734
8.8.11	hostroutesaccept	735
8.8.12	redistribute	736
8.8.13	split-horizon	737
8.8.14	update-timer	738
8.8.15	show ip rip	738
8.8.16	show ip rip interface brief	740
8.8.17	show ip rip interface	741
9	IP Multicast Commands	743
9.1	Multicast Commands	744

9.1.1	ip mcast boundary	744
9.1.2	ip multicast	745
9.1.3	ip multicast staticroute	746
9.1.4	ip multicast ttl-threshold	747
9.1.5	disable ip multicast mdebug mtrace	748
9.1.6	mrinfo	749
9.1.7	mstat	750
9.1.8	mtrace	751
9.1.9	no ip mcast mroute	752
9.1.10	show ip mcast	753
9.1.11	show ip mcast boundary	754
9.1.12	show ip mcast interface	754
9.1.13	show ip mcast mroute	755
9.1.14	show ip mcast mroute group	756
9.1.15	show ip mcast mroute source	757
9.1.16	show ip mcast mroute static	758
9.1.17	show mrinfo	759
9.1.18	show mstat	760
9.1.19	show mtrace	761
9.2	DVMRP Commands	762
9.2.1	ip dvmrp	763
9.2.2	ip dvmrp metric	764
9.2.3	ip dvmrp trapflags	765
9.2.4	ip dvmrp	766
9.2.5	show ip dvmrp	767
9.2.6	show ip dvmrp interface	768
9.2.7	show ip dvmrp neighbor	769
9.2.8	show ip dvmrp nexthop	770
9.2.9	show ip dvmrp prune	771
9.2.10	show ip dvmrp route	772
9.3	IGMP Commands	773
9.3.1	ip igmp	773
9.3.2	ip igmp version	774
9.3.3	ip igmp last-member-query-count	775
9.3.4	ip igmp last-member-query-interval	776
9.3.5	ip igmp query-interval	777
9.3.6	ip igmp query-max-response-time	778
9.3.7	ip igmp robustness	779
9.3.8	ip igmp startup-query-count	780
9.3.9	ip igmp startup-query-interval	781

9.3.10	show ip igmp	782
9.3.11	show ip igmp groups	782
9.3.12	show ip igmp interface	784
9.3.13	show ip igmp interface membership	786
9.3.14	show ip igmp interface stats	788
9.4	PIM-DM Commands	789
9.4.1	ip pimdm	790
9.4.2	ip pimdm holdtimes	791
9.4.3	ip pimdm mode	792
9.4.4	ip pimdm hello-interval	793
9.4.5	show ip pimdm	794
9.4.6	show ip pimdm interface	795
9.4.7	show ip pimdm interface stats	796
9.4.8	show ip pimdm neighbor	797
9.4.9	ip pim-trapflags	798
9.5	PIM-SM Commands	799
9.5.1	ip pimsm mode	800
9.5.2	ip pimsm bsr-border	801
9.5.3	ip pimsm dr-priority	802
9.5.4	ip pimsm join-prune-interval	803
9.5.5	ip pimsm hello-interval	804
9.5.6	ip pimsm bsr-candidate	805
9.5.7	ip pimsm register-threshold	806
9.5.8	ip pimsm rp-address	807
9.5.9	ip pimsm rp-candidate	808
9.5.10	ip pimsm ssm default	808
9.5.11	ip pimsm ssm	809
9.5.12	show ip pimsm	810
9.5.13	show ip pimsm bsr	811
9.5.14	show ip pimsm interface	811
9.5.15	show ip pimsm neighbor	811
9.5.16	show ip pimsm rp mapping	812
9.5.17	show ip pimsm rphash	812
9.5.18	show ip pimsm candidate	813
10	Quality of Service (QoS) Commands	815
10.1	MAC ACL Commands	816
10.1.1	mac access-list extended	817
10.1.2	mac access-list extended rename	818

10.1.3	{deny permit}	819
10.1.4	mac access-group	821
10.1.5	show mac access-lists	822
10.2	IP ACL Commands	824
10.2.1	access-list	825
10.2.2	access-list fragments	827
10.2.3	ip access-group	828
10.2.4	show ip access-lists	829
10.2.5	show access-lists global	831
10.2.6	show access-lists	832
10.3	CoS Commands	833
10.3.1	cos-queue max-bandwidth	834
10.3.2	cos-queue min-bandwidth	835
10.3.3	cos-queue strict	836
10.3.4	traffic-shape	837
10.3.5	show interfaces cos-queue	837
11	Protocol-based VLAN Commands	839
11.1	Show Commands	840
11.1.1	show port protocol	840
11.2	Configuration Commands	841
11.2.1	vlan protocol group	841
11.2.2	vlan protocol group add protocol	842
11.2.3	vlan protocol group remove	843
11.2.4	protocol group	843
11.2.5	protocol vlan group	844
11.2.6	protocol vlan group all	845
12	Index	847
13	Glossary	859
14	Further support	877

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 "Routing Configuration User Manual" document contains the information you need to start operating the routing function. It takes you step-by-step from a small router application through to the router configuration of a complex network. The manual enables you to configure your router by following the examples.

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

Some commands, such as **clear vlan**, do not require parameters. Other commands, such as **network parms**, have parameters for which you must supply a value. Parameters are positional — you must type the values in the correct order. Optional parameters will follow required parameters. For example:

■ 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 following conventions apply to the command name:

- ▶ The command name is displayed in this document in courier font and is to be typed exactly as shown.
- ▶ Once you have entered enough letters of a command name to uniquely identify the command, pressing the **<Space bar>** or **<Tab key>** will cause the system to complete the word.
- ▶ Entering Ctrl-Z will return you to the root level command prompt.

1.1.2 Parameters

Parameters are order dependent.

Parameters are displayed in this document in *italic font*, which are to be replaced with a name or number.

To use spaces as part of parameter name, enclose it in double quotes. For example, the expression "System Name with Spaces" forces the system to accept the spaces.

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`. Vertical bars `|` separate alternative, mutually exclusive, elements.
- ▶ The `{}` curly braces indicate that a parameter must be chosen from the list of choices.
- ▶ Braces within square brackets `[{}]` indicate a required choice within an optional element.

1.1.3 Values

ipaddr

This parameter is a valid IP address. Presently the IP address can be entered in following formats:

a (32 bits)

a.b (8.24 bits)

a.b.c (8.8.16 bits)

a.b.c.d (8.8.8.8 bits)

In addition to these formats, decimal, hexadecimal and octal formats are supported through the following input formats (where *n* is any valid hexadecimal, octal or decimal number):

0xn (CLI assumes hexadecimal format)

0n (CLI assumes octal format with leading zeros)

n (CLI assumes decimal format)

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.

routerid

The value of <router id> must be entered in 4-digit dotted-decimal notation (for example, 0.0.0.1). A router ID of 0.0.0.0 is invalid.

Interface

Valid slot and port number separated by forward slashes. For example, 0/1 represents slot number 0 and port number 1. See "Slot-Port Naming Convention" on

page 45.

Logical Interface

Logical slot and port number. This is applicable in the case of a port-channel (LAG) and vlan router interfaces (9/x). The operator can use the logical slot/port to configure the port-channel. See “Slot-Port Naming Convention” on page 45.

Character strings Use double quotation marks to identify character strings, for example, “System Name with Spaces”. An empty string (“”) is not valid.

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

Certain special key combinations speed up use of the CLI. They are listed in this section. Also, help is available for the CLI by typing **HELP**:

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-N	go to next line in history buffer
Ctrl-Z	return to root command prompt
Tab, <SPACE>	command-line completion
Exit	go to next lower command prompt
?	list choices

1.1.7 Special characters in scripts

Some of the configuration parameters are strings that can contain special characters. When the switch creates a script from the running configuration (by use of the command `#show running-config <scriptname.cli>`), these special characters are written to the script with a so-called escape character preceding them. This ensures that when applying the script, these characters are regarded as a normal part of the configuration parameter, not having the special meaning they usually have.

Character (plain)	Meaning, when entered in the CLI
!	Begin of a comment, ! and the rest of the line will be ignored
"	Begin or end of a string that may contain space characters
'	Begin or end of a string that may contain space characters
?	Shows possible command keywords or parameters
\	The backslash is used as an escape character to mask characters that normally have a special meaning

Tab. 2: Special characters

Character (escaped)	Meaning, when entered in the CLI
\!	! becomes part of the string
\"	" becomes part of the string
\'	' becomes part of the string
\?	? becomes part of the string
\\	\ becomes part of the string

Tab. 3: Special characters escaped

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. 4: 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 "..."	
link-aggregation "..."	
spanning-tree configuration name "..."	
ptp subdomain-name "..."	

Tab. 5: Commands in Global Config mode

Command	Note
name "..."	

Tab. 6: Commands in Interface Config mode

Command	Note
vlan name <n> "..."	

Tab. 7: 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 (\): \, !, ", ', ?
```

1.1.8 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
ip ospf authentication encrypt <secret> <id>	Software L3P
ip ospf authentication simple <secret>	Software L3P
ip rip authentication encrypt <secret> <id>	Software L3E and L3P
ip rip authentication simple <secret>	Software L3E and L3P
ip vrrp <id> authentication simple <secret>	Software L3E and L3P
radius server key acct <ip> <password>	
radius server key auth <ip> <password>	
users passwd <username> <password>	
users snmpv3 encryption <username> des <password>	

Tab. 8: Commands in Global Config mode

Command	Note
area <ip> virtual-link <ip> authentication encrypt <secret> <id>	Encrypted Authentication
area <ip> virtual-link <ip> authentication simple <secret>	Simple Authentication

Tab. 9: Commands in Router OSPF mode (software L3P)

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

1.1.9 Slot-Port Naming Convention

Switch software references physical entities such as cards and ports using a Slot/Port naming convention. This convention is also used to identify certain logical entities such as Link Aggregation (LAG) interfaces.

The slot number has two uses. In the case of physical ports it identifies the card containing the ports. In the case of logical ports it also identifies the type of interface or port.

Physical slot numbers

Physical slot numbers begin with one, and are allocated up to the maximum number of physical slots

Logical slot numbers

Logical slots immediately follow physical slots and identify LAG or router interfaces. For LAG the slot number 8 is used. For VLAN-based interfaces the slot number 9 is used.

The port identifies the specific physical port or logical interface being managed on a given slot.

Physical Ports

The physical ports for each slot are numbered sequentially starting from one.

Logical Interfaces

There are two types of logical interfaces: LAG and VLAN-based routing interfaces.

- ▶ LAG interfaces are only used for bridging functions. Each LAG interface consists of a set of up to eight physical ports and is identified by its own slot/port designation.
- ▶ VLAN routing interfaces are only used for routing functions.

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
<code>show port all</code> (in Privileged EXEC)	<p>Displays the Ports</p> <p>slot/port</p> <p>Type - Indicates if the port is a special type of port</p> <p>Admin Mode - Selects the Port Control Administration State</p> <p>Physical Mode - Selects the desired port speed and duplex mode</p> <p>Physical Status - Indicates the port speed and duplex mode</p> <p>Link Status - Indicates whether the link is up or down</p> <p>Link Trap - Determines whether or not to send a trap when link status changes</p> <p>LACP Mode - Displays whether LACP is enabled or disabled on this port.</p>

Table 10: Quick Start up Physical Port Data

■ Quick Start up User Account Management

Command	Details
<code>show users</code> (in Privileged EXEC)	<p>Displays all of the users that are allowed to access the switch</p> <p>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).</p> <p>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.</p>
<code>show login session</code> (in User EXEC)	Displays all of the login session information

Table 11: 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 11: 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 methods.

- ▶ Simple Network Management Protocol - SNMP
- ▶ 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
<code>show network</code> (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>
<code>network parms</code> <code><ipaddr> <net-mask> [gateway]</code> (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> <p>Subnet Mask range from 0.0.0.0 to 255.255.255.255</p>

Table 12: Quick Start up IP Address

Command	Details
	Gateway Address range from 0.0.0.0 to 255.255.255.255

Table 12: 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: <code>tftp://ipAddr/filepath/fileName</code> . The nvram:startup-config option downloads the configuration file using tftp and system:image option downloads the code file.

Table 13: 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 14: 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
- ▶ Router OSPF Config Mode
- ▶ Router RIP Config Mode
- ▶ MAC Access-list 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.

Table 15: Command Mode

Command Mode	Access Method	Prompt	Exit or Access Next Mode
Line Config Mode	From the Global Configuration mode, enter the <code>lineconfig</code> command	(Hirschmann Product) (line) #	To exit to the Global Config mode enter <code>exit</code> . To return to User Exec mode enter <code>ctrl-Z</code> .
Router OSPF Config Mode	From the Global Configuration mode, enter the <code>router ospf</code> command	(Hirschmann Product) (Config-router) #	To exit to the Global Config mode enter <code>exit</code> . To return to User Exec mode enter <code>ctrl-Z</code> .
Router RIP Config Mode	From the Global Config mode, enter the <code>router rip</code> command	(Hirschmann Product) (Config-router) #	To exit to the Global Config mode enter <code>exit</code> . To return to User Exec mode enter <code>ctrl-Z</code> .
MAC Access-list Config Mode	From the Global Config mode enter the <code>mac access-list extended <name></code> command.	(Hirschmann Product) (Config mac-access-list) #	To exit to the Global Config mode, enter the <code>exit</code> command. To return to the User EXEC mode, enter <code>Ctrl-Z</code> .

Table 15: 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.

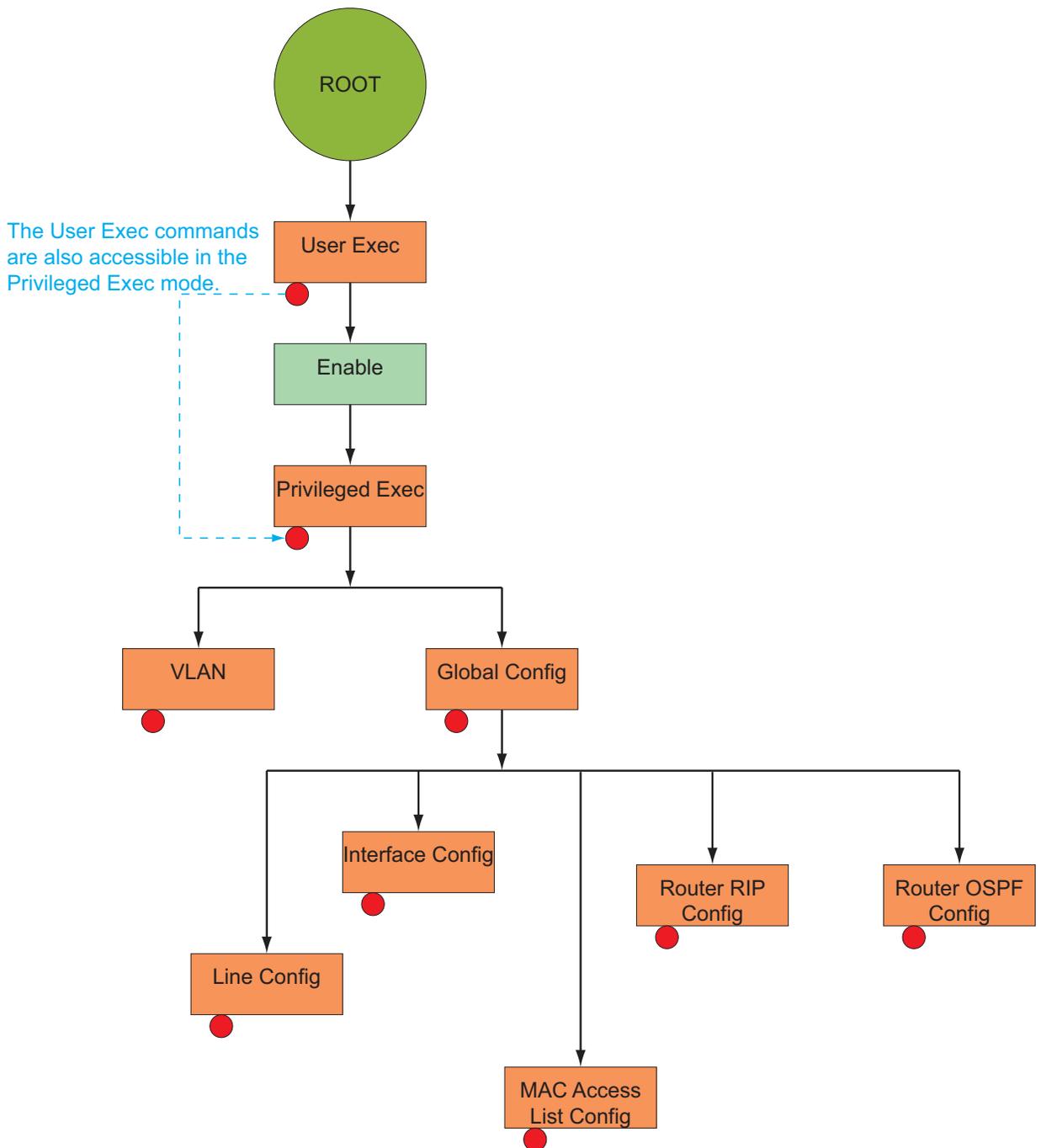


Fig. 1: Mode-based CLI

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) #
```

Router OSPF Config Mode:

In this mode, the operator is allowed to access the router OSPF configuration commands. The command prompt at this level is:

```
(Hirschmann Product) (Config) # router ospf  
Command Prompt: (Hirschmann Product) (Config  
router) #
```

Router RIP Config Mode:

In this mode, the operator is allowed to access the router RIP configuration commands. The command prompt at this level is:

```
(Hirschmann Product) (Config) # router rip  
Command Prompt: (Hirschmann Product) (Config router) #
```

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 fast-link-detection

This command displays the Bridge Fast Link Detection setting.

Format

```
show bridge fast-link-detection
```

Mode

```
Privileged EXEC and User EXEC
```

4.1.9 show bridge framesize

This command displays the maximum size of frame (packet size) setting.

Format

```
show bridge framesize
```

Mode

```
Privileged EXEC and User EXEC
```

4.1.10 show bridge vlan-learning

This command displays the bridge vlan-learning mode.

Format

```
show bridge vlan-learning
```

Mode

Privileged EXEC and User EXEC

4.1.11 bridge framesize

Activation of long frames. Configure 1522 or 1632¹⁾ or 9022²⁾ 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).

bridge framesize 9022 ¹⁾

Configure 9022 ²⁾ as maximum size of frame (packet size, jumbo frames).

¹⁾ On MACH4000, MACH100, MACH1000 and PowerMICE: 1552

²⁾ Available for the MACH104 and MACH1040 devices.

4.1.12 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

4.1.13 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.

4.1.14 show authentication

This command displays users assigned to authentication login lists.

Format

```
show authentication [users <listname>]
```

Mode

Privileged EXEC and User EXEC

4.1.15 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.

4.1.16 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.

4.1.17 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.

GMRP PDU's received - The count of GMRP PDU's received in the GARP layer.

GMRP PDU's Transmitted - The count of GMRP PDU's transmitted from the GARP layer.

GMRP Failed Registrations - The number of times attempted GMRP registrations could not be completed.

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

Dot1x Statistics

EAPOL Frames Received- The number of valid EAPOL frames of any type that have been received by this authenticator.

EAPOL Frames Transmitted - The number of EAPOL frames of any type that have been transmitted by this authenticator.

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.

4.1.18 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

4.1.19 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

4.1.20 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.

4.1.21 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.

4.1.22 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 gmrp” on page 248](#).

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.

4.1.23 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 256](#)).

4.1.24 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.

4.1.25 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. The output is displayed in the script format, which can be used to configure another switch with the same configuration.

Format

```
show running-config [all | <scriptname>]
```

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.

<scriptname>

Script file name for writing active configuration.

Note: Make sure that the file extension is cli, that the file name does not exceed 16 characters, does not start with a dot (.) and does not contain a directory.

4.1.26 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 alphanumeric 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.

Running Software Release

The operating system's software version number.

Running Software Build Date

The operating system's software build date.

Stored Software Release

The stored operating system's software version number.

Stored Software Build Date

The stored operating system's software build date.

Backup Software Release

The backup operating system's software version number.

Backup Software Build Date

The backup 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.
MAR1020-99TTTTMMMMTTTTTTTTTTTTTTTTTTUC9HPHH

Fan Status

The status of the MACH4000 fan.

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).

4.1.27 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
```

4.1.28 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 Debug Commands

4.2.1 debug tcpdump help

Run diagnostics commands. With the TCP dump you run a packet analyzer for capturing network traffic.

This command displays the supported options and expressions for the tcpdump command.

Format

```
debug tcpdump help
```

Mode

Privileged EXEC

4.2.2 debug tcpdump start cpu

Run diagnostics commands. With the TCP dump you run a packet analyzer for capturing network traffic.

This command starts a capture on the CPU interface with the options and expressions in the <command> parameter.

Without the <command> parameter this command starts a capture on the CPU interface using default options and no explicit filtering.

Format

```
debug tcpdump start cpu <command>
```

Mode

Privileged EXEC

4.2.3 debug tcpdump start cpu filter

Run diagnostics commands. With the TCP dump you run a packet analyzer for capturing network traffic.

This command starts a capture on the CPU interface with the options and expressions in the filter file.

Format

```
debug tcpdump start cpu filter <capturefilter>
```

Mode

Privileged EXEC

4.2.4 debug tcpdump stop

Run diagnostics commands. With the TCP dump you run a packet analyzer for capturing network traffic.

This command stops a running capture on the CPU interface.

Format

```
debug tcpdump stop
```

Mode

Privileged EXEC

4.2.5 debug tcpdump filter show

Run diagnostics commands. With the TCP dump you run a packet analyzer for capturing network traffic.

This command shows a saved filter file stored in flash memory.

Format

```
debug tcpdump filter show <capturefilter>
```

Mode

Privileged EXEC

4.2.6 debug tcpdump filter list

Run diagnostics commands. With the TCP dump you run a packet analyzer for capturing network traffic.

This command lists all saved filter files stored in flash memory.

Format

```
debug tcpdump filter list
```

Mode

Privileged EXEC

4.2.7 debug tcpdump filter delete

Run diagnostics commands. With the TCP dump you run a packet analyzer for capturing network traffic.

This command removes a saved filter file from the flash memory.

Format

```
debug tcpdump filter delete <capturefilter>
```

Mode

Privileged EXEC

4.3 Management VLAN Commands

4.3.1 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

4.4 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.

4.4.1 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

4.4.2 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

4.4.3 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 DSCP mapping and VLAN mapping table
(PowerMICE, MACH104, MACH1040, MACH4000)

– 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 or

Interface Config

(PowerMICE, MACH104, MACH1040, MACH4000)

■ 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 or

Interface Config

(PowerMICE, MACH104, MACH1040, MACH4000)

4.4.4 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
```

4.4.5 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.

4.4.6 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.

4.4.7 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

4.4.8 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

4.4.9 dvlan-tunnel ethertype

Note: This command is available for the RS20/RS30/RS40, RSB20, MS20/MS30, RSR20/RSR30, MACH100, MACH104, MACH1000, MACH1040,

MACH4002-24G/48G (XG), OCTOPUS, OS20/OS30 devices.

This command configures the ethertype for all core ports. The ethertype may have the values of 802.1q, vMAN or custom. The configured ethertype is used for VLAN classification on all ports which are configured as core ports.

Default

```
802.1Q
```

Format

```
dvlan-tunnel ethertype  
                {802.1Q | vman | custom <0-65535>}
```

Mode

```
Global Config
```

802.1Q

Configure the etherType as 0x8100.

custom

Custom configure the etherType for the DVlan tunnel.

Range for the optional value of the custom ethertype: 0 to 65535.

vman

Configure the etherType as 0x88A8.

4.4.10 mode dvlan-tunnel

Note: This command is available for the RS20/RS30/RS40, RSB20, MS20/MS30, RSR20/RSR30, MACH100, MACH104, MACH1000, MACH1040, MACH4002-24G/48G (XG), OCTOPUS, OS20/OS30 devices.

Use this command to configure the port either as core port or access port.

Default

Disabled

Format

```
mode dvlan-tunnel {access | core}
```

Mode

Interface Config

access

Configure this port as a customer port.

core

Configure this port as a provider network port.

■ no mode dvlan-tunnel

Use this command to configure the port as normal switch port and to disable the DVLAN tunneling.

Default

Disabled

Format

```
no mode dvlan-tunnel
```

Mode

Interface Config

4.4.11 show dvlan-tunnel

Note: This command is available for the RS20/RS30/RS40, RSB20, MS20/MS30, RSR20/RSR30, MACH100, MACH104, MACH1000, MACH1040, MACH4002-24G/48G (XG), OCTOPUS, OS20/OS30 devices.

Use this command to display the DVLAN-Tunnel mode and used ether-type for the specified interface(s).

Format

```
show dvlan-tunnel [interface {slot/port} | all]
```

Modes

Privileged EXEC

User EXEC

<slot/port>

Enter an interface in slot/port format.

all

Enter 'all' for all interfaces.

Interface

Display the number of the interface (slot/port).

Possible values (example): 1/1, 1/2, 2/1, 2/2, 2/3.

Mode

Display the DVLAN-Tunnel mode.

Possible values: normal,

EtherType

Display the used ether-type.

Possible values: 802.1Q, vman, custom.

4.5 Link Aggregation(802.3ad) Commands

4.5.1 link-aggregation staticcapability

This command enables the support of link-aggregations (static LAGs) on the device. By default, the static capability for all link-aggregations is disabled.

Default

disabled

Format

```
link-aggregation staticcapability
```

Mode

Global Config

■ no link-aggregation staticcapability

This command disables the support of static link-aggregations (LAGs) on the device.

Default

disabled

Format

```
no link-aggregation staticcapability
```

Mode

Global Config

4.5.2 show link-aggregation brief

This command displays the static capability of all link-aggregations (LAGs) on the device as well as a summary of individual link-aggregations.

Format

```
show link-aggregation brief
```

Mode

Privileged EXEC and User EXEC

Static Capability

This field displays whether or not the device has static capability enabled.

For each link-aggregation the following information is displayed:

Name

This field displays the name of the link-aggregation.

Link State

This field indicates whether the link is up or down.

Mbr Ports

This field lists the ports that are members of this link-aggregation, in <slot/port> notation.

Max. num. of LAGs

Displays the maximum number of concurrently configured link aggregations on this device.

Slot no. for LAGs

Displays the slot number for all configured link aggregations on this device.

4.6 Management Commands

These commands manage the switch and show current management settings.

4.6.1 telnet

This command establishes a new outbound telnet connection to a remote host. The host value must be a valid IP address. Valid values for port should be a valid decimal integer in the range of 0 to 65535, where the default value is 23. If [debug] is used, the current telnet options enabled is displayed. The optional line parameter sets the outbound telnet operational mode as 'line-mode', where by default, the operational mode is 'character mode'. The echo option enables local echo and only takes effect when the local switch is accessed via the serial connection (V.24).

Format

```
telnet <host> <port> [debug] [line] [echo]
```

Mode

Privileged EXEC and User EXEC

4.6.2 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

4.6.3 transport output telnet

This command regulates new outbound telnet connections. If enabled, new outbound telnet sessions can be established until it reaches the maximum number of simultaneous outbound telnet sessions allowed.

If disabled, no new outbound telnet session can be established. An established session remains active until the session is ended or an abnormal network error ends it.

Default

enabled

Format

```
transport output telnet
```

Mode

Line Config

■ no transport output telnet

This command disables new outbound telnet connections. If disabled, no new outbound telnet connection can be established.

Format

```
no transport output telnet
```

Mode

Line Config

4.6.4 session-limit

This command specifies the maximum number of simultaneous outbound telnet sessions. A value of 0 indicates that no outbound telnet session can be established.

Default

4

Format`session-limit <0-5>`**Mode**

Line Config

■ no session-limit

This command sets the maximum number of simultaneous outbound telnet sessions to the default value.

Format`no session-limit`**Mode**

Line Config

4.6.5 session-timeout

This command sets the telnet session timeout value. The timeout value unit of time is minutes.

Default

5

Format

```
session-timeout <1-160>
```

Mode

Line Config

■ no session-timeout

This command sets the telnet session timeout value to the default. The timeout value unit of time is minutes.

Format

```
no session-timeout
```

Mode

Line Config

4.6.6 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

4.6.7 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

4.6.8 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

4.6.9 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

4.6.10 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

4.6.11 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

4.6.12 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
```

4.6.13 digital-input

This command configures the MICE IO-Module digital inputs.

Format

```
digital-input  
  admin-state {enable | disable}  
  refresh-interval <refresh-interval>  
  log-event {all | <slot/input>} {enable | disable}  
  snmp-trap {all | <slot/input>} {enable | disable}
```

Mode

```
Global Config
```

admin-state

This command enables or disables the polling task for digital inputs of the MICE IO-Module. When disabled, no event logging or SNMP traps will work. Default value: `disable`.

`disable` Disable the IO-Module digital inputs admin state.

`enable` Enable the IO-Module digital inputs admin state.

refresh-interval

This command configures the digital inputs refresh interval. Each input configured for event logging or SNMP traps is polled with this interval.

`<refresh-interval>` The refresh interval is in the range of 1..10 seconds. Default value: 1.

log-event

This command enables or disables the event logging of input status changes for one or all digital inputs. Default value: `disable`.

The input state will be checked according to the interval set with `IO-<refresh-interval>`.

`all` Configure the IO-Module event logging for all digital inputs.

`<slot/input>` Configure the IO-Module event logging for a single digital input.

`disable` Disable event logging for digital input status changes.

`enable` Enable event logging for digital input status changes.

snmp-trap

This command enables or disables the sending of SNMP traps in case of input status changes for one or all digital inputs. Default value: `disable`.

The trap will be sent to all SNMP trap receivers configured with `snmptrap`.

The input state will be checked according to the interval set with `IO-<refresh-interval>`.

`all` Configure the IO-Module SNMP trap for all digital inputs.

`<slot/input>` Configure the IO-Module SNMP trap for a single digital input.

`disable` Disable SNMP traps for digital input status changes.

`enable` Enable SNMP traps for digital input status changes.

4.6.14 digital-output

This command configures the IO-Module digital outputs.

Format

```
digital-output
  admin-state {enable | disable}
  refresh-interval <refresh-interval>
  retry-count <refresh-interval>
  log-event {all | <slot/output>} {enable|disable}
  snmp-trap {all | <slot/output>} {enable|disable}
  mirror all | <slot>/<output> {disable |
                                from <IPaddress> <slot>/<input>}
```

Mode

Global Config

admin-state

This command enables or disables the polling task for digital outputs of the MICE IO-Module. When disabled, no event logging or SNMP traps will work. Default value: `disable`.

`disable` Disable the IO-Module digital outputs admin state.
`enable` Enable the IO-Module digital outputs admin state.

refresh-interval

This command configures the IO-Module digital outputs refresh interval. Each output configured for input mirroring is refreshed (input is polled) with this interval.

`<refresh-interval>` The refresh interval is in the range of 1..10 seconds. Default value: 1.

retry-count

This command configures the number of retry counts for setting digital outputs of the MICE IO-Module. Each output configured for input mirroring is set to the default value (low) when after the number of configured retries no SNMP get request was answered.

`<refresh-interval>` The refresh interval is in the range of 1..10 seconds. Default value: 1.

log-event

This command enables or disables the event logging of output status changes for one or all digital outputs. Default value: `disable`.

The output state will be checked according to the interval set with IO-

`<refresh-interval>`.

Configure the IO-Module event logging for one or all digital outputs.

`all` Configure the IO-Module event logging for all digital outputs.

`<slot/output>` Configure the IO-Module event logging for a single digital output.

`disable` Disable event logging for digital output status changes.

`enable` Enable event logging for digital output status changes.

snmp-trap

This command enables or disables the sending of SNMP traps in case of output status changes for one or all digital outputs. Default value: `disable`.

The trap will be sent to all SNMP trap receivers configured with `snmptrap`.

The output state will be checked according to the interval set with `IO-
<refresh-interval>`.

`all` Configure the IO-Module SNMP trap for all digital outputs.

`<slot/output>` Configure the IO-Module SNMP trap for a single digital output.

`disable` Disable SNMP traps for digital output status changes.

`enable` Enable SNMP traps for digital output status changes.

mirror

Configure the IO-Module mirroring for one or all digital outputs. This command determines the input mirrored to the currently selected output.

To disable mirroring, the following commands are equivalent:

```
digital-output mirror 1/2 disable  
digital-output mirror 1/2 from 0.0.0.0 1/1
```

<all>: Configure the IO-Module mirroring for all digital outputs.

<slot/output>: Configure the IO-Module mirroring for a single digital output. The **<slot>** value determines the IO-module slot number on the device with the selected IP address.

disable: Disable the IO-Module mirroring for a single digital output.

from: Enable the IO-Module mirroring for a single digital output from **<IP-address>** **<slot/input>**

<IPaddress>: The IP address value determines the IP address used for reading the input value. Use IP address 127.0.0.1 or the system IP address to mirror inputs from a local IO module. When IP address is 0.0.0.0 no input is mirrored to the output (the output value is set to 'low'). Default value: 0.0.0.0.

<slot/input>: The **<input>** value determines the input number on this device. Default value: 1/1.

4.6.15 show digital-input

This command shows the input value or configuration from all available digital inputs of the MICE I/O Module.

Format

```
show digital-input
```

Mode

```
Global Config
```

Digital Input System Information:

Admin State

Show the IO-Module digital inputs Admin State.

Possible values: Disabled, Enabled.

Refresh Interval [s]

Show the IO-Module digital inputs Refresh Interval in seconds.

Value range: 1..10.

Digital Input Information:

Input

Show numbers of the IO-Module digital input.

Possible values (example): 1/1, 1/2, 1/3, 1/4,
3/1, 3/2, 3/3, 3/4

Value

Show the value of the IO-Module digital inputs.

Possible values: Not available, High, Low.

Log-Event

Show if Event logging is enabled or disabled for the IO-Module digital inputs.

Possible values: Disabled, Enabled.

SNMP-trap

Show if SNMP traps are enabled or disabled for the IO-Module digital inputs.

Possible values: Disabled, Enabled.

4.6.16 show digital-input config

This command shows the IO-Module digital inputs global configuration.

Format

```
show digital-input config
```

Mode

```
Global Config
```

Digital Input System Information:**Admin State**

Show the IO-Module digital inputs Admin State.

Possible values: Disabled, Enabled.

Refresh Interval [s]

Show the IO-Module digital inputs Refresh Interval in seconds.

Value range: 1..10.

4.6.17 show digital-input all

This command shows the IO-Module value or configuration for all inputs.

Format

```
show digital-input all {all | config | value}
```

Mode

Global Config

all

Show the IO-Module configuration and value for all inputs

config

Show the IO-Module configuration for all inputs.

value

Show the IO-Module value for all inputs.

Digital Input Information:

Input

Show numbers of the IO-Module digital input.

Possible values (example): 1/1, 1/2, 1/3, 1/4,
3/1, 3/2, 3/3, 3/4

Value

Show the value of the IO-Module digital inputs.

Possible values: Not available, High, Low.

Log-Event

Show if Event logging is enabled or disabled for the IO-Module digital inputs. Possible values: Disabled, Enabled.

SNMP-trap

Show if SNMP traps are enabled or disabled for the IO-Module digital inputs. Possible values: Disabled, Enabled.

4.6.18 show digital-input <slot/input>

This command shows the IO-Module value or configuration for a single input.

Format

```
show digital-input <slot/input>
                               {all | config | value}
```

Mode

Global Config

all

Show the IO-Module configuration and value for one input.

config

Show the IO-Module configuration for one input.

value

Show the IO-Module value for one input.

Digital Input <slot/input> Value

Show the value of the IO-Module digital input.

Possible values: Not available, High, Low.

Digital Input <slot/input> Log-Event

Show if Event logging is enabled or disabled for the IO-Module digital input. Possible values: Disabled, Enabled.

Digital Input <slot/input> SNMP-trap

Show if SNMP traps are enabled or disabled for the IO-Module digital input. Possible values: Disabled, Enabled.

4.6.19 show digital-output

This command shows the output value or configuration from all available digital outputs of the MICE I/O Module.

Format

```
show digital-output
```

Mode

```
Global Config
```

Digital output System Information:

Admin State

Show the IO-Module digital outputs Admin State.
Possible values: Disabled, Enabled.

Refresh Interval [s]

Show the IO-Module digital outputs Refresh Interval in seconds.
Value range: 1..10.

Retry Count

Show the value of the IO-Module digital outputs Retry count.
Value range: 1..10.

Digital output Information:

Output

Show numbers of the IO-Module digital output.
Possible values (example): 1/1, 1/2, 1/3, 1/4,
3/1, 3/2, 3/3, 3/4

Value

Show the value of the IO-Module digital outputs.
Possible values: Not available, High, Low.

Log-Event

Show if Event logging is enabled or disabled for the IO-Module digital outputs.
Possible values: Disabled, Enabled.

SNMP-trap

Show if SNMP traps are enabled or disabled for the IO-Module digital outputs.
Possible values: Disabled, Enabled.

Mirror from IP

Show the IP address used for reading the input value.
Possible values: `None`, `a.b.c.d` (valid IP address).

Input

Show the input number of the device used for reading the input value.
Possible values (example): `1/1`, `1/2`, `1/3`, `1/4`,
`3/1`, `3/2`, `3/3`, `3/4`

4.6.20 show digital-output config

This command shows the IO-Module digital outputs global configuration.

Format

```
show digital-output config
```

Mode

```
Global Config
```

Digital output System Information:**Admin State**

Show the IO-Module digital outputs Admin State.
Possible values: `Disabled`, `Enabled`.

Refresh Interval [s]

Show the IO-Module digital outputs Refresh Interval in seconds.
Value range: `1..10`.

Retry Count

Show the value of the IO-Module digital outputs Retry count.
Value range: `1..10`.

4.6.21 show digital-output all

This command shows the IO-Module value or configuration for all outputs.

Format

```
show digital-output all {all | config | value}
```

Mode

Global Config

all

Show the IO-Module configuration and value for all outputs

config

Show the IO-Module configuration for all outputs.

value

Show the IO-Module value for all outputs.

Digital output Information:

output

Show numbers of the IO-Module digital output.

Possible values (example): 1/1, 1/2, 1/3, 1/4,
3/1, 3/2, 3/3, 3/4

Value

Show the value of the IO-Module digital outputs.

Possible values: Not available, High, Low.

Log-Event

Show if Event logging is enabled or disabled for the IO-Module digital outputs. Possible values: Disabled, Enabled.

SNMP-trap

Show if SNMP traps are enabled or disabled for the IO-Module digital outputs. Possible values: Disabled, Enabled.

Mirror from IP

Show the IP address used for reading the input value.

Possible values: None, a.b.c.d (valid IP address).

Input

Show the input number of the device used for reading the input value.

Possible values (example): 1/1, 1/2, 1/3, 1/4,
3/1, 3/2, 3/3, 3/4

4.6.22 show digital-output <slot/output>

This command shows the IO-Module value or configuration for a single output.

Format

```
show digital-output <slot/output>
                               {all | config | value}
```

Mode

Global Config

all

Show the IO-Module configuration and value for one output.

config

Show the IO-Module configuration for one output.

value

Show the IO-Module value for one output.

Digital output <slot/output> Value

Show the value of the IO-Module digital output.

Possible values: Not available, High, Low, Invalid.

Digital output <slot/output> Log-Event

Show if Event logging is enabled or disabled for the IO-Module digital output.

Possible values: Disabled, Enabled.

Digital output <slot/output> SNMP-trap

Show if SNMP traps are enabled or disabled for the IO-Module digital output.

Possible values: Disabled, Enabled.

Digital Output <slot/output> Mirror from IP

Show the IP address used for reading the input value.

Possible values: Not configured, a.b.c.d (valid IP address).

4.6.23 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.

4.6.24 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.

4.6.25 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.

4.6.26 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.

4.6.27 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.

4.6.28 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.

4.6.29 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

4.6.30 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

4.6.31 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

4.6.32 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.

4.6.33 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

4.6.34 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

4.6.35 show ethernet-ip

This command displays the admin state of the EtherNet/IP function.

Format

```
show ethernet-ip
```

Mode

Privileged EXEC and User EXEC

4.6.36 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`.

4.6.37 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] | [].

4.6.38 show profinetio

This command displays the admin state of the PROFINET IO function.

Format

```
show profinetio
```

Mode

Privileged EXEC and User EXEC

4.6.39 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.

4.6.40 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
```

4.6.41 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.

4.6.42 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.

4.6.43 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.

4.6.44 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*.

4.6.45 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 (4 for version L2P)

Allow New Telnet Sessions

Indicates that new telnet sessions will not be allowed when set to no. The factory default value is `yes`.

4.6.46 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 and 802.1X)

Enable/disable sending port security event traps (for MAC/IP port security as well as for 802.1X).

Spanning Tree Flag

May be enabled or disabled. The factory default is enabled. Indicates whether spanning tree traps will be sent.

4.6.47 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.

4.6.48 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.

4.6.49 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.

4.6.50 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

4.6.51 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
```

4.6.52 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

4.6.53 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

4.6.54 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

4.6.55 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
```

4.6.56 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
```

4.6.57 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
```

4.6.58 snmp-server location

This command configures the system location.

Format

```
snmp-server location <system location>
```

Mode

```
Global Config
```

4.6.59 snmp-server sysname

This command configures the system name.

Format

```
snmp-server sysname <system name>
```

Mode

Global Config

4.6.60 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

4.6.61 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

4.6.62 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

4.6.63 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

4.6.64 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

4.6.65 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 as well as to 802.1X 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

4.6.66 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

4.6.67 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

4.6.68 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.

4.6.69 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
```

4.6.70 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.

4.6.71 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

4.6.72 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

4.7 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.

4.7.1 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

4.7.2 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
```

4.7.3 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

4.7.4 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 16

■ no logging console

This command disables logging to the console.

Format

```
no logging console
```

4.7.5 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. 16: Possible severity levels

4.7.6 logging host reconfigure

The Logging Host Index for which to change the IP Address.

Format

```
logging host reconfigure <hostindex> <hostaddress>
```

Mode

```
Global Config
```

4.7.7 logging host remove

The Logging Host Index to be removed.

Format

```
logging host remove <hostindex>
```

Mode

```
Global Config
```

4.7.8 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
```

4.7.9 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

4.7.10 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).

4.7.11 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).

4.7.12 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

4.7.13 logging syslog port

Enter the port number of the syslog server.

Default

514

Format

logging syslog port <portid>

Mode

Global Config

4.8 Scripting Commands

Configuration Scripting allows the user to generate text-formatted script files representing the current configuration. These configuration script files can be uploaded to a PC and edited, downloaded to the system and applied to the system. Configuration scripts can be applied to one or more switches with no/minor modifications.

Use the `show running-config` command to capture the running configuration into a script. Use the `copy` command to transfer the configuration script to and from the switch.

Scripts are intended to be used on systems with default configuration but users are not prevented from applying scripts on systems with non-default configurations.

Note:

- ▶ The file extension must be “.cli”.
- ▶ A maximum of ten scripts are allowed on the switch.
- ▶ The combined size of all script files on the switch shall not exceed 1024 KB.

4.8.1 script apply

This command applies the commands in the script to the switch. We recommend that the system have default configurations but users are not prevented from applying scripts on systems with non-default configurations. The `<scriptname>` parameter is the name of the script to apply.

Format

```
script apply <scriptname>
```

Mode

```
Privileged EXEC
```

4.8.2 script delete

This command deletes a specified script where the <scriptname> parameter is the name of the script to be deleted. The 'all' option deletes all the scripts present on the switch.

Format

```
script delete {<scriptname> | all}
```

Mode

Privileged EXEC

4.8.3 script list

This command lists all scripts present on the switch as well as the remaining available space.

Format

```
script list [aca]
```

Mode

Privileged EXEC

Configuration Script

Name of the script.

Without the optional ACA parameter: Listing of the scripts in the switch's flash memory.

With the optional ACA parameter: Listing of the scripts on the external ACA 21-USB.

Size

Size of the script.

4.8.4 script show

This command displays the contents of a script file. The parameter <script-name> is the name of the script file.

Format

```
script show <scriptname>
```

Mode

Privileged EXEC

The format of display is

```
Line <no>: <Line contents>
```

4.8.5 script validate

This command validates a script file by parsing each line in the script file where <scriptname> is the name of the script to validate. The validate option is intended to be used as a tool for script development.

Validation helps to identify potential errors concerning a script on the device.

Format

```
script validate <scriptname>
```

Mode

Privileged EXEC

4.9 Device Configuration Commands

4.9.1 addport

This command adds one port to the Link Aggregation (LAG). The given interface is a logical slot and port number of a configured Link Aggregation.

Note: Before adding a port to a Link Aggregation, set the physical mode of the port. See 'speed' command.

Format

```
addport <logical slot/port>
```

Mode

```
Interface Config
```

4.9.2 adminmode

This command enables the whole Link Aggregation as one single port.

Note: Before adding a port to a Link Aggregation, set the physical mode of the port. See 'speed' command.

Format

```
adminmode
```

Mode

```
Interface Config
```

■ no adminmode

This command disables the whole Link Aggregation as one single port.

Format

```
no adminmode
```

Mode

```
Interface Config
```

4.9.3 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.

4.9.4 auto-disable reset

Use this command to reset the specific interface and reactivate the port.

Format

```
auto-disable reset
```

Mode

```
Interface Config
```

4.9.5 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.

4.9.6 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
```

4.9.7 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
```

4.9.8 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.

4.9.9 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.

4.9.10 deleteport

This command deletes the port from the link-aggregation (LAG). The interface is a logical slot and port number of a configured link aggregation.

Note: This command has to be issued in the member port's interface config mode.

Format

```
deleteport <logical slot/port>
```

Mode

```
Interface Config
```

4.9.11 deleteport all

This command deletes all configured ports from the link-aggregation (LAG). The interface is a logical slot and port number of a configured link-aggregation.

Format

```
deleteport <logical slot/port> all
```

Mode

```
Global Config
```

4.9.12 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.

4.9.13 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
```

4.9.14 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
```

4.9.15 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

4.9.16 mac notification (Global Config)

Use this command to change the settings for MAC address change notification globally on the device. This command enables the sending of MAC notification traps or sets the MAC notification interval in seconds.

Format

```
mac notification {operation |  
                  interval <0..2147483647> }
```

Mode

Global Config

operation

Enable sending of MAC notification traps.

interval

Set the MAC notification interval.

<0..2147483647>

MAC notification interval in seconds.

■ no mac notification operation

This command disables sending of MAC notification traps globally.

Format

```
no mac notification operation
```

Mode

Global Config

4.9.17 mac notification (Interface Config)

Use this command to change the settings for MAC address change notification for one port. This command enables MAC notification for this port or sets the mode for which action the device sends a MAC notification.

Format

```
mac notification {operation |  
                  mode { add | remove | all } }
```

Mode

Interface Config

operation

Enable sending of MAC notification traps.

mode

Set the mode for which action the device sends a MAC notification.

add

The device sends MAC notification traps when entries are added to the FDB.

remove

The device sends MAC notification traps when entries are removed from the FDB.

all

The device sends MAC notification traps when entries are changed in the FDB.

■ no mac notification operation

This command disables sending of MAC notification traps for this port.

Format

```
no mac notification operation
```

Mode

Interface Config

4.9.18 monitor session <session-id>

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 <session-id>
  [ 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<session-id>**

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 <session-id> [mode]
```

Mode

Global Config

session-id

Session number (currently, session number 1 is supported).

4.9.19 monitor session <session-id> 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 <session-id> mode
```

Mode

Global Config

session-id

Session number (currently, session number 1 is supported).

■ no monitor session <session-id> mode

This command sets the monitor session (port monitoring) mode to disable.

Format

```
no monitor session <session-id> mode
```

Mode

Global Config

session-id

Session number (currently, session number 1 is supported).

4.9.20 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.

This command can be called multiple times with different ports to add more than one source port to the session.

It is possible to add/remove ports to/from an active session.

Note:

- The device supports a maximum of one session.
- The maximum number of source ports is 8.
- Ports configured as mirror source or destination ports have to be physical ports.

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

Default

none

Format

```
monitor session <session-id> {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 | destination} interface
```

Mode

Global Config

session-id

Session number (currently, session number 1 is supported).

4.9.21 link-aggregation

This command configures a new Link Aggregation (LAG) and generates a logical slot/port number for the Link Aggregation. Display this number using the “show link-aggregation”.

Note: Before including a port in a Link Aggregation, set the port physical mode. See ‘speed’ command.

Format

```
link-aggregation <name>
```

Mode

Global Config

4.9.22 link-aggregation adminmode

This command enables a Link Aggregation (LAG). The interface is a logical slot/port for a configured Link Aggregation. The option `all` sets every configured Link Aggregation with the same administrative mode setting.

Format

```
link-aggregation adminmode all
```

Mode

```
Global Config
```

■ no link-aggregation adminmode

This command disables a Link Aggregation (LAG). The interface is a logical slot/port for a configured Link Aggregation. The option `all` sets every configured Link Aggregation with the same administrative mode setting.

Format

```
no link-aggregation adminmode all
```

Mode

```
Global Config
```

4.9.23 link-aggregation linktrap

This command enables link trap notifications for the link-aggregation (LAG). The interface is a logical slot/port for a configured link-aggregation. The option `all` sets every configured link-aggregation with the same administrative mode setting.

Default

`enabled`

Format

```
link-aggregation linktrap {<logical slot/port> |  
all}
```

Mode

Global Config

■ no link-aggregation linktrap

This command disables link trap notifications for the link-aggregation (LAG). The interface is a logical unit, slot and port slot and port for a configured link-aggregation. The option `all` sets every configured link-aggregation with the same administrative mode setting.

Format

```
no link-aggregation linktrap {<logical slot/port> |  
all}
```

Mode

GlobalConfig

4.9.24 link-aggregation name

This command defines a name for the link-aggregation (LAG). The interface is a logical slot/port for a configured link-aggregation, and name is an alphanumeric string up to 15 characters. This command is used to modify the name that was associated with the link-aggregation when it was created.

Format

```
link-aggregation name {<logical slot/port> | all |  
<name>}
```

Mode

Global Config

4.9.25 rmon-alarm add

This command adds an RMON alarm.

Format

```
rmon-alarm add <index>  
                [<mib-variable>  
                <rising-threshold>  
                <falling-threshold>]
```

Mode

Global Config

index

Enter the index of the RMON alarm.

mib-variable

Enter the MIB variable.

rising-threshold

Enter the rising threshold for the RMON alarm.

falling-threshold

Enter the falling threshold for the RMON alarm.

4.9.26 rmon-alarm delete

This command deletes an RMON alarm.

Format

```
rmon-alarm delete <index>
```

Mode

Global Config

index

Enter the index of the RMON alarm.

4.9.27 rmon-alarm enable

This command enables an RMON alarm.

Format

```
rmon-alarm enable <index>
```

Mode

Global Config

index

Enter the index of the RMON alarm.

4.9.28 rmon-alarm disable

This command disables an RMON alarm.

Format

```
rmon-alarm disable <index>
```

Mode

Global Config

index

Enter the index of the RMON alarm.

4.9.29 rmon-alarm modify mib-variable

This command modifies the mib-variable of an RMON alarm.

Format

```
rmon-alarm modify <index> mib-variable <mib-variable>
```

Mode

Global Config

index

Enter the index of the RMON alarm.

mib-variable

Enter the MIB variable.

4.9.30 rmon-alarm modify thresholds

This command modifies the thresholds of an RMON alarm.

Format

```
rmon-alarm modify <index> thresholds
                               <rising-threshold>
                               <falling-threshold>
```

Mode

Global Config

index

Enter the index of the RMON alarm.

rising-threshold

Enter the rising threshold for the RMON alarm.

falling-threshold

Enter the falling threshold for the RMON alarm.

4.9.31 rmon-alarm modify interval

This command modifies the interval of an RMON alarm.

Format

```
rmon-alarm modify <index> interval <interval>
```

Mode

Global Config

index

Enter the index of the RMON alarm.

interval

Enter the interval for the RMON alarm.

4.9.32 rmon-alarm modify sample-type

This command modifies the sample-type of an RMON alarm.

Format

```
rmon-alarm modify <index> sample-type {absolute|delta}
```

Mode

Global Config

index

Enter the index of the RMON alarm.

absolute

Sample-type for RMON alarm is absolute.

delta

Sample-type for RMON alarm is delta.

4.9.33 rmon-alarm modify startup-alarm

This command modifies the startup-alarm of an RMON alarm.

Format

```
rmon-alarm modify <index> startup-alarm  
                    {rising | falling | risingorfalling}
```

Mode

Global Config

index

Enter the index of the RMON alarm.

rising

Start-up alarm if the value is rising.

falling

Start-up alarm if the value is falling.

risingorfalling

Start-up alarm if the value is rising or falling.

4.9.34 rmon-alarm modify rising-event

This command modifies the rising-event of an RMON alarm.

Format

```
rmon-alarm modify <index> rising-event  
                    <rising-event-index>
```

Mode

Global Config

index

Enter the index of the RMON alarm.

rising-event-index

Enter the index for the rising event for the RMON alarm.

4.9.35 rmon-alarm modify falling-event

This command modifies the falling-event of an RMON alarm.

Format

```
rmon-alarm modify <index> falling-event  
                    <falling-event-index>
```

Mode

Global Config

index

Enter the index of the RMON alarm.

falling-event-index

Enter the index for the falling event for the RMON alarm.

4.9.36 set garp timer join

This command sets the GVRP join time per port and per GARP. Join time is the interval between the transmission of GARP Protocol Data Units (PDUs) registering (or re-registering) membership for a VLAN or multicast group. This command has an effect only when GVRP is enabled. The time is from 10 to 100 (centiseconds). The value 20 centiseconds is 0.2 seconds.

Default

20

Format

```
set garp timer join <10-100>
```

Mode

Global Config

Interface Config

■ no set garp timer join

This command sets the GVRP join time per port and per GARP to 20 centiseconds (0.2 seconds). This command has an effect only when GVRP is enabled.

Format

```
no set garp-timer join
```

Mode

Global Config

Interface Config

4.9.37 set garp timer leave

This command sets the GVRP leave time per port. Leave time is the time to wait after receiving an unregister request for a VLAN or a multicast group before deleting the VLAN entry. This can be considered a buffer time for another station to assert registration for the same attribute in order to maintain uninterrupted service.time is 20 to 600 (centiseconds). The value 60 centiseconds is 0.6 seconds.

Note: This command has an effect only when GVRP is enabled.

Default

60

Format

```
set garp timer leave <20-600>
```

Mode

Global Config
Interface Config

■ no set garp timer leave

This command sets the GVRP leave time per port to 60 centiseconds (0.6 seconds).

Note: This command has an effect only when GVRP is enabled.

Format

```
no set garp timer leave
```

Mode

Global Config
Interface Config

4.9.38 set garp timer leaveall

This command sets how frequently *Leave All PDUs* are generated per port. A *Leave All PDU* indicates that all registrations will be unregistered. Participants would need to rejoin in order to maintain registration. The value applies per port and per GARP participation. The time may range from 200 to 6000 (centiseconds). The value 1000 centiseconds is 10 seconds.

Note: This command has an effect only when GVRP is enabled.

Default

1000

Format

```
set garp timer leaveall <200-6000>
```

Mode

Global Config

Interface Config

■ no set garp timer leaveall

This command sets how frequently *Leave All PDUs* are generated per port to 1000 centiseconds (10 seconds).

Note: This command has an effect only when GVRP is enabled.

Format

```
no set garp timer leaveall
```

Mode

Global Config

Interface Config

4.9.39 **set gmrp adminmode**

This command enables GARP Multicast Registration Protocol (GMRP) on the system. The default value is `disable`.

Format

```
set gmrp adminmode
```

Mode

```
Privileged EXEC and Global Config
```

■ **no set gmrp adminmode**

This command disables GARP Multicast Registration Protocol (GMRP) on the system.

Format

```
no set gmrp adminmode
```

Mode

```
Privileged EXEC and Global Config
```

4.9.40 set gmrp interfacemode

This command enables GARP Multicast Registration Protocol on a selected interface. If an interface which has GARP enabled is enlisted as a member of a Link Aggregation (LAG), GARP functionality will be disabled on that interface. GARP functionality will subsequently be re-enabled if Link Aggregation (LAG) membership is removed from an interface that has GARP enabled.

Default

enabled

Format

```
set gmrp interfacemode
```

Mode

Interface Config

■ no set gmrp interfacemode

This command disables GARP Multicast Registration Protocol on a selected interface. If an interface which has GARP enabled is enlisted as a member of a Link Aggregation (LAG), GARP functionality will be disabled on that interface. GARP functionality will subsequently be re-enabled if Link Aggregation (LAG) membership is removed from an interface that has GARP enabled.

Format

```
no set gmrp interfacemode
```

Mode

Interface Config

4.9.41 set gmrp interfacemode

This command enables GARP Multicast Registration Protocol on all interfaces. If an interface which has GARP enabled is enabled for routing or is enlisted as a member of a link-aggregation (LAG), GARP functionality will be disabled on that interface. GARP functionality will subsequently be re-enabled if routing is disabled and link-aggregation (LAG) membership is removed from an interface that has GARP enabled.

Default

disabled

Format

```
set gmrp interfacemode
```

Mode

Global Config

■ no set gmrp interfacemode

This command disables GARP Multicast Registration Protocol on a selected interface.

Format

```
no set gmrp interfacemode
```

Mode

Global Config

4.9.42 set gmrp forward-all-groups

This command enables the GMRP Multicast Registration Protocol feature 'Forward All Groups' for all ports.

Default

disabled

Format

```
set gmrp forward-all-groups
```

Mode

Interface Config

Global Config

■ no set gmrp forward-all-groups

This command disables the GMRP Multicast Registration Protocol feature 'Forward All Groups' for all ports.

Format

```
no set gmrp forward-all-groups
```

Mode

Interface Config

Global Config

4.9.43 set gmrp forward-unknown

Note: This command is available for the devices of the MS20/MS30, RS20/RS30/RS40, MACH102, MACH104, MACH1000, MACH1040, OCTOPUS, RSR20/RSR30 family.

Use this command to configure if the device should forward unknown GMRP multicast packets. The setting can be discard or flood. The default is flood.

Default

flood

Format

```
set gmrp forward-unknown {discard | flood}
```

Mode

Global Config

discard

The device discards unknown GMRP multicast packets.

flood

The device floods unknown GMRP multicast packets.

■ no set gmrp forward-unknown

This command disables the GMRP Multicast Registration Protocol feature 'Forward Unknown' for all ports.

Format

```
no set gmrp forward-unknown
```

Mode

Global Config

4.9.44 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
```

4.9.45 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

4.9.46 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

4.9.47 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

4.9.48 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

4.9.49 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

4.9.50 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

4.9.51 set igmp interfacemode

This command enables IGMP Snooping on all interfaces. If an interface which has IGMP Snooping enabled is enabled for port-based routing or is enlisted as a member of a link-aggregation (LAG), IGMP Snooping functionality will be disabled on that interface. IGMP Snooping functionality will subsequently be re-enabled if routing is disabled or link-aggregation (LAG) membership is removed from an interface that has IGMP Snooping enabled.

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
```

4.9.52 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).

4.9.53 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).

4.9.54 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

4.9.55 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.

4.9.56 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

4.9.57 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

4.9.58 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

4.9.59 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.

4.9.60 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.

4.9.61 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.

4.9.62 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.

4.9.63 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.

4.9.64 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.

4.9.65 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.

4.9.66 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`

4.9.67 show garp

This command displays Generic Attributes Registration Protocol (GARP) information.

Format

```
show garp
```

Mode

```
Privileged EXEC and User EXEC
```

GMRP Admin Mode

This displays the administrative mode of GARP Multicast Registration Protocol (GMRP) for the system.

4.9.68 show gmrp configuration

This command displays Generic Attributes Registration Protocol (GARP) information for one or all interfaces.

Format

```
show gmrp configuration {<slot/port> | all}
```

Mode

```
Privileged EXEC and User EXEC
```

Interface

This displays the slot/port of the interface that this row in the table describes.

Join Timer

Specifies the interval between the transmission of GARP PDUs registering (or re-registering) membership for an attribute. Current attributes are a VLAN or multicast group. There is an instance of this timer on a per-Port, per-GARP participant basis. Permissible values are 10..100 centiseconds (0.1 to 1.0 seconds). The factory default is 20 centiseconds (0.2 seconds). The finest granularity of specification is 1 centisecond (0.01 seconds).

Leave Timer

Specifies the period of time to wait after receiving an unregister request for an attribute before deleting the attribute. Current attributes are a VLAN or multicast group. This may be considered a buffer time for another station to assert registration for the same attribute in order to maintain uninterrupted service. There is an instance of this timer on a per-Port, per-GARP participant basis. Permissible values are 20..600 centiseconds (0.2 to 6.0 seconds). The factory default is 60 centiseconds (0.6 seconds). The finest granularity of specification is 1 centisecond (0.01 seconds).

LeaveAll Timer

This Leave All Time controls how frequently LeaveAll PDUs are generated. A LeaveAll PDU indicates that all registrations will shortly be deregistered. Participants will need to rejoin in order to maintain registration. There is an instance of this timer on a per-Port, per-GARP participant basis. The Leave All Period Timer is set to a random value in the range of LeaveAllTime to 1.5*LeaveAllTime. Permissible values are 200..6000 centiseconds (2 to 60 seconds). The factory default is 1000 centiseconds (10 seconds). The finest granularity of specification is 1 centisecond (0.01 seconds).

Port GMRP Mode

Indicates the GMRP administrative mode for the port. It may be enabled or disabled. If this parameter is disabled, Join Time, Leave Time and Leave All Time have no effect. The factory default is disabled.

4.9.69 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.

4.9.70 show mac-filter-table gmrp

This command displays the GARP Multicast Registration Protocol (GMRP) entries in the Multicast Forwarding Database (MFDB) table.

Format

```
show mac-filter-table gmrp
```

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. In an IVL system the MAC address will be displayed as 8 bytes.

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:).

4.9.71 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:).

4.9.72 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`, `GMRP` 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.

4.9.73 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).

4.9.74 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:).

4.9.75 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.

4.9.76 show mac notification

This command displays the MAC address change notification configuration.

Format

```
show mac notification
```

Mode

Privileged EXEC

MAC notification settings

This table displays the MAC notification settings (status and interval) for the device.

MAC notification status

This field displays the status of MAC notification traps for the device.
Possible values: `enabled`, `disabled`.

MAC notification interval

This field displays the MAC notification interval for the device.
Possible values: `1..2147483647`.

Interface

This field displays the number of the interface in `slot/port` format.

MAC notify

This field displays the status of MAC notification traps for this port.
Possible values: `enabled`, `disabled`

Mode

This field displays the mode for which action the device sends a MAC notification trap.
Possible values: `add`, `remove`, `all`

Last MAC address

This field displays the last MAC address added or removed from the address table for this interface.
Possible values: Valid MAC address in `aa:bb:cc:dd:ee:ff` notation.

Last MAC status

This field displays the status of the last MAC address on this interface.
Possible values: `added`, `removed`, `other`.

4.9.77 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.

4.9.78 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.

4.9.79 show link-aggregation

This command displays an overview of all link-aggregations (LAGs) on the switch.

Format

```
show link-aggregation {<logical slot/port> | all}
```

Mode

Privileged EXEC and User EXEC

Logical slot/port

Valid slot and port number separated by forward slashes.

Name

The name of this link-aggregation (LAG). You may enter any string of up to 15 alphanumeric characters.

Link State

Indicates whether the Link is up or down.

Admin Mode

May be enabled or disabled. The factory default is enabled.

Link Trap Mode

This object determines whether or not to send a trap when link status changes. The factory default is enabled.

STP Mode

The Spanning Tree Protocol Administrative Mode associated with the port or link-aggregation (LAG). The possible values are:

`Disable` – Spanning tree is disabled for this port.

`Enable` – Spanning tree is enabled for this port.

Mbr Ports

A listing of the ports that are members of this link-aggregation (LAG), in slot/port notation. There can be a maximum of eight ports assigned to a given link-aggregation (LAG).

Port Speed

Speed of the link-aggregation port.

Type

This field displays the status designating whether a particular link-aggregation (LAG) is statically or dynamically maintained. The possible values of this field are `Static`, indicating that the link-aggregation is statically maintained; and `Dynamic`, indicating that the link-aggregation is dynamically maintained.

Active Ports

This field lists the ports that are actively participating in the link-aggregation (LAG).

4.9.80 show rmon-alarm

This command displays switch configuration information.

Format

```
show rmon-alarm
```

Mode

Privileged EXEC and User EXEC

4.9.81 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.

4.9.82 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.

4.9.83 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.

4.9.84 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.

4.9.85 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.

4.9.86 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.

4.9.87 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.

4.9.88 show voice vlan

Use this command to display the current global Voice VLAN Administrative Mode.

Voice VLAN is a feature used to automatically separate voice and data traffic on a port, by VLAN and/or priority. A primary benefit of using Voice VLAN is to ensure that the sound quality of an IP phone is safeguarded from deteriorating when the data traffic on the port is high.

Format

```
show voice vlan
```

Mode

```
Privileged EXEC
```

Administrative Mode

Possible values: `Disable`, `Enable`

4.9.89 show voice vlan interface

Use this command to display a summary of the current Voice VLAN configuration for a specific interface.

<slot/port> indicates a specific physical interface.

all indicates all valid interfaces.

Format

```
show voice vlan interface {<slot/port> | all}
```

Mode

Privileged EXEC

<slot/port>

Indicates a specific physical interface.

all

Indicates all valid interfaces.

Interface

Displays the physical interface.

Voice VLAN Interface Mode

Displays the Voice VLAN Interface Mode.

Possible values: Disabled, Enabled.

Voice VLAN Authentication

Displays the Voice VLAN Authentication.

Possible values: Disabled, Enabled.

Voice VLAN Port Status

Displays the Voice VLAN Port Status.

Possible values: Disabled, Enabled.

4.9.90 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

4.9.91 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

4.9.92 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
```

4.9.93 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
```

4.9.94 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
```

4.9.95 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
```

4.9.96 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

4.9.97 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.

4.9.98 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
```

4.9.99 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
```

4.9.100 storm-control ingress-limiting

This command enables or disables the ingress limiter globally.

Format

```
storm-control ingress-limiting {disable | enable}
```

Mode

```
Global Config
```

4.9.101 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
```

4.9.102 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
```

4.9.103 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
```

4.9.104 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
```

4.9.105 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
```

4.9.106 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

4.9.107 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

4.9.108 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
```

4.9.109 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
```

4.9.110 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
```

4.9.111 vlan database

This command switches into the global VLAN mode.

Default

```
Admit All
```

Format

```
vlan database
```

Mode

```
Privileged EXEC
```

4.9.112 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

4.9.113 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

4.9.114 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.

4.9.115 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.

4.9.116 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
```

4.9.117 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

4.9.118 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

4.9.119 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
```

4.9.120 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

4.9.121 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
```

4.9.122 voice vlan (Global Config Mode)

This command enables the Voice VLAN feature.

Voice VLAN is a feature used to automatically separate voice and data traffic on a port, by VLAN and/or priority. A primary benefit of using Voice VLAN is to ensure that the sound quality of an IP phone is safeguarded from deteriorating when the data traffic on the port is high.

Default

Disabled

Format

```
voice vlan
```

Mode

Global Config

■ no voice vlan

This command disables the Voice VLAN feature.

Default

Disabled

Format

```
no voice vlan
```

Mode

Global Config

4.9.123 voice vlan <id>

Use this command to configure VLAN tagging and 802.1p priority.

Format

```
voice vlan <id> [dot1p <priority>] }
```

Mode

Interface Config

<id>

Enter the Voice VLAN ID.

dot1p

Configure Voice VLAN 802.1p priority tagging for voice traffic.

<priority>

The priority tag range is 0–7.

■ no voice vlan

This command disables the Voice VLAN feature on the interface.

Default

Disabled

Format

```
no voice vlan
```

Mode

Interface Config

4.9.124 voice vlan dot1p

Use this command to configure Voice VLAN 802.1p priority tagging for voice traffic.

Format

```
voice vlan dot1p <priority>
```

Mode

```
Interface Config
```

<priority>

Configure Voice VLAN 802.1p priority tagging for voice traffic.
The priority tag range is 0–7.

4.9.125 voice vlan none

Use this command to allow the IP phone to use its own configuration to send untagged voice traffic.

Format

```
voice vlan none
```

Mode

```
Interface Config
```

4.9.126 voice vlan untagged

Use this command to configure the phone to send untagged voice traffic.

Format

```
voice vlan untagged
```

Mode

```
Interface Config
```

4.9.127 voice vlan auth

Use this command to set Voice VLAN Authentication Mode. If disabled, VOIP devices which are detected via LLDP-med will have access to the Voice VLAN without authentication.

Default

```
Enabled
```

Format

```
voice vlan auth [enabled | disabled]
```

Mode

```
Interface Config
```

disable

VOIP devices which are detected via LLDP-MED will have access to the Voice VLAN without authentication.

enable

VOIP devices which are detected via LLDP-MED will not have access to the Voice VLAN without authentication.

4.10 User Account Management Commands

These commands manage user accounts.

4.10.1 disconnect

This command closes a telnet session.

Format

```
disconnect {<sessionID> | all}
```

Mode

```
Privileged EXEC
```

Session ID

Enter the session ID (1-11).

4.10.2 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.

4.10.3 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.

4.10.4 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.

4.10.5 users login <user>

Enter user name.

Format

```
users login <user> <listname>
```

Mode

Global Config

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]]]').

■ 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.

4.10.6 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

4.10.7 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.

4.10.8 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

4.10.9 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
```

4.10.10 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
```

4.10.11 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
```

4.11 System Utilities

This section describes system utilities.

4.11.1 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*.

4.11.2 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.

4.11.3 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.

4.11.4 cablestatus

This command tests the cable attached to an interface for short or open circuit. During the test the traffic is interrupted on this port.

Format

```
cablestatus <slot/port>
```

Mode

Privileged EXEC

4.11.5 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

4.11.6 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

4.11.7 clear arp-table-switch

This command clears the agent's ARP table (cache).

Format

```
clear arp-table-switch
```

Mode

Privileged EXEC

4.11.8 clear config

This command resets the configuration in RAM to the factory defaults without powering off the switch.

Format

```
clear config
```

Mode

```
Privileged EXEC
```

4.11.9 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
```

4.11.10 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
```

4.11.11 clear hiper-ring

This command clears the HIPER Ring configuration (deletes it).

Format

```
clear hiper-ring
```

Mode

```
Privileged EXEC
```

4.11.12 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
```

4.11.13 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

4.11.14 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

4.11.15 clear link-aggregation

This command clears all link-aggregations (LAGs).

Format

```
clear link-aggregation
```

Mode

Privileged EXEC

4.11.16 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

4.11.17 clear traplog

This command clears the trap log.

Format

```
clear traplog
```

Mode

Privileged EXEC

4.11.18 clear ring-coupling

This command clears the ring-coupling configuration.

Format

```
clear ring-coupling
```

Mode

Privileged EXEC

4.11.19 clear vlan

This command resets VLAN configuration parameters to the factory defaults.

Format

```
clear vlan
```

Mode

Privileged EXEC

4.11.20 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).

4.11.21 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 aca:script <sourcefilename> nvram:script
    [targetfilename]
copy aca:capturefilter <sourcefilename>
    nvram:capturefilter [targetfilename]
```

```
copy aca:sfp-white-list <sourcefilename>
  nvram:sfp-white-list
copy nvram:backup-image system:image
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:script <sourcefilename> aca:script
  [targetfilename]
copy nvram:script <sourcefilename> <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://ip/filepath/fileName>
  nvram:sfp-white-list
copy tftp://<server_ip>/<path_to_pem>
  nvram:https-cert
copy <url> nvram:clibanner
copy <url> nvram:capturefilter <destfilename>
copy aca:capturefilter <sourcefilename>
  nvram:capturefilter <destfilename>
copy <url> nvram:script <destfilename>
copy <url> nvram:startup-config
copy <url> system:image
copy <url> system:running-config
copy <url> system:bootcode
```

Mode

Privileged EXEC

■ **copy aca:script <sourcefilename>
nvram:script [targetfilename]**

Copies the script from the Auto Configuration Adapter.

– `sourcefilename`: Filename of source configuration Script. File-name length may be max. 20 characters, including extension '.cli' or '.CLI'.

– `targetfilename`: Filename on the switch's NVRAM. Filename length may be max. 20 characters, including extension '.cli'.

■ **copy aca:capturefilter <sourcefilename>
nvram:capturefilter [targetfilename]**

Copies a capture filter file from the Auto Configuration Adapter.

– `sourcefilename`: Filename of source capture filter expressions file.

– `targetfilename`: Filename on the switch's NVRAM.

■ **copy aca:sfp-white-list <sourcefilename>
nvram:sfp-white-list**

Use this command to load the SFP white list file from a ACA21.

Note: In order to delete the SFP white list file from the flash memory: use the command `clear sfp-white-list`.

The `clear config factory` command deletes the SFP white list, too.

■ **copy nvram:backup-image system:image**

Use this command to swap current and backup images. The backup image (backup.bin) and current image (main.bin) will exchange the file name, after reboot the both OS and configuration files will be swapped.

■ copy <tftp://ip/filepath/fileName> nvram:sfp-white-list

Use this command to load the SFP white list file from a TFTP server.

Note: In order to delete the SFP white list file from the flash memory: use the command `clear sfp-white-list`.

The `clear config factory` command deletes the SFP white list, too.

■ copy tftp://<server_ip>/<path_to_pem> nvram:https-cert

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:script <sourcefilename>
aca:script [targetfilename]**

Uploads configuration script file. Save the script to the AutoConfiguration Adapter.

- sourcefilename: Filename length may be max. 20 characters, including extension '.cli' or '.CLI'.
- targetfilename: Filename length may be max. 20 characters, including extension '.cli' or '.CLI'.

■ **copy nvram:script <sourcefilename> <url>**

Uploads Configuration Script file using <tftp://ip/filepath/fileName>. Filename length may be max. 20 characters, including extension '.cli'.

- sourcefilename: Filename length may be max. 20 characters, including extension '.cli' or '.CLI'.

■ 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 337

■ **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:script <destfilename>**

Downloads Configuration Script file using <tftp://ip/filepath/fileName>.

– `destfilename`: Filename length may be max. 20 characters, including extension '.cli' or '.CLI'.

■ **copy <url> nvram:sshkey-dsa**

Downloads IP secure shell (SSH) DSA key file by tftp using <tftp://ip/filepath/fileName>.

■ copy <url> nvram:sshkey-rsa1

Downloads IP secure shell (SSH) RSA1 key file by tftp using <tftp://ip/filepath/fileName>.

■ copy <url> nvram:sshkey-rsa2

Downloads IP secure shell (SSH) RSA2 key file by tftp using <tftp://ip/filepath/fileName>.

■ 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 boot-code 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".

■ clear sfp-white-list

Use this command to delete the SFP white list file from the flash memory.

Note: The `clear config factory` command deletes the SFP white list, too.

4.11.22 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

4.11.23 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.

4.11.24 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
```

4.11.25 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
```

4.11.26 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

4.11.27 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.

4.11.28 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.

4.11.29 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.

4.11.30 reboot

This command resets the switch (cold start) after a given time delay, for warm start. See “reload” on page 335. 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.

4.11.31 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).

4.11.32 reload

This command enables you to reset the switch (warm start) after a given time delay, for cold start [See “reboot” on page 333](#).

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.

4.11.33 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.

4.11.34 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

4.11.35 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

4.12 LLDP - Link Layer Discovery Protocol

These commands show and configure the LLDP parameters in compliance with IEEE 802.1 AB.

4.12.1 show lldp

This command shows all LLDP settings.

Format

```
show lldp
```

Mode

```
Privileged EXEC and User EXEC
```

4.12.2 show lldp config

This command shows all LLDP configuration settings.

Format

```
show lldp config
```

Mode

```
Privileged EXEC and User EXEC
```

4.12.3 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

4.12.4 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

4.12.5 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

4.12.6 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
```

4.12.7 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
```

4.12.8 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
```

4.12.9 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

4.12.10 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.

4.12.11 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

inlinepower

Enable or disable the sending of the port's Power over Ethernet capabilities (PoE, IEEE 802.3af).

Note: This command is available for devices supporting PoE.

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.

4.12.12 show lldp med

Use this command to display a summary of the current LLDP MED global configuration.

Format

```
show lldp med
```

Mode

Privileged EXEC

Fast Start Repeat Count

Display the Fast Start Repeat Count, e.g. the number of LLDP PDUs that will be transmitted when the product is enabled.

Value range: 1..10.

Device class

Display the Device class.

4.12.13 show lldp med interface

Use this command to display a summary of the current LLDP MED configuration for a specific interface.

Format

```
show lldp med interface {<unit/slot/port> | all}
```

Mode

Privileged EXEC

<unit/slot/port>

Indicates a specific physical interface.

all

Indicates all valid LLDP interfaces.

Interface

Displays the physical interface.

Link

Displays the link status.

Possible values: Up, Down.

configMED

Displays if confignotification for the Media Endpoint Devices is

Enabled/Disabled.

operMED

Displays if operation for the Media Endpoint Devices is

Enabled/Disabled.

ConfigNotify

Displays the ConfigNotify.

Possible values: Enabled, Disabled.

TLVsTx

Displays the TLVsTx.

4.12.14 show lldp med local-device detail

Use this command to display detailed information about the LLDP MED data that a specific interface transmits. <unit/slot/port> indicates a specific physical interface.

Format

```
show lldp med local-device detail {<slot/port>}
```

Mode

Privileged EXEC

<slot/port>

Indicates a specific physical interface.

Interface

Displays the physical interface.

Network Policies

Displays the Network Policies.

4.12.15 show lldp med remote-device

Use this command to display the summary information about remote devices that transmit current LLDP MED data to the system. You can show information about LLDP MED remote data received on all valid LLDP interfaces or on a specific physical interface.

Format

```
show lldp med remote-device{<slot/port> | all}
```

Mode

Privileged EXEC

<slot/port>

Indicates a specific physical interface.

all

Indicates all valid LLDP interfaces.

Local Interface

Displays the local interface.

RemoteID

Displays the RemoteID.

Device Class

Displays the Device Class.

4.12.16 show lldp med remote-device detail

Use this command to display detailed information about remote devices that transmit current LLDP MED data to an interface on the system.

Format

```
show lldp med remote-device detail <slot/port>
```

Mode

Privileged EXEC

Local Interface

Displays the local interface.

4.12.17 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 |  
  inlinepower | 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).

4.12.18 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 354](#)).

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
```

4.12.19 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

4.12.20 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.).

4.12.21 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.).

4.12.22 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.).

4.12.23 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.

4.12.24 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.).

4.12.25 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

4.12.26 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

4.12.27 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

4.12.28 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

4.12.29 lldp 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
```

4.12.30 lldp med

LLDP for Media Endpoint Devices (LLDP-MED) is an extension to LLDP that operates between endpoint devices such as IP phones, Voice / Media Gateways, Media Servers, IP Communications Controllers or other VoIP devices or servers, and network devices such as switches. It specifically provides support for voice over IP (VoIP) applications. In this purpose, it provides an additional set of common advertisement messages (TLVs), for capabilities discovery, network policy, Power over Ethernet, inventory management and location information.

Use this command to enable MED. By enabling MED, you will be effectively enabling the transmit and receive function of LLDP.

Default

Enabled

Format

lldp med

Mode

Interface Config

■ no lldp med

Use this command to disable MED.

Format

no lldp med

Mode

Interface Config

4.12.31 lldp med all

Use this command to configure LLDP-MED on all the ports.

Default

Enabled

Format

lldp med all

Mode

Global Config

4.12.32 lldp med confignotification

Use this command to configure all the ports to send the topology change notification.

Default

Disabled

Format

lldp med confignotification

Mode

Interface Config

■ no lldp med confignotification

Use this command to disable notifications.

Format

no lldp med confignotification

Mode

Interface Config

4.12.33 lldp med confignotification all

Use this command to configure all the ports to send the topology change notification.

Default

Disabled

Format

```
lldp med confignotification all
```

Mode

Global Config

4.12.34 lldp med faststartrepeatcount

Use this command to set the value of the fast start repeat count.

Default

3

Format

```
lldp med faststartrepeatcount [count]
```

Mode

Global Config

[count]

The number of LLDP PDUs that will be transmitted when the product is enabled. The range is 1 to 10.

■ no lldp med faststartrepeatcount

Use this command to return to the factory default value.

Format

```
no lldp med faststartrepeatcount
```

Mode

Global Config

4.12.35 lldp med transmit-tlv

Use this command to specify which optional Type Length Values (TLVs) in the LLDP-MED set will be transmitted in the Link Layer Discovery Protocol Data Units (LLDPDUs).

Default

By default, the capabilities and network policy TLVs are included.

Format

```
lldp med transmit-tlv [capabilities]
                               [network-policy]
```

Mode

Interface Config

capabilities

Include/Exclude LLDP capabilities TLV.

network-policy

Include/Exclude LLDP network policy TLV.

■ no lldp med transmit-tlv

Use this command to remove a TLV.

Format

```
no lldp med transmit-tlv [capabilities]
                               [network-policy]
```

Mode

Interface Config

4.12.36 lldp med transmit-tlv all

Use this command to specify which optional Type Length Values (TLVs) in the LLDP MED set will be transmitted in the Link Layer Discovery Protocol Data Units (LLDPDUs).

Default

By default, the capabilities and network policy TLVs are included.

Format

```
lldp med transmit-tlv all [capabilities]
                               [network-policy]
```

Mode

Global Config

capabilities

Include/Exclude LLDP capabilities TLV.

network-policy

Include/Exclude LLDP network policy TLV.

■ no lldp med med transmit-tlv all

Use this command to remove a TLV.

Format

```
no lldp med transmit-tlv all [capabilities]
                               [network-policy]
```

Mode

Global Config

4.12.37 lldp notification

Configure the port's LLDP notification setting (on or off, Default value: off).

Format

```
lldp notification <{off|on}>
```

Mode

```
Interface Config
```

4.12.38 lldp 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
```

4.12.39 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
```

4.12.40 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
```

4.12.41 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
```

4.12.42 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
```

4.12.43 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
```

4.12.44 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
```

4.12.45 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
```

4.12.46 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
```

4.12.47 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
```

4.12.48 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
```

4.12.49 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
```

4.12.50 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
```

4.12.51 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
```

4.12.52 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
```

4.12.53 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
```

4.12.54 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
```

4.12.55 lldp tlv vlan-name

Configure the port's LLDP TLV inclusion of VLAN Name.

Format

```
lldp tlv vlan-name <{off|on}>
```

Mode

```
Interface Config
```

4.12.56 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
```

4.13 SNTP - Simple Network Time Protocol

These commands show and configure the SNTP parameters.

4.13.1 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).

4.13.2 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).

4.13.3 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.

4.13.4 show sntp operation

This command shows if the SNTP function is enabled or disabled.

Format

```
show sntp operation
```

Mode

Privileged EXEC and User EXEC

4.13.5 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.

4.13.6 show sntp status

This command shows the SNTP state, synchronization and error messages.

Format

```
show sntp status
```

Mode

Privileged EXEC and User EXEC

4.13.7 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.

4.13.8 no sntp

This command disables sntp.

Format

```
no sntp
```

Mode

Global Config

4.13.9 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
```

4.13.10 sntp anycast transmit-interval

The transmit interval in seconds, default: 120.

Format

```
sntp anycast transmit-interval <1-3600>
```

Mode

```
Global Config
```

4.13.11 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
```

4.13.12 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
```

4.13.13 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.

4.13.14 sntp client offset

The offset between UTC and local time in minutes, default: 60.

Format

```
sntp client offset <-1000 to 1000>
```

Mode

Global Config

4.13.15 sntp client request-interval

The synchronization interval in seconds, default: 30.

Format

```
sntp client request-interval <1-3600>
```

Mode

```
Global Config
```

4.13.16 no sntp client server

Disable the SNTP client servers.

Format

```
no sntp client server
```

Mode

```
Global Config
```

4.13.17 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
```

4.13.18 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
```

4.13.19 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
```

4.13.20 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

4.13.21 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.

4.13.22 sntp time system

Set the current sntp time.

Format

```
sntp time system <YYYY-MM-DD HH:MM:SS>
```

Mode

Global Config

4.14 PTP - Precision Time Protocol

These commands show and configure the PTP (IEEE 1588) parameters.

Note: The operation parameter is available for all devices. All other parameters are additionally available for MS20/MS30, MACH1040, MACH104 and PowerMICE.

4.14.1 show ptp

This command shows all PTP settings.

Format

```
show ptp
```

Mode

Privileged EXEC and User EXEC

PTP (Global) Operation

Show the global PTP (IEEE 1588) operation setting. This field shows if PTP is enabled/disabled on this device.

Possible values: Enabled, Disabled

PTP (Global) Clock Mode

Show which PTP clock mode is currently configured.

Possible values: v1-simple-mode, v2-simple-mode, v1-boundary-clock, v2-boundary-clock-onestep, v2-boundary-clock-twostep, v2-transparent-clock}

PTP (Global) Sync. Upper Bound

Show the upper bound for the PTP clock synchronization status (unit: nanoseconds).

Possible values: 31..1000000000 nsec

PTP (Global) Sync. Lower Bound

Show the lower bound for the PTP clock synchronization status (unit: nanoseconds).

Possible values: 0..999999999 nsec

PTP Preferred Master

Show if the local switch shall be regarded as a preferred master clock or not.

Possible values: False, True

PTP Subdomain Name

Show the PTP subdomain name.

Possible values: Up to 16 characters from ASCII hex value 0x21 (!) up to and including hex value 0x7e (~).

PTP Sync. Interval

Show the configured Precision Time Protocol sync interval.

The sync interval is the interval (in seconds) between successive sync messages issued by a master clock.

Possible values: sec-1, sec-2, sec-8, sec-16, sec-64

PTP Status, Is Synchronized

Show if the device is synchronized (true or false).

Possible values: False, True

PTP Status, Offset From Master

Show the device's offset from the master (unit: nanoseconds), i.e. the deviation of the local clock from the reference clock.

PTP Status, Max. Offset Absolute

Show the device's maximum offset absolute (unit: nanoseconds).

PTP Status, Delay To Master

Show the device's delay to the master (unit: nanoseconds), i.e. the single signal runtime between the local device and reference clock.

PTP Status, Grandmaster UUID

Show grandmaster Universally Unique Identifier, i.e. the MAC address of the grandmaster clock (Unique Universal Identifier).

Possible values: 32 hexadecimal numbers
(hh hh hh hh hh hh hh hh).

PTP Status, Parent UUID

Show parent Universally Unique Identifier, i.e. the MAC address of the master clock with which the local time is directly synchronized.

Possible values: 32 hexadecimal numbers
(hh hh hh hh hh hh hh hh).

PTP Status, Clock Stratum

Show the qualification of the local clock.

PTP Status, Clock Identifier

Show the device's clock properties (e.g. accuracy, epoch, etc.).

PTPv1 Boundary Clock Ports

Show port number, operation status, burst status of the PTPv1 Boundary Clock Ports.

Port

Show the number of the interface (in slot/port notation).

Operation

Show if sending and receiving / processing PTP synchronization messages is enabled or disabled on the device.

Possible values: Enabled, Disabled

Burst

Show the status of the burst feature for synchronization running during a synchronization interval.

Possible values: Enabled, Disabled

Status

Show the ports PTP status.

Possible values: Initializing, faulty, disabled, listening, pre-master, master, passive, uncalibrated, slave.

4.14.2 show ptp configuration

This command shows the configured PTP (IEEE 1588) values depending on the currently configured clock mode.

Format

```
show ptp configuration
```

Mode

Privileged EXEC and User EXEC

PTP (Global) Clock Mode

Show which PTP clock mode is currently configured.

PTP (Global) Sync. Upper Bound

Show the upper bound for the PTP clock synchronization status (unit: nanoseconds).

PTP (Global) Sync. Lower Bound

Show the lower bound for the PTP clock synchronization status (unit: nanoseconds).

4.14.3 show ptp operation

Show the global PTP (IEEE 1588) operation setting (the administrative setting). This command shows if PTP is enabled/disabled on this device.

Format

```
show ptp operation
```

Mode

Privileged EXEC and User EXEC

4.14.4 show ptp port

This command shows the PTP (IEEE 1588) port configuration settings depending on the currently configured clock mode.

Format

```
show port [<slot/port>|all]
```

Mode

Privileged EXEC and User EXEC

<slot/port>

Show the port-related PTP (IEEE 1588) settings for the given port.

all

Show the port-related PTP (IEEE 1588) settings for all ports.

4.14.5 show ptp status

This command shows the device's global PTP (IEEE 1588) status (the operating states).

Format

```
show ptp status
```

Mode

Privileged EXEC and User EXEC

PTP Status, Is Synchronized

Show if the device is synchronized (true or false).

PTP Status, Offset From Master

Show the device's offset from the master (unit: nanoseconds).

PTP Status, Max. Offset Absolute

Show the device's maximum offset absolute (unit: nanoseconds).

PTP Status, Delay To Master

Show the device's delay to the master (unit: nanoseconds).

PTP Status, Grandmaster UUID

Show grandmaster Universally Unique Identifier (32 hexadecimal numbers).

PTP Status, Parent UUID

Show parent Universally Unique Identifier (32 hexadecimal numbers).

PTP Status, Clock Stratum

Show the device's clock stratum.

PTP Status, Clock Identifier

Show the device's clock identifier.

4.14.6 ptp clock-mode

Configure the Precision Time Protocol (PTP, IEEE 1588) clock mode. If the clock mode is changed, PTP will be initialized. The default is `disable`.

Format

```
ptp clock-mode {v1-simple-mode
                |v2-simple-mode
                |v1-boundary-clock
                |v2-boundary-clock-onestep
                |v2-boundary-clock-twostep
                |v2-transparent-clock}
```

Mode

Global Config

v1-simple-mode

Set the clock mode to 'v1 Simple Mode'. This is a client only mode without hardware support. The device only accepts PTPv1 sync messages and sets the time directly. No BMC algorithm will run.

v2-simple-mode

Set the clock mode to 'v2 Simple Mode'. This is a client only mode without hardware support. The device only accepts PTPv2 sync (or follow_up) messages and sets the time directly. No BMC algorithm will run.

v1-boundary-clock

Set the clock mode to 'v1 Boundary Clock'. This specifies the mode as described in the IEEE1588 standard.

v2-boundary-clock-onestep

Set the clock mode to 'v2 Boundary Clock one-step'. This specifies the boundary-clock mode as described in the IEEE1588-2008 (PTPv2) standard. The precise timestamp is inserted directly into the sync-packet (one-step Mode).

v2-boundary-clock-twostep

Set the clock mode to 'v2 Boundary Clock two-step'. This specifies the boundary-clock mode as described in the IEEE1588-2008 (PTPv2) standard. The precise timestamp is transmitted via a follow-up packet (two-step Mode).

v2-transparent-clock

Set the clock mode to 'v2 Transparent Clock'. This specifies the transparent-clock mode (one-step) as described in the IEEE1588-2008 (PTPv2) standard.

4.14.7 ptp operation

Enable or disable the Precision Time Protocol (IEEE 1588).
The default is "disable"

Format

```
ptp operation {disable|enable}
```

Mode

Global Config

disable

Disable the Precision Time Protocol (IEEE 1588).

enable

Enable the Precision Time Protocol (IEEE 1588).

4.14.8 ptp sync-lower-bound

Configure the lower bound for the PTP clock synchronization
(unit: nanoseconds, min.: 0, max.: 999999999 (10⁹-1), default: 30).

Note: The lower bound always has to be smaller than the upper bound.

Format

```
ptp sync-lower-bound <0-999999999>
```

Mode

Global Config

4.14.9 ptp sync-upper-bound

Configure the upper bound for the PTP clock synchronization (unit: nanoseconds, min.: 31, max.: 1000000000 (10⁹), default: 5000).

Note: The upper bound always has to be larger than the lower bound.

Format

```
ptp sync-upper-bound <31-1000000000>
```

Mode

```
Global Config
```

4.14.10 ptp v1 preferred-master

Configure the PTPv1 (IEEE1588-2002) specific settings.

Specify if the local switch shall be regarded as a preferred master clock (i. e., if it will remain master in the presence of disconnection or connection of other clocks).

Format

```
ptp v1 preferred-master {true|false}
```

Mode

```
Global Config
```

true

The local switch shall be regarded as a preferred master clock.

false

The local switch shall not be regarded as a preferred master clock.

4.14.11 ptp v1 re-initialize

Configure the PTPv1 (IEEE1588-2002) specific settings.

Re-initialize the clocks in the local subdomain with the currently configured settings. Changes in the subdomain name or the sync interval will only take effect after this command.

Format

```
ptp v1 re-initialize
```

Mode

```
Global Config
```

4.14.12 ptp v1 subdomain-name

Configure the PTPv1 (IEEE1588-2002) specific settings.

Enter a Precision Time Protocol subdomain name. The default is "_DFLT".

Note: Changes are only applied after the 're-initialize' command or after a re-boot if the configuration was saved.

Format

```
ptp v1 subdomain-name <subdomain name>
```

Mode

```
Global Config
```

<subdomain name>

Enter a PTP subdomain name (up to 16 characters). Valid characters range from hex value 0x21 (!) up to and including hex value 0x7e (~).

Enter special characters (\, !, ', ", ?) by preceding them with the escape character (\), e. g., as \\, \!, \', \", \?. The subdomain name must not be empty. The default is "_DFLT".

4.14.13 ptp v1 sync-interval

Configure the PTPv1 (IEEE1588-2002) specific settings.

Configure the Precision Time Protocol sync interval. The sync interval is the interval (in seconds) between successive sync messages issued by a master clock.

Valid values are: `sec-1`, `sec-2`, `sec-8`, `sec-16`, and `sec-64`.

Default is `sec-2`.

Note: Changes are only applied after the 're-initialize' command or after a reboot if the configuration was saved.

Format

```
ptp v1 sync-interval {sec-1|sec-2|sec-8|sec-16|
                    sec-64}
```

Mode

Global Config

sec-1

Set the PTP sync interval to `sec-1` (1 sec).

sec-2

Set the PTP sync interval to `sec-2` (2 sec).

sec-8

Set the PTP sync interval to `sec-8` (8 sec).

sec-16

Set the PTP sync interval to `sec-16` (16 sec).

sec-64

Set the PTP sync interval to `sec-64` (64 sec).

4.14.14 ptp v2bc priority1

Configure the PTPv2 Boundary Clock (IEEE1588-2008) specific settings. Configure the priority1 value (0 . . 255) for the BMC as described in IEEE1588-2008.

Format

```
ptp v2bc priority1 <0-255>
```

Mode

```
Global Config
```

4.14.15 ptp v2bc priority2

Configure the PTPv2 Boundary Clock (IEEE1588-2008) specific settings. Configure the priority2 value (0 . . 255) for the BMC as described in IEEE1588-2008.

Format

```
ptp v2bc priority2 <0-255>
```

Mode

```
Global Config
```

4.14.16 ptp v2bc domain

Configure the PTPv2 Boundary Clock (IEEE1588-2008) specific settings. Configure the domain number (0..255) as described in IEEE1588-2008.

Format

```
ptp v2bc domain <0-255>
```

Mode

```
Global Config
```

4.14.17 ptp v2bc utc-offset

Configure the PTPv2 Boundary Clock (IEEE1588-2008) specific settings. Configure the current UTC offset in seconds.

Format

```
ptp v2bc utc-offset <seconds>
```

Mode

```
Global Config
```

4.14.18 ptp v2bc utc-offset-valid

Configure the PTPv2 Boundary Clock (IEEE1588-2008) specific settings. Configure the UTC offset valid flag.

Format

```
ptp v2bc utc-offset-valid {true|false}
```

Mode

```
Global Config
```

4.14.19 ptp v2bc vlan

Configure the PTPv2 Boundary Clock (IEEE1588-2008) specific settings. Use this command to configure the VLAN in which PTP packets are send. With a value of none all packets are send untagged.

Format

```
ptp v2bc vlan {none | <0-4042>}
```

Mode

```
Interface Config
```

4.14.20 ptp v2bc vlan-priority

Configure the PTPv2 Boundary Clock (IEEE1588-2008) specific settings. Use this command to configure the VLAN priority.

Format

```
ptp v2bc vlan-priority <0-7>
```

Mode

```
Interface Config
```

4.14.21 ptp v1 burst

Enable or disable the burst feature for synchronization runs during a synchronization interval. Default is disable.

Format

```
ptp v1 burst {enable|disable}
```

Mode

```
Interface Config
```

enable

During a synchronization interval, there are 2 to 8 synchronization runs. This permits faster synchronization when the network load is high.

disable

During a synchronization interval, there is only one synchronization run.

4.14.22 ptp v1 operation

Enable or disable the sending and receiving / processing of PTP synchronization messages. Default is enable.

Format

```
ptp v1 operation {enable|disable}
```

Mode

```
Interface Config
```

enable

Port sends and receives/ processes PTP synchronization messages.

disable

Port blocks PTP synchronization messages.

4.14.23 ptp v2bc operation

Enable or disable the sending and receiving / processing of PTP synchronization messages.

Format

```
ptp v2bc operation {disable|enable}
```

Mode

```
Interface Config
```

enable

Port sends and receives/ processes PTP synchronization messages.

disable

Port blocks PTP synchronization messages.

4.14.24 ptp v2bc announce-interval

Configure the Announce Interval in seconds {1|2|4|8|16}.

Format

```
ptp v2bc announce-interval {1|2|4|8|16}
```

Mode

```
Interface Config
```

4.14.25 ptp v2bc announce-timeout

Configure the Announce Receipt Timeout (2..10).

Format

```
ptp v2bc announce-timeout <2-10>
```

Mode

```
Interface Config
```

4.14.26 ptp v2bc sync-interval

Configure the Sync Interval in seconds {0.5|1|2}.

Format

```
ptp v2bc sync-interval {0.25|0.5|1|2}
```

Mode

```
Interface Config
```

4.14.27 ptp v2bc delay-mechanism

Configure the delay mechanism {e2e|p2p|disabled} of the transparent-clock.

Format

```
ptp v2bc delay-mechanism {e2e|p2p|disabled}
```

Mode

```
Interface Config
```

4.14.28 ptp v2bc pdelay-interval

Configure the Peer Delay Interval in seconds {1|2|4|8|16|32}. This interval is used if delay-mechanism is set to p2p.

Format

```
ptp v2bc pdelay-interval {1|2|4|8|16|32}
```

Mode

```
Interface Config
```

4.14.29 ptp v2bc network-protocol

Configure the network-protocol {ieee802_3|udp_ipv4} of the transparent-clock.

Format

```
ptp v2bc network-protocol {ieee802_3 | udp_ipv4}
```

Mode

```
Interface Config
```

4.14.30 ptp v2bc v1-compatibility-mode

Set the PTPv1 Hardware compatibility mode {auto|on|off}.

Format

```
ptp v2bc v1-compatibility-mode {auto|on|off}
```

Mode

```
Interface Config
```

4.14.31 ptp v2bc asymmetry

Specifies the asymmetrie in nanoseconds of the link connected to this port {+-1000000000}.

Format

```
ptp v2bc asymmetry <value in ns>
```

Mode

```
Interface Config
```

4.14.32 ptp v2tc asymmetry

Specifies the asymmetrie in nanoseconds of the link connected to this port {+-1000000000}.

Format

```
ptp v2tc asymmetry <value in ns>
```

Mode

```
Interface Config
```

4.14.33 ptp v2tc delay-mechanism

Configure the PTPv2 Transparent Clock (IEEE1588-2008) specific settings. Configure the delay mechanism {e2e | p2p | disabled} of the transparent-clock.

Format

```
ptp v2tc delay-mechanism {e2e|p2p}
```

Mode

```
Global Config
```

4.14.34 ptp v2tc management

Configure the PTPv2 Transparent Clock (IEEE1588-2008) specific settings. Enable or disable the management of the transparent-clock (disable for fast packet rates).

Format

```
ptp v2tc management {enable|disable}
```

Mode

```
Global Config
```

4.14.35 ptp v2tc multi-domain-mode

Configure the PTPv2 Transparent Clock (IEEE1588-2008) specific settings. Enable or disable the transparent-clock for one (primary-domain) or all domain numbers.

Format

```
ptp v2tc multi-domain-mode {enable|disable}
```

Mode

```
Global Config
```

4.14.36 ptp v2tc network-protocol

Configure the PTPv2 Transparent Clock (IEEE1588-2008) specific settings. Configure the network-protocol {ieee802_3|udp_ipv4} of the transparent-clock.

Format

```
ptp v2tc network-protocol {ieee802_3|udp_ipv4}
```

Mode

Global Config

4.14.37 ptp v2tc operation

Enable or disable the sending and receiving/ processing of PTP synchronization messages.

Format

```
ptp v2tc operation {disable|enable}
```

Mode

Interface Config

enable

Port sends and receives/ processes PTP synchronization messages.

disable

Port blocks PTP synchronization messages.

4.14.38 ptp v2tc pdelay-interval

Configure the Peer Delay Interval in seconds {1|2|4|8|16|32}. This interval is used if delay-mechanism is set to p2p.

Format

```
ptp v2tc pdelay-interval {1|2|4|8|16|32}
```

Mode

```
Interface Config
```

4.14.39 ptp v2tc primary-domain

Configure the PTPv2 Transparent Clock (IEEE1588-2008) specific settings. Configure the primary-domain {for syntonization} of the transparent-clock.

Format

```
ptp v2tc primary-domain <0-255>
```

Mode

```
Global Config
```

4.14.40 ptp v2tc profile

Note: This command is available for the devices of the MACH104, MACH1040, PowerMICE and MS20/MS30 family.

Configure the PTPv2 Transparent Clock (IEEE1588-2008) specific settings. Use this command to configure the PTP v2TC parameters to match the default of a profile.

Format

```
ptp v2tc profile
           { power | default-e2e | default-p2p }
```

Mode

Global Config

default-e2e

Configure the PTP v2TC parameters to match the default of a profile (end-to-end transparent clock).

default-p2p

Configure the PTP v2TC parameters to match the default of a profile (peer-to-peer transparent clock).

power

Configure the PTP v2TC parameters to match the default of a profile (power profile C37.238).

4.14.41 ptp v2tc syntonization

Configure the PTPv2 Transparent Clock (IEEE1588-2008) specific settings. Enable or disable the syntonization of the transparent-clock.

Format

```
ptp v2tc syntonization {enable|disable}
```

Mode

Global Config

4.14.42 ptp v2tc vlan

Configure the PTPv2 Transparent Clock (IEEE1588-2008) specific settings. Use the command to configure the VLAN in which PTP packets are send. With a value of none all packets are send untagged.

Format

```
ptp v2tc vlan {none | <0-4042>}
```

Mode

```
Global Config
```

4.14.43 ptp v2tc power-tlv-check

Note: This command is available for the devices of the MACH104, MACH1040, PowerMICE and MS20/MS30 family.

Configure the PTPv2 Transparent Clock (IEEE1588-2008) specific settings. Use the command to configure the Power TLV Check.

Default

```
Disable
```

Format

```
ptp v2tc power-tlv-check {enable | disable}
```

Mode

```
Global Config
```

enable

Only announce messages including the TLVs specified in the power profile (C37.238) are accepted for syntonization.

disable

Disable v2tc power-tlv-check.

4.14.44 ptp v2tc vlan-priority

Configure the PTPv2 Transparent Clock (IEEE1588-2008) specific settings. Use the command to configure the VLAN priority of tagged ptp packets.

Format

```
ptp v2tc vlan-priority <0-7>
```

Mode

```
Global Config
```

4.14.45 ptp v2tc sync-local-clock

Configure the PTPv2 Transparent Clock (IEEE1588-2008) specific settings. Use the command to enable or disable synchronization of the local clock (only valid if syntonization is enabled).

Format

```
ptp v2tc sync-local-clock {enable | disable}
```

Mode

```
Global Config
```

4.15 PoE - Power over Ethernet

These commands show and configure the Power over Ethernet (IEEE 802.3af) parameters.

4.15.1 show inlinepower

This command shows global PoE inline power settings.

Format

```
show inlinepower
```

Mode

```
Privileged EXEC and User EXEC
```

4.15.2 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 . . 30 . 000 (in Watts)
- 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 . . 30 . 000 (in Watts)
- Default value: 0. (disable the limitation of PoE inline power)

4.15.3 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`.

4.15.4 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 <watts> | 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...30.000 (in watts)
- 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).

4.15.5 clear inlinepower

Reset the inline power parameters to default settings.

Format

```
clear inlinepower
```

Mode

```
Privileged EXEC
```

4.16 PoE+ - Power over Ethernet Plus

Additionally to the PoE (Power over Ethernet) commands, these commands show and configure the Power over Ethernet Plus (IEEE 802.3at) parameters.

Note: PoE+ is available for:

- MACH104-16TX-PoEP devices
- MACH 102 devices with media module M1-8TP-RJ45 PoEP

4.16.1 show inlinepower slot

This command shows the PoE+ configuration settings and states per slot.

Format

```
show inlinepower slot [<slot> | all]
```

Mode

Privileged EXEC and User EXEC

Slot

For MACH102 devices with M1-8TP-RJ45 PoEP media modules:

Slot = Slot number of the PoE+ module (valid range: 1 - 2)

For MACH104-16TX-PoEP devices: Slot = 1

Nominal Power

Shows the configured nominal power budget which the device provides for the PoE+ ports of the PoE+ module.

Maximum Power

Shows the nominal power which the device provides for the PoE+ ports of the PoE+ module (valid range: 0 - 248 W).

Reserved Power

Shows the maximum power which the device provides for all PoE+ devices together which are connected to the PoE+ module, based on their classification.

Delivered Power

Shows the current demand for power on all PoE+ ports of the module (valid range: 0 - 248 W).

Send Traps

Shows, if the function is enabled/disabled. If send traps is enabled, the device will send a trap if the power threshold exceeds or falls below the power limit or if the PoE+ power supply is switched on/off on one or more ports.

Power Threshold

Power threshold in per cent of the nominal power. If the power is exceeding/falling below this threshold, the device will send a trap.

4.16.2 inlinepower budget slot

Configure the available power budget per slot in Watts.

Format

```
inlinepower budget slot <slot> <0..1000>
```

Mode

```
Global Config
```

Slot

For MACH102 devices with M1-8TP-RJ45 PoEP media modules:

Slot = Slot number of the PoE+ module (valid range: 1 - 2)

For MACH104-16TX-PoEP devices: Slot = 1

4.16.3 inlinepower threshold slot

Configure the usage power threshold expressed in per cents for comparing the measured power for this slot and initiating an alarm if the threshold is exceeded.

Format

```
inlinepower threshold slot <slot> <0..99>
```

Mode

Global Config

Slot

For MACH102 devices with M1-8TP-RJ45 PoEP media modules:

Slot = Slot number of the PoE+ module (valid range: 1 - 2)

For MACH104-16TX-PoEP devices: Slot = 1

4.16.4 inlinepower trap slot

Configure the alarm that is send if the configured threshold for this slot is exceeded.

Format

```
inlinepower trap slot <slot> {enable | disable}
```

Mode

Global Config

Slot

For MACH102 devices with M1-8TP-RJ45 PoEP media modules:

Slot = Slot number of the PoE+ module (valid range: 1 - 2)

For MACH104-16TX-PoEP devices: Slot = 1

4.17 Port monitor

These commands show and configure the port monitor parameters.

The port monitor feature monitors certain port (or global) states or changes and performs a certain action, when the specified condition occurs.

Using this commands, you can disable a port and send a trap (see "port admin shutdown").

Disabling a port by condition will not modify the configuration and therefore not keep the port in disabled state after reload/reboot.

To enable the action if a port state occurs

- ▶ enable the port monitor globally,
- ▶ enable the port monitor on the port,
- ▶ configure condition(s) that is (are) performed in port state on a port and
- ▶ an action that is performed on that port, when the condition complies.

The condition can be link flapping or CRC/Fragments error, an action can be sending a trap or disabling that port (and send a trap).

If a port was disabled by the Port-Monitor the port can be enabled again with a port monitor reset command (see "port-monitor reset").

4.17.1 show port-monitor

Use this command to display the global Port Monitor settings.

Format

```
show port-monitor
```

Mode

```
Global Config
```

Port Monitor

Display if Port Monitor function is enabled or disabled.

Condition crc-fragment interval (seconds)

Display the condition of the CRC fragment interval in seconds.

Condition crc-fragment count

Display the condition of the CRC fragment count.

Condition link flap interval (seconds)

Display the condition of the link flap interval in seconds.

Condition link flap count

Display the condition of the link flap count.

4.17.2 show port-monitor <slot/port>

Use this command to display the Port Monitor details for the port.

Format

```
show port-monitor <slot/port>
```

Mode

```
Global Config
```

Port Monitor

Display if Port Monitor is enabled or disabled.

Link Flap

Display if Link Flap is enabled or disabled.

Crc-Fragment

Display if CRC Fragment is enabled or disabled.

Speed-duplex

Display the link speed and duplex condition for the port.

Possible values: `Enabled`, `Disabled`.

Active Condition

Display the active condition for the port.

Possible values: `Link-Flap`, `None`.

Action

Display the action (disable port or send trap) to be triggered on the port. Possible values: `Disable-Port`, `Trap-Only`.

Port Oper State

Display the link state of the port. Possible values: `Up`, `Down`.

4.17.3 show port-monitor brief

Use this command to display the Port Monitor brief summary.

Format

```
show port-monitor brief
```

Mode

Global Config

Intf

Display the number of the interface (slot/port).

Admin Mode

Display if Port Monitor is enabled or disabled.

Link Flap

Display if Link Flap is enabled or disabled.

Crc Fragment

Display if CRC Fragment is enabled or disabled.

Speed duplex

Display the link speed and duplex condition for the port.

Possible values: Enabled, Disabled.

Active Condition

Display the active condition for the port.

Possible values: Link-Flap, None.

Action

Display the action (disable port or send trap) to be triggered on the port. Possible values: Disable-Port, Trap-Only.

Port Oper State

Display the link state of the port. Possible values: Up, Down.

4.17.4 show port-monitor crc-fragment

Use this command to display the CRC fragment counter.

Format

```
show port-monitor crc-fragment <slot/port>
```

Mode

```
Global Config
```

<slot/port>

Display the Port Monitor interface details.

Crc_fragments in last interval

Display the CRC fragments in last interval.

Crc_fragments total

Display the CRC fragments total.

4.17.5 show port-monitor link-flap

Use this command to display the Link Flap counter for the port.

Format

```
show port-monitor link-flap <slot/port>
```

Mode

```
Global Config
```

<slot/port>

Display the Port Monitor interface details.

Link flaps in last interval

Display the Link flaps in last interval.

Link flaps total

Display the Link flaps total.

4.17.6 show port-monitor overload-detection

Use this command to display the overload detection details for the port.

Format

```
show port-monitor overload-detection <slot/port>
```

Mode

Global Config

<slot/port>

Display the Port Monitor interface details.

Overload-detection traffic type

Display the overload-detection traffic type for the interface.

Overload-detection threshold type

Display the overload-detection threshold type for the interface.

Overload-detection lower threshold

Display the overload-detection lower threshold for the interface.

Overload-detection upper threshold

Display the overload-detection upper threshold for the interface.

4.17.7 show port-monitor speed-duplex

Use this command to display the link speed and duplex configured modes.

Format

```
show port-monitor speed-duplex <slot/port>
```

Mode

Global Config

<slot/port>

Display the Port Monitor interface details for link speed and duplex condition.

Intf

Display the number of the interface (`slot/port`).

Allowed values

Display the allowed values for link speed and duplex combinations for the interfaces of the device.

Possible values: `hdx-10`, `fdx-10`, `hdx-100`, `fdx-100`, `hdx-1000`, `fdx-1000`, `fdx-10000`.

Allowed modes

Speed-duplex

Display the allowed link speed and duplex combinations for the specific interface.

Possible values: `hdx-10`, `fdx-10`, `hdx-100`, `fdx-100`, `hdx-1000`, `fdx-1000`, `fdx-10000`.

4.17.8 port-monitor (Global Config)

Use this command to enable or disable the Port Monitor globally.

Note: This command does not reset the port disable states.

Default

Disable

Format

```
port-monitor {enable | disable}
```

Mode

Global Config

4.17.9 port-monitor (Interface Config)

Use this command to enable or disable the Port Monitor on the port.

Note: This command does not reset the port disable states.

Default

Disable

Format

```
port-monitor {enable | disable}
```

Mode

Interface Config

4.17.10 port-monitor action

Use this command to configure the Port Monitor action (disable a port or send a trap).

Note: Disable the Port Monitor action will reset the port from port-state.

Default

```
auto-disable
```

Format

```
port-monitor action  
                {port-disable | trap-only | auto-disable}
```

Mode

```
Interface Config
```

port-disable

Disable the port when the configured Port Monitor condition triggers.

trap-only

Send a trap when the configured Port Monitor condition triggers.

auto-disable

Notify Auto Disable when the configured Port Monitor condition triggers.

4.17.11 port-monitor condition link-flap (Global Config)

Use this command to configure the Link Flap settings (Link Flap counter and interval for Link Flap detection).

Default

Disable

Format

```
port-monitor condition link-flap
                        {count <1..100> | interval <1..180>}
```

Mode

Global Config

count

Configure the Link Flap counter.

Default: 5. Value range: 1 ..100.

interval

Configure the measure interval in seconds for Link Flap detection.

Default: 10 seconds. Value range: 1 ..180 seconds.

4.17.12 port-monitor condition link-flap (Interface Config)

Use this command to enable or disable Link Flap condition on a port to trigger an action.

Default

Disable

Format

```
port-monitor condition link-flap {enable | disable}
```

Mode

Interface Config

4.17.13 port-monitor condition crc-fragment (Global Config)

Use this command to configure the crc-fragment settings (crc-fragment counter and interval for crc-fragment detection).

Default

Disable

Format

```
port-monitor condition crc-fragment
    {count <1..1000000> | interval <5..180>}
```

Mode

Global Config

count

Configure the crc-fragment counter.

Default: 1000. Value range: 1..1000000.

interval

Configure the measure interval in seconds for crc-fragment detection.

Default: 10 seconds. Value range: 5..180 seconds.

4.17.14 port-monitor condition crc-fragment (Interface Config)

Use this command to enable or disable crc-fragment settings on a port to trigger an action.

Default

Disable

Format

```
port-monitor condition crc-fragment  
                    {enable | disable}
```

Mode

Interface Config

4.17.15 port-monitor condition speed-duplex- monitor (Interface Config)

Use this command to enable or disable the link speed and duplex condition on a port to trigger an action.

Default

Disable

Format

```
port-monitor condition speed-duplex-monitor  
                    {enable | disable}
```

Mode

Interface Config

4.17.16 port-monitor condition speed-duplex-monitor speed (Interface Config)

Use this command to configure the allowed link speed and duplex combinations on a port.

Default

```
{hdx-10, fdx-10, hdx-100, fdx-100, hdx-1000,
 fdx-1000, fdx-10000}
```

Format

```
port-monitor condition speed-duplex-monitor speed
 <speed-duplex1>
  [<speed-duplex2>
   [<speed-duplex3>
    [<speed-duplex4>
     [<speed-duplex5>
      [<speed-duplex6>
       [<speed-duplex7>]]]]]]]
```

Mode

Interface Config

4.17.17 port-monitor condition speed-duplex-monitor clear (Interface Config)

Use this command to clear the allowed link speed and duplex combinations on a port. This will trigger the configured action if the link speed and duplex condition is enabled.

Default

```
{hdx-10, fdx-10, hdx-100, fdx-100, hdx-1000,
 fdx-1000, fdx-10000}
```

Format

```
port-monitor condition speed-duplex-monitor clear
```

Mode

Interface Config

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).

5.2.6 arc

Use this command to configure ARC (Automatic Ring Configuration). ARC supports MRP.

The ARC protocol is a simple protocol that checks a ring configuration and, if suitable, configures all clients of this ring automatically.

The check cycle includes an analysis of the ARC devices for an already active ring configuration and wrong ring configuration values. The ARC devices can detect loop situations and other ARC Managers in the ring. Errors are reported to the ARC Manager. With this information the ARC Manager can decide whether a configuration of the ring clients is possible or not.

Format

```
arc { manager {enable | disable} |
      client {enable | disable | checkOnly} |
      check |
      configure}
```

Mode

Global Config

client

Configure the ARC client.

- `enable`: Enable the ARC client for configuring and checking.
- `disable`: Disable the ARC client for configuring and checking.
- `checkOnly`: The device can only be checked but not configured by ARC.

manager

Configure the ARC manager.

- `enable`: Enable the ARC manager for configuring and checking.
- `disable`: Disable the ARC manager for configuring and checking.

check

Check the topology. All important values will be taken from the current ring configuration on the devices.

configure

Configure the topology. All important values will be taken from the current ring configuration of the ARC manager.

5.2.7 show arc

This command displays the current ARC configuration and the result of the last action.

Format

```
show arc
```

Mode

```
Global Config
```

Client Settings:

Display the Client Settings for the current ARC configuration.

Admin Status

Display if the ARC client is enabled or disabled.

MAC address of the ARC Manager

Display the MAC address of the ARC Client.

IP address of the ARC Manager

Display the IP address of the ARC Client.

Port 1

Display the number of Ring Port 1 for the client (slot/port).

Port 2

Display the number of Ring Port 2 for the client (slot/port).

Manager Settings:

Display the Manager Settings for the current ARC configuration.

Admin Status

Display the ARC manager is enabled or disabled

Protocol

Display the Protocol. Possible values: mrp,

Port 1

Display the number of Ring Port 1 for the manager (slot/port).

Port 2

Display the number of Ring Port 2 for the manager (slot/port).

VLAN ID

Display the VLAN ID. Possible values: 0 -

Last Action Result

Display the Result of the Last Action.

Possible values: Ring is open, Already Configured, Loop Source, Multiple RM, Configuration failed, Port not in full duplex mode, ARC not supported by the ring devices.

Last Check result:

Display the Result of the last check.

- Nr: Display the number of the check result.
- Mac Address: Display the concerned MAC address.
- IP Address: Display the concerned IP address.
- Type: Display the type of the result. Possible values: Error, Warning.

Possible check results (examples):

Error - Ring is open

Warning - Already Configured - HIPER Ring - Port1: 1.1 - Port2: 1.2

Warning - Already Configured - MRP - Port1: 1.9 - Port2: 1.10 - VLAN ID: 0

Warning - Already Configured - Fast HIPER Ring - Port1: 1.3 - Port2: 1.4

Error - Loop Source - Hop count: 1 - Port1: 1.1 - Port2: 1.4 - Port3: 1.15

Error - Multiple RM - MRP

Error - Configuration failed - MRP

Warning - Port not in full duplex mode - Port1: 1.1 Half - Port2: 1.2 Full

Warning - ARC not supported by the ring devices

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.

Note: This does not clear the 802.1X Port Security.

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

5.8 DHCP Server Commands

These commands configure the DHCP server 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') clear some or all of the settings to factory defaults.

5.8.1 DHCP server configuration example

The example shown below has the following task: The IP address is only to be served, if a request is coming via interface 1/1 with specified Mac address.

```
<Hirschmann PowerMICE> >enable
<Hirschmann PowerMICE> #configure
<Hirschmann PowerMICE> <Config>#dhcp-server operation
enable
<Hirschmann PowerMICE> <Config>#dhcp-server pool add 1
static 192.168.0.10
<Hirschmann PowerMICE> <Config>#dhcp-server pool modify
1 mode interface 1/1
<Hirschmann PowerMICE> <Config>#dhcp-server pool modify
1 mode mac 00:80:63:12:34:56
<Hirschmann PowerMICE> <Config>#dhcp-server pool modify
1 option gateway 192.168.0.1
<Hirschmann PowerMICE> <Config>#dhcp-server pool enable
1
<Hirschmann PowerMICE> <Config>#interface 1/1
<Hirschmann PowerMICE> <interface 1/1>#dhcp-server oper-
ation enable
```

```
<Hirschmann PowerMICE> <config>#dhcp-server pool modify
1 option vendor-specific <f1 08 0a 7e 7e 02 0a 7f 7f 02>
```

This configuration leads to the following result:

```
<Hirschmann PowerMICE> #show dhcp-server pool 1

ID..... 1
Status..... Enabled
Start Address..... 192.168.0.10
End Address..... 192.168.0.10
Leasetime..... 86400
Hirschmann Device..... Disabled
Mode..... Interface(1/1)
MAC..... 00:80:63:12:34:56
Options:
Configpath.....
Gateway..... 192.168.0.1
Subnet Mask..... 255.255.255.0
WINS..... 0.0.0.0
DNS..... 0.0.0.0
Hostname.....
Vendor Specific Information..... "f1 08 0a 7e 7e 02 0a
7f 7f 02"
```

5.8.2 show dhcp-server

Display DHCP Server global and interface information.

Format

```
show dhcp-server
```

Mode

Privileged EXEC and User EXEC

DHCP Server

Display the DHCP server operation setting.

Possible values: *Enabled, Disabled*

DHCP Address Probe

Display the DHCP server address probe setting.

Possible values: *Enabled, Disabled*

DHCP, Port-Related Settings:

Port

Display the port number in <slot/port> notation.

Mode

Display the DHCP server interface information.

Possible values: *enable, disable*

DHCP, Pools:

Display the DHCP server pool related information.

5.8.3 show dhcp-server operation

Display DHCP Server global information.

Format

```
show dhcp-server operation
```

Mode

Privileged EXEC and User EXEC

DHCP Server

Display the DCHP server operation setting.

Possible values: Enabled, Disabled

DHCP Address Probe

Display the DCHP server address probe setting.

Possible values: Enabled, Disabled

5.8.4 show dhcp-server port

Display the DCHP port-related settings for all ports or specific port only.

Format

```
show dhcp-server port {all | <slot/port>}
```

Mode

Privileged EXEC and User EXEC

show dhcp-server port all

Display the DCHP port-related settings for all ports.

show dhcp-server port <slot/port>

Display the DCHP port-related settings for the specified port only.

5.8.5 show dhcp-server pool

Display DHCP server pool information for all pool or detailed information for a specific pool.

Format

```
show dhcp-server pool {all | <id>}
```

Mode

Privileged EXEC and User EXEC

show dhcp-server pool all

Display the DHCP server pool information for all IDs.

show dhcp-server pool <id>

Display the DHCP server pool information for the specified ID only.

5.8.6 dhcp-server addr-probe

Use this command to enable or disable the probing of allocated addresses with an ICMP Echo request.

Format

```
dhcp-server addr-probe {disable|enable}
```

Mode

Global Config

dhcp-server addr-probe enable

Enable the DHCP server address probe. This is the default.
The DHCP server will send ICMP echo request before offering an IP.

dhcp-server addr-probe disable

Disable the DHCP server address probe.
The DHCP server will offer an IP without checking if already in use.

5.8.7 dhcp-server operation

Enable or disable the DHCP server globally. Default: disable.

Format

```
dhcp-server operation {disable|enable}
```

Mode

Interface Config

dhcp-server operation disable

Disable the DHCP server. This is the default.

dhcp-server operation enable

Enable the DHCP server.

5.8.8 dhcp-server pool add <id>

Add a pool with a single IP address (static) or with an IP range (dynamic)

Format

```
dhcp-server pool {add <id> {static <ipaddr>
                        |dynamic <start ipaddr> <end ipaddr>}}
```

Mode

Global Config

dhcp-server pool add <id> {static <ipaddr>}

Add a pool with a single IP address (static).

dhcp-server pool add <id> {dynamic <start ipaddr> <end ipaddr>}

Add a pool with an IP range (dynamic).

5.8.9 dhcp-server pool modify <id> mode

Add or delete one or more pool modes.

Format

```
dhcp-server pool modify <id> mode
    {interface {all | <slot/port>} 1)
    | mac {none | <macaddr>} 1)
    | clientid {none | <clientid>} 1)
    | relay {none | <ipaddr>}
    | remoteid {none | <remoteid>} 1)
    | circuitid {none | <circuitid>} 1)}
```

Mode

Global Config

dhcp-server pool modify <id> mode interface all 1)

Set pool to all interfaces.

dhcp-server pool modify <id> mode interface <slot/port> 1)

Set pool to a specific interface.

dhcp-server pool modify <id> mode mac none 1)

Use none to remove the mode.

dhcp-server pool modify <id> mode mac <macaddr> 1)

Enter macaddr in xx:xx:xx:xx:xx:xx format.

dhcp-server pool modify <id> mode clientid none 1)

Use none to remove the mode.

dhcp-server pool modify <id> mode clientid <clientid> 1)

Enter clientid in xx:xx:....:xx format.

dhcp-server pool modify <id> mode relay none

Use none to remove the mode.

dhcp-server pool modify <id> mode relay <ipaddr>

Enter IP address of the relay.

dhcp-server pool modify <id> mode remoteid none 1)

Use none to remove the mode.

dhcp-server pool modify <id> mode remoteid <remoteid> ¹⁾

Enter remoteid in xx:xx:....:xx format.

dhcp-server pool modify <id> mode circuitid none ¹⁾

Use none to remove the mode.

dhcp-server pool modify <id> mode circuitid <circuitid> ¹⁾

Enter circuitid in xx:xx:....:xx format.

¹⁾ Available for pools with single IP address only.

5.8.10 dhcp-server pool modify <id> option

Modify pool options.

Format

```
dhcp-server pool modify <id> option
    {configpath <url> |
    gateway <ipaddr> |
    netmask <netmask> |
    wins <ipaddr> |
    dns <ipaddr> |
    hostname <name>}
    vendor-specific <string>}
```

Mode

Global Config

dhcp-server pool modify <id> option configpath <url>

Option configpath. Enter the configpath URL in 'tftp://<servername-or-ip>/<file>' format.

dhcp-server pool modify <id> option gateway <ipaddr>

Option default gateway. Enter the gateway IP address.

dhcp-server pool modify <id> option netmask <netmask>

Option netmask. Enter the netmask.

dhcp-server pool modify <id> option wins <ipaddr>

Option wins. Enter WINS IP address.

dhcp-server pool modify <id> option dns <ipaddr>

Option DNS. Enter the DNS IP address.

dhcp-server pool modify <id> option hostname <name>

Option hostname. Enter the host name.

dhcp-server pool modify <id> option vendor-specific <string>

Option vendor-specific information. Enter vendor specific information as hex in xx:xx: . . . :xx format..

5.8.11 dhcp-server pool modify leasetime

Modify pool leasetime. Enter the leasetime in seconds.

Format

```
dhcp-server pool modify leasetime <seconds>
```

Mode

Global Config

5.8.12 dhcp-server pool modify <id> hirschmann-device

Set this pool to Hirschmann devices only or to all devices.

Format

```
dhcp-server pool modify <id> hirschmann-device  
{enable|disable}
```

Mode

Global Config

dhcp-server pool modify <id> hirschmann-device disable

Use pool for all devices.

dhcp-server pool modify <id> hirschmann-device enable

Use pool for Hirschmann devices only.

5.8.13 dhcp-server pool enable

Enable a specific pool.

Format

```
dhcp-server pool enable <id>
```

Mode

Global Config

5.8.14 dhcp-server pool disable

Disable a specific pool.

Format

```
dhcp-server pool disable <id>
```

Mode

Global Config

5.8.15 dhcp-server pool delete

Delete a specific pool.

Format

```
dhcp-server pool delete <id>
```

Mode

Global Config

5.9 Sub-Ring Commands

These commands configure the sub-ring 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.

5.9.1 show sub-ring

Display sub-ring information for all sub-rings or detailed information for a specific sub-ring.

Format

```
show sub-ring {all-ids | <id>}
               {id | info | mode | operation | protocol | port |
               summary | ring-name | vlan | mrp-domainID |
               partner-mac}
```

Mode

Privileged EXEC and User EXEC

show sub-ring

Display the sub-ring information.

show sub-ring all-ids

Display the sub-ring information for all existing Sub-Ring IDs.

show sub-ring <id>

Display the sub-ring information for the specified ID.

id

Display the given Sub-Ring's ID.

info

Display status information for the given Sub-Ring ID.

mode

Display the switch's mode for the given Sub-Ring ID.

operation

Display the switch's operative setting for the given Sub-Ring ID.

Note: In case of configuration problems, this value may differ from the administrative setting (may become 'Disabled').

protocol

Display the switch's protocol setting for the given Sub-Ring ID.

port

Display the ports for the given Sub-Ring ID.

summary

Display a summary for the given Sub-Ring ID.

ring-name

Display ring name for the given Sub-Ring ID.

vlan

Display the VLAN ID for the given Sub-Ring ID.

mrp-domainID

Display the MRP domain ID for the given Sub-Ring ID.

partner-mac

Display the partner MAC for the given Sub-Ring ID.

5.9.2 sub-ring <id> mode

Configure the switch's Sub-Ring mode for the given ID (manager or redundant-manager).

Format

```
sub-ring <id> mode {manager |  
                    redundant-manager |  
                    single-manager}
```

Mode

Global Config

<id>

Specify the Sub-Ring ID whose settings you want to configure.

manager

Switch is manager for the given Sub-Ring ID.

redundant-manager

Switch is redundant-manager for the given Sub-Ring ID.

single-manager

Switch is single-manager for the given Sub-Ring ID.

5.9.3 sub-ring <id> operation

Enable or disable the switch for the given Sub-Ring ID.

Format

```
sub-ring <id> operation {enable|disable}
```

Mode

Global Config

<id>

Specify the Sub-Ring ID whose settings you want to configure.

enable

Enable the switch for the given Sub-Ring ID.

disable

Disable the switch for the given Sub-Ring ID.

5.9.4 sub-ring <id> protocol

Set MRP or FHR as sub-ring protocol for the given Sub-Ring ID.

Format

```
sub-ring <id> protocol standard_mrp
```

Mode

Global Config

<id>

Specify the Sub-Ring ID whose settings you want to configure.

standard_mrp

Set MRP as sub-ring protocol for the given Sub-Ring ID.

5.9.5 sub-ring <id> port

Specify the switch's ports for the given Sub-Ring ID.

Format

```
sub-ring <id> port <slot/port>
```

Mode

```
Global Config
```

<id>

Specify the Sub-Ring ID whose settings you want to configure.

<slot/port>

Specify the port (in slot/port notation).

5.9.6 sub-ring <id> ring-name

Set a ring name for the given Sub-Ring ID.

Format

```
sub-ring <id> ring-name <ring-name>
```

Mode

```
Global Config
```

<id>

Specify the Sub-Ring ID whose settings you want to configure.

<ring-name>

Enter a name for the given Sub-Ring ID. The name may be up to 254 characters long and contain only printable characters. If you do not give a name, the current name will be set to an empty string ("").

5.9.7 sub-ring <id> vlan

Specify the VLAN for the given Sub-Ring ID.

Format

```
sub-ring <id> vlan <0-4042>
```

Mode

```
Global Config
```

<id>

Specify the Sub-Ring ID whose settings you want to configure.

<0-4042>

Enter the VLAN for the given Sub-Ring ID
(min.: 0, max.: 4042, default: 0).

5.9.8 sub-ring <id> mrp-domainID

Set an MRP domain ID for the given Sub-Ring ID.

Format

```
sub-ring <id> mrp-domainID {<id> |
                                default-domainID}
```

Mode

Global Config

<id>

sub-ring <id>: Specify the Sub-Ring ID whose settings you want to configure.

<id>

Enter an MRP domainID for the given Sub-Ring ID.

The ID has to be 16 bytes long and contain only printable characters.

default-domainID

Enter the default MRP domainID for the given Sub-Ring ID.

The MRP domainID will be set to 255.255.255.255.255.255
255.255.255.255.255.255.255.255.255

5.9.9 sub-ring delete-ring

Delete all existing Sub-Rings IDs or a specific Sub-Ring ID.

Format

```
sub-ring delete-ring {all-ids | <id>}
```

Mode

Global Config

all-ids

Delete all existing Sub-Ring IDs.

<id>

Delete the given Sub-Ring ID. Format: a number in the range 1-2147483647 ($2^{31} - 1$). An ID of 0 is invalid.

5.9.10 sub-ring new-ring

Create a new Sub-Ring ID. The configuration will consist of default parameters and its operation will be disabled.

Format

```
sub-ring new-ring <id>
```

Mode

Global Config

<id>

Enter a new Sub-Ring ID. Format: a number in the range 1-2147483647 ($2^{31} - 1$). An ID of 0 is invalid.

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 authentication login

This command creates an authentication login list. The `<listname>` is up to 15 alphanumeric characters and is not case sensitive. Up to 10 authentication login lists can be configured on the switch. When a list is created, the authentication method “local” is set as the first method.

When the optional parameters “Option1”, “Option2” and/or “Option3” are used, an ordered list of methods are set in the authentication login list. If the authentication login list does not exist, a new authentication login list is first created and then the authentication methods are set in the authentication login list. The maximum number of authentication login methods is three. The possible method values are `local`, `radius` and `reject`.

The value of `local` indicates that the user’s locally stored ID and password are used for authentication. The value of `radius` indicates that the user’s ID and password will be authenticated using the RADIUS server. The value of `reject` indicates the user is never authenticated.

To authenticate a user, the authentication methods in the user’s login will be attempted in order until an authentication attempt succeeds or fails.

Note: The default login list included with the default configuration can not be changed.

Note: When assigning a list to the 'admin' account, include an authentication method that allows administrative access even when remote authentication is unavailable.

Format

```
authentication login <listname> [method1 [method2  
[method3]]]
```

Mode

```
Global Config
```

■ no authentication login

This command deletes the specified authentication login list.

You will be unable to delete if any of the following conditions are true:

- ▶ The login list name is invalid or does not match an existing authentication login list
- ▶ The specified authentication login list is assigned to any user or to the non configured user for any component
- ▶ The login list is the default login list included with the default configuration and was not created using 'authentication login'.
The default login list cannot be deleted.

Format

```
no authentication login <listname>
```

Mode

```
Global Config
```

6.1.2 authorization network radius

Use this command to enable the switch to accept VLAN assignment by the RADIUS server.

Format

```
authorization network radius
```

Mode

```
Privileged EXEC
```

■ no authorization network radius

Use this command to disable the switch to accept VLAN assignment by the RADIUS server.

Format

```
no authorization network radius
```

Mode

```
Global Config
```

6.1.3 clear dot1x statistics

This command resets the 802.1X statistics for the specified port or for all ports.

Format

```
clear dot1x statistics {<slot/port> | all}
```

Mode

```
Privileged EXEC
```

6.1.4 clear radius statistics

This command is used to clear all RADIUS statistics.

Format

```
clear radius statistics
```

Mode

Privileged EXEC

6.1.5 dot1x defaultlogin

This command assigns the authentication login list to use for non-configured users for 802.1X port security. This setting is over-ridden 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

```
dot1x defaultlogin <listname>
```

Mode

Global Config

6.1.6 dot1x dynamic-vlan enable

Use this command to enable the switch to create VLANs dynamically when a RADIUS-assigned VLAN does not exist in the switch.

Default

```
disabled
```

Format

```
dot1x dynamic-vlan enable
```

Mode

```
Global Config
```

■ no dot1x dynamic-vlan enable

Use this command to disable the switch to create VLANs dynamically when a RADIUS-assigned VLAN does not exist in the switch.

Default

```
disabled
```

Format

```
no dot1x dynamic-vlan enable
```

Mode

```
Global Config
```

6.1.7 dot1x guest-vlan

This command configures VLAN as guest vlan on an interface. The command specifies an active VLAN as an IEEE 802.1x guest VLAN. The range is 1 to the maximum VLAN ID supported by the platform.

Format

```
dot1x guest-vlan <vlan-id>
```

Mode

```
Interface Config
```

<vlan-id>

Enter an existing VLAN ID.

■ no dot1x guest-vlan

This command is used to disable Guest VLAN for the port.

Format

```
no dot1x guest-vlan
```

Mode

```
Global Config
```

6.1.8 dot1x initialize

This command begins the initialization sequence on the specified port. This command is only valid if the control mode for the specified port is 'auto'. If the control mode is not 'auto' an error will be returned.

Format

```
dot1x initialize <slot/port>
```

Mode

Privileged EXEC

6.1.9 dot1x login

This command assigns the specified authentication login list to the specified user for 802.1X port security. The <user> parameter must be a configured user and the <list-name> parameter must be a configured authentication login list.

Format

```
dot1x login <user> <listname>
```

Mode

Global Config

6.1.10 dot1x mac-auth-bypass

This command enables the MAC-authorized-bypass on that interface.

Default

disabled

Format

```
dot1x mac-auth-bypass
```

Mode

Interface Config

■ no dot1x mac-auth-bypass

This command disables the MAC-authorized-bypass on that interface.

Default

disabled

Format

```
no dot1x mac-auth-bypass
```

Mode

Interface Config

6.1.11 dot1x max-req

This command sets the maximum number of times the authenticator state machine on this port will transmit an EAPOL EAP Request/Identity frame before timing out the supplicant. The <count> value must be in the range 1 - 10.

Default

2

Format

```
dot1x max-req <count>
```

Mode

Interface Config

■ no dot1x max-req

This command sets the maximum number of times the authenticator state machine on this port will transmit an EAPOL EAP Request/Identity frame before timing out the supplicant.

Format

```
no dot1x max-req
```

Mode

Interface Config

6.1.12 dot1x max-users

Use this command to set the maximum number of clients supported on an interface when MAC-based 802.1X authentication is enabled on the port. The count value is in the range 1-16 and the default value is 16.

Default

16

Format

```
dot1x max-users <count>
```

Mode

Interface Config

■ no dot1x max-users

The 'no' form of this command resets the maximum number of clients allowed to its default value of 16.

Format

```
no dot1x max-users
```

Mode

Interface Config

6.1.13 dot1x port-control

This command sets the authentication mode to be used on the specified port. The control mode may be one of the following.

- ▶ `force-unauthorized`: The authenticator PAE unconditionally sets the controlled port to unauthorized. Thus the port is always blocked.
- ▶ `force-authorized`: The authenticator PAE unconditionally sets the controlled port to authorized. Thus the port is always opened.
- ▶ `auto`: The authenticator PAE sets the controlled port mode to reflect the outcome of the authentication exchanges between the supplicant, authenticator and the authentication server. The port mode is controlled by the protocol.
- ▶ `mac-based`: Enable MAC-based 802.1X authentication on the port.

Default

```
force-authorized
```

Format

```
dot1x port-control {force-unauthorized | force-authorized | auto | mac-based}
```

Mode

```
Interface Config
```

■ no dot1x port-control

This command sets the port-control mode for the specified port to the default mode (`force-authorized`).

Format

```
no dot1x port-control
```

Mode

```
Interface Config
```

6.1.14 dot1x port-control all

This command sets the authentication mode to be used on all ports. The control mode may be one of the following.

- ▶ `force-unauthorized`: The authenticator PAE unconditionally sets the controlled port to unauthorized. Thus the ports are always blocked.
- ▶ `force-authorized`: The authenticator PAE unconditionally sets the controlled port to authorized. Thus the ports are always opened.
- ▶ `auto`: The authenticator PAE sets the controlled port mode to reflect the outcome of the authentication exchanges between the supplicant, authenticator and the authentication server. The port mode is controlled by the protocol.
- ▶ `mac-based`: Enable the MAC-based 802.1X authentication on the port.

Default

```
force-authorized
```

Format

```
dot1x port-control all {force-unauthorized | force-authorized | auto | mac-based}
```

Mode

```
Global Config
```

■ no dot1x port-control all

This command sets the port-control mode for all the ports to the default mode (`force-authorized`).

Format

```
no dot1x port-control all
```

Mode

```
Global Config
```

6.1.15 dot1x re-authenticate

This command begins the re-authentication sequence on the specified port. This command is only valid if the control mode for the specified port is 'auto'. If the control mode is not 'auto' an error will be returned.

Format

```
dot1x re-authenticate <slot/port>
```

Mode

Privileged EXEC

6.1.16 dot1x re-authentication

This command enables re-authentication of the supplicant for the specified port.

Default

disabled

Format

```
dot1x re-authentication
```

Mode

Interface Config

■ no dot1x re-authentication

This command disables re-authentication of the supplicant for the specified port.

Format

```
no dot1x re-authentication
```

Mode

Interface Config

6.1.17 dot1x safe-vlan

Use this command to enable the safe-vlan assignment on the switch.

Note: This command is available for the RS20/RS30/RS40, RSB20, MS20/MS30, RSR20/RSR30, MACH100, MACH1000, PowerMICE, MACH4000, OCTOPUS devices.

Default

disabled

Format

```
dot1x safe-vlan
```

Mode

Global Config

■ no dot1x safe-vlan

Use this command to disable the safe-vlan assignment on the switch.

Default

disabled

Format

```
no dot1x safe-vlan
```

Mode

Global Config

6.1.18 dot1x system-auth-control

This command is used to enable the dot1x authentication support on the switch. By default, the authentication support is disabled. While disabled, the dot1x configuration is retained and can be changed, but is not activated.

Default

```
disabled
```

Format

```
dot1x system-auth-control
```

Mode

```
Global Config
```

■ no dot1x system-auth-control

This command is used to disable the dot1x authentication support on the switch.

Format

```
no dot1x system-auth-control
```

Mode

```
Global Config
```

6.1.19 dot1x timeout

This command sets the value, in seconds, of the timer used by the authenticator state machine on this port. Depending on the token used and the value (in seconds) passed, various timeout configurable parameters are set. The following tokens are supported.

- ▶ reauth-period: Sets the value, in seconds, of the timer used by the authenticator state machine on this port to determine when re-authentication of the supplicant takes place. The reauth-period must be a value in the range 1 - 65535.

- ▶ **quiet-period**: Sets the value, in seconds, of the timer used by the authenticator state machine on this port to define periods of time in which it will not attempt to acquire a supplicant. The quiet-period must be a value in the range 0 - 65535.
- ▶ **tx-period**: Sets the value, in seconds, of the timer used by the authenticator state machine on this port to determine when to send an EAPOL EAP Request/Identity frame to the supplicant. The quiet-period must be a value in the range 1 - 65535.
- ▶ **supp-timeout**: Sets the value, in seconds, of the timer used by the authenticator state machine on this port to timeout the supplicant. The supp-timeout must be a value in the range 1 - 65535.
- ▶ **server-timeout**: Sets the value, in seconds, of the timer used by the authenticator state machine on this port to timeout the authentication server. The supp-timeout must be a value in the range 1 - 65535.

Defaults

```
reauth-period: 3600 seconds
quiet-period: 60 seconds
tx-period: 30 seconds
supp-timeout: 30 seconds
server-timeout: 30 seconds
```

Format

```
dot1x timeout {{reauth-period <seconds>} | {quiet-
period <seconds>} | {tx-period <seconds>} | {supp-
timeout <seconds>} | {server-timeout <seconds>}}
```

Mode

```
Interface Config
```

■ no dot1x timeout

This command sets the value, in seconds, of the timer used by the authenticator state machine on this port to the default values. Depending on the token used, the corresponding default values are set.

Format

```
no dot1x timeout {reauth-period | quiet-period |
tx-period | supp-timeout | server-timeout}
```

Mode

```
Interface Config
```

6.1.20 dot1x timeout guest-vlan-period

Use this command to configure the timeout value for the guest-vlan-period. The time, in seconds, for which the authenticator waits to see if any EAPOL packets are received on a port before authorizing the port and placing the port in the guest vlan (if configured). The guest vlan timer is only relevant when guest vlan has been configured on that specific port.

Default guest-vlan-period: 90 seconds.

Default

90

Format

```
dot1x timeout guest-vlan-period <seconds>
```

Mode

Interface Config

<seconds>

Enter an integer in the range of 1-300.

■ no dot1x timeout guest-vlan-period

The 'no' form of this command resets the timeout value for the guest-vlan-period to its default value (90 seconds).

Format

```
no dot1x timeout guest-vlan-period
```

Mode

Interface Config

6.1.21 dot1x unauthenticated-vlan

Use this command to configure the unauthenticated VLAN associated with the specified interface. The unauthenticated VLAN ID can be a valid VLAN ID from 0 to maximum supported VLAN ID. The unauthenticated VLAN must be statically configured in the VLAN database to be operational. By default, the unauthenticated VLAN is 0, i.e. invalid and not operational.

Default

0

Format

```
dot1x unauthenticated-vlan <vlan-id>
```

Mode

Interface Config

<vlan-id>

Enter an existing VLAN ID.

■ no dot1x unauthenticated-vlan

The 'no' form of this command resets the value for the unauthenticated VLAN to its default value.

Format

```
no dot1x unauthenticated-vlan
```

Mode

Interface Config

6.1.22 dot1x user

This command adds the specified user to the list of users with access to the specified port or all ports. The <user> parameter must be a configured user.

Format

```
dot1x user <user> {<slot/port> | all}
```

Mode

```
Global Config
```

■ no dot1x user

This command removes the user from the list of users with access to the specified port or all ports.

Format

```
no dot1x user <user> {<slot/port> | all}
```

Mode

```
Global Config
```

6.1.23 ip ssh protocol

Use this command to configure the IP secure shell (SSH) parameters, the first and the optional second SSH protocol level).

Possible settings: v1, v2 or v1 & v2.

Format

```
ip ssh [protocol <protocollevel1>
        [<protocollevel2>]]
```

Default

```
2 1
```

Mode

Privileged Exec

<protocollevel1>

Enter the first SSH Protocol Level (Version).

Possible values: 1, 2

<protocollevel2>

Optionally enter the second SSH Protocol Level (Version).

Possible values: 1, 2

■ no ip ssh

This command sets IP secure shell (SSH) parameters to default value.

Format

```
no ip ssh
```

Mode

Privileged Exec

6.1.24 radius accounting mode

This command is used to enable the RADIUS accounting function.

Default

```
disabled
```

Format

```
radius accounting mode
```

Mode

```
Global Config
```

■ no radius accounting mode

This command is used to set the RADIUS accounting function to the default value - i.e. the RADIUS accounting function is disabled.

Format

```
no radius accounting mode
```

Mode

```
Global Config
```

6.1.25 radius server host

This command is used to configure the RADIUS authentication and accounting server.

If the 'auth' token is used, the command configures the IP address to use to connect to a RADIUS authentication server. Up to 3 servers can be configured per RADIUS client. If the maximum number of configured servers is reached, the command will fail until one of the servers is removed by executing the no form of the command. If the optional <port> parameter is

used, the command will configure the UDP port number to use to connect to the configured RADIUS server. In order to configure the UDP port number, the IP address must match that of a previously configured RADIUS authentication server. The port number must lie between 1 - 65535, with 1812 being the default value.

If the 'acct' token is used, the command configures the IP address to use for the RADIUS accounting server. Only a single accounting server can be configured. If an accounting server is currently configured, it must be removed from the configuration using the no form of the command before this command succeeds. If the optional <port> parameter is used, the command will configure the UDP port to use to connect to the RADIUS accounting server. The IP address specified must match that of a previously configured accounting server. If a port is already configured for the accounting server then the new port will replace the previously configured value. The port must be a value in the range 1 - 65535, with 1813 being the default value.

Format

```
radius server host {auth | acct} <ipaddr> [<port>]
```

Mode

Global Config

■ no radius server host

This command is used to remove the configured RADIUS authentication server or the RADIUS accounting server. If the 'auth' token is used, the previously configured RADIUS authentication server is removed from the configuration. Similarly, if the 'acct' token is used, the previously configured RADIUS accounting server is removed from the configuration. The <ipaddr> parameter must match the IP address of the previously configured RADIUS authentication / accounting server.

Format

```
no radius server host {auth | acct} <ipaddress>
```

Mode

Global Config

6.1.26 radius server key

This command is used to configure the shared secret between the RADIUS client and the RADIUS accounting / authentication server. Depending on whether the 'auth' or 'acct' token is used, the shared secret will be configured for the RADIUS authentication or RADIUS accounting server. The IP address provided must match a previously configured server. When this command is executed, the secret will be prompted. The secret must be an alphanumeric value not exceeding 20 characters.

Format

```
radius server key {auth | acct} <ipaddr>
```

Mode

```
Global Config
```

6.1.27 radius server msgauth

This command enables the message authenticator attribute for a specified server.

Default

```
radius server msgauth <ipaddr>
```

Mode

```
Global Config
```

6.1.28 radius server primary

This command is used to configure the primary RADIUS authentication server for this RADIUS client. The primary server is the one that is used by default for handling RADIUS requests. The remaining configured servers are only used if the primary server cannot be reached. A maximum of three servers can be configured on each client. Only one of these servers can be configured as the primary. If a primary server is already configured prior to this command being executed, the server specified by the IP address used in this command will become the new primary server. The IP address must match that of a previously configured RADIUS authentication server.

Format

```
radius server primary <ipaddr>
```

Mode

```
Global Config
```

6.1.29 radius server retransmit

This command sets the maximum number of times a request packet is retransmitted when no response is received from the RADIUS server. The retries value is an integer in the range of 1 to 15.

Default

4

Format

```
radius server retransmit <retries>
```

Mode

Global Config

■ no radius server retransmit

This command sets the maximum number of times a request packet is re-transmitted, when no response is received from the RADIUS server, to the default value, i.e. 10.

Format

```
no radius server retransmit
```

Mode

Global Config

6.1.30 radius server timeout

This command sets the timeout value (in seconds) after which a request must be retransmitted to the RADIUS server if no response is received. The timeout value is an integer in the range of 1 to 30.

Default

6

Format

```
radius server timeout <seconds>
```

Mode

Global Config

■ no radius server timeout

This command sets the timeout value (in seconds) after which a request must be retransmitted to the RADIUS server if no response is received, to the default value, i.e. 6.

Format

```
no radius server timeout
```

Mode

Global Config

6.1.31 show radius accounting

This command is used to display the configured RADIUS accounting mode, accounting server and the statistics for the configured accounting server.

Format

```
show radius accounting [statistics <ipaddr>]
```

Mode

Privileged EXEC and User EXEC

If the optional token 'statistics <ipaddr>' is not included, then only the accounting mode and the RADIUS accounting server details are displayed.

Mode

Enabled or disabled

IP Address

The configured IP address of the RADIUS accounting server

Port

The port in use by the RADIUS accounting server

Secret Configured

Yes or No

If the optional token 'statistics <ipaddr>' is included, the statistics for the configured RADIUS accounting server are displayed. The IP address parameter must match that of a previously configured RADIUS accounting server. The following information regarding the statistics of the RADIUS accounting server is displayed.

Accounting Server IP Address

IP Address of the configured RADIUS accounting server

Round Trip Time

The time interval, in hundredths of a second, between the most recent Accounting-Response and the Accounting-Request that matched it from the RADIUS accounting server.

Requests

The number of RADIUS Accounting-Request packets sent to this accounting server. This number does not include retransmissions.

Retransmission

The number of RADIUS Accounting-Request packets retransmitted to this RADIUS accounting server.

Responses

The number of RADIUS packets received on the accounting port from this server.

Malformed Responses

The number of malformed RADIUS Accounting-Response packets received from this server. Malformed packets include packets with an

invalid length. Bad authenticators and unknown types are not included as malformed accounting responses.

Bad Authenticators

The number of RADIUS Accounting-Response packets containing invalid authenticators received from this accounting server.

Pending Requests

The number of RADIUS Accounting-Request packets sent to this server that have not yet timed out or received a response.

Timeouts

The number of accounting timeouts to this server.

Unknown Types

The number of RADIUS packets of unknown types, which were received from this server on the accounting port.

Packets Dropped

The number of RADIUS packets received from this server on the accounting port and dropped for some other reason.

6.1.32 show authentication

This command displays the ordered authentication methods for all authentication login lists.

Format

```
show authentication
```

Mode

```
Privileged EXEC and User EXEC
```

Authentication Login List

This displays the authentication login listname.

Method 1

This displays the first method in the specified authentication login list, if any.

Method 2

This displays the second method in the specified authentication login list, if any.

Method 3

This displays the third method in the specified authentication login list, if any.

6.1.33 show authentication users

This command displays information about the users assigned to the specified authentication login list. If the login is assigned to non-configured users, the user “default” will appear in the user column.

Format

```
show authentication users <listname>
```

Mode

Privileged EXEC and User EXEC

User

This field displays the user assigned to the specified authentication login list.

Component

This field displays the component (User or 802.1X) for which the authentication login list is assigned.

6.1.34 show dot1x

This command is used to show a summary of the global dot1x configuration, summary information of the dot1x configuration for a specified port or all ports, the detailed dot1x configuration for a specified port and the dot1x statistics for a specified port - depending on the tokens used.

Format

```
show dot1x [{summary {<slot/port> | all} | {detail  
<slot/port>} | {statistics <slot/port>}]
```

Mode

Privileged EXEC and User EXEC

If none of the optional parameters are used, the global dot1x configuration summary is displayed.

Administrative mode

Indicates whether authentication control on the switch is enabled or disabled.

VLAN Assignment Mode

Indicates whether the VLAN Assignment Mode is enabled or disabled.

Dynamic VLAN Creation Mode

Indicates whether the Dynamic VLAN Creation Mode is enabled or disabled.

Safe VLAN Mode

Indicates whether the Safe VLAN Mode is enabled or disabled.

If the optional parameter 'summary {<slot/port> | all}' is used, the dot1x configuration for the specified port or all ports are displayed.

Port

The interface whose configuration is displayed.

Control Mode

The configured control mode for this port. Possible values are
force-unauthorized | force-authorized | auto |
mac-based

Operating Control Mode

The control mode under which this port is operating. Possible values are
authorized | unauthorized

Reauthentication Enabled

Indicates whether re-authentication is enabled on this port

Key Transmission Enabled

Indicates if the key is transmitted to the supplicant for the specified port

If the optional parameter 'detail <slot/port>' is used, the detailed dot1x configuration for the specified port are displayed.

Port

The interface whose configuration is displayed

Protocol Version

The protocol version associated with this port. The only possible value is 1, corresponding to the first version of the dot1x specification.

PAE Capabilities

The port access entity (PAE) functionality of this port.
Possible values: `Authenticator`, `Supplicant`.

Control Mode

Display the state of the Control Mode.
Possible values: `auto`, `forceauthorized`, ...

Authenticator PAE State

Current state of the authenticator PAE state machine.
Possible values: `Initialize`, `Disconnected`, `Connecting`, `Authenticating`, `Authenticated`, `Aborting`, `Held`, `ForceAuthorized`, and `ForceUnauthorized`.

Backend Authentication State

Current state of the backend authentication state machine.
Possible values: `Request`, `Response`, `Success`, `Fail`, `Timeout`, `Idle`, `Initialize`.

Quiet Period

The timer used by the authenticator state machine on this port to define periods of time in which it will not attempt to acquire a supplicant. The value is expressed in seconds and will be in the range 0..65535.

Transmit Period

The timer used by the authenticator state machine on the specified port to determine when to send an EAPOL EAP Request/Identity frame to the supplicant. The value is expressed in seconds and will be in the range of 1..65535.

Guest VLAN ID

Display the Guest VLAN ID.
Default value: 0.

Guest VLAN Period (secs)

Display the Guest VLAN Period.
Default value: 90 seconds.

Supplicant Timeout

The timer used by the authenticator state machine on this port to timeout the supplicant. The value is expressed in seconds and will be in the range of 1 . . 65535.

Server Timeout

The timer used by the authenticator on this port to timeout the authentication server. The value is expressed in seconds and will be in the range of 1 . . 65535.

Maximum Requests

The maximum number of times the authenticator state machine on this port will retransmit an EAPOL EAP Request/Identity before timing out the supplicant. The value will be in the range of 1 . . 10.

VLAN Id

Display the VLAN Id.

VLAN Assigned Reason

Display the state of the VLAN Assigned Reason parameter.
Possible values: RADIUS, Not Assigned.

Reauthentication Period

The timer used by the authenticator state machine on this port to determine when reauthentication of the supplicant takes place. The value is expressed in seconds and will be in the range of 1 . . 65535.

Reauthentication Enabled

Indicates if reauthentication is enabled on this port.
Possible values: True, False

Key Transmission Enabled

Indicates if the key is transmitted to the supplicant for the specified port.
Possible values: True, False.

Control Direction

Indicates the control direction for the specified port or ports.
Possible values: both, in.

Maximum Users

Display the value of Maximum Users.

Unauthenticated VLAN ID

Display the value of Unauthenticated VLAN ID

Session Timeout

Display the value of Session Timeout

Session Termination Action

Display the value of Session Termination Action

MAC-Authorized-Bypass

Display the value of MAC-Authorized-Bypass

If the optional parameter 'statistics <slot/port>' is used, the dot1x statistics for the specified port are displayed.

Port

The interface whose statistics are displayed.

EAPOL Frames Received

The number of valid EAPOL frames of any type that have been received by this authenticator.

EAPOL Frames Transmitted

The number of EAPOL frames of any type that have been transmitted by this authenticator.

EAPOL Start Frames Received

The number of EAPOL start frames that have been received by this authenticator.

EAPOL Logoff Frames Received

The number of EAPOL logoff frames that have been received by this authenticator.

Last EAPOL Frame Version

The protocol version number carried in the most recently received EAPOL frame.

Last EAPOL Frame Source

The source MAC address carried in the most recently received EAPOL frame.

EAP Response/Id Frames Received

The number of EAP response/identity frames that have been received by this authenticator.

EAP Response Frames Received

The number of valid EAP response frames (other than resp/id frames) that have been received by this authenticator.

EAP Request/Id Frames Transmitted

The number of EAP request/identity frames that have been transmitted by this authenticator.

EAP Request Frames Transmitted

The number of EAP request frames (other than request/identity frames) that have been transmitted by this authenticator.

Invalid EAPOL Frames Received

The number of EAPOL frames that have been received by this authenticator in which the frame type is not recognized.

EAP Length Error Frames Received

The number of EAPOL frames that have been received by this authenticator in which the frame type is not recognized.

6.1.35 show dot1x users

This command displays 802.1X port security user information for locally configured users.

Format

```
show dot1x users <slot/port>
```

Mode

Privileged EXEC and User EXEC

User

Users configured locally to have access to the specified port.

6.1.36 show dot1x clients

This command displays 802.1X port security client information for locally configured clients.

Format

```
show dot1x clients <slot/port>
```

Mode

Privileged EXEC

Logical Interface

Display the Logical Interface.

Interface

Display the Interface.

User Name

Display the User Name.

Supp MAC Address

Display the Supp MAC Address.

Session Time

Display the Session Time.

Vlan Id

Display the Vlan Id.

Vlan Assigned Reason

Display the Vlan Assigned Reason.
Possible values: RADIUS,

Session Timeout

Display the Session Timeout.

Session Termination Action

Display the Session Termination Action.
Possible values: Reauthenticate,

6.1.37 show ip ssh

This command displays the IP secure shell (SSH) information.

Format

```
show ip ssh
```

Mode

Privileged EXEC

Administrative Mode

Display the SSH administrative mode setting.

Possible values: Disabled, Enabled.

Protocol Levels

Display the SSH protocol levels setting.

Possible values: Versions 1 and 2, Version 1, Version 2
(default setting: Versions 1 and 2).

SSH Sessions Currently Active

Display the number of SSH sessions being currently set up.

Possible values: 1 . . 5.

Max SSH Sessions Allowed

Display the max. number of SSH sessions that can be set up simultaneously.

Possible values: 1 . . 5 (default setting: 5).

SSH Timeout

Display the SSH timeout in minutes.

Possible values: 1 . . 160 (default setting: 5).

6.1.38 show radius

This command is used to display the various RADIUS configuration items for the switch as well as the configured RADIUS servers. If the optional token 'servers' is not included, the following RADIUS configuration items will be displayed.

Format

```
show radius [servers]
```

Mode

Privileged EXEC and User EXEC

Primary Server IP Address

Indicates the configured server currently in use for authentication

Number of configured servers

The configured IP address of the authentication server

Max number of retransmits

The configured value of the maximum number of times a request packet is retransmitted

Timeout Duration

The configured timeout value, in seconds, for request re-transmissions

Accounting Mode

Yes or No

If the optional token 'servers' is included, the following information regarding the configured RADIUS servers is displayed.

IP Address

IP Address of the configured RADIUS server

Port

The port in use by this server

Type

Primary or secondary

Secret Configured

Yes / No

6.1.39 show radius statistics

This command is used to display the statistics for RADIUS or configured server . To show the configured RADIUS server statistic, the IP Address specified must match that of a previously configured RADIUS server. On execution, the following fields are displayed.

Format

```
show radius statistics [ipaddr]
```

Mode

Privileged EXEC and User EXEC

If ip address is not specified than only Invalid Server Address field is displayed. Otherwise other listed fields are displayed.

Invalid Server Addresses

The number of RADIUS Access-Response packets received from unknown addresses.

Server IP Address

Round Trip Time

The time interval, in hundredths of a second, between the most recent Access-Reply | Access-Challenge and the Access-Request that matched it from the RADIUS authentication server.

Access Requests

The number of RADIUS Access-Request packets sent to this server. This number does not include retransmissions.

Access Retransmission

The number of RADIUS Access-Request packets retransmitted to this RADIUS authentication server.

Access Accepts

The number of RADIUS Access-Accept packets, including both valid and invalid packets, which were received from this server.

Access Rejects

The number of RADIUS Access-Reject packets, including both valid and invalid packets, which were received from this server.

Access Challenges

The number of RADIUS Access-Challenge packets, including both valid and invalid packets, which were received from this server.

Malformed Access Responses

The number of malformed RADIUS Access-Response packets received from this server. Malformed packets include packets with an invalid length. Bad authenticators or signature attributes or unknown types are not included as malformed access responses.

Bad Authenticators

The number of RADIUS Access-Response packets containing invalid authenticators or signature attributes received from this server.

Pending Requests

The number of RADIUS Access-Request packets destined for this server that have not yet timed out or received a response.

Timeouts

The number of authentication timeouts to this server.

Unknown Types

The number of RADIUS packets of unknown types, which were received from this server on the authentication port.

Packets Dropped

The number of RADIUS packets received from this server on the authentication port and dropped for some other reason.

6.1.40 show users authentication

This command displays all user and all authentication login information. It also displays the authentication login list assigned to the default user.

Format

```
show users authentication
```

Mode

Privileged EXEC

User

This field lists every user that has an authentication login list assigned.

System Login

This field displays the authentication login list assigned to the user for system login.

802.1x Port Security

This field displays the authentication login list assigned to the user for 802.1X port security.

6.1.41 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 575.

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)

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 Routing Commands

This chapter provides a detailed explanation of the Routing commands.

8.1 ARP Commands

This chapter provides a detailed explanation of the Address Resolution Protocol (ARP) commands. The commands are divided by functionality into the following different groups:

- ▶ Show commands are used to display switch 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.
- ▶ Copy commands are used to transfer configuration and informational files to and from the switch.

8.1.1 arp

This command creates an ARP entry. The value for *<ipaddress>* is the IP address of a device on a subnet attached to an existing routing interface. *<macaddr>* is a unicast MAC address for that device.

The format is 6 two-digit hexadecimal numbers that are separated by colons, for example 00:06:29:32:81:40.

Format

```
arp <ipaddress> <macaddr>
```

Mode

Global Config

■ no arp

This command deletes an ARP entry. The value for *<arpentry>* is the IP address of the interface. The value for *<ipaddress>* is the IP address of a device on a subnet attached to an existing routing interface. *<macaddr>* is a unicast MAC address for that device.

Format

```
no arp <ipaddress> <macaddr>
```

Mode

Global Config

8.1.2 ip proxy-arp

This command enables proxy ARP on a router interface.

Without proxy ARP, a device only responds to an ARP request if the target IP address is an address configured on the interface where the ARP request arrived. With proxy ARP, the device may also respond if the target IP address is reachable. The device only responds if all next hops in its route to the destination are through interfaces other than the interface that received the ARP request.

Default

```
enabled
```

Format

```
ip proxy-arp
```

Mode

```
Interface Config
```

■ no ip proxy-arp

This command disables proxy ARP on a router interface.

Format

```
no ip proxy-arp
```

Mode

```
Interface Config
```

8.1.3 arp cachesize

This command configures the ARP cache size.

Format

```
arp cachesize <288-2048>
```

Mode

Global Config

■ no arp cachesize

This command configures the default ARP cache size which is 2048.

Format

```
no arp cachesize
```

Mode

Global Config

8.1.4 arp dynamicrenew

This command enables ARP component to automatically renew ARP entries of type dynamic when they age out.

Format

```
arp dynamicrenew
```

Mode

```
Global Config
```

■ no arp dynamicrenew

This command disables ARP component from automatically renewing ARP entries of type dynamic when they age out.

Format

```
no arp dynamicrenew
```

Mode

```
Global Config
```

8.1.5 arp purge

This command causes the specified IP address to be removed from the ARP cache. Only entries of type dynamic or gateway are affected by this command.

Format

```
arp purge <ipaddr>
```

Mode

```
Privileged EXEC
```

8.1.6 arp resptime

This command configures the ARP request response timeout.

The value for *<seconds>* is a valid positive integer, which represents the IP ARP entry response timeout time in seconds.

The range for *<seconds>* is 1..10 seconds.

Default

1

Format

```
arp resptime <1-10>
```

Mode

Global Config

■ no arp resptime

This command configures the default ARP request response timeout.

Format

```
no arp resptime
```

Mode

Global Config

8.1.7 arp retries

This command configures the ARP count of maximum requests for retries.

The value for *<retries>* is an integer, which represents the maximum number of requests for retries.

The range for *<retries>* is an integer between 0..10 retries.

Default

4

Format

```
arp retries <0-10>
```

Mode

Global Config

■ no arp retries

This command configures the default ARP count of maximum requests for retries.

Format

```
no arp retries
```

Mode

Global Config

8.1.8 arp selective-learning

This command enables selective learning of ARPs. Normally, the router learns ARP entries from every ARP request it sees. With this feature enabled it will learn only from ARP requests that ask for one of its own interfaces.

Default

Disabled

Format

```
arp selective-learning
```

Mode

Global Config

■ no arp selective-learning

This command disables selective learning of ARPs

Format

```
no arp selective-learning
```

Mode

Global Config

8.1.9 arp timeout

This command configures the ARP entry ageout time.

The value for *<seconds>* is a valid positive integer, which represents the IP ARP entry ageout time in seconds.

The range for *<seconds>* is between 15..21600 seconds.

Default

1200

Format

```
arp timeout <15-21600>
```

Mode

Global Config

■ no arp timeout

This command configures the default ARP entry ageout time.

Format

```
no arp timeout
```

Mode

Global Config

8.1.10 clear arp-cache

This command causes all ARP entries of type dynamic to be removed from the ARP cache. If the *gateway* parameter is specified, the dynamic entries of type gateway are purged as well.

Format

```
clear arp-cache [gateway]
```

Mode

Privileged EXEC

8.1.11 show arp

This command displays the Address Resolution Protocol (ARP) cache. The displayed results are not the total ARP entries. To view the total ARP entries, the operator should view the `show arp` results in conjunction with the `show arp switch` results.

Format

```
show arp
```

Mode

```
Privileged EXEC
```

Age Time (seconds)

Is the time it takes for an ARP entry to age out. This value was configured into the unit. Age time is measured in seconds.

Response Time (seconds)

Is the time it takes for an ARP request timeout. This value was configured into the unit. Response time is measured in seconds.

Retries

Is the maximum number of times an ARP request is retried. This value was configured into the unit.

Cache Size

Is the maximum number of entries in the ARP table. This value was configured into the unit.

Dynamic Renew Mode

Displays whether the ARP component automatically attempts to renew dynamic ARP entries when they age out.

Selective Learning Mode

Shows whether the router learns from all ARP requests (Disabled) or only from those targeted to one of its own interfaces (Enabled).

Total Entry Count Current / Peak

Field listing the total entries in the ARP table and the peak entry count in the ARP table.

Static Entry Count Current / Max

Field listing the static entry count in the ARP table and maximum static entry count in the ARP table.

The following are displayed for each ARP entry.

IP Address

Is the IP address of a device on a subnet attached to an existing routing interface.

MAC Address

Is the hardware MAC address of that device.

Interface

Is the routing slot/port associated with the device ARP entry.

Type

Is the type that was configured into the unit. The possible values are Local, Gateway, Dynamic and Static.

Age

This field displays the current age of the ARP entry since last refresh (in hh:mm:ss format)

8.1.12 show arp brief

This command displays the brief Address Resolution Protocol (ARP) table information.

Format

```
show arp brief
```

Mode

Privileged EXEC

Age Time (seconds)

Is the time it takes for an ARP entry to age out. This value was configured into the unit. Age time is measured in seconds.

Response Time (seconds)

Is the time it takes for an ARP request timeout. This value was configured into the unit. Response time is measured in seconds.

Retries

Is the maximum number of times an ARP request is retried. This value was configured into the unit.

Cache Size

Is the maximum number of entries in the ARP table. This value was configured into the unit.

Dynamic Renew Mode

Displays whether the ARP component automatically attempts to renew dynamic ARP entries when they age out.

Selective Learning Mode

Shows whether the router learns from all ARP requests (Disabled) or only from those targeted to one of its own interfaces (Enabled).

Total Entry Count Current / Peak

Field listing the total entries in the ARP table and the peak entry count in the ARP table.

Static Entry Count Current / Max

Field listing the static entry count in the ARP table and maximum static entry count in the ARP table.

8.1.13 show arp switch

This command displays connectivity between the switch and other devices. The Address Resolution Protocol (ARP) cache identifies the MAC addresses of the IP stations communicating with the switch.

Format

```
show arp switch
```

Mode

```
Privileged EXEC
```

MAC Address

A unicast MAC address for which the switch has forwarding and/or filtering information. The format is 6 two-digit hexadecimal numbers that are separated by colons, for

```
example 01:23:45:67:89:AB
```

IP Address

The IP address assigned to each interface.

Interface

Valid slot and port number separated by forward slashes.

8.2 IP Routing

This chapter provides a detailed explanation of the IP Routing commands. The commands are divided by functionality into the following different groups:

- ▶ Show commands are used to display switch 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.

Note: Shared VLAN learning and routing are mutually exclusive. Make sure that shared VLAN learning is disabled before using IP routing (see [“bridge vlan-learning”](#) on page 122).

8.2.1 routing

This command enables routing for an interface.

The current value for this function is displayed under "show ip interface" labeled as "Routing Mode".

Default

```
disabled
```

Format

```
routing
```

Mode

```
Interface Config
```

■ no routing

This command disables routing for an interface.

The current value for this function is displayed under "show ip interface" labeled as "Routing Mode".

Format

```
no routing
```

Mode

```
Interface Config
```

8.2.2 ip routing

This command enables the IP Router Admin Mode for the master switch.

Format

```
ip routing
```

Mode

```
Global Config
```

■ no ip routing

This command disables the IP Router Admin Mode for the master switch.

Format

```
no ip routing
```

Mode

```
Global Config
```

8.2.3 ip address

This command configures an IP address on an interface. The IP address may be a secondary IP address.

The value for *<ipaddr>* is the IP Address of the interface.

The value for *<subnetmask>* is a 4-digit dotted-decimal number which represents the subnet mask of the interface. This changes the label IP address in `show ip interface`.

Format

```
ip address <ipaddr> <subnetmask> [secondary]
```

Mode

```
Interface Config
```

■ no ip address

This command deletes an IP address from an interface.

The value for *<ipaddr>* is the IP Address of the interface.

The value for *<subnetmask>* is a 4-digit dotted-decimal number which represents the Subnet Mask of the interface.

Format

```
no ip address <ipaddr> <subnetmask> [secondary]
```

Mode

```
Interface Config
```

8.2.4 ip mtu

This command configures the MTU size (maximum transfer unit) for IP protocol on the specified interface.

The value for `<68-9000>` is the MTU value for IP protocol.

Default

1500

Format

```
ip mtu <68-9000>
```

Mode

Interface Config

■ no ip mtu

This command sets the MTU size (maximum transfer unit) for IP protocol on the specified interface to the default value (1500).

Format

```
no ip mtu
```

Mode

Interface Config

8.2.5 ip netdirbroadcast

This command enables net directed broadcasts of IP frames.
Use no command to disable.

The current value for this function is displayed under "show ip interface" labeled as "Forward Net Directed Broadcasts".

Default

```
disabled
```

Format

```
ip netdirbroadcast
```

Mode

```
Interface Config
```

■ no ip netdirbroadcast

This command disables net directed broadcasts of IP frames.

The current value for this function is displayed under "show ip interface" labeled as "Forward Net Directed Broadcasts".

Format

```
no ip netdirbroadcast
```

Mode

```
Interface Config
```

8.2.6 ip route

This command configures a static route. The `<ip_addr>` is a valid ip address. The `<subnet_mask>` is a valid subnet mask. The `<nextHopRtr>` is a valid IP address of the next hop router.

The `<preference>` is an integer value from 1 to 255. The user can specify the preference value (sometimes called "administrative distance") of an individual static route. Among routes to the same destination, the route with the lowest preference value is the route entered into the forwarding database. By specifying the preference of a static route, the user controls whether a static route is more or less preferred than routes from dynamic routing protocols. The preference also controls whether a static route is more or less preferred than other static routes to the same destination.

The value 255 stands for „unreachable“. This means that the appropriate route is never entered into the forwarding database.

If the optional parameter `<track>` and a tracking id are given, the route is removed from the routing table if the tracking instance is down. When the tracking instance comes up, the route is added to the route table again.

Note: The following must be present before the static routes are visible:

- ▶ Enable ip routing globally.
- ▶ Enable ip routing for the interface.
- ▶ The associated link must also be up.

To see all configured static routes use the command `show ip route static`.

Default

```
preference - 1
```

Format

```
ip route <ip_addr> <subnet_mask> <nextHopRtr> [<preference>] [track<trackid>]
```

Mode

```
Global Config
```

■ no ip route

This command deletes all next hops to a destination static route. If the optional `<nextHopRtr>` parameter is designated, the next hop is deleted and if the optional preference value is designated, the preference value of the static route is reset to its default.

If the optional parameter `<track>` is given, tracking is disabled for this nextHop.

Format

```
no ip route <ip_addr> <subnet_mask> [{<nextHopRtr>
  [track] | <preference>}]
```

Mode

Global Config

8.2.7 ip route default

This command configures the default route. The value for *<nextHopRtr>* is a valid IP address of the next hop router. The *<preference>* is an integer value from 1 to 255.

If the optional parameter *<track>* and a tracking id are given, the route is removed from the routing table if the tracking instance is down. When the tracking instance comes up, the route is added to the route table again.

Default

```
preference - 1
```

Format

```
ip route default <nextHopRtr> [<preference>]  
[track<trackid>]
```

Mode

```
Global Config
```

■ no ip route default

This command deletes all configured default routes. If the optional *<nextHopRtr>* parameter is designated, the specific next hop is deleted from the configured default route and if the optional preference value is designated, the preference of the configured default route is reset to its default.

If the optional parameter *<track>* is given, tracking is disabled for this nextHop.

Format

```
no ip route default [{<nextHopRtr> [track]  
| <preference>}]
```

Mode

```
Global Config
```

8.2.8 ip route distance

This command sets the default distance for static routes. Lower route preference values are preferred when determining the best route. The `ip route` and `ip route default` commands allow you to optionally set the distance of an individual static route. The default distance is used when no distance is specified in these commands. Changing the default distance does not update the distance of existing static routes, even if they were assigned the original default distance. The new default distance will only be applied to static routes created after invoking the `ip route distance` command.

The value 255 stands for „unreachable“. This means that the appropriate route is never entered into the forwarding database.

Default

1

Format

```
ip route distance <1-255>
```

Mode

Global Config

■ no ip route distance

This command sets the default static route preference value in the router. Lower route preference values are preferred when determining the best route.

Format

```
no ip route distance
```

Mode

Global Config

8.2.9 ip forwarding

This command enables forwarding of IP frames.

Default

enabled

Format

ip forwarding

Mode

Global Config

■ no ip forwarding

This command disables forwarding of IP frames.

Format

no ip forwarding

Mode

Global Config

8.2.10 ip vlan-single-mac

PowerMICE and MACH4000 without MACH4002-24G.../MACH4002-48G...: In normal operating mode, packets that routed over VLAN router interfaces, are not sent with the VLAN router interface's MAC address as the source MAC address but with the physical port's MAC Address. This is compliant with the standard. Some terminal devices with incorrect IP implementation may have problems with that situation, resulting in them being unreachable via a VLAN router interface. For that reason, the SW Release 02.0.02 introduces the feature "Single MAC Mode". In this mode, all VLAN interfaces and all physical ports (except the port based router interfaces) use the same MAC address.

Default

```
enabled
```

Format

```
ip vlan-single-mac
```

Mode

```
Global Config
```

■ no ip vlan-single-mac

This command disables VLAN Single Mac Address Mode.

Format

```
no ip vlan-single-mode
```

Mode

```
Global Config
```

8.2.11 show ip brief

This command displays all the summary information of the IP. This command takes no options.

Format

```
show ip brief
```

Modes

```
Privileged EXEC
```

```
User EXEC
```

Default Time to Live

The computed TTL (Time to Live) of forwarding a packet from the local router to the final destination.

Routing Mode

Shows whether the routing mode is enabled or disabled.

IP Forwarding Mode

Shows whether forwarding of IP frames is enabled or disabled. This is a configured value.

Maximum Next Hops

The maximum number of next hops which can be used for a given destination.

Vlan Single Mac Address Mode

Shows if the Vlan Single Mac Address Mode is enabled or disabled.

Note: This output is available for the MACH4002-48+4G and PowerMICE devices.

ARP-Entries

Unicast Routes

Multicast Routes

Shows the current and configured sizes of the tables for ARP entries, unicast routes and multicast routes. The configured values become active if they are saved locally and the switch is rebooted.

Note: This output is available for the MACH4002-24G... and MACH4002-48G... devices.

8.2.12 ip table-sizes

Note: This command is available for the MACH4002-24G... and MACH4002-48G... devices.

Sets the size of various routing table sizes. The values can be changed but won't have any effect on the switch until they are saved locally and the switch is rebooted.

Default

```
2228 arp entries (2048 + interfaces)
1860 unicast routes
512 multicast routes
```

Format

```
ip table-sizes <number>
```

Mode

```
Global Config
```

■ no ip table-sizes

Resets the sizes of the routing tables to their default values.

Default

```
2228 arp entries (2048 + interfaces)
1860 unicast routes
512 multicast routes
```

Format

```
no ip table-sizes
```

Mode

```
Global Config
```

8.2.13 ip table-sizes arp-entries

Note: This command is available for the MACH 4002-24G... and MACH 4002-48G... devices.

This command sets the size of the arp table. Number is a positive integer value describing the maximum number of ARP entries the tables can hold.

Default

2228

Format

```
ip table-sizes arp-entries <number>
```

Mode

Global Config

■ no ip table-sizes arp-entries

This command resets the size of the arp table to its default value.

Default

2228

Format

```
no ip table-sizes arp-entries
```

Mode

Global Config

8.2.14 ip table-sizes unicast-routes

Note: This command is available for the MACH 4002-24G... and MACH 4002-48G... devices.

This command sets the size of the unicast routing table. Number is a positive integer value describing the maximum number of unicast routes the tables can hold.

Default

1860

Format

```
ip table-sizes unicast-routes <number>
```

Mode

Global Config

■ no ip table-sizes unicast-routes

This command resets the size of the unicast routing table to its default value.

Default

1860

Format

```
no ip table-sizes unicast-routes
```

Mode

Global Config

8.2.15 ip table-sizes multicast-routes

Note: This command is available for the MACH 4002-24G... and MACH 4002-48G... devices.

This command sets the size of the multicast routing table. Number is a positive integer value describing the maximum number of multicast routes the tables can hold.

Default

```
512
```

Format

```
ip table-sizes multicast-routes <number>
```

Mode

```
Global Config
```

■ no ip table-sizes multicast-routes

This command resets the size of the unicast routing table to its default value.

Default

```
512
```

Format

```
no ip table-sizes multicast-routes
```

Mode

```
Global Config
```

8.2.16 show ip interface

This command displays all pertinent information about the IP interface.

Format

```
show ip interface <slot/port>
```

Modes

Privileged EXEC

User EXEC

Primary IP Address

Is an IP address representing the subnet configuration of the router interface. This value was configured into the unit.

Subnet Mask

Is a mask of the network and host portion of the IP address for the router interface. This value was configured into the unit.

Secondary IP Address

The secondary ip addresses of the router interface in case of multinetting.

Routing Mode

Is the administrative mode of router interface participation. The possible values are enable or disable. This value was configured into the unit.

Administrative Mode

Is the administrative mode of the specified interface. The possible values of this field are enable or disable. This value was configured into the unit.

Forward Net Directed Broadcasts

Indicates if IP forwards net-directed broadcasts on this interface. Possible values are Enable or Disable.

Proxy ARP

Shows if the Proxy ARP is enabled or disabled on this router interface.

Active State

Displays whether the interface is active or inactive. An interface is considered active if its link is up and it is in forwarding state.

Link Speed Data Rate

Is an integer representing the physical link data rate of the specified interface. This is measured in Megabits per second (Mbps).

MAC Address

Is the burned in physical address of the specified interface. The format is 6 two-digit hexadecimal numbers that are separated by colons.

Encapsulation Type

Is the encapsulation type for the specified interface. The types are: Ethernet or SNAP.

IP MTU

The maximum transfer unit for the specified interface.

8.2.17 show ip interface brief

This command displays summary information about IP configuration settings for all ports in the router. This command takes no options.

Format

```
show ip interface brief
```

Modes

```
Privileged EXEC
```

```
User EXEC
```

Interface

Valid slot and port number separated by forward slashes.

IP Address

The IP address of the routing interface in 32-bit dotted decimal format.

IP Mask

The IP mask of the routing interface in 32-bit dotted decimal format.

Netdir Bcast

Indicates if IP forwards net-directed broadcasts on this interface. Possible values are Enable or Disable.

MultiCast Fwd

Indicates the multicast forwarding operational mode on the interface. Possible values are Enable or Disable.

8.2.18 show ip route

This command displays the entire route table. This command takes no options.

Format

```
show ip route
```

Mode

Privileged EXEC

Network Address

Is an IP address identifying the network on the specified interface.

Subnet Mask

Is a mask of the network and host portion of the IP address for the router interface.

Protocol

Tells which protocol added the specified route. The possibilities are: local, static, OSPF or RIP.

Total Number of Routes

The total number of routes.

For each Next Hop

Next Hop Intf

The outgoing router interface to use when forwarding traffic to the next destination.

Next Hop IP Address

The outgoing router IP address to use when forwarding traffic to the next router (if any) in the path toward the destination.

8.2.19 show ip route bestroutes

This command causes the entire route table to be displayed. This command takes no options.

Format

```
show ip route bestroutes
```

Mode

Privileged EXEC

Network Address

Is an IP route prefix for the destination.

Subnet Mask

Is a mask of the network and host portion of the IP address for the specified interface.

Protocol

Tells which protocol added the specified route. The possibilities are: local, static, OSPF or RIP.

Total Number of Routes

The total number of routes in the route table.

For each Next Hop

Next Hop Intf

The outgoing router interface to use when forwarding traffic to the next destination.

Next Hop IP Address

The outgoing router IP address to use when forwarding traffic to the next router (if any) in the path toward the destination. The next router will always be one of the adjacent neighbors or the IP address of the local interface for a directly attached network.

8.2.20 show ip route entry

This command displays the entire route table.

Format

```
show ip route entry
```

Mode

Privileged EXEC

Network Address

Is a valid network address identifying the network on the specified interface.

Subnet Mask

Is a mask of the network and host portion of the IP address for the attached network.

Protocol

Tells which protocol added the specified route. The possibilities are: local, static, OSPF or RIP.

For each Next Hop

Next Hop Interface

The outgoing router interface to use when forwarding traffic to the next destination.

Next Hop IP Address

The outgoing router IP address to use when forwarding traffic to the next router (if any) in the path toward the destination.

Metric

The cost associated with this route.

Preference

The administrative distance associated with this route.

8.2.21 show ip route preferences

This command displays detailed information about the route preferences. Route preferences are used in determining the best route. Lower router preference values are preferred over higher router preference values.

Format

```
show ip route preferences
```

Modes

Privileged EXEC

User EXEC

Local

This field displays the local route preference value.

Static

This field displays the static route preference value.

OSPF Intra

This field displays the OSPF Intra route preference value.

OSPF Inter

This field displays the OSPF Inter route preference value.

OSPF Ext T1

This field displays the OSPF Type-1 route preference value.

OSPF Ext T2

This field displays the OSPF Type-2 route preference value.

RIP

This field displays the RIP route preference value.

8.2.22 show ip route static

This command displays the entire static route table.

Format

```
show ip route static
```

Mode

Privileged EXEC

Network Address

Is a valid network address identifying the network on the specified interface.

Subnet Mask

Is a mask of the network and host portion of the IP address for the attached network.

For each Next Hop

Pref

The administrative distance associated with this route.

Next Hop IP Address

The outgoing router IP address to use when forwarding traffic to the next router in the path toward the destination.

Intf.

The outgoing router interface to use when forwarding traffic to the next destination. This is only shown if there is a working router interface with a subnet matching the next hop ip address.

Track ID

The id of the tracked object (if any).

Track State

The state of the tracked object (up or down) if the route uses tracking.

8.2.23 show ip stats

This command displays IP statistical information. Refer to RFC 1213 for more information about the fields that are displayed.

Format

```
show ip stats
```

Modes

```
Privileged EXEC
```

```
User EXEC
```

Received on routing interfaces:

IpInReceives

Display the total number of input datagrams.

Received by CPU:

IpInHdrErrors

Display the number of input datagrams discarded due to errors in their IP headers.

IpInAddrErrors

Display the number of input datagrams discarded because the IP address in their IP header's destination field was not a valid.

Routed by the device:

IpForwDatagrams

Display number of input datagrams for which this entity was not their final IP destination, as a result of which an attempt was made to find a route to forward them to that final destination. In entities which do not act as IP Gateways, this counter will include only those packets which were Source-Routed via this entity, and the Source-Route option processing was successful.

Received by CPU:**IpInUnknownProtos**

Display number of locally-addressed datagrams received successfully but discarded because of an unknown or unsupported protocol.

IpInDiscards

Display the The number of input IP datagrams for which no problems were encountered to prevent their continued processing, but which were discarded (e.g., for lack of buffer space).

Note that this counter does not include any datagrams discarded while awaiting re-assembly.

IpInDelivers

Display the total number of input datagrams successfully delivered to IP user-protocols (including ICMP).

IpOutRequests

Display the total number of IP datagrams which local IP user-protocols (including ICMP) supplied to IP in requests for transmission.

Note that this counter does not include any datagrams counted in ipForwDatagrams.

IpOutDiscards

Display the number of output IP datagrams for which no problem was encountered to prevent their transmission to their destination, but which were discarded (e.g., for lack of buffer space).

Note that this counter would include datagrams counted in ipForwDatagrams if any such packets met this (discretionary) discard criterion.

IpOutNoRoutes

Display the number of IP datagrams discarded because no route could be found to transmit them to their destination.

Note that this counter includes any packets counted in ipForwDatagrams which meet this 'no-route' criterion.

Note that this includes any datagrams which a host cannot route because all of its default gateways are down.

Reassembly/fragmentation (not supported):**IpReasmTimeout**

Display the maximum number of seconds which received fragments are held while they are awaiting reassembly at this entity.

IpReasmReqds

Display the number of IP fragments received which needed to be reassembled at this entity.

IpReasmOKs

Display the number of IP datagrams successfully re-assembled.

IpReasmFails

Display the number of failures detected by the IP re-assembly algorithm (for whatever reason: timed out, errors, etc).

Note that this is not necessarily a count of discarded IP fragments since some algorithms (notably the algorithm in RFC 815) can lose track of the number of fragments by combining them as they are received.

IpFragOKs

Display the number of IP datagrams that have been successfully fragmented at this entity.

Received by CPU:**IpFragFails**

Display the number of IP datagrams that have been discarded because they needed to be fragmented at this entity but could not be, e.g., because their Don't Fragment flag was set.

IpFragCreates

Display the number of IP datagram fragments that have been generated as a result of fragmentation at this entity.

Faulty packets:**IpRoutingDiscards**

Display the number of routing entries which were chosen to be discarded even though they are valid. One possible reason for discard-

ing such an entry could be to free-up buffer space for other routing entries.

Received / sent by CPU:

IcmlnMsgs

Display the total number of ICMP messages which the entity received.

Note that this counter includes all those counted by `icmlnErrors`.

IcmlnErrors

Display the number of ICMP messages which the entity received but determined as having ICMP-specific errors (bad ICMP checksums, bad length, etc.).

IcmlnDestUnreachs

Display the number of ICMP Destination Unreachable messages received.

IcmlnTimeExcds

Display the number of ICMP Time Exceeded messages received.

IcmlnParmProbs

Display the number of ICMP Parameter Problem messages received.

IcmlnSrcQuenchs

Display the number of ICMP Source Quench messages received.

IcmlnRedirects

Display the number of ICMP Redirect messages received.

IcmlnEchos

Display the number of ICMP Echo (request) messages received.

IcmlnEchoReps

Display the number of ICMP Echo (request) messages received.

IcmlnTimestamps

Display the number of ICMP Timestamp (request) messages received.

IcmlnTimestampReps

Display the number of ICMP Timestamp Reply messages received.

IcmpInAddrMasks

Display the number of ICMP Address Mask Request messages received.

IcmpInAddrMaskReps

Display the number of ICMP Address Mask Reply messages received.

IcmpOutMsgs

Display the total number of ICMP messages which this entity attempted to send.

Note that this counter includes all those counted by icmpOutErrors.

IcmpOutErrors

Display the number of ICMP messages which this entity did not send due to problems discovered within ICMP such as a lack of buffers. This value should not include errors discovered outside the ICMP layer such as the inability of IP to route the resultant datagram. In some implementations there may be no types of error which contribute to this counter's value.

IcmpOutDestUnreachs

Display the number of ICMP Destination Unreachable messages sent.

IcmpOutTimeExcds

Display the number of ICMP Time Exceeded messages sent.

IcmpOutParmProbs

Display the number of ICMP Parameter Problem messages sent.

IcmpOutSrcQuenchs

Display the number of ICMP Source Quench messages sent.

IcmpOutRedirects

Display the number of ICMP Redirect messages sent. For a host, this object will always be zero, since hosts do not send redirects.

IcmpOutEchoReps

Display the number of ICMP Echo Reply messages sent.

IcmpOutTimestamps

Display the number of ICMP Timestamp (request) messages sent.

IcmpOutTimestampReps

Display the number of ICMP Timestamp Reply messages sent.

IcmpOutAddrMasks

Display the number of ICMP Address Mask Request messages sent.

IcmpOutAddrMaskReps

Display the number of ICMP Address Mask Reply messages sent.

Outgoing ICMP packets dropped by limiter

Display the number of outgoing ICMP packets dropped by limiter.

8.3 Router Discovery Protocol Commands

This chapter provides a detailed explanation of the Router Discovery commands. The commands are divided by functionality into the following different groups:

- ▶ Show commands are used to display switch 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.
- ▶ Copy commands are used to transfer configuration and informational files to and from the switch.

8.3.1 ip irdp

This command enables Router Discovery on an interface.

Default

disabled

Format

ip irdp

Mode

Interface Config

■ no ip irdp

This command disables Router Discovery on an interface.

Format

no ip irdp

Mode

Interface Config

8.3.2 ip irdp address

This command configures the address to be used to advertise the router for the interface. The valid values for *ipaddr* are 224.0.0.1 and 255.255.255.255.

Default

```
224.0.0.1
```

Format

```
ip irdp address <ipaddr>
```

Mode

```
Interface Config
```

■ no ip irdp address

This command configures the default address to be used to advertise the router for the interface.

Format

```
no ip irdp address
```

Mode

```
Interface Config
```

8.3.3 ip irdp holdtime

This command configures the value, in seconds, of the holdtime field of the router advertisement sent from this interface.

The range is the `maxadvertinterval` to 9000 seconds.

Default

```
3 * maxinterval
```

Format

```
ip irdp holdtime <maxadvertinterval-9000>
```

Mode

```
Interface Config
```

■ no ip irdp holdtime

This command configures the default value, in seconds, of the holdtime field of the router advertisement sent from this interface.

Format

```
no ip irdp holdtime
```

Mode

```
Interface Config
```

8.3.4 ip irdp maxadvertinterval

This command configures the maximum time, in seconds, allowed between sending router advertisements from the interface.

The range for maxadvertinterval is 4 to 1800 seconds.

Default

600

Format

```
ip irdp maxadvertinterval <4-1800>
```

Mode

Interface Config

■ no ip irdp maxadvertinterval

This command configures the default maximum time, in seconds.

Format

```
no ip irdp maxadvertinterval
```

Mode

Interface Config

8.3.5 ip irdp minadvertinterval

This command configures the minimum time, in seconds, allowed between sending router advertisements from the interface.

The range for `minadvertinterval` is 3 to the value of `maxadvertinterval`.

Default

`0.75 * maxadvertinterval`

Format

`ip irdp minadvertinterval <3-maxadvertinterval>`

Mode

Interface Config

■ no ip irdp minadvertinterval

This command sets the default minimum time to the default.

Format

`no ip irdp minadvertinterval`

Mode

Interface Config

8.3.6 ip irdp preference

This command configures the preferability of the address as a default router address, relative to other router addresses on the same subnet. The range is -2147483648 to -1 to 0 to 1 to 2147483647.

Default

0

Format

```
ip irdp preference <-2147483648-2147483647>
```

Mode

Interface Config

■ no ip irdp preference

This command configures the default preferability of the address as a default router address, relative to other router addresses on the same subnet.

Format

```
no ip irdp preference
```

Mode

Interface Config

8.3.7 show ip irdp

This command displays the router discovery information for all interfaces, or a specified interface.

Format

```
show ip irdp {<slot/port> | all}
```

Modes

Privileged EXEC

User EXEC

Ad Mode

Displays the advertise mode which indicates whether router discovery is enabled or disabled on this interface.

Advertise Address

Displays the address which is used to advertise the router on this interface.

Max Int

Displays the maximum advertise interval which is the maximum time allowed between sending router advertisements from the interface in seconds.

Min Int

Displays the minimum advertise interval which is the minimum time allowed between sending router advertisements from the interface in seconds.

Hold Time

Displays advertise lifetime which is the value of the lifetime field of the router advertisement sent from the interface in seconds.

Preferences

Displays the preference of the address as a default router address, relative to other router addresses on the same subnet.

8.4 Virtual LAN Routing Commands

This chapter provides a detailed explanation of the Virtual LAN Routing commands. The commands are divided by functionality into the following different groups:

- ▶ Show commands are used to display switch 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.
- ▶ Copy commands are used to transfer configuration and informational files to and from the switch.

8.4.1 vlan routing

This command creates routing on a VLAN. The *<vlanid>* value has a range from 1 to 4042. Submitting this command creates a new logical interface 9/x.

Format

```
vlan routing <vlanid>
```

Mode

VLAN Database

■ no vlan routing

This command deletes routing on a VLAN. The *<vlanid>* value has a range from 1 to 4042. Submitting this command deletes the logical interface 9/x.

Format

```
no vlan routing <vlanid>
```

Mode

VLAN Database

8.4.2 show ip vlan

This command displays the VLAN routing information for all VLANs with routing enabled in the system.

Format

```
show ip vlan
```

Modes

Privileged EXEC

User EXEC

VLAN ID

Is the identifier of the VLAN.

Logical Interface

Indicates the logical slot/port associated with the VLAN routing interface.

IP Address

Displays the IP Address associated with this VLAN.

Subnet Mask

Indicates the subnet mask that is associated with this VLAN.

MAC Address

Displays the MAC Address associated with this VLAN.

8.5 Tracking Commands

This chapter provides a detailed explanation of the Tracking commands. The commands are divided by functionality into the following different groups:

- ▶ Show commands are used to display tracking information.
- ▶ Configuration Commands are used to configure the tracking function.

8.5.1 track interface

Connects a trackid to an interface to monitor. The trackid is an integer value from 1 to 128 (L3P: 256). Link-up-delay and link-down-delay can be configured from 0 to 255 seconds. If a delay parameter is omitted, the default delay is 0.

Format

```
track <trackid> interface <slot/port>
[link-up-delay <0-255>] [link-down-delay <0-255>]
```

Mode

Global Config

■ no track

Frees a <trackid> and track object and end tracking for this object. The <trackid> is an integer value from 1 to 128 (L3P: 256) and the id of an existing track object.

Format

```
no track <trackid>
```

Mode

Global Config

8.5.2 track logical

Combines up to eight tracking instances into one single instance using a logical operation (AND or OR). The trackids are integer values from 1 to 128 (L3P: 256).

Format

```
track <trackid> logical {and|or} <trackid1>
[<trackid2> [ ... [<trackid8>...]]
```

Mode

Global Config

8.5.3 track mode

Enables a track object. The trackid is an integer value from 1 to 128 (L3P:256) and the id of an existing track object.

Format

```
track <trackid> mode
```

Mode

Global Config

■ no track mode

Disables a track object. The trackid is an integer value from 1 to 128 (L3P:256) and the id of an existing track object. A disabled track object is defined to be up regardless of the state of the monitored object.

Format

```
no track <trackid> mode
```

Mode

Global Config

8.5.4 track ping

Enables tracking of a remote ip host or router by sending ICMP echo requests (ping). The trackid is an integer value from 1 to 128 (L3P: 256). The timeout is given in milliseconds. If `<miss>` consecutive answers are not received, the object switches to `down`, if `<success>` consecutive answers are received, the object switches to `up`. If interface is set to `auto`, the best route is used automatically.

The parameters can be omitted, but those given must be in the order shown below.

Note: To enable the ping to be sent via the interface, make sure that it concerns a routing interface.

Format

```
track <trackid> ping <remote-ip>
<interface {<slot/port> | auto}>
[interval <1-10>] [miss <1-10>]
[success <1-10>] [timeout <10-10000>]
```

Defaults

```
Interface: auto
Interval: 1 second
Miss: 3
Success: 2
Timeout: 100 milliseconds
```

Mode

```
Global Config
```

8.5.5 track trap

Enables sending of a state change trap for a track object. The <trackid> is an integer value from 1 to 128 (L3P:256) and the id of an existing track object.

Format

```
track <trackid> trap
```

Mode

```
Global Config
```

■ no track trap

Disables sending of the state change trap for a track object. The <trackid> is an integer value from 1 to 128 (L3P:256) and the id of an existing track object.

Format

```
no track <trackid> trap
```

Mode

```
Global Config
```

8.5.6 show track

Displays information about all configured track objects.

Depending on the configuration, up to five tables are shown. There are separate tables for each tracking type (interface, logical, ping) and one for instances that do not yet have a valid type.

Additionally, a list of unconfigured track objects with registered applications (e.g. VRRP) is displayed.

Format

```
show track
```

Modes

```
Privileged EXEC
```

```
User EXEC
```

*General Information***ID**

The id of the track object.

Type

The type of the track object.

Status

Shows whether the monitored tracking object is up or down.

Mode

Shows whether the track object is activated.

No. Of Changes

Shows how often the State of the object changed since the track object was enabled.

Time since last change

Shows the time elapsed between the last change in state or mode.

*Additional Information for Interface Objects***Intf**

The Interface that is tracked by this object.

Link Delay Down

The time before a down event is signalled to the applications.

Link Delay Up

The time before an up event is signalled to the applications.

*Additional Information for Logical Objects***Instances**

A comma separated list of tracking instances combined into this object. If the list is incomplete (ends with "...") see `show track <id>` for the complete list.

*Additional Information for Ping Objects***IP Address**

The target IP address to monitor.

Intvl

The time interval between sending ping packets.

8.5.7 show track <id>

Displays detailed information about the given track object. The <trackid> is an integer value from 1 to 128 (L3P:256) and the id of an existing track object.

Format

```
show track <trackid>
```

Modes

Privileged EXEC

User EXEC

*General Information***ID**

The id of the track object.

Type

The type of the track object.

Status

Shows whether the monitored object is up or down.

Send State Change Traps

Shows whether the track trap is activated.

Mode

Shows whether the track object is activated.

No. Of Changes

Shows how often the State of the object changed since the track object was enabled.

Time since last change

Shows the time elapsed between the last change in State or mode.

Applications

The list of applications registered to this track object.

*Additional Information for Interface Objects***Interface**

The slot and port of the tracked interface.

Link-down-delay

Time in seconds before a link-down event is announced to the applications.

Link-up-delay

Time in seconds before a link-up event is announced to the applications.

*Additional Information for Logical Objects***Operator**

The logical operator used to combine the states of the members (AND or OR).

Instances included

A comma separated list of tracking instances combined into this entry.

*Additional Information for Ping Objects***Target IP Address**

The IP address of the remote host that is monitored.

Interface

The slot and port of the interface used to reach the remote host. If none is configured, the interface of the current best route is shown.

Ping Interval

The time between sending ping packets for this object.

Lost pings until down

Number of consecutive ping answers that must be lost (not received before the timeout) to change the state to Down.

Replies until up

Number of consecutive ping answers that must be received (before the timeout) to change the state to up.

Timeout for each Ping

The ping replies must arrive within this timeout in milliseconds to be counted as received.

8.5.8 show track applications

Displays a List of all applications registered to a track object. An application is shown for each track object it is registered to. If the track object is not yet configured, the last two columns are empty.

Format

```
show track applications
```

Modes

```
Privileged EXEC  
User EXEC
```

TrackId

The id of the track object.

Application

The identifier string of the application.

Changes

Shows how often the State of the object changed since the track object was enabled.

Time since last change

Shows the time elapsed between the last change in state or mode.

8.6 VRRP Commands

This chapter provides a detailed explanation of the Virtual Router Redundancy Protocol (VRRP) commands. The commands are divided by functionality into the following different groups:

- ▶ Show commands are used to display switch 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.
- ▶ Copy commands are used to transfer configuration and informational files to and from the switch.

8.6.1 ip vrrp

This command enables the global administrative mode of VRRP in the router.

Default

```
disabled
```

Format

```
ip vrrp
```

Mode

```
Global Config
```

■ no ip vrrp

This command disables the global administrative mode of VRRP in the router.

Format

```
no ip vrrp
```

Mode

```
Global Config
```

8.6.2 ip vrrp domain send-member-advertisements

This command controls whether the members of a VRRP domain send advertisements themselves as a fallback if the supervisor is still up but can't get advertisements from the master because of a single vlan failure.

Default

```
disabled
```

Format

```
ip vrrp domain <domain-id> send-member-advertisements
```

Mode

```
Global Config
```

■ no ip vrrp domain send-member-advertisements

This command disables the sending of advertisements for the members of the domain.

Format

```
no ip vrrp domain <domain-id> send-member-advertisements
```

Mode

```
Global Config
```

8.6.3 ip vrrp trap

This command enables vrrp traps.

Default

disabled

Format

```
ip vrrp trap {authentication-failure|new-master}
```

Mode

Global Config

authentication-failure

Enable or disable the sending of a trap if this router detects an authentication failure on any of its VRRP interfaces.

new-master

Enable or disable the sending of a trap if this router becomes new master for any of its VRRP interfaces.

■ no ip vrrp trap

This command disables vrrp traps.

Format

```
no ip vrrp trap {authentication-failure|new-master}
```

Mode

Global Config

8.6.4 ip vrrp

This command enables the VRRP protocol on an interface. The parameter `<vrID>` is the virtual router ID which has an integer value ranging from 1 to 255.

Default

none

Format

```
ip vrrp <vrID>
```

Mode

Interface Config

■ no ip vrrp

This command disables the VRRP protocol on an interface. The parameter `<vrID>` is the virtual router ID which has an integer value ranging from 1 to 255.

Note: If you intend to disable the protocol instance, first deactivate it using the `no ip vrrp <vrID> mode` command.

Format

```
no ip vrrp <vrID>
```

Mode

Interface Config

8.6.5 ip vrrp mode

This command enables the virtual router configured on the specified interface. Enabling the status field starts a virtual router. The parameter <vrID> is the virtual router ID which has an integer value ranging from 1 to 255.

Default

```
disabled
```

Format

```
ip vrrp <vrID> mode
```

Mode

```
Interface Config
```

■ no ip vrrp mode

This command disables the virtual router configured on the specified interface. Disabling the status field stops a virtual router.

Format

```
no ip vrrp <vrID> mode
```

Mode

```
Interface Config
```

8.6.6 ip vrrp ip

This command sets the virtual router *ipaddress* value for an interface. The value for *<ipaddr>* is the IP Address which is to be configured on that interface for VRRP. This may be a secondary virtual IP address. The parameter *<vrID>* is the virtual router ID which has an integer value ranging from 1 to 255.

Default

none

Format

```
ip vrrp <vrID> ip <ipaddr> [secondary]
```

Mode

Interface Config

8.6.7 ip vrrp authentication

This command sets the authorization details value for the virtual router configured on a specified interface. The parameter *{none | simple}* specifies the authorization type for virtual router configured on the specified interface. The parameter *[key]* is optional, it is only required when authorization type is simple text password. The parameter *<vrID>* is the virtual router ID which has an integer value ranging from 1 to 255.

Default

```
no authorization
```

Format

```
ip vrrp <vrID> authentication {none | simple <key>}
```

Mode

```
Interface Config
```

■ no ip vrrp authentication

This command sets the default authorization details value for the virtual router configured on a specified interface.

Format

```
no ip vrrp <vrID> authentication
```

Mode

```
Interface Config
```

8.6.8 ip vrrp preempt

This command sets the preemption mode value for the virtual router configured on a specified interface. The parameter `<vrID>` is the virtual router ID which has an integer value ranging from 1 to 255.

Default

enabled

Format

```
ip vrrp <vrID> preempt
```

Mode

Interface Config

■ no ip vrrp preempt

This command sets the default preemption mode value for the virtual router configured on a specified interface.

Format

```
no ip vrrp <vrID> preempt
```

Mode

Interface Config

8.6.9 ip vrrp delay-preemption

This command enables a delay before a virtual router preempts a master with a lower priority. This way dynamic routing protocols have some time to set up the routing tables before the router actually becomes Master. The delay time is given in seconds, the parameter `<vrID>` is the virtual router ID which is an integer value ranging from 1 to 255.

Default

Disabled (0 seconds)

Format

```
ip vrrp <vrID> delay-preemption <seconds>
```

Mode

Interface Config

■ no ip vrrp delay-preemption

This command disables the delay before a virtual router preempts a master with a lower priority.

Format

```
no ip vrrp <vrID> delay-preemption
```

Mode

Interface Config

8.6.10 ip vrrp priority

This command sets the priority value for the virtual router configured on a specified interface. The priority of the interface is a priority integer from 1 to 254. The parameter `<vrID>` is the virtual router ID which has an integer value ranging from 1 to 255.

The priority of a virtual router cannot be set to a value lower than the sum of the decrement values of all tracking entries for that virtual router.

Default

```
100
```

Format

```
ip vrrp <vrID> priority <1-254>
```

Mode

```
Interface Config
```

■ no ip vrrp priority

This command sets the default priority value for the virtual router configured on a specified interface.

Format

```
no ip vrrp <vrID> priority
```

Mode

```
Interface Config
```

8.6.11 ip vrrp timers advertise

This command sets the virtual router's advertisement packet interval. The parameter is an integer representing the advertisement interval from 1 to 255 seconds. The parameter <vrID> is the virtual router ID which is an integer value ranging from 1 to 255.

Default

1

Format

```
ip vrrp <vrID> timers advertise <1-255>
```

Mode

Interface Config

■ ip vrrp timers advertise milliseconds

This command sets the virtual router's advertisement packet interval. Use this command, if you want to set an interval below 1 second. Use the above command to set intervals greater than one second. The parameter is an integer representing the advertisement interval in milliseconds. The parameter <vrID> is the virtual router ID which is an integer value ranging from 1 to 255.

Default

1000 milliseconds (1 second)

Format

```
ip vrrp <vrID> timers advertise milliseconds <100-1000>
```

Mode

Interface Config

■ no ip vrrp timers advertise

This command sets the default advertisement interval for a virtual router.

Format

```
no ip vrrp <vrID> timers advertise
```

Mode

Interface Config

8.6.12 ip vrrp advertisement-address

This command sets the destination address for the VRRP advertisement packets. This can either be the multicast group address for all vrrp routers (224.0.0.18) or the unicast address of a backup router for this virtual interface. A Unicast address must be within the same subnet as the interface's ip address but must not be equal to it. The parameter <vrID> is the virtual router ID which is an integer value ranging from 1 to 255.

Default

```
224.0.0.18
```

Format

```
ip vrrp <vrID> advertisement-address <ipaddress>
```

Mode

```
Interface Config
```

■ no ip vrrp advertisement-address

This command resets the destination address for the VRRP advertisement packets to its default value 224.0.0.18

Format

```
no ip vrrp <vrID> advertisement-address
```

Mode

```
Interface Config
```

8.6.13 ip vrrp link-down-notification

This command enables a notification to a backup router when the virtual router loses its link. The parameter `<vrID>` is the virtual router ID which is an integer value ranging from 1 to 255. Give a unicast IP address of a backup router as the last parameter.

Default

Disabled (0.0.0.0)

Format

```
ip vrrp <vrID> link-down-notification <ipAddress>
```

Mode

Interface Config

■ no ip vrrp link-down-notification

This command disables the link down notification.

Format

```
no ip vrrp <vrID> link-down-notification
```

Mode

Interface Config

8.6.14 ip vrrp track

With this command the virtual router is configured to observe a tracked object. The trackid and the object to track are configured with the command „track“. The Parameter trackid is an integer value, the range is determined by the tracking module. The decrement value is an integer from 1 to 253. The sum of all decrement values for a given virtual router must not exceed the priority configured for that virtual router.

Default

20

Format

```
ip vrrp <vrID> track <trackid> [decrement <1-253>]
```

Mode

Interface Config

■ no ip vrrp track

This command configures the virtual router to stop observing a tracked object.

Format

```
no ip vrrp <vrID> track <trackid>
```

Mode

Interface Config

8.6.15 ip vrrp domain

This command configures a virtual router into a VRRP domain and can make it the supervisor of that domain.

Default

0 (no domain)

Format

```
ip vrrp <vrID> domain <1-8> [supervisor]
```

Mode

Interface Config

■ no ip vrrp domain supervisor

This command configures the virtual router not to be the supervisor of the domain. It will still be a member of the domain.

Format

```
no ip vrrp <vrID> domain <1-8> supervisor
```

Mode

Interface Config

■ no ip vrrp domain

This command removes the virtual router from any domain it is in. If the domain-id is given, the virtual router will only be removed from that domain.

Format

```
no ip vrrp <vrID> domain [<1-8>]
```

Mode

Interface Config

8.6.16 show ip vrrp interface stats

This command displays the statistical information about each virtual router configured on the switch.

Format

```
show ip vrrp interface stats <slot/port> <vrID>
```

Modes

Privileged EXEC

User EXEC

Uptime

The time that the virtual router has been up, in days, hours, minutes and seconds.

Protocol

Represents the protocol configured on the interface.

State Transitioned to Master

Represents the total number of times the virtual router state has changed to MASTER.

Advertisement Received

Represents the total number of VRRP advertisements received by this virtual router.

Advertisement Interval Errors

Represents the total number of VRRP advertisements received for which advertisement interval is different than the configured value for this virtual router.

Authentication Failure

Represents the total number of VRRP packets received that don't pass the authentication check.

IP TTL errors

Represents the total number of VRRP packets received by the virtual router with IP TTL (time to live) not equal to 255.

Zero Priority Packets Received

Represents the total number of VRRP packets received by virtual router with a priority of '0'.

Zero Priority Packets Sent

Represents the total number of VRRP packets sent by the virtual router with a priority of '0'.

Invalid Type Packets Received

Represents the total number of VRRP packets received by the virtual router with invalid 'type' field.

Address List Errors

Represents the total number of VRRP packets received for which address list does not match the locally configured list for the virtual router.

Invalid Authentication Type

Represents the total number of VRRP packets received with unknown authentication type.

Authentication Type Mismatch

Represents the total number of VRRP advertisements received for which 'auth type' not equal to locally configured one for this virtual router.

Packet Length Errors

Represents the total number of VRRP packets received with packet length less than length of VRRP header.

8.6.17 show ip vrrp

This command displays whether VRRP functionality is enabled or disabled on the switch. It also displays some global parameters which are required for monitoring. This command takes no options.

Format

```
show ip vrrp
```

Modes

```
Privileged EXEC
```

```
User EXEC
```

Admin Mode

Displays the administrative mode for VRRP functionality on the switch.

Authentication Failure Trap

Represents the administrative mode for VRRP authentication failure trap function.

New Master Trap

Represents the administrative mode of the New Master Trap function.

Fast instances configured

Shows the number of virtual routers with an advertisement interval of less than one second. 16 of these fast instances can be configured at a time.

Router Checksum Errors

Represents the total number of VRRP packets received with an invalid VRRP checksum value.

Router Version Errors

Represents the total number of VRRP packets received with Unknown or unsupported version number.

Router VRID Errors

Represents the total number of VRRP packets received with invalid VRID for this virtual router.

8.6.18 show ip vrrp domain

This command displays information about a VRRP domain.

Format

```
show ip vrrp domain <1-8>
```

Modes

Privileged EXEC

User EXEC

Interface

Valid slot and port number separated by forward slashes.

VRID

Represents the router ID of the virtual router.

State

Represents the state (Master/backup) of the virtual router.

Role

Represents the role of the virtual router in this domain (Member or Supervisor).

Members Send Advertisements

Displays whether the members of the domain send advertisements themselves.

Supervisor Priority

Displays the current priority of the supervisor of the domain. This priority is used by all members.

Supervisor Advertisement Address

The IP address the supervisor sends its advertisement packets to.

8.6.19 show ip vrrp interface

This command displays all configuration information and VRRP router statistics of a virtual router configured on a specific interface.

Format

```
show ip vrrp interface <slot/port> <vrID>
```

Modes

Privileged EXEC

User EXEC

Primary IP Address

This field represents the configured primary IP Address for the Virtual router.

Secondary IP Addresses

This field represents the configured secondary IP Address for the Virtual router.

VMAC address

Represents the VMAC address of the specified router.

Authentication type

Represents the authentication type for the specific virtual router.

Priority

Represents the priority value for the specific virtual router.

Advertisement interval

Represents the advertisement interval for the specific virtual router.

Pre-Empt Mode

Is the preemption mode configured on the specified virtual router.

Administrative Mode

Represents the status (Enable or Disable) of the specific router.

State

Represents the state (Master/backup) of the virtual router.

Current Priority

Displays the current priority used by this virtual router. This can be different from the configured priority if tracking or domains are used.

Preemption Delay

Shows the time preemption of a master with lower priority is delayed.

Link Down Notification

Shows the IP address link down notifications are sent to.

VRRP Domain

Displays the domain this virtual router is in.

VRRP Domain Role

Shows the role that this virtual router has in its domain (Member or Supervisor)

VRRP Domain State

Shows if the domain is completely configured or if the supervisor is missing or down.

Advertisement Address

Shows the IP address the virtual router sends its advertisement packets to.

Tracking

Shows the trackids this virtual router is observing.

Decrement

The value by which the priority of the virtual router is decremented when the tracked object goes down.

State

Shows if the tracked object is up or down. If the trackid is not a configured tracking object, it is always shown as up.

8.6.20 show ip vrrp interface brief

This command displays information about each virtual router configured on the switch. This command takes no options. It displays information about each virtual router.

Format

```
show ip vrrp interface brief
```

Modes

Privileged EXEC

User EXEC

Interface

Valid slot and port number separated by forward slashes.

VRID

Represents the router ID of the virtual router.

IP Address

The primary virtual router IP address.

Mode

Represents whether the virtual router is enabled or disabled.

State

Represents the state (Master/backup) of the virtual router.

Domain

Displays the domain this virtual router is in. (S) shows that the virtual router is the supervisor of that domain.

8.7 OSPF Commands

This chapter provides a detailed explanation of the Open Shortest Path First (OSPF) commands. The commands are divided by functionality into the following different groups:

- ▶ Show commands are used to display switch 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.
- ▶ Copy commands are used to transfer configuration and informational files to and from the switch.

8.7.1 enable (OSPF)

This command sets the administrative mode of OSPF in the router to active.

Default

enabled

Format

enable

Mode

Router OSPF Config

■ no enable (OSPF)

This command sets the administrative mode of OSPF in the router to inactive.

Format

no enable

Mode

Router OSPF Config

8.7.2 ip ospf

This command enables OSPF on a router interface.

Default

disabled

Format

```
ip ospf
```

Mode

Interface Config

■ no ip ospf

This command disables OSPF on a router interface.

Format

```
no ip ospf
```

Mode

Interface Config

8.7.3 1583compatibility

This command enables OSPF 1583 compatibility.

Note: 1583 compatibility mode is enabled by default. If all OSPF routers in the routing domain are capable of operating according to RFC 2328, OSPF 1583 compatibility mode should be disabled.

Default

enabled

Format

1583compatibility

Mode

Router OSPF Config

■ no 1583compatibility

This command disables OSPF 1583 compatibility.

Format

no 1583compatibility

Mode

Router OSPF Config

8.7.4 area default-cost

This command configures the monetary default cost for the stub area. This is the cost for the default route injected into the attached stub area. The operator must specify the area id and an integer value between 1-16777215.

Format

area <areaid> default-cost <1-16777215>

Mode

Router OSPF Config

8.7.5 area nssa

This command configures the specified areaid to function as an NSSA.

Format

```
area <areaid> nssa
```

Mode

```
Router OSPF Config
```

■ no area nssa

This command disables nssa from the specified area id.

Format

```
no area <areaid> nssa
```

Mode

```
Router OSPF Config
```

8.7.6 area nssa default-info-originate

This command configures the metric value and type for the default route advertised into the NSSA. The optional metric parameter specifies the metric of the default route and is to be in a range of 1-16777215. If no metric is specified, the default value is 1. The metric type can be comparable (nssa-external 1) or non-comparable (nssa-external 2).

Format

```
area <areaid> nssa default-info-originate [<metric>]  
[{comparable | non-comparable}]
```

Mode

```
Router OSPF Config
```

8.7.7 area nssa no-redistribute (OSPF)

This command configures the NSSA ABR so that learned external routes will not be redistributed to the NSSA.

Format

```
area <areaid> nssa no-redistribute
```

Mode

```
Router OSPF Config
```

8.7.8 area nssa no-summary (OSPF)

This command configures the NSSA so that summary LSAs are not advertised from the Backbone into the NSSA.

Format

```
area <areaid> nssa no-summary
```

Mode

```
Router OSPF Config
```

8.7.9 area nssa translator-role (OSPF)

This command configures the translator role of the NSSA. A value of `always` causes the router to assume the role of the translator the instant it becomes a border router and a value of `candidate` causes the router to participate in the translator election process when it attains border router status.

Format

```
area <areaid> nssa translator-role {always | candidate}
```

Mode

```
Router OSPF Config
```

8.7.10 area nssa translator-stab-intv

This command configures the translator *<stabilityinterval>* of the NSSA. The *<stabilityinterval>* is the period of time that an elected translator continues to perform its duties after it determines that its translator status has been deposited by another router.

Format

```
area <areaid> nssa translator-stab-intv <stabilityinterval>
```

Modes

Router OSPF Config

8.7.11 area range

This command creates a specified area range for a specified area. The *<ipaddr>* is a valid IP address. The *<subnetmask>* is a valid subnet mask. The LSDB type must be specified by either *summarylink* or *nssaexternallink*, and the advertising of the area range can be allowed or suppressed.

Format

```
area <areaid> range <ipaddr> <subnetmask> {summarylink | nssaexternallink} [advertise | not-advertise]
```

Mode

Router OSPF Config

■ no area range

This command deletes a specified area range. The *<ipaddr>* is a valid IP address. The *<subnetmask>* is a valid subnet mask.

Format

```
no area <areaid> range <ipaddr> <subnetmask>
```

Mode

Router OSPF Config

8.7.12 area stub

This command creates a stub area for the specified area ID. A stub area is characterized by the fact that AS External LSAs are not propagated into the area. Removing AS External LSAs and Summary LSAs can significantly reduce the link state database of routers within the stub area.

Format

```
area <areaid> stub
```

Mode

```
Router OSPF Config
```

■ no area stub

This command deletes a stub area for the specified area ID.

Format

```
no area <areaid> stub
```

Mode

```
Router OSPF Config
```

8.7.13 area stub summarylsa

This command configures the Summary LSA mode for the stub area identified by `<areaid>`. The Summary LSA mode is configured as enabled.

Default

disabled

Format

```
area <areaid> stub summarylsa
```

Mode

Router OSPF Config

■ no area stub summarylsa

This command configures the default Summary LSA mode for the stub area identified by `<areaid>`.

Format

```
no area <areaid> stub summarylsa
```

Mode

Router OSPF Config

8.7.14 area virtual-link

This command creates the OSPF virtual interface for the specified `<areaid>` and `<neighbor>`. The `<neighbor>` parameter is the Router ID of the neighbor.

Format

```
area <areaid> virtual-link <neighbor>
```

Mode

```
Router OSPF Config
```

■ no area virtual-link

This command deletes the OSPF virtual interface from the given interface, identified by `<areaid>` and `<neighbor>`. The `<neighbor>` parameter is the Router ID of the neighbor.

Format

```
no area <areaid> virtual-link <neighbor>
```

Mode

```
Router OSPF Config
```

8.7.15 area virtual-link authentication

This command configures the authentication type and key for the OSPF virtual interface identified by `<areaid>` and `<neighbor>`. The `<neighbor>` parameter is the Router ID of the neighbor. The value for `<type>` is either `none`, `simple`, or `encrypt`. The `[key]` is composed of standard displayable, non-control keystrokes from a Standard 101/102-key keyboard. The authentication key must be 8 bytes or less if the authentication type is `simple`. If the type is `encrypt`, the key may be up to 256 bytes. Unauthenticated interfaces do not need an authentication key. If the type is `encrypt`, a key id in the range of 0 and 255 must be specified. The default value for authentication type is `none`. Neither the default password key nor the default key id are configured.

Default

`none`

Format

```
area <areaid> virtual-link <neighbor> authentication
{none | {simple <key>} | {encrypt <key> <keyid>}}
```

Mode

Router OSPF Config

■ no area virtual-link authentication

This command configures the default authentication type for the OSPF virtual interface identified by `<areaid>` and `<neighbor>`. The `<neighbor>` parameter is the Router ID of the neighbor.

Format

```
no area <areaid> virtual-link <neighbor> authentication
```

Mode

Router OSPF Config

8.7.16 area virtual-link dead-interval

This command configures the dead interval for the OSPF virtual interface on the virtual interface identified by `<areaid>` and `<neighbor>`. The `<neighbor>` parameter is the Router ID of the neighbor.

The range for `<seconds>` is 1..65535.

Default

40

Format

```
area <areaid> virtual-link <neighbor> dead-interval
<1-65535>
```

Mode

Router OSPF Config

■ no area virtual-link dead-interval

This command configures the default dead interval for the OSPF virtual interface on the virtual interface identified by `<areaid>` and `<neighbor>`. The `<neighbor>` parameter is the Router ID of the neighbor.

Format

```
no area <areaid> virtual-link <neighbor> dead-inter-
val
```

Mode

Router OSPF Config

8.7.17 area virtual-link hello-interval

This command configures the hello interval for the OSPF virtual interface on the virtual interface identified by `<areaid>` and `<neighbor>`. The `<neighbor>` parameter is the Router ID of the neighbor.

The range for `<seconds>` is 1..65535.

Default

10

Format

```
area <areaid> virtual-link <neighbor> hello-interval
<1-65535>
```

Mode

Router OSPF Config

■ no area virtual-link hello-interval

This command configures the default hello interval for the OSPF virtual interface on the virtual interface identified by `<areaid>` and `<neighbor>`. The `<neighbor>` parameter is the Router ID of the neighbor.

Format

```
no area <areaid> virtual-link <neighbor> hello-
interval
```

Mode

Router OSPF Config

8.7.18 area virtual-link retransmit-interval

This command configures the retransmit interval for the OSPF virtual interface on the virtual interface identified by `<areaid>` and `<neighbor>`. The `<neighbor>` parameter is the Router ID of the neighbor.

The range for `<seconds>` is 0..3600.

Default

5

Format

```
area <areaid> virtual-link <neighbor> retransmit-  
interval <0-3600>
```

Mode

Router OSPF Config

■ no area virtual-link retransmit-interval

This command configures the default retransmit interval for the OSPF virtual interface on the virtual interface identified by `<areaid>` and `<neighbor>`.

The `<neighbor>` parameter is the Router ID of the neighbor.

Format

```
no area <areaid> virtual-link <neighbor> retransmit-  
interval
```

Mode

Router OSPF Config

8.7.19 area virtual-link transmit-delay

This command configures the transmit delay for the OSPF virtual interface on the virtual interface identified by *<areaid>* and *<neighbor>*. The *<neighbor>* parameter is the Router ID of the neighbor.

The range for *<seconds>* is 0..3600 (1 hour).

Default

1

Format

```
area <areaid> virtual-link <neighbor> transmit-delay  
<0-3600>
```

Mode

Router OSPF Config

■ no area virtual-link transmit-delay

This command configures the default transmit delay for the OSPF virtual interface on the virtual interface identified by *<areaid>* and *<neighbor>*. The *<neighbor>* parameter is the Router ID of the neighbor.

Format

```
no area <areaid> virtual-link <neighbor> transmit-  
delay
```

Mode

Router OSPF Config

8.7.20 default-information originate (OSPF)

This command is used to control the advertisement of default routes.

Default

```
metric -- unspecified;  
type -- 2
```

Format

```
default-information originate [always] [metric <0-  
16777215>] [metric-type {1 | 2}]
```

Mode

Router OSPF Config

■ no default-information originate (OSPF)

This command is used to control the advertisement of default routes.

Format

```
no default-information originate {always | metric |  
metric-type}
```

Mode

Router OSPF Config

8.7.21 default-metric (OSPF)

This command is used to set a default for the metric of distributed routes.

Format

```
default-metric <1-16777215>
```

Mode

```
Router OSPF Config
```

■ no default-metric (OSPF)

This command is used to set a default for the metric of distributed routes.

Format

```
no default-metric
```

Mode

```
Router OSPF Config
```

8.7.22 distance ospf

This command sets the route preference value of OSPF in the router. Lower route preference values are preferred when determining the best route. The type of OSPF can be intra, inter, type-1, or type-2. The OSPF specification (RFC 2328) requires that preferences must be given to the routes learned via OSPF in the following order: intra < inter < type-1 < type-2. The *<preference>* range is

- ▶ 1 to 255 for intra
- ▶ 2 to 253 for inter
- ▶ 3 to 253 for type-1
- ▶ 4 to 255 for type-2.

Default

```
intra -- 8;
inter -- 10;
type-1 -- 13;
type-2 -- 150.
```

Format

```
distance ospf {intra | inter | type1 | type2}
<preference>
```

Mode

Router OSPF Config

■ no distance ospf

This command sets the default route preference value of OSPF in the router. The type of OSPF can be intra, inter, type-1, or type-2.

Format

```
no distance ospf {intra | inter | type1 | type2}
```

Mode

Router OSPF Config

8.7.23 distribute-list out

This command is used to specify the access list to filter routes received from the source protocol.

Format

```
distribute-list <1-199> out {rip | bgp | static | con-  
nected}
```

Mode

Router OSPF Config

■ no distribute-list out

This command is used to specify the access list to filter routes received from the source protocol.

Format

```
no distribute-list <1-199> out {rip | bgp | static |  
connected}
```

Mode

Router OSPF Config

8.7.24 exit-overflow-interval

This command configures the exit overflow interval for OSPF. It describes the number of seconds after entering Overflow state that a router will wait before attempting to leave the Overflow State. This allows the router to again originate non-default AS-external-LSAs. When set to 0, the router will not leave Overflow State until restarted.

The range for *<seconds>* is 0..2147483647 seconds.

Default

0

Format

```
exit-overflow-interval <0-2147483647>
```

Mode

Router OSPF Config

■ no exit-overflow-interval

This command configures the default exit overflow interval for OSPF.

Format

```
no exit-overflow-interval
```

Mode

Router OSPF Config

8.7.25 external-lsdb-limit

This command configures the external LSDB limit for OSPF. If the value is -1, then there is no limit. When the number of non-default AS-external-LSAs in a router's link-state database reaches the external LSDB limit, the router enters overflow state. The router never holds more than the external LSDB limit non-default AS-external-LSAs in its database. The external LSDB limit MUST be set identically in all routers attached to the OSPF backbone and/or any regular OSPF area.

The range for *<limit>* is -1..2147483647.

Default

-1

Format

```
external-lsdb-limit <-1-2147483647>
```

Mode

Router OSPF Config

■ no external-lsdb-limit

This command configures the default external LSDB limit for OSPF.

Format

```
no external-lsdb-limit
```

Mode

Router OSPF Config

8.7.26 ip ospf areaid

This command sets the OSPF area to which the specified router interface belongs. The value for *<areaid>* is an IP address, formatted as a 4-digit dotted-decimal number that uniquely identifies the area to which the interface connects. Assigning an area id, which does not exist on an interface, causes the area to be created with default values.

Format

```
ip ospf areaid <areaid>
```

Mode

```
Interface Config
```

8.7.27 ip ospf authentication

This command sets the OSPF Authentication Type and Key for the specified interface. The value of *<type>* is either none, simple or encrypt. The *[key]* is composed of standard displayable, non-control keystrokes from a Standard 101/102-key keyboard. The authentication key must be 8 bytes or less if the authentication type is simple. If the type is encrypt, the key may be up to 256 bytes. If the type is encrypt a *<keyid>* in the range of 0 and 255 must be specified.

Default

The default authentication type is none.

Default

The default password key is not configured. Unauthenticated interfaces do not need an authentication key.

Default

The default keyid is not configured. Unauthenticated interfaces do not need an authentication key id.

Format

```
ip ospf authentication {none | {simple <key>} |  
                        {encrypt <key> <keyid>}}
```

Mode

Interface Config

■ no ip ospf authentication

This command sets the default OSPF Authentication Type for the specified interface.

Format

```
no ip ospf authentication
```

Mode

Interface Config

8.7.28 ip ospf cost

This command configures the cost on an OSPF interface. The *<cost>* parameter has a range of 1 to 65535.

Default

10

Format

```
ip ospf cost <1-65535>
```

Mode

Interface Config

■ no ip ospf cost

This command configures the default cost on an OSPF interface.

Format

```
no ip ospf cost
```

Mode

Interface Config

8.7.29 ip ospf dead-interval

This command sets the OSPF dead interval for the specified interface. The value for *<seconds>* is a valid positive integer, which represents the length of time in seconds that a router's Hello packets have not been seen before its neighbor routers declare that the router is down. The value for the length of time must be the same for all routers attached to a common network. This value should be some multiple of the Hello Interval (i.e. 4). Valid values range for *<seconds>* is 1..2147483647.

Default

40

Format

```
ip ospf dead-interval <1-2147483647>
```

Mode

Interface Config

■ no ip ospf dead-interval

This command sets the default OSPF dead interval for the specified interface.

Format

```
no ip ospf dead-interval
```

Mode

Interface Config

8.7.30 ip ospf hello-interval

This command sets the OSPF hello interval for the specified interface. The value for *<seconds>* is a valid positive integer, which represents the length of time in seconds. The value for the length of time must be the same for all routers attached to a network.

Valid values range from 1 . . 65535.

Default

10

Format

```
ip ospf hello-interval <1-65535>
```

Mode

Interface Config

■ no ip ospf hello-interval

This command sets the default OSPF hello interval for the specified interface.

Format

```
no ip ospf hello-interval
```

Mode

Interface Config

8.7.31 ip ospf priority

This command sets the OSPF priority for the specified router interface. The priority of the interface is a priority integer from 0 to 255. A value of 0 indicates that the router is not eligible to become the designated router on this network.

Default

1, which is the highest router priority.

Format

```
ip ospf priority <0-255>
```

Mode

Interface Config

■ no ip ospf priority

This command sets the default OSPF priority for the specified router interface.

Format

```
no ip ospf priority
```

Mode

Interface Config

8.7.32 ip ospf retransmit-interval

This command sets the OSPF retransmit Interval for the specified interface. The retransmit interval is specified in seconds. The value for *<seconds>* is the number of seconds between link-state advertisement retransmissions for adjacencies belonging to this router interface. This value is also used when retransmitting database description and link-state request packets. Valid values range from 0 . . 3600 (1 hour).

Default

5

Format

```
ip ospf retransmit-interval <0-3600>
```

Mode

Interface Config

■ no ip ospf retransmit-interval

This command sets the default OSPF retransmit Interval for the specified interface.

Format

```
no ip ospf retransmit-interval
```

Mode

Interface Config

8.7.33 ip ospf transmit-delay

This command sets the OSPF Transit Delay for the specified interface. The transmit delay is specified in seconds. In addition, it sets the estimated number of seconds it takes to transmit a link state update packet over this interface. Valid values for *<seconds>* range from 1 to 3600 (1 hour).

Default

1

Format

```
ip ospf transmit-delay <1-3600>
```

Mode

Interface Config

■ no ip ospf transmit-delay

This command sets the default OSPF Transit Delay for the specified interface.

Format

```
no ip ospf transmit-delay
```

Mode

Interface Config

8.7.34 ip ospf mtu-ignore

This command disables OSPF maximum transmission unit (MTU) mismatch detection. OSPF Database Description packets specify the size of the largest IP packet that can be sent without fragmentation on the interface. When a router receives a Database Description packet, it examines the MTU advertised by the neighbor. By default, if the MTU is larger than the router can accept, the Database Description packet is rejected and the OSPF adjacency is not established.

Default

enabled

Format

```
ip ospf mtu-ignore
```

Mode

Interface Config

■ no ip ospf mtu-ignore

This command enables the OSPF MTU mismatch detection.

Format

```
no ip ospf mtu-ignore
```

Mode

Interface Config

8.7.35 router-id

This command sets a 4-digit dotted-decimal number uniquely identifying the router ospf id. The *<ipaddress>* is a configured value.

Format

```
router-id <ipaddress>
```

Mode

Router OSPF Config

8.7.36 redistribute

This command configures OSPF protocol to allow redistribution of routes from the specified source protocol/routers.

Default

```
metric -- unspecified;  
type -- 2;  
tag -- 0
```

Format

```
redistribute {rip | bgp | static | connected} [metric  
<0-16777215>] [metric-type {1 | 2}] [tag <0-4294967295>]  
[subnets]
```

Mode

```
Router OSPF Config
```

■ no redistribute

This command configures OSPF protocol to prohibit redistribution of routes from the specified source protocol/routers.

Format

```
no redistribute {rip | bgp | static | connected} [met-  
ric] [metric-type] [tag] [subnets]
```

Mode

```
Router OSPF Config
```

8.7.37 maximum-paths

This command sets the number of paths that OSPF can report for a given destination where maxpaths is platform dependent.

Default

4

Format

```
maximum-paths <maxpaths>
```

Mode

```
OSPF Router Config
```

■ no maximum-paths

This command resets the number of paths that OSPF can report for a given destination back to its default value.

Format

```
no maximum-paths
```

Mode

```
OSPF Router Config
```

8.7.38 trapflags

This command enables OSPF traps.

Default

enabled

Format

trapflags

Mode

Router OSPF Config

■ no trapflags

This command disables OSPF traps.

Format

no trapflags

Mode

Router OSPF Config

8.7.39 show ip ospf

This command displays information relevant to the OSPF router.

Format

show ip ospf

Mode

Privileged EXEC

Router ID

Is a 32 bit integer in dotted decimal format identifying the router, about which information is displayed. This is a configured value.

OSPF Admin Mode

The administrative mode of OSPF in the router. This is a configured value.

ASBR Mode

Reflects whether the ASBR mode is enabled or disabled. Enable implies that the router is an autonomous system border router. Router automatically becomes an ASBR when it is configured to redistribute routes learnt from other protocol. The possible values for the ASBR status is enabled (if the router is configured to re-distribute routes learnt by other protocols) or disabled (if the router is not configured for the same).

RFC 1583 Compatibility

Reflects whether 1583 compatibility is enabled or disabled. This is a configured value.

Default-metric

Default value for redistributed routes.

Source

Source protocol/routes that are being redistributed.

Metric-value

Metric of the routes being redistributed.

Type-value

External Type 1 or External Type 2 routes.

Tag-value

Decimal value attached to each external route.

Subnets

For redistributing routes into OSPF, the scope of redistribution for the specified protocol.

Distribute-list

TAccess list used to filter redistributed routes.

Default-info originate

Indicates whether the default routes received from other source protocols are advertised or not

The information below will only be displayed if OSPF is enabled.

ABR Status

Reflects the whether or not the router is an OSPF Area Border Router.

Exit Overflow Interval

The number of seconds that, after entering OverflowState, a router will attempt to leave OverflowState.

External LSA count

The number of external (LS type 5) link-state advertisements in the link-state database.

External LSA Checksum

A number which represents the sum of the LS checksums of external link-state advertisements contained in the link-state database.

New LSAs Originated

The number of new link-state advertisements that have been originated.

LSAs Received

The number of link-state advertisements received determined to be new instantiations.

External LSDB Limit

The maximum number of non-default AS-external-LSAs entries that can be stored in the link-state database.

Max Paths

Maximum number of paths that OSPF can report for a given destination.

8.7.40 show ip ospf area

This command displays information about the area. The `<areaid>` identifies the OSPF area that is being displayed.

Format

```
show ip ospf area <areaid>
```

Modes

Privileged EXEC

User EXEC

AreaID

Is the area id of the requested OSPF area.

Aging Interval

Is a number representing the aging interval for this area.

External Routing

Is a number representing the external routing capabilities for this area.

Authentication Type

Is the configured authentication type to use for this area.

Spf Runs

Is the number of times that the intra-area route table has been calculated using this area's link-state database.

Area Border Router Count

The total number of area border routers reachable within this area.

Area LSA Count

Total number of link-state advertisements in this area's link-state database, excluding AS External LSA's.

Area LSA Checksum

A number representing the Area LSA Checksum for the specified AreaID excluding the external (LS type 5) link-state advertisements.

Stub Mode

Represents whether the specified Area is a stub area or not. The possible values are enabled and disabled. This is a configured value.

Import Summary LSAs**Metric Value**

Is a number representing the Metric Value for the specified area.

Metric Type

Is the Default Metric Type for the specified Area.

8.7.41 show ip ospf database

This command displays the link state database.

Note: The information below is only displayed if OSPF is enabled.

Note: The OSPF database information is grouped into sections by link-type and area. The groups are as follows:

- ▶ Router Link States
- ▶ Network Link States
- ▶ Network Summary States
- ▶ Summary ASBR States

The AS-Externals are not grouped by area.

Format

```
show ip ospf database
```

Modes

```
Privileged EXEC
```

```
User EXEC
```

For each link-type and area, the following information is displayed.

Link Id

Is a number that "uniquely identifies an LSA that a router originates from all other self originated LSA's of the same LS type.

Adv Router

The Advertising Router. Is a 32 bit dotted decimal number representing the LSDB interface.

Age

Is a number representing the age of the link state advertisement in seconds.

Sequence

Is a number that represents which LSA is more recent.

Checksum

Is the total number LSA checksum.

Options

This is an integer. It indicates that the LSA receives special handling during routing calculations.

Rtr Opt

Router Options are valid for router links only.

8.7.42 show ip ospf interface

This command displays the information for the IFO object or virtual interface tables.

Format

```
show ip ospf interface <slot/port>
```

Modes

Privileged EXEC

User EXEC

IP Address

Represents the IP address for the specified interface.

Subnet Mask

A mask of the network and host portion of the IP address for the OSPF interface.

OSPF Admin Mode

States whether OSPF is enabled or disabled on a router interface.

OSPF Area ID

Represents the OSPF Area Id for the specified interface.

Router Priority

A number representing the OSPF Priority for the specified interface.

Retransmit Interval

A number representing the OSPF Retransmit Interval for the specified interface.

Hello Interval

A number representing the OSPF Hello Interval for the specified interface.

Dead Interval

A number representing the OSPF Dead Interval for the specified interface.

LSA Ack Interval

A number representing the OSPF LSA Acknowledgement Interval for the specified interface.

Transit Delay Interval

A number representing the OSPF Transit Delay for the specified interface.

Authentication Type

The OSPF Authentication Type for the specified interface are: none, simple, and encrypt.

The information below will only be displayed if OSPF is enabled.

OSPF Interface Type

Broadcast LANs, such as Ethernet and IEEE 802.5, take the value broadcast. The OSPF Interface Type will be 'broadcast'.

State

The OSPF Interface States are: down, loopback, waiting, point-to-point, designated router, and backup designated router.

Designated Router

The router ID representing the designated router.

Backup Designated Router

The router ID representing the backup designated router.

Number of Link Events

The number of link events.

Metric Cost

The cost of the OSPF interface.

8.7.43 show ip ospf interface brief

This command displays brief information for the IFO object or virtual interface tables.

Format

```
show ip ospf interface brief
```

Modes

```
Privileged EXEC
```

```
User EXEC
```

Interface

Valid slot and port number separated by forward slashes.

OSPF Admin Mode

```
States whether OSPF is enabled or disabled on a  
router interface.
```

OSPF Area ID

```
Represents the OSPF Area Id for the specified  
interface.
```

Router Priority

```
A number representing the OSPF Priority for the  
specified interface.
```

Hello Interval

```
A number representing the OSPF Hello Interval for  
the specified interface.
```

Dead Interval

```
A number representing the OSPF Dead Interval for  
the specified interface.
```

Retransmit Interval

```
A number representing the OSPF Retransmit Interval  
for the specified interface.
```

Transit Delay Interval

```
A number representing the OSPF Transit Delay for  
the specified interface.
```

LSA Ack Interval

```
A number representing the OSPF LSA Acknowledgement  
Interval for the specified interface.
```

8.7.44 show ip ospf interface stats

This command displays the statistics for a specific interface. The information below will only be displayed if OSPF is enabled.

Format

```
show ip ospf interface stats <slot/port>
```

Modes

Privileged EXEC

User EXEC

OSPF Area ID

The area id of this OSPF interface.

Spf Runs

The number of times that the intra-area route table has been calculated using this area's link-state database.

Area Border Router Count

The total number of area border routers reachable within this area. This is initially zero, and is calculated in each SPF pass.

AS Border Router Count

The total number of Autonomous System border routers reachable within this area.

Area LSA Count

The total number of link-state advertisements in this area's link-state database, excluding AS External LSAs.

IP Address

The IP address associated with this OSPF interface.

OSPF Interface Events

The number of times the specified OSPF interface has changed its state, or an error has occurred.

Virtual Events

The number of state changes or errors that occurred on this virtual link.

Neighbor Events

The number of times this neighbor relationship has changed state, or an error has occurred.

External LSA Count

The number of external (LS type 5) link-state advertisements in the link-state database.

LSAs Received

The number of LSAs received.

Originate New LSAs

The number of LSAs originated.

8.7.45 show ip ospf neighbor

This command displays the OSPF neighbor table list. When a particular neighbor ID is specified, detailed information about a neighbor is given. The information below will only be displayed if OSPF is enabled and the interface has a neighbor. The IP address is the IP address of the neighbor.

Format

```
show ip ospf neighbor <ipaddr> <slot/port>
```

Modes

Privileged EXEC

User EXEC

Interface

Valid slot and port number separated by forward slashes..

Router Id

Is a 4-digit dotted-decimal number identifying neighbor router.

Options

An integer value that indicates the optional OSPF capabilities supported by the neighbor. The neigh-

bor's optional OSPF capabilities are also listed in its Hello packets. This enables received Hello Packets to be rejected (i.e., neighbor relationships will not even start to form) if there is a mismatch in certain crucial OSPF capabilities.

Router Priority

Displays the OSPF priority for the specified interface. The priority of an interface is a priority integer from 0 to 255. A value of '0' indicates that the router is not eligible to become the designated router on this network.

State

The types are:

Down- initial state of the neighbor conversation - no recent information has been received from the neighbor.

Attempt - no recent information has been received from the neighbor but a more concerted effort should be made to contact the neighbor.

Init - an Hello packet has recently been seen from the neighbor, but bi-directional communication has not yet been established.

2 way - communication between the two routers is bi-directional.

Exchange start - the first step in creating an adjacency between the two neighboring routers, the goal is to decide which router is the master and to decide upon the initial DD sequence number.

Exchange - the router is describing its entire link state database by sending Database Description packets to the neighbor.

Loading - Link State Request packets are sent to the neighbor asking for the more recent LSAs that have been discovered (but not yet received) in the Exchange state.

Full - the neighboring routers are fully adjacent and they will now appear in router-LSAs and network-LSAs.

Events

The number of times this neighbor relationship has changed state, or an error has occurred.

Permanence

This variable displays the status of the entry, either dynamic or permanent. This refers to how the neighbor became known.

Hellos Suppressed

This indicates whether Hellos are being suppressed to the neighbor. The types are enabled and disabled.

Retransmission Queue Length

Is an integer representing the current length of the retransmission queue of the specified neighbor router Id of the specified interface.

8.7.46 show ip ospf neighbor brief

This command displays the OSPF neighbor table list. When a particular neighbor ID is specified, detailed information about a neighbor is given. The information below will only be displayed if OSPF is enabled.

Format

```
show ip ospf neighbor brief {<slot/port> | all}
```

Modes

Privileged EXEC

User EXEC

Router ID

A 4 digit dotted decimal number representing the neighbor interface.

IP Address

An IP address representing the neighbor interface.

Neighbor Interface Index

Is a slot/port identifying the neighbor interface index.

8.7.47 show ip ospf range

This command displays information about the area ranges for the specified *<areaid>*. The *<areaid>* identifies the OSPF area whose ranges are being displayed.

Format

```
show ip ospf range <areaid>
```

Modes

Privileged EXEC

User EXEC

Area ID

The area id of the requested OSPF area.

IP Address

An IP Address which represents this area range.

Subnet Mask

A valid subnet mask for this area range.

Lsdb Type

The type of link advertisement associated with this area range.

Advertisement

The status of the advertisement. Advertisement has two possible settings: enabled or disabled.

8.7.48 show ip ospf stub table

This command displays the OSPF stub table. The information below will only be displayed if OSPF is initialized on the switch.

Format

```
show ip ospf stub table
```

Modes

Privileged EXEC

User EXEC

Area ID

Is a 32-bit identifier for the created stub area.

Type of Service

Is the type of service associated with the stub metric. The switch only supports Normal TOS.

Metric Val

The metric value is applied based on the TOS. It defaults to the least metric of the type of service among the interfaces to other areas. The OSPF cost for a route is a function of the metric value.

Metric Type

Is the type of metric advertised as the default route.

Import Summary LSA

Controls the import of summary LSAs into stub areas.

8.7.49 show ip ospf virtual-link

This command displays the OSPF Virtual Interface information for a specific area and neighbor. The `<areaid>` parameter identifies the area and the `<neighbor>` parameter identifies the neighbor's Router ID.

Format

```
show ip ospf virtual-link <areaid> <neighbor>
```

Modes

Privileged EXEC

User EXEC

Area ID

The area id of the requested OSPF area.

Neighbor Router ID

The input neighbor Router ID.

Hello Interval

The configured hello interval for the OSPF virtual interface.

Dead Interval

The configured dead interval for the OSPF virtual interface.

Iftransit Delay Interval

The configured transit delay for the OSPF virtual interface.

Retransmit Interval

The configured retransmit interval for the OSPF virtual interface.

Authentication Type

The configured authentication type of the OSPF virtual interface.

State

The OSPF Interface States are: down, loopback, waiting, point-to-point, designated router, and backup designated router. This is the state of the OSPF interface.

Neighbor State

The neighbor state.

8.7.50 show ip ospf virtual-link brief

This command displays the OSPF Virtual Interface information for all areas in the system.

Format

```
show ip ospf virtual-link brief
```

Modes

Privileged EXEC

User EXEC

Area Id

The area id of the requested OSPF area.

Neighbor

The neighbor interface of the OSPF virtual interface.

Hello Interval

The configured hello interval for the OSPF virtual interface.

Dead Interval

The configured dead interval for the OSPF virtual interface.

Retransmit Interval

The configured retransmit interval for the OSPF virtual interface.

Transit Delay

The configured transit delay for the OSPF virtual interface.

8.8 RIP Commands

This chapter provides a detailed explanation of the Routing Information Protocol (RIP) commands. The commands are divided by functionality into the following different groups:

- ▶ Show commands are used to display switch 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.
- ▶ Copy commands are used to transfer configuration and informational files to and from the switch.

8.8.1 enable (RIP)

This command sets the administrative mode of RIP in the router to active.

Default

```
enabled
```

Format

```
enable
```

Mode

```
Router RIP Config
```

■ no enable (RIP)

This command sets the administrative mode of RIP in the router to inactive.

Format

```
no enable
```

Mode

```
Router RIP Config
```

8.8.2 ip rip

This command enables RIP on a router interface.

Default

disabled

Format

```
ip rip
```

Mode

Interface Config

■ no ip rip

This command disables RIP on a router interface.

Format

```
no ip rip
```

Mode

Interface Config

8.8.3 auto-summary

This command enables the RIP auto-summarization mode.

Default

disabled

Format

auto-summary

Mode

Router RIP Config

■ no auto-summary

This command disables the RIP auto-summarization mode.

Format

no auto-summary

Mode

Router RIP Config

8.8.4 default-information originate (RIP)

This command is used to control the advertisement of default routes.

Format

```
default-information originate
```

Mode

```
Router RIP Config
```

■ no default-information originate (RIP)

This command is used to control the advertisement of default routes.

Format

```
no default-information originate
```

Mode

```
Router RIP Config
```

8.8.5 default-metric (RIP)

This command is used to set a default for the metric of distributed routes.

Format

```
default-metric <0-15>
```

Mode

```
Router RIP Config
```

■ no default-metric (RIP)

This command is used to reset the default metric of distributed routes to its default value.

Format

```
no default-metric
```

Mode

```
Router RIP Config
```

8.8.6 distance rip

This command sets the route preference value of RIP in the router. Lower route preference values are preferred when determining the best route.

Default

15

Format

```
distance rip <1-255>
```

Mode

Router RIP Config

■ no distance rip

This command sets the default route preference value of RIP in the router.

Format

```
no distance rip
```

Mode

Router RIP Config

8.8.7 distribute-list out

This command is used to specify the access list to filter routes received from the source protocol.

Default

0

Format

```
distribute-list <1-199> out {ospf | bgp | static | con-  
nected}
```

Mode

Router RIP Config

■ no distribute-list out

This command is used to specify the access list to filter routes received from the source protocol.

Format

```
no distribute-list <1-199> out {ospf | bgp | static |  
connected}
```

Mode

Router RIP Config

■ no default-information originate

This command is used to control the advertisement of default routes.

Format

```
no default-information originate
```

Mode

Router RIP Config

8.8.8 ip rip authentication

This command sets the RIP Version 2 Authentication Type and Key for the specified interface. The value of `<type>` is either `none`, `simple`, or `encrypt`.

The value for authentication key [`key`] must be 16 bytes or less. The [`key`] is composed of standard displayable, non-control keystrokes from a Standard 101/102-key keyboard. If the value of `<type>` is `encrypt`, a `keyid` in the range of 0 and 255 must be specified.

Default

The default authentication type is `none`.

Default

The default password key is an empty string. Unauthenticated interfaces do not need an authentication key.

Default

The default key id is not defined. Unauthenticated interfaces do not need an authentication key id.

Format

```
ip rip authentication {none | {simple <key>} | {encrypt
<key> <keyid>}}
```

Mode

Interface Config

■ no ip rip authentication

This command sets the default RIP Version 2 Authentication Type for an interface.

Format

```
no ip rip authentication
```

Mode

Interface Config

8.8.9 ip rip receive version

This command configures the interface to allow RIP control packets of the specified version(s) to be received.

The value for *<mode>* is one of: *rip1* to receive only RIP version 1 formatted packets, *rip2* for RIP version 2, *both* to receive packets from either format, or *none* to not allow any RIP control packets to be received.

Default

```
both
```

Format

```
ip rip receive version {rip1 | rip2 | both | none}
```

Mode

```
Interface Config
```

■ no ip rip receive version

This command configures the interface to allow RIP control packets of the default version(s) to be received.

Format

```
no ip rip receive version
```

Mode

```
Interface Config
```

8.8.10 ip rip send version

This command configures the interface to allow RIP control packets of the specified version to be sent.

The value for *<mode>* is one of: `rip1` to broadcast RIP version 1 formatted packets, `rip1c` (RIP version 1 compatibility mode) which sends RIP version 2 formatted packets via broadcast, `rip2` for sending RIP version 2 using multicast, or `none` to not allow any RIP control packets to be sent.

Default

```
rip2
```

Format

```
ip rip send version {rip1 | rip1c | rip2 | none}
```

Mode

```
Interface Config
```

■ no ip rip send version

This command configures the interface to allow RIP control packets of the default version to be sent.

Format

```
no ip rip send version
```

Mode

```
Interface Config
```

8.8.11 hostroutesaccept

This command enables the RIP hostroutesaccept mode.

Default

enabled

Format

hostroutesaccept

Mode

Router RIP Config

■ no hostroutesaccept

This command disables the RIP hostroutesaccept mode.

Format

no hostroutesaccept

Mode

Router RIP Config

8.8.12 redistribute

This command configures RIP protocol to redistribute routes from the specified source protocol/routers. There are five possible match options. When you submit the command `redistribute ospf match <match-type>` the match-type or types specified are added to any match types presently being redistributed. Internal routes are redistributed by default.

Default

```
metric -- not-configured; match -- internal
```

Format for OSPF as source protocol

```
redistribute ospf [metric <0-15>] [match [internal]
[external 1] [external 2] [nssa-external 1] [nssa-external-2]]
```

Format for other source protocol

```
redistribute {bgp | static | connected} [metric <0-15>]
```

Mode

```
Router RIP Config
```

■ no redistribute

This command de-configures RIP protocol to redistribute routes from the specified source protocol/routers.

Format

```
no redistribute {ospf | bgp | static | connected} [metric]
[match [internal] [external 1] [external 2] [nssa-external 1]
[nssa-external-2]]
```

Mode

```
Router RIP Config
```

8.8.13 split-horizon

This command sets the RIP split horizon mode.

Default

```
simple
```

Format

```
split-horizon {none | simple | poison}
```

Mode

```
Router RIP Config
```

■ no split-horizon

This command sets the default RIP split horizon mode.

Format

```
no split-horizon
```

Mode

```
Router RIP Config
```

8.8.14 update-timer

This command configures the RIP update interval in seconds. Shorter update intervals can improve the RIP convergence time significantly. However, update intervals shorter than 10 seconds should be used only for small networks. The other RIP timers are set by the switch accordingly:

Timeout: 6 times the update interval.

Garbage Collection : 10 times the update interval.

Default

30

Format

```
update-timer <1-1000>
```

Mode

Router RIP Config

■ no update-timer

This command sets the default RIP update interval.

Format

```
no update-timer
```

Mode

Router RIP Config

8.8.15 show ip rip

This command displays information relevant to the RIP router.

Format

```
show ip rip
```

Modes

Privileged EXEC

User EXEC

RIP Admin Mode

Enable or disable.

Split Horizon Mode

None, simple or poison reverse. Split horizon is a technique for avoiding problems caused by including routes in updates sent to the router from which the route was originally learned. The options are: None - no special processing for this case. Simple - a route will not be included in updates sent to the router from which it was learned. Poisoned reverse - a route will be included in updates sent to the router from which it was learned, but the metric will be set to infinity. The default is simple

Auto Summary Mode

Enable or disable. If enabled, groups of adjacent routes are summarized into single entries, in order to reduce the total number of entries. The default is enable.

Host Routes Accept Mode

Enable or disable. If enabled the router accepts host routes. The default is enable.

Update Timer Interval

Current RIP update interval in seconds.

Global Route Changes

The number of route changes made to the IP Route Database by RIP. This does not include the refresh of a route's age.

Global queries -

The number of responses sent to RIP queries from other systems.

Default Metric

Sets a default for the metric of redistributed routes. This field displays the default metric if one has already been set or blank if not configured earlier. The valid values are (1 to 15)

Default Route Advertise

The default route.

8.8.16 show ip rip interface brief

This command displays general information for each RIP interface. For this command to display successful results routing must be enabled per interface (i.e. ip rip).

Format

```
show ip rip interface brief
```

Modes

Privileged EXEC

User EXEC

Interface

Valid slot and port number separated by forward slashes.

IP Address

The IP source address used by the specified RIP interface.

Send Version

The RIP version(s) used when sending updates on the specified interface. The types are none, RIP-1, RIP-1c, RIP-2.

Receive Version

The RIP version(s) allowed when receiving updates from the specified interface. The types are none, RIP-1, RIP-2, Both

RIP Mode

RIP administrative mode of router RIP operation; enable activates, disable de-activates it.

Link State

The mode of the interface (up or down).

8.8.17 show ip rip interface

This command displays information related to a particular RIP interface.

Format

```
show ip rip interface <slot/port>
```

Modes

Privileged EXEC

User EXEC

Interface

Valid slot and port number separated by forward slashes. This is a configured value.

IP Address

The IP source address used by the specified RIP interface. This is a configured value.

Send version

The RIP version(s) used when sending updates on the specified interface. The types are none, RIP-1, RIP-1c, RIP-2. This is a configured value.

Receive version

The RIP version(s) allowed when receiving updates from the specified interface. The types are none, RIP-1, RIP-2, Both. This is a configured value.

RIP Admin Mode

RIP administrative mode of router RIP operation; enable activates, disable de-activates it. This is a configured value.

Link State

Indicates whether the RIP interface is up or down. This is a configured value.

Authentication Type

The RIP Authentication Type for the specified interface. The types are none, simple, and encrypt. This is a configured value.

Default Metric

A number which represents the metric used for default routes in RIP updates originated on the specified interface. This is a configured value.

The following information will be invalid if the link state is down.

Bad Packets Received

The number of RIP response packets received by the RIP process which were subsequently discarded for any reason.

Bad Routes Received

The number of routes contained in valid RIP packets that were ignored for any reason.

Updates Sent

The number of triggered RIP updates actually sent on this interface.

9 IP Multicast Commands

This chapter provides a detailed explanation of the IP Multicast Routing commands.

9.1 Multicast Commands

The following commands are used to configure IP Multicast.

9.1.1 ip mcast boundary

This command adds an administrative scope multicast boundary specified by <groupipaddr> and <mask> for which this multicast administrative boundary is applicable. <groupipaddr> is a group IP address and <mask> is a group IP mask.

Format

```
ip mcast boundary <groupipaddr> <mask>
```

Mode

```
Interface Config
```

■ no ip mcast boundary

This command deletes an administrative scope multicast boundary specified by <groupipaddr> and <mask> for which this multicast administrative boundary is applicable. <groupipaddr> is a group IP address and <mask> is a group IP mask.

Format

```
no ip mcast boundary <groupipaddr> <mask>
```

Mode

```
Interface Config
```

9.1.2 ip multicast

This command sets the administrative mode of the IP multicast forwarder in the router to active. For multicast routing to become operational, IGMP must be currently enabled. An error message will be displayed on the CLI if multicast routing is enabled while IGMP is disabled. However, the IP multicast mode configuration is stored in the multicast configuration file and is automatically enabled once IGMP is enabled.

Default

```
disabled
```

Format

```
ip multicast
```

Mode

```
Global Config
```

■ no ip multicast

This command sets the administrative mode of the IP multicast forwarder in the router to inactive. For multicast routing to become operational, IGMP must be currently enabled. An error message will be displayed on the CLI if multicast routing is enabled while IGMP is disabled. However, the IP multicast mode configuration is stored in the multicast configuration file and is automatically enabled once IGMP is enabled.

Format

```
no ip multicast
```

Mode

```
Global Config
```

9.1.3 ip multicast staticroute

This command creates a static route which is used to perform RPF checking in multicast packet forwarding. The combination of the *<sourceipaddr>* and the *<mask>* fields specify the network IP address of the multicast packet source. The *<groupipaddr>* is the IP address of the next hop toward the source. The *<metric>* is the cost of the route entry for comparison with other routes to the source network and is a value in the range of 0 and 255. The *current* incoming interface is used for RPF checking for multicast packets matching this multicast static route entry.

Default

none

Format

```
ip multicast staticroute <sourceipaddr> <mask>  
<rpfiaddr> <metric> <slot/port>
```

Mode

Global Config

■ no ip multicast staticroute

This command add deletes a static route in the static mcast table. The *<sourceipaddr>* is the IP address of the multicast packet source.

Format

```
no ip multicast staticroute <sourceipaddr>
```

Mode

Global Config

9.1.4 ip multicast ttl-threshold

This command applies the given *<ttlthreshold>* to a routing interface. The *<ttlthreshold>* is the TTL threshold which is to be applied to the multicast Data packets which are to be forwarded from the interface. The value for *<ttlthreshold>* has range from 0 to 255.

Default

1

Format

```
ip multicast ttl-threshold <ttlvalue>
```

Mode

Interface Config

■ no ip multicast ttl-threshold

This command applies the default *<ttlthreshold>* to a routing interface. The *<ttlthreshold>* is the TTL threshold which is to be applied to the multicast Data packets which are to be forwarded from the interface.

Format

```
no ip multicast ttl-threshold
```

Mode

Interface Config

9.1.5 disable ip multicast mdebug mtrace

This command is used to disable the processing capability of mtrace query on this router. If the mode is enable, the mtrace queries received by the router are processed and forwarded appropriately by the router. If the mode is disable, this router does not respond to the mtrace queries it receives from other router devices.

Default

none

Format

```
disable ip multicast mdebug mtrace
```

Mode

Global Config

■ no disable ip multicast mdebug mtrace

This command is used to enable the processing capability of mtrace query on this router. If the mode is enable, the mtrace queries received by the router are processed and forwarded appropriately by the router. If the mode is disable, this router does not respond to the mtrace queries it receives from other router devices.

Format

```
no disable ip multicast mdebug mtrace
```

Mode

Global Config

9.1.6 mrimfo

This command is used to query the neighbor information of a multicast-capable router specified by [ipaddr]. The default value is the IP address of the system at which the command is issued. The mrimfo command can take up to 2 minutes to complete. Only one mrimfo command may be in process at a time. The results of this command will be available in the results bufferpool which can be displayed by using "show mrimfo".

Default

none

Format

```
mrimfo [<ipaddr>]
```

Mode

Privileged EXEC

9.1.7 mstat

This command is used to find the IP Multicast packet rate and loss information path from a source to a receiver (unicast router id of the host running mstat). The results of this command will be available in the results bufferpool which can be displayed by using the command “show mstat” on page 760. If a debug command is already in progress, a message is displayed and the new request fails.

The <source> is the IP address of the remote multicast-capable source. The [receiver] is the IP address of the receiver. The default value is the IP address of the system at which the command is issued. The [group] is a multicast address of the group to be displayed. The default value is 224.2.0.1 (the group used for the multicast backbone).

Note: The group and receiver IP addresses can be entered in any order.

Default

none

Format

```
mstat <source> [<group/receiver>] [<group/
receiver>]
```

Mode

Privileged EXEC

9.1.8 mtrace

This command is used to find the IP Multicast path from a source to a receiver (unicast router ID of the host running mtrace). A trace query is passed hop-by-hop along the reverse path from the receiver to the source, collecting hop addresses, packet counts, and routing error conditions along the path, and then the response is returned to the requestor. The results of this command are available in the results buffer pool which can be displayed by using the command “show mtrace” on page 761.

The <source> is the IP address of the remote multicast-capable source. The [receiver] is the IP address of the receiver. The default value is the IP address of system at which the command is issued. The [group] is the multicast address of the group to be displayed. The default value is 224.2.0.1 (the group used for the multicast backbone).

If a debug command is already in execution, a message is displayed and the new request fails.

Note: The group and destination IP addresses can be entered in any order.

Default

none

Format

```
mtrace <sourceipaddr> [<group/destination>]
[<group/destination >]
```

Mode

Privileged EXEC

9.1.9 no ip mcast mroute

This command is used to clear entries in the mroute table. The all parameters is used to clear all entries.

The source parameter is used to clear the routes in the mroute table entries containing the specified *<sourceipaddr>* or *<sourceipaddr> [groupipaddr]* pair. The source address is the source IP address of the multicast packet. The group address is the Group Destination IP address of the multicast packet.

The group parameter is used to clear the routes in the mroute table entries containing the specified *<groupipaddr>*. The group address is the Group Destination IP address of the multicast packet.

Default

none

Format

```
no ip mcast mroute {group <groupipaddr> | source  
<sourceipaddr> [<groupipaddr>] | all}
```

Mode

Global Config

9.1.10 show ip mcast

This command displays the system-wide multicast information.

Format

```
show ip mcast
```

Modes

```
Privileged EXEC
```

```
User EXEC
```

Admin Mode

```
The administrative status of multicast.
```

Protocol State

```
The current state of the multicast protocol. Possible values are Operational or Non-Operational.
```

Table Max Size

```
The maximum number of entries allowed in the multicast table.
```

Number Of Packets For Which Source Not Found

```
The number of packets for which the source is not found.
```

Number Of Packets For Which Group Not Found

```
The number of packets for which the group is not found.
```

Protocol

```
The multicast protocol running on the router. Possible values are PIMDM, PIMSM or DVMRP.
```

Entry Count

```
The number of entries in the multicast table.
```

Highest Entry Count

```
The highest entry count in the multicast table.
```

9.1.11 show ip mcast boundary

This command displays all the configured administrative scoped multicast boundaries.

Format

```
show ip mcast boundary {<slot/port> | all}
```

Modes

Privileged EXEC

User EXEC

Interface

Valid slot and port number separated by forward slashes.

Group Ip

The group IP address

Mask

The group IP mask

9.1.12 show ip mcast interface

This command displays the multicast information for the specified interface.

Format

```
show ip mcast interface <slot/port>
```

Modes

Privileged EXEC

User EXEC

Interface

Valid slot and port number separated by forward slashes.

TTL

The time-to-live value for this interface.

9.1.13 show ip mcast mroute

This command displays a summary or all the details of the multicast table.

Format

```
show ip mcast mroute {detail | summary}
```

Modes

Privileged EXEC

User EXEC

If the “detail” parameter is specified, the following fields are displayed:

Source IP Addr

The IP address of the multicast data source.

Group IP Addr

The IP address of the destination of the multicast packet.

Expiry Time

The time of expiry of this entry in seconds.

Up Time

The time elapsed since the entry was created in seconds.

RPF Neighbor

The IP address of the RPF neighbor.

Flags

The flags associated with this entry.

If the “summary” parameter is specified, the following fields are displayed:

Source IP Addr

The IP address of the multicast data source.

Group IP Addr

The IP address of the destination of the multicast packet.

Protocol

The multicast routing protocol by which the entry was created.

Incoming Interface

The interface on which the packet for the source/group arrives.

Outgoing Interface List

The list of outgoing interfaces on which the packet is forwarded.

9.1.14 show ip mcast mroute group

This command displays the multicast configuration settings such as flags, timer settings, incoming and outgoing interfaces, RPF neighboring routers, and expiration times of all the entries in the multicast mroute table containing the given *<groupipaddr>*.

Format

```
show ip mcast mroute group <groupipaddr> {detail
|summary}
```

Modes

Privileged EXEC

User EXEC

Source IP Addr

The IP address of the multicast data source.

Group IP Addr

The IP address of the destination of the multicast packet.

Protocol

The multicast routing protocol by which this entry was created.

Incoming Interface

The interface on which the packet for this group arrives.

Outgoing Interface List

The list of outgoing interfaces on which this packet is forwarded.

9.1.15 show ip mcast mroute source

This command displays the multicast configuration settings such as flags, timer settings, incoming and outgoing interfaces, RPF neighboring routers, and expiration times of all the entries in the multicast mroute table containing the given `<sourceipaddr>` or `<sourceipaddr> [<groupipaddr>]` pair.

Format

```
show ip mcast mroute source <sourceipaddr> {summary  
| <groupipaddr>}
```

Modes

Privileged EXEC

User EXEC

If the detail parameter is specified the follow fields are displayed:

Source IP Addr

The IP address of the multicast data source.

Group IP Addr

The IP address of the destination of the multicast packet.

Expiry Time

The time of expiry of this entry in seconds.

Up Time

The time elapsed since the entry was created in seconds.

RPF Neighbor

The IP address of the RPF neighbor.

Flags

The flags associated with this entry.

If the summary parameter is specified the follow fields are displayed:

Source IP Addr

The IP address of the multicast data source.

Group IP Addr

The IP address of the destination of the multicast packet.

Protocol

The multicast routing protocol by which this entry was created.

Incoming Interface

The interface on which the packet for this source arrives.

Outgoing Interface List

The list of outgoing interfaces on which this packet is forwarded.

9.1.16 show ip mcast mroute static

This command displays all the static routes configured in the static mcast table if is specified or displays the static route associated with the particular *<sourceipaddr>*.

Format

```
show ip mcast mroute static [<sourceipaddr>]
```

Modes

Privileged EXEC

User EXEC

Source Address

The IP address of the multicast packet source.

Source Mask

The mask applied to the IP address of the multicast packet source.

RPF Address

The IP address to be used as RPF for the given source and mask.

Metric

The metric value corresponding to the source address.

Interface

Valid slot and port number separated by forward slashes.

9.1.17 show mrimfo

This command is used to display the neighbor information of a multicast-capable router from the results buffer pool of the router subsequent to the execution/completion of a "mrimfo [ipaddr]" command. The results subsequent to the completion of the latest "mrimfo" will be available in the buffer pool after a maximum duration of two minutes after the completion of the 'show mrimfo' command. A subsequent issue 'mrimfo' will overwrite the contents of the buffer pool with fresh results.

Default

none

Format

show mrimfo

Mode

Privileged EXEC

Router Interface

The IP address of this neighbor

Neighbor

The neighbor associated with the router interface

Metric

The metric value associated with this neighbor

TTL

The TTL threshold associated with this neighbor

Flags

Status of the neighbor

9.1.18 show mstat

This command is used to display the results of packet rate and loss information from the results buffer pool of the router, subsequent to the execution/completion of a 'mstat <source> [group] [receiver]' command. Within two minutes of the completion of the 'mstat' command, the results will be available in the buffer pool. The next issuing of "mstat" would overwrite the buffer pool with fresh results.

Default

none

Format

show mstat

Mode

Privileged EXEC

9.1.19 show mtrace

This command is used to display results of multicast trace path from the results buffer pool of the router, subsequent to the execution/completion of a "mtrace <source> [group] [receiver]" command. The results subsequent to the completion of the "mtrace" will be available in the buffer pool within two minutes and thereafter. A subsequent "mtrace" command would overwrite the results in the buffer pool.

Default

none

Format

```
show mtrace
```

Modes

Privileged EXEC

User EXEC

Hops Away From Destination

The ordering of intermediate routers between the source and the destination

Intermediate Router Address

The address of the intermediate router at the specified hop distance

Mcast Protocol In Use

The multicast routing protocol used for the out interface of the specified intermediate router.

TTL Threshold

The Time-To-Live threshold of the out interface on the specified intermediate router.

Time Elapsed Between Hops (msecs)

The time between arrival at one intermediate router to the arrival at the next.

9.2 DVMRP Commands

This section provides a detailed explanation of the Distance Vector Multicast Routing Protocol (DVMRP) commands.

DVMRP is a dense mode multicast protocol and is most appropriate for use in networks where bandwidth is relatively plentiful and there is at least one multicast group member in each subnet. DVMRP assumes that all hosts are part of a multicast group until it is informed of multicast group changes. When the dense-mode multicast router is informed of a group membership change, the multicast delivery tree is pruned. DVMRP uses a distributed routing algorithm to build per-source-group multicast trees. It is also called Broadcast and Prune Multicasting protocol. It dynamically generates per-source-group multicast trees using Reverse Path Multicasting. Trees are calculated and updated dynamically to track membership of individual groups.

The commands are divided into the following 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.

9.2.1 ip dvmrp

This command sets administrative mode of DVMRP in the router to active. IGMP must be enabled before DVMRP can be enabled.

Default

disabled

Format

ip dvmrp

Mode

Global Config

■ no ip dvmrp

This command sets administrative mode of DVMRP in the router to inactive.

Format

no ip dvmrp

Mode

Global Config

9.2.2 ip dvmrp metric

This command configures the metric for an interface. This value is used in the DVMRP messages as the cost to reach this network. This field has a range of 1 to 31.

Default

1

Format

```
ip dvmrp metric <metric>
```

Mode

Interface Config

■ no ip dvmrp metric

This command resets the metric for an interface to the default value. This value is used in the DVMRP messages as the cost to reach this network.

Format

```
no ip dvmrp metric
```

Mode

Interface Config

9.2.3 ip dvmrp trapflags

This command enables the DVMRP trap mode.

Default

disabled

Format

```
ip dvmrp trapflags
```

Mode

Global Config

■ no ip dvmrp trapflags

This command disables the DVMRP trap mode.

Format

```
no ip dvmrp trapflags
```

Mode

Global Config

9.2.4 ip dvmrp

This command sets the administrative mode of DVMRP on an interface to active.

Default

disabled

Format

ip dvmrp

Mode

Interface Config

■ no ip dvmrp

This command sets the administrative mode of DVMRP on an interface to inactive.

Format

no ip dvmrp

Mode

Interface Config

9.2.5 show ip dvmrp

This command displays the system-wide information for DVMRP.

Format

```
show ip dvmrp
```

Modes

```
Privileged EXEC
```

```
User EXEC
```

Admin Mode

```
This field indicates whether DVMRP is enabled or disabled.
```

Version String

```
The version of DVMRP being used.
```

Number of Routes

```
The number of routes in the DVMRP routing table.
```

Reachable Routes

```
The number of entries in the routing table with non-infinite metrics.
```

The following fields are displayed for each interface.

Interface

```
Valid slot and port number separated by forward slashes.
```

Interface Mode

```
The mode of this interface. Possible values are Enabled and Disabled.
```

State

```
The current state of DVMRP on this interface. Possible values are Operational or Non-Operational.
```

9.2.6 show ip dvmrp interface

This command displays the interface information for DVMRP on the specified interface.

Format

```
show ip dvmrp interface <slot/port>
```

Modes

Privileged EXEC

User EXEC

Interface Mode

This field indicates whether DVMRP is enabled or disabled on the specified interface.

Metric

The metric of this interface. This is a configured value.

Local Address

The IP Address of the interface.

This Field is displayed only when DVMRP is operational on the interface.

Generation ID

The Generation ID value for the interface. This is used by the neighboring routers to detect that the DVMRP table should be resent.

The following fields are displayed only if DVMRP is enabled on this interface.

Received Bad Packets

The number of invalid packets received.

Received Bad Routes

The number of invalid routes received.

Sent Routes

The number of routes that have been sent on this interface.

9.2.7 show ip dvmrp neighbor

This command displays the neighbor information for DVMRP.

Format

```
show ip dvmrp neighbor
```

Modes

Privileged EXEC

User EXEC

IfIndex

The value of the interface used to reach the neighbor.

Nbr IP Addr

The IP Address of the DVMRP neighbor for which this entry contains information.

State

The state of the neighboring router. The possible value for this field are ACTIVE or DOWN.

Up Time

The time since this neighboring router was learned.

Expiry Time

The time remaining for the neighbor to age out.

This field is not applicable if the State is DOWN.

Generation ID

The Generation ID value for the neighbor.

Major Version

The major version of DVMRP protocol of neighbor.

Minor Version

The minor version of DVMRP protocol of neighbor.

Capabilities

The capabilities of neighbor.

Received Routes

The number of routes received from the neighbor.

Rcvd Bad Pkts

The number of invalid packets received from this neighbor.

Rcvd Bad Routes

The number of correct packets received with invalid routes.

9.2.8 show ip dvmrp nexthop

This command displays the next hop information on outgoing interfaces for routing multicast datagrams.

Format

```
show ip dvmrp nexthop
```

Modes

Privileged EXEC

User EXEC

Source IP

The sources for which this entry specifies a next hop on an outgoing interface.

Source Mask

The IP Mask for the sources for which this entry specifies a next hop on an outgoing interface.

Next Hop Interface

The interface in slot/port format for the outgoing interface for this next hop.

Type

The network is a LEAF or a BRANCH.

9.2.9 show ip dvmrp prune

This command displays the table listing the router's upstream prune information.

Format

```
show ip dvmrp prune
```

Modes

Privileged EXEC

User EXEC

Group IP

This field identifies the multicast Address that is pruned.

Source IP

This field displays the IP Address of the source that has pruned.

Source Mask

This field displays the network Mask for the prune source. It should be all 1s or both the prune source and prune mask must match.

Expiry Time (secs)

This field indicates the expiry time in seconds. This is the time remaining for this prune to age out.

9.2.10 show ip dvmrp route

This command displays the multicast routing information for DVMRP.

Format

```
show ip dvmrp route
```

Modes

Privileged EXEC

User EXEC

Source Address

This field displays the multicast address of the source group.

Source Mask

This field displays the IP Mask for the source group.

Upstream Neighbor

This field indicates the IP Address of the neighbor which is the source for the packets for a specified multicast address.

Interface

This field displays the interface used to receive the packets sent by the sources.

Metric

This field displays the distance in hops to the source subnet. This field has a different meaning than the Interface Metric field.

Expiry Time (secs)

This field indicates the expiry time in seconds. This is the time remaining for this route to age out.

Up Time (secs)

This field indicates the time when a specified route was learnt, in seconds.

9.3 IGMP Commands

This section provides a detailed explanation of the Internet Group Management Protocol (IGMP) commands. The commands are divided into the following 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.

9.3.1 ip igmp

This command enables Multicast Routing.

This command also enables IGMP and IGMP snooping (MACH4000).

Default

```
disabled
```

Format

```
ip igmp
```

Mode

```
Global Config
```

■ no ip igmp

This command sets the administrative mode of IGMP in the router to inactive.

Format

```
no ip igmp
```

Mode

```
Global Config
```

9.3.2 ip igmp version

This command configures the version of IGMP for an interface. The value for <version> is either 1, 2 or 3.

Default

2

Format

```
ip igmp version <version>
```

Mode

Interface Config

■ no ip igmp version

This command resets the version of IGMP to the default value.

Format

```
no ip igmp version
```

Mode

Interface Config

9.3.3 ip igmp last-member-query-count

This command sets the number of Group-Specific Queries sent before the router assumes that there are no local members on the interface. The range for <count> is 1..20.

Format

```
ip igmp last-member-query-count <count>
```

Mode

```
Interface Config
```

■ no ip igmp last-member-query-count

This command resets the number of Group-Specific Queries to the default value.

Format

```
no ip igmp last-member-query-count
```

Mode

```
Interface Config
```

9.3.4 ip igmp last-member-query-interval

This command configures the Maximum Response Time being inserted into Group-Specific Queries sent in response to Leave Group messages on the interface.

The range for <tenth_seconds> is 0..255 tenths of a second.

Default

10 tenths of a second (1 second)

Format

```
ip igmp last-member-query-interval <tenth_seconds>
```

Mode

Interface Config

<tenth_seconds>

Enter last member query interval in tenths of a second.

Valid range: 0 to 255.

■ no ip igmp last-member-query-interval

This command resets the Maximum Response Time being inserted into Group-Specific Queries sent in response to Leave Group messages on the interface to the default value.

Format

```
no ip igmp last-member-query-interval
```

Mode

Interface Config

9.3.5 ip igmp query-interval

This command configures the query interval for the specified interface. This is the frequency at which IGMP Host-Query packets are transmitted on this interface.

The range for <seconds> is 1..3600 seconds.

Default

125 seconds

Format

```
ip igmp query-interval <seconds>
```

Mode

Interface Config

■ no ip igmp query-interval

This command resets the query interval for the specified interface to the default value. This is the frequency at which IGMP Host-Query packets are transmitted on this interface.

Format

```
no ip igmp query-interval
```

Mode

Interface Config

9.3.6 ip igmp query-max-response-time

This command configures the maximum response time interval for the specified interface, which is the maximum query response time advertised in IGMPv2 queries on this interface. The time interval is specified in tenths of a second.

The range for <seconds> is 0..255 tenths of a second.

Default

100

Format

```
ip igmp query-max-response-time <seconds>
```

Mode

Interface Config

■ no ip igmp query-max-response-time

This command resets the maximum response time interval for the specified interface, which is the maximum query response time advertised in IGMPv2 queries on this interface to the default value. The maximum response time interval is reset to the default time.

Format

```
no ip igmp query-max-response-time
```

Mode

Interface Config

9.3.7 ip igmp robustness

This command configures the robustness that allows tuning of the interface. The robustness is the tuning for the expected packet loss on a subnet. If a subnet is expected to have a lot of loss, the Robustness variable may be increased for the interface.

The range for <robustness> is 1..255.

Default

2

Format

```
ip igmp robustness <robustness>
```

Mode

Interface Config

■ no ip igmp robustness

This command sets the robustness value to default.

Format

```
no ip igmp robustness
```

Mode

Interface Config

9.3.8 ip igmp startup-query-count

This command sets the number of Queries sent out on startup, separated by the Startup Query Interval on the interface.

The range for <count> is 1..20.

Default

2

Format

```
ip igmp startup-query-count <count>
```

Mode

Interface Config

■ no ip igmp startup-query-count

This command resets the number of Queries sent out on startup, separated by the Startup Query Interval on the interface to the default value.

Format

```
no ip igmp startup-query-count
```

Mode

Interface Config

9.3.9 ip igmp startup-query-interval

This command sets the interval between General Queries sent on startup on the interface. The time interval value is in seconds.

The range for <interval> is 1..300 seconds.

Default

1

Format

```
ip igmp startup-query-interval <interval>
```

Mode

Interface Config

■ no ip igmp startup-query-interval

This command resets the interval between General Queries sent on startup on the interface to the default value.

Format

```
no ip igmp startup-query-interval
```

Mode

Interface Config

9.3.10 show ip igmp

This command displays the system-wide IGMP information.

Format

```
show ip igmp
```

Modes

Privileged EXEC

User EXEC

IGMP Admin Mode

This field displays the administrative status of IGMP. This is a configured value.

Interface

Valid slot and port number separated by forward slashes.

Interface Mode

This field indicates whether IGMP is enabled or disabled on the interface. This is a configured value.

Protocol State

This field indicates the current state of IGMP on this interface. Possible values are Operational or Non-Operational.

9.3.11 show ip igmp groups

This command displays the registered multicast groups on the interface. If [detail] is specified this command displays the registered multicast groups on the interface in detail.

Format

```
show ip igmp groups <slot/port> [detail]
```

Mode

Privileged EXEC
User EXEC

If detail is not specified, the following fields are displayed:

IP Address

This displays the IP address of the interface participating in the multicast group.

Subnet Mask

This displays the subnet mask of the interface participating in the multicast group.

Interface Mode

This displays whether IGMP is enabled or disabled on this interface.

The following fields are not displayed if the interface is not enabled:

Querier Status

This displays whether the interface has IGMP in Querier mode or Non-Querier mode.

Groups

This displays the list of multicast groups that are registered on this interface.

If detail is specified, the following fields are displayed:

Multicast IP Address

This displays the IP Address of the registered multicast group on this interface.

Last Reporter

This displays the IP Address of the source of the last membership report received for the specified multicast group address on this interface.

Up Time

This displays the time elapsed since the entry was created for the specified multicast group address on this interface.

Expiry Time

This displays the amount of time remaining to remove this entry before it is aged out.

Version1 Host Timer

This displays the time remaining until the local router will assume that there are no longer any IGMP version 1 multicast members on the IP subnet attached to this interface. This could be an integer value or "-----" if there is no Version 1 host present.

Version2 Host Timer

This displays the time remaining until the local router will assume that there are no longer any IGMP version 2 multicast members on the IP subnet attached to this interface. This could be an integer value or "-----" if there is no Version 2 host present.

Group Compatibility Mode

The group compatibility mode (v1, v2 or v3) for this group on the specified interface.

9.3.12 show ip igmp interface

This command displays the IGMP information for the interface.

Format

```
show ip igmp interface <slot/port>
```

Modes

Privileged EXEC

User EXEC

Interface

Valid slot and port number separated by forward slashes.

IGMP Admin Mode

The administrative status of IGMP.

Interface Mode

This field indicates whether IGMP is enabled or disabled on the interface.

IGMP Version

The version of IGMP running on the interface. This value can be configured to create a router capable of running either IGMP version 1 or 2.

Query Interval

The frequency at which IGMP Host-Query packets are transmitted on this interface.

Query Max Response Time

The maximum query response time advertised in IGMPv2 queries on this interface.

Robustness

The tuning for the expected packet loss on a subnet. If a subnet is expected to have a lot of loss, the Robustness variable may be increased for that interface.

Startup Query Interval

The interval between General Queries sent by a Querier on startup.

Startup Query Count

The number of Queries sent out on startup, separated by the Startup Query Interval.

Last Member Query Interval

The Maximum Response Time inserted into Group-Specific Queries sent in response to Leave Group messages.

Last Member Query Count

The number of Group-Specific Queries sent before the router assumes that there are no local members.

9.3.13 show ip igmp interface membership

This command displays the list of interfaces that have registered in the multicast group.

Format

```
show ip igmp interface membership <multiipaddr>
[detail]
```

Mode

Privileged EXEC

Interface

Valid unit, slot and port number separated by forward slashes.

Interface IP

The IP address of the interface participating in the multicast group.

State

The interface that has IGMP in Querier mode or Non-Querier mode.

Group Compatibility Mode

The group compatibility mode (v1, v2 or v3) for the specified group on this interface.

Source Filter Mode

The source filter mode (Include/Exclude) for the specified group on this interface. This is "-----" for IGMPv1 and IGMPv2 Membership Reports.

If detail is specified, the following fields are displayed:

Interface

Valid unit, slot and port number separated by forward slashes.

Group Compatibility Mode

The group compatibility mode (v1, v2 or v3) for the specified group on this interface.

Source Filter Mode

The source filter mode (Include/Exclude) for the specified group on this interface. This is "-----" for IGMPv1 and IGMPv2 Membership Reports.

Source Hosts

The list of unicast source IP Addresses in the group record of the IGMPv3 Membership Report with the specified multicast group IP Address. This is "-----" for IGMPv1 and IGMPv2 Membership Reports.

Expiry Time

The amount of time remaining to remove this entry before it is aged out. This is "-----" for IGMPv1 and IGMPv2 Membership Reports.

9.3.14 show ip igmp interface stats

This command displays the IGMP statistical information for the interface. The statistics are only displayed when the interface is enabled for IGMP.

Format

```
show ip igmp interface stats <slot/port>
```

Modes

Privileged EXEC

User EXEC

Querier Status

The status of the IGMP router, whether it is running in Querier mode or Non-Querier mode.

Querier IP Address

The IP Address of the IGMP Querier on the IP subnet to which this interface is attached.

Querier Up Time

The time since the interface Querier was last changed.

Querier Expiry Time

The amount of time remaining before the Other Querier Present Timer expires. If the local system is the querier, the value of this object is zero.

Wrong Version Queries

The number of queries received whose IGMP version does not match the IGMP version of the interface.

Number of Joins

The number of times a group membership has been added on this interface.

Number of Groups

The current number of membership entries for this interface

9.4 PIM-DM Commands

This section provides a detailed explanation of the Protocol Independent Multicast - Dense Mode (PIM-DM) commands.

PIM-DM is most appropriate for networks with relatively plentiful bandwidth and with at least one multicast member in each subnet. PIM-DM assumes that all hosts are part of a multicast group and forwards packets to hosts until informed that group membership has changed. A group membership change results in the multicast delivery tree being pruned.

The commands are divided into the following 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.

9.4.1 ip pimdm

This command enables the administrative mode of PIM-DM in the router.

Default

disabled

Format

ip pimdm

Mode

Global Config

■ no ip pimdm

This command disables the administrative mode of PIM-DM in the router. IGMP must be enabled before PIM-DM can be enabled.

Format

no ip pimdm

Mode

Global Config

9.4.2 ip pimdm holdtimes

This command configures the holdtimes for prunes and asserts. This field has a range of 30 to 64800 seconds (= 18 hours)

Default

210

Format

```
ip pimdm holdtimes <seconds>
```

Mode

Global Config

■ no ip pimdm holdtimes

This command resets the holdtimes to the default value.

Format

```
no ip pimdm holdtimes
```

Mode

Global Config

9.4.3 ip pimdm mode

This command sets administrative mode of PIM-DM on an interface in the router to enabled.

Default

disabled

Format

```
ip pimdm mode <slot/port>
```

Mode

Interface Config

■ no ip pimdm mode

This command sets administrative mode of PIM-DM on an interface in the router to disabled.

Format

```
no ip pimdm mode <slot/port>
```

Mode

Interface Config

9.4.4 ip pimdm hello-interval

This command configures the transmission frequency of hello messages between PIM enabled neighbors. This field has a range of 1 to 3600 seconds.

Default

30

Format

```
ip pimdm query-interval <seconds>
```

Mode

Interface Config

■ no ip pimdm hello-interval

This command resets the transmission frequency of hello messages between PIM enabled neighbors to the default value.

Format

```
no ip pimdm query-interval
```

Mode

Interface Config

9.4.5 show ip pimdm

This command displays the system-wide information for PIM-DM.

Format

```
show ip pimdm
```

Modes

Privileged EXEC

User EXEC

PIM-DM Admin Mode

This field indicates whether PIM-DM is enabled or disabled.

Holdtimes

This field displays the configured holdtimes for prunes and asserts.

Interface

Valid slot and port number separated by forward slashes.

Interface Mode

This field indicates whether PIM-DM is enabled or disabled on this interface.

State

The current state of PIM-DM on this interface. Possible values are Operational or Non-Operational.

9.4.6 show ip pimdm interface

This command displays the interface information for PIM-DM on the specified interface.

Format

```
show ip pimdm interface <slot/port>
```

Modes

Privileged EXEC

User EXEC

Interface Mode

This field indicates whether PIM-DM is enabled or disabled on the specified interface.

PIM-DM Interface Hello Interval

The frequency at which PIM hello messages are transmitted on this interface. By default, the value is 30 seconds.

9.4.7 show ip pimdm interface stats

This command displays the statistical information for PIM-DM on the specified interface.

Format

```
show ip pimdm interface stats {<slot/port> | all}
```

Modes

Privileged EXEC

User EXEC

Interface

Valid slot and port number separated by forward slashes.

IP Address

The IP Address that represents the PIM-DM interface.

Nbr Count

The neighbor count for the PIM-DM interface.

Hello Interval

The time interval between two hello messages sent from the router on the given interface.

Designated Router

The IP Address of the Designated Router for this interface.

9.4.8 show ip pimdm neighbor

This command displays the neighbor information for PIM-DM on the specified interface.

Format

```
show ip pimdm neighbor {<slot/port> | all}
```

Modes

Privileged EXEC

User EXEC

Neighbor Address

The IP Address of the neighbor on an interface.

Interface

Valid slot and port number separated by forward slashes.

Up Time

The time since this neighbor has become active on this interface.

Expiry Time

The expiry time of the neighbor on this interface.

9.4.9 ip pim-trapflags

This command enables the PIM trap mode for both Sparse Mode (SM) and Dense Mode. (DM).

Default

disabled

Format

```
ip pim-trapflags
```

Mode

Global Config

■ no ip pim-trapflags

This command sets the PIM trap mode to the default.

Format

```
no ip pim-trapflags
```

Mode

Global Config

9.5 PIM-SM Commands

This section provides a detailed explanation of the Protocol Independent Multicast - Sparse Mode (PIM-SM) commands.

PIM-SM routes multicast packets to multicast groups, and is designed to efficiently establish distribution trees across wide area networks (WANs).

The Sparse Mode (SM) version of PIM is most appropriate for networks with relatively limited bandwidth and where group membership is widely distributed across regions. Sparse mode protocols begin with the assumption that few routers in the network will be involved in any given multicast path. Sparse mode routers minimize network traffic by adding branches to the tree only when explicitly requested to do so. Therefore, sparse mode protocols such as PIM-SM are better suited to WANs than the dense mode protocols.

PIM-SM uses the following concepts:

- ▶ Rendezvous Point (RP): The root of a shared distribution tree down which all multicast traffic flows.
- ▶ Designated Router (DR): Responsible for sending join messages to the RP for group members and for sending register messages to the RP for sources.
- ▶ Bootstrap Router (BSR): mechanism which provides a way in which viable group-to-RP mappings can be created and distributed to all the PIM-SM routers in a domain. This component implements the functionality for handling C-RP Advertisement and Bootstrap messages, for RP-Set creation and distribution in the PIM domain, as well as the procedures for BSR election.

The commands are divided into the following 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.

9.5.1 ip pimsm mode

This command is used to administratively enable PIM-SM multicast routing mode on a particular router interface.

Default

disabled

Format

```
ip pimsm mode
```

Mode

Interface Config

■ no ip pimsm mode

This command is used to administratively disable PIM-SM multicast routing mode on a particular router interface.

Format

```
no ip pimsm mode
```

Mode

Interface Config

9.5.2 ip pimsm bsr-border

Use this command to prevent bootstrap router (BSR) messages from being sent or received through an interface.

Default

disabled

Format

```
ip pimsm bsr-border
```

Mode

Interface Config

■ no ip pimsm bsr-border

Use this command to disable the interface from being the BSR border.

Format

```
no ip pimsm bsr-border
```

Mode

Interface Config

9.5.3 ip pimsm dr-priority

Use this command to set the priority value for which a router is elected as the designated router (DR).

Default

1

Format

```
ip pimsm dr-priority <0-2147483647>
```

Mode

Interface Config

<0-2147483647>

Enter the Designated Router priority <0 - 2147483647>.

■ no ip pimsm dr-priority

Use this command to set the DR priority for the interface to the default value.

Format

```
no ip pimsm dr-priority
```

Mode

Interface Config

9.5.4 ip pimsm join-prune-interval

This command is used to configure the interface join/prune interval for the PIM-SM router. The join/prune interval is specified in seconds. This parameter can be configured to a value from 1 to 18,000.

Default

60

Format

```
ip pimsm join-prune-interval <1-18000>
```

Mode

Interface Config

■ no ip pimsm join-prune-interval

Use this command to set the join/prune interval to the default value.

Format

```
no ip pimsm join-prune-interval
```

Mode

Interface Config

9.5.5 ip pimsm hello-interval

This command is used to configure the PIM-SM hello interval for the specified interface. The hello interval is specified in seconds. This parameter can be configured to a value from 1 to 18,000.

Default

30

Format

```
ip pimsm hello-interval <1-18000>
```

Mode

Interface Config

■ no ip pimsm hello-interval

Use this command to set the hello-interval to the default value.

Format

```
no ip pimsm hello-interval
```

Mode

Interface Config

9.5.6 ip pimsm bsr-candidate

This command is used to configure the router to announce its candidacy as a bootstrap router (BSR).

Format

```
ip pimsm bsr-candidate interface <slot/port>
                               [hash-mask-length] [priority]
```

Mode

Global Config

■ no ip pimsm bsr-candidate

This command is used to disable the router to announce its candidacy as a bootstrap router (BSR).

Format

```
no ip pimsm bsr-candidate interface <slot/port>
    [hash-mask-length] [priority]
```

Mode

Global Config

9.5.7 ip pimsm register-threshold

This command configures the Register Threshold rate for the Rendezvous Point router to switch to a source-specific shortest path. The valid values are 0 to 2,000 kilobits/sec.

Default

0

Format

```
ip pimsm register-threshold <0-2000>
```

Mode

Global Config

<0-2000>

Enter the rate in kilobits per seconds <0-2000>.

■ no ip pimsm register-threshold

This command resets the register threshold rate for the Rendezvous Pointer router to the default value.

Format

```
no ip pimsm register-threshold
```

Mode

Global Config

9.5.8 ip pimsm rp-address

This command is used to statically configure the Rendezvous Point (RP) address for one or more multicast groups.

Default

0

Format

```
ip pimsm rp-address <rp-address> <group-address>
                               <group-mask> [override]
```

Mode

Global Config

<rp-address>

Enter the IP Address of the RP.

<group-address>

Enter the Group Address supported by the RP.

<group-mask>

Enter the Group Mask for the Group Address.

[override]

The optional keyword `override` indicates that if there is a conflict, the RP configured with this command prevails over the RP learned by BSR.

■ no ip pimsm rp-address

This command is used to statically remove the RP address for one or more multicast groups.

Format

```
no ip pimsm rp-address <rpaddress> <group-address>
                               <group-mask>
```

Mode

Global Config

9.5.9 ip pimsm rp-candidate

This command is used to configure the router to advertise itself as a PIM candidate rendezvous point (RP) to the bootstrap router (BSR).

Format

```
ip pimsm rp-candidate interface <slot/port>
                               <group-address> <group-mask>
```

Mode

Global Config

<group-address>

Enter the Group Address supported by the RP.

<group-mask>

Enter the Group Mask for the Group Address.

■ no ip pimsm rp-candidate

This command is used to disable the router to advertise itself as a PIM candidate rendezvous point (RP) to the bootstrap router (BSR).

Format

```
no ip pimsm rp-candidate interface <slot/port>
                               <group-address> <group-mask>
```

Mode

Global Config

9.5.10 ip pimsm ssm default

This command is used to define the SSM range access list to 232/8.

Format

```
ip pimsm ssm default
```

Mode

Global Config

9.5.11 ip pimsm ssm

This command is used to define the SSM range.

Format

```
ip pimsm ssm <group-address> [group-mask]
```

Mode

```
Global Config
```

<group-address>

Enter the Group Address supported by the RP.

<group-mask>

Enter the Group Mask for the Group Address.

■ no ip pimsm

This command is used to disable the SSM range

Format

```
no ip pimsm ssm <group-address> [group-mask]
```

Mode

```
Global Config
```

9.5.12 show ip pimsm

This command is used to display the PIM-SM parameters.

Format

```
ip pimsm ssm
```

Mode

```
Privileged EXEC  
User EXEC
```

Admin Mode

```
Enable/Disable
```

Data Threshold Rate (Kbps)

```
Display the Data Threshold Rate in Kbps.  
Default: 0
```

Register Threshold Rate (Kbps)

```
Display the Register Threshold Rate in Kbps.  
Default: 0
```

SSM RANGE TABLE

```
Display the SSM RANGE TABLE information (Group Address/Prefix  
Length).
```

Group Address/Prefix Length

```
Display the Group Address/Prefix Length.
```

PIM-SM INTERFACE STATUS

```
Display the PIM-SM INTERFACE STATUS table information  
(Interface, Interface-Mode, Operational-Status).
```

Interface

```
Display the Interface information.
```

Interface-Mode

```
Display the Interface-Mode information.
```

Operational-Status

```
Display the Operational-Status information.
```

9.5.13 show ip pimsm bsr

This command is used to display PIM-SM BSR table information.

Format

```
ip pimsm ssm bsr
```

Mode

```
Privileged EXEC
```

```
User EXEC
```

9.5.14 show ip pimsm interface

This command is used to display PIM-SM status of the router.

Format

```
ip pimsm ssm interface
```

Mode

```
Privileged EXEC
```

```
User EXEC
```

9.5.15 show ip pimsm neighbor

This command is used to display router's PIM neighbors on the interface.

Format

```
ip pimsm ssm neighbor
```

Mode

```
Privileged EXEC
```

```
User EXEC
```

9.5.16 show ip pimsm rp mapping

Use this command to display all group-to-RP mappings of which the router is aware (either configured or learned from the bootstrap router (BSR)). If no RP is specified, all active RPs are displayed.

Format

```
ip pimsm ssm rp mapping [rp-address]
```

Mode

Privileged EXEC

User EXEC

9.5.17 show ip pimsm rphash

This command is used to display the PIM-SM RP information for a specific group.

Format

```
ip pimsm ssm rphash <group-address>
```

Mode

Privileged EXEC

User EXEC

9.5.18 show ip pimsm candidate

This command is used to display PIM-SM candidate-RP table information.

Format

```
ip pimsm ssm candidate
```

Mode

```
Privileged EXEC
```

```
User EXEC
```


10 Quality of Service (QoS) Commands

This chapter provides a detailed explanation of the Quality of Service (QoS) commands.

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.

10.1 MAC ACL Commands

MAC Access Control Lists (ACLs) ensure that only authorized users have access to specific resources while blocking off any unwarranted attempts to reach network resources.

Note:

- ▶ The maximum number of ACLs of any type that can be created is 100.
- ▶ ACLs are supported in the inbound direction only.
- ▶ Only Ethernet II frame types are supported.
- ▶ The maximum number of rules per MAC ACL is 10.
- ▶ The maximum number of rules per interface is 20 (100 for Software Version L3P).
- ▶ ACLs are configured separately for Layer 2 and Layer 3 / Layer 4 and cannot be applied to the same interface (PowerMICE, MACH104, MACH1040 and MACH4000 without MACH4002-24G.../MACH4002-48G...).
- ▶ ACLs are configured separately for Layer 2 and Layer 3/Layer 4 and can be applied to the same interface (MACH4002-24G.../MACH4002-48G...).
- ▶ Wildcard masking for MAC ACLs (srcmacmask, dstmacmask) operates differently from a subnet mask. A wildcard mask is in essence the inverse of a subnet mask. With a subnet mask, the mask has ones (1's) in the bit positions that are used for the network address, and has zeros (0's) for the bit positions that are not used. In contrast, a wildcard mask has (0's) in a bit position that must be checked. A '1' in a bit position of the ACL mask indicates the corresponding bit can be ignored.

10.1.1 mac access-list extended

Note: This command is available for the devices of the MACH104, MACH1040 and MACH4000 families and for the PowerMICE devices.

This command creates a MAC Access Control List (ACL) identified by <name>, consisting of classification fields defined for the Layer 2 header of an Ethernet frame. The <name> parameter is a case-sensitive alphanumeric string from 1 to 31 characters uniquely identifying the MAC access list. If a MAC ACL by this name already exists, this command enters Mac-Access-List config mode to allow updating the existing MAC ACL.

Note: The CLI mode is changed to Mac-Access-List Config when this command is successfully executed.

Format

```
mac access-list extended <name>
```

Mode

```
Interface Config  
Global Config
```

name

```
Enter access-list name up to 31 characters in  
length.
```

■ no mac access-list extended

This command deletes a MAC ACL identified by <name> from the system.

Format

```
no mac access-list extended <name>
```

Mode

```
Global Config
```

name

```
Enter access-list name up to 31 characters in  
length.
```

10.1.2 mac access-list extended rename

Note: This command is available for the devices of the MACH104, MACH1040 and MACH4000 families and for the PowerMICE devices.

This command changes the name of a MAC Access Control List (ACL). The *<oldname>* parameter is the name of an existing MAC ACL. The *<newname>* parameter is a case-sensitive alphanumeric string from 1 to 31 characters uniquely identifying the MAC access list.

This command fails if a MAC ACL by the name *<newname>* already exists.

Format

```
mac access-list extended rename <oldname> <newname>
```

Mode

```
Global Config
```

10.1.3 {deny|permit}

This command creates a new rule for the current MAC access list. Each rule is appended to the list of configured rules for the list.

Note: The 'no' form of this command is not supported, since the rules within a MAC ACL cannot be deleted individually. Rather, the entire MAC ACL must be deleted and re-specified.

Note: An implicit 'deny all' MAC rule always terminates the access list.

A rule may either deny or permit traffic according to the specified classification fields. At a minimum, the source and destination MAC value and mask pairs must be specified, each of which may be substituted using the keyword any to indicate a match on any value in that field. The bpdud keyword may be specified for the destination MAC value/mask pair indicating a well-known BPDUD MAC value of 01-80-c2-xx-xx-xx (hex), where 'xx' indicates a don't care. The remaining command parameters are all optional, but the most frequently used parameters appear in the same relative order as shown in the command format.

The Ethertype may be specified as either a keyword or a four-digit hexadecimal value from 0x0600-0xFFFF. The currently supported *<ethertypekey>* values are: appletalk, arp, ibmsna, ipv4, ipv6, ipx, mplsmcast, mplsucast, netbios, novell, pppoe, rarp. Each of these translates into its equivalent Ethertype value(s).

Ethertype Keyword	Corresponding Value
appletalk	0x809B
arp	0x0806
ibmsna	0x80D5
ipv4	0x0800
ipv6	0x86DD
ipx	0x8037
mplsmcast	0x8848
mplsucast	0x8847
netbios	0x8191
novell	0x8137, 0x8138

Table 17: Ethertype Keyword and 4-digit Hexadecimal Value

Ethertype Keyword	Corresponding Value
pppoe	0x8863, 0x8864
rarp	0x8035

Table 17: Ethertype Keyword and 4-digit Hexadecimal Value

The `vlan` and `cos` parameters refer to the VLAN identifier and 802.1p user priority fields, respectively, of the VLAN tag. For packets containing a double VLAN tag, this is the first (or outer) tag.

The `assign-queue` parameter allows specification of a particular 802.1p user priority for traffic that matches this rule. The allowed `<queue-id>` value is 0-7. The matching traffic is transmitted with the modified 802.1p user priority and also with modified IP-DSCP value for IP frames.

The `redirect` parameter allows the traffic matching this rule to be forwarded to the specified `<slot/port>`. The `assign-queue` and `redirect` parameters are only valid for a 'permit' rule.

Format

```
{deny|permit} {{<srcmac> <srcmacmask>} | any} {{<dstmac>
<dstmacmask>} | any| bpdu} [<ethertypekey> | <0x0600-
0xFFFF>] [vlan eq <0-4095> | cos <0-7>] [secondary-vlan
eq <0-4095>] [secondary-cos <0-7>] [assign-queue <queue-
id>] [redirect <slot/port>]
```

Note: The special command form `{deny|permit} any` is used to match all Ethernet layer 2 packets, and is the equivalent of the IP access list "match every" rule.

Mode

```
Mac-Access-List Config
```

10.1.4 mac access-group

This command attaches a specific MAC Access Control List (ACL) identified by *<name>* to an interface in the inbound direction. The *<name>* parameter must be the name of an existing MAC ACL.

An optional sequence number may be specified to indicate the order of this MAC access list relative to other MAC access lists already assigned to this interface and direction. A lower number indicates higher precedence order. If a sequence number is already in use for this interface, the specified MAC access list replaces the currently attached MAC access list using that sequence number. If the sequence number is not specified for this command, a sequence number that is one greater than the highest sequence number currently in use for this interface and direction is used.

This command specified in Interface Config mode only affects a single interface, whereas the Global Config mode setting is applied to all interfaces.

Format

```
mac access-group <name> in [sequence <1-4294967295>]
```

Modes

Global Config

Interface Config

name

Enter name of MAC Access Control List.

<1-4294967295>

Enter the sequence number (greater than 0) to rank precedence for this interface and direction. A lower sequence number has higher precedence.

■ no mac access-group

This command removes a MAC ACL identified by *<name>* from the interface in a given direction.

Format

```
no mac access-group <name> [in]
```

Modes

```
Global Config  
Interface Config
```

name

Enter name of MAC Access Control List.

10.1.5 show mac access-lists

Note: This command is available for the devices of the MACH104, MACH1040 and MACH4000 families and for the PowerMICE devices.

This command displays a MAC access list and all of the rules that are defined for the MAC ACL. The *[name]* parameter is used to identify a specific MAC ACL to display.

Format

```
show mac access-lists [name]
```

name

Enter name of MAC Access Control List.

Mode

```
Privileged EXEC
```

Rule Number

The ordered rule number identifier defined within the MAC ACL.

Action

Displays the action associated with each rule. The possible values are permit or deny.

Source MAC Address

Displays the source MAC address for this rule.

Source MAC Mask

Displays the source MAC mask for this rule.

Destination MAC Address

Displays the destination MAC address for this rule.

Destination MAC Mask

Displays the destination MAC mask for this rule.

Ethertype

Displays the Ethertype keyword or custom value for this rule.

VLAN ID

Displays the VLAN identifier value or range for this rule.

COS

Displays the COS (802.1p) value for this rule.

Secondary VLAN

Displays the Secondary VLAN identifier value or range for this rule. This field is contained in the inner tag of a double VLAN-tagged packet.

Secondary COS

Displays the Secondary COS (802.1p) value for this rule. This field is contained in the inner tag of a double VLAN-tagged packet.

Assign Queue

Displays the 802.1p user priority to which packets matching this rule are assigned.

Redirect Interface

Displays the slot/port to which packets matching this rule are forwarded.

10.2 IP ACL Commands

IP Access Control Lists (ACLs) ensure that only authorized users have access to specific resources while blocking off any unwarranted attempts to reach network resources.

Note:

- ▶ IP ACL configuration for IP packet fragments is not supported.
- ▶ ACLs are supported in the inbound direction only.
- ▶ The maximum number of ACLs of any type that can be created is 100.
- ▶ The maximum number of rules per IP ACL is 10.
- ▶ The maximum number of rules per interface is 20 (100 for Software Version L3P).
- ▶ ACLs are configured separately for Layer 2 and Layer 3/Layer 4 and cannot be applied to the same interface. (PowerMICE and MACH4000 without MACH4002-24G.../MACH4002-48G...)
- ▶ ACLs are configured separately for Layer 2 and Layer 3/Layer 4 and can be applied to the same interface. (MACH4002-24G.../MACH4002-48G...)
- ▶ Wildcard masking for IP ACLs (srcmask, dstmask) operates differently from a subnet mask. A wildcard mask is in essence the inverse of a subnet mask. With a subnet mask, the mask has ones (1's) in the bit positions that are used for the network address, and has zeros (0's) for the bit positions that are not used. In contrast, a wildcard mask has (0's) in a bit position that must be checked. A '1' in a bit position of the ACL mask indicates the corresponding bit can be ignored. The mask for the TOS value (tosmask) uses the common notation, i.e. the mask has ones (1's) in the bit positions that must be checked.

10.2.1 access-list

Note: This command is available for the devices of the MACH4000 family, for the PowerMICE devices and for the MACH1040 devices.

This command creates an IP Access Control List (ACL) that is identified by the parameter `<accesslistnumber>`.

The IP ACL number (`<accesslistnumber>`) is an integer from 1 to 199. The `<accesslistnumber>` range 1 to 99 is for an IP standard ACL and the `<accesslistnumber>` range 100 to 199 is for an IP extended ACL.

The IP ACL rule is specified with either a *permit* or *deny* action.

The protocol to filter for an IP ACL rule is specified by giving the protocol to be used like *icmp*, *igmp*, *ip*, *tcp*, *udp*.

The command specifies a source ipaddress and source mask for match condition of the IP ACL rule specified by the *srcip* and *srcmask* parameters.

The source layer 4 port match condition for the IP ACL rule is specified by the *port value* parameter. The range of values is from 0 to 65535. The `<start-port>` and `<endport>` parameters identify the first and last ports that are

part of the port range. They have values from 0 to 65535. The ending port must have a value equal or greater than the starting port. The starting port, ending port, and all ports in between will be part of the destination port range.

The `<portvalue>` parameter uses a single keyword notation and currently has the values of *domain*, *echo*, *ftp*, *ftpdata*, *http*, *smtp*, *snmp*, *telnet*, *tftp*, and *www*. Each of these values translates into its equivalent port number, which is used as both the start and end of a port range.

The command specifies a destination ipaddress and destination mask for match condition of the IP ACL rule specified by the *dstip* and *dstmask* parameters.

The command specifies the TOS for an IP ACL rule depending on a match of precedence or DSCP values using the parameters *dscp*, *precedence*, *tos*/*tosmask*.

The assign-queue parameter allows specification of a particular 802.1p user priority for traffic that matches this rule. The allowed `<queue-id>` value is 0-7. The matching traffic is transmitted with the modified 802.1p user priority and also with modified IP-DSCP value for IP frames.

The command specifies the redirect interface which is the slot/port to which packets matching this rule are forwarded.

Default

none

(IP Standard ACL)

Format

```
access-list <1-99>
  {deny | permit}
  {every | <srcip> <srcmask>}
  [assign-queue <queue-id>] |
  [redirect <slot/port>]
```

Mode

Global Config

(*IP Extended ACL*)

Format

```
access-list <100-199>
  {deny | permit}
  {every | icmp | igmp | ip | tcp | udp | <number>}
  {<srcip> <srcmask> | any}
  [{eq {<portkey> | <portvalue>}}]
  {<dstip> <dstmask> | any}
  [{eq {<portkey> | <portvalue>}}] |
  [precedence <precedence> | tos <tos> <tosmask> |
  dscp <dscp>] | [assign-queue <queue-id>] |
  [redirect <slot/port>]]}
```

Mode

Global Config

■ no access-list

This command deletes an IP ACL that is identified by the parameter *<accesslistnumber>* from the system.

Format

```
no access-list <accesslistnumber>
```

Mode

Global Config

accesslistnumber

Valid range: 1-99, 100-199

10.2.2 access-list fragments

Note: This command is available for the devices of the MACH104 and MACH1040 family and for the MACH4002-24G... and MACH4002-48G... devices.

This command enables IP fragments processing.

Default

none

Format

```
access-list fragments
```

Modes

Global Config

■ no access-list fragments

This command disables IP fragments processing.

Default

none

Format

```
no access-list fragments
```

Mode

Global Config

10.2.3 ip access-group

Note: This command is available for the devices of the MACH4000 family and for the PowerMICE devices.

This command attaches a specified IP ACL to one interface or to all interfaces.

An optional sequence number may be specified to indicate the order of this IP access list relative to other IP access lists already assigned to this interface. A lower number indicates higher precedence order. If a sequence number is already in use for this interface, the specified access list replaces the currently attached IP access list using that sequence number. If the sequence number is not specified for this command, a sequence number that is one greater than the highest sequence number currently in use for this interface and direction is used.

Default

none

Format

```
ip access-group <accesslistnumber> in> [<1-4294967295>]
```

Modes

Interface Config

Global Config

accesslistnumber

Enter the ACL ID in the range of 1 to 199.

<1-4294967295>

Enter the sequence number (greater than 0) to rank precedence for this interface and direction. A lower sequence number has higher precedence.

■ no ip access-group

This command removes a specified IP ACL from an interface.

Default

none

Format

```
no ip access-group <accesslistnumber> <in>
```

Mode

Interface Config

Global Config

accesslistnumber

Enter the ACL ID in the range of 1 to 199.

10.2.4 show ip access-lists

Note: This command is available for the devices of the MACH4000 family and for the PowerMICE devices.

This command displays an IP ACL.

<accesslistnumber> is the number used to identify the IP ACL.

Format

```
show ip access-lists <accesslistnumber>
```

Modes

Privileged EXEC

accesslistnumber

Enter the ACL ID in the range of 1 to 199.

Rule Number

This displays the number identifier for each rule that is defined for the IP ACL.

Action

This displays the action associated with each rule. The possible values are permit or deny.

Protocol

This displays the protocol to filter for this rule.

Source IP Address

This displays the source IP address for this rule.

Source IP Mask

This field displays the source IP Mask for this rule.

Source L4 Port

This field displays the source port for this rule.

Destination IP Address

This displays the destination IP address for this rule.

Destination IP Mask

This field displays the destination IP Mask for this rule.

Destination L4 Port

This field displays the destination port for this rule.

Service Type Field Match

This field indicates whether an IP DSCP, IP Precedence, or IP TOS match condition is specified for this rule.

Service Type Field Value

This field indicates the value specified for the Service Type Field Match (IP DSCP, IP Precedence, or IP TOS).

10.2.5 show access-lists global

Note: This command is available for the devices of the MACH104 and MACH1040 family and for the MACH4002-24G... and MACH4002-48G... devices.

This command displays global access list information.

Format

```
show access-lists global
```

Modes

Privileged EXEC

L4 Fragment Processing

This field displays the status of IP fragments processing.

Possible values: Enabled, Disabled.

10.2.6 show access-lists

Note: This command is available for the devices of the MACH4000 family and for the PowerMICE devices.

This command displays IP ACLs and MAC access control lists information for a designated interface and direction.

Format

```
show access-lists interface <slot/port> <in>
```

Modes

Privileged EXEC

ACL Type

Type of access list (IP or MAC).

ACL ID

Access List name for a MAC access list or the numeric identifier for an IP access list.

Sequence Number

An optional sequence number may be specified to indicate the order of this access list relative to other access lists already assigned to this interface and direction. A lower number indicates higher precedence order. If a sequence number is already in use for this interface and direction, the specified access list replaces the currently attached access list using that sequence number. If the sequence number is not specified by the user, a sequence number that is one greater than the highest sequence number currently in use for this interface and direction is used. Valid range is (1 to 4294967295).

10.3 CoS Commands

This chapter provides a detailed explanation of the QoS Class of Service (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.

10.3.1 cos-queue max-bandwidth

This command specifies the maximum transmission bandwidth limit for each interface queue. Also known as rate shaping, this has the effect of smoothing temporary traffic bursts over time so that the transmitted traffic rate is bounded. The switch supports 8 queues per interface. A value from 0-100 (percentage of link rate) must be specified for each supported queue, with 0 indicating no maximum bandwidth is in effect.

Format

```
cos-queue max-bandwidth <bw-0> <bw-1> ... <bw-n>
```

Modes

Global Config

Interface Config (not MACH 4002 24G/48G)

<bw-n>

Enter the minimum bandwidth percentage for Queue n.
Valid range: n = 0 ...7.

■ no cos-queue max-bandwidth

This command restores the default for each queue's maximum bandwidth value.

Format

```
no cos-queue max-bandwidth
```

Mode

Global Config

Interface Config (not MACH 4002 24G/48G)

10.3.2 cos-queue min-bandwidth

This command specifies the minimum transmission bandwidth guarantee for each interface queue. The switch supports 8 queues per interface. A value from 0-100 (percentage of link rate) must be specified for each supported queue, with 0 indicating no guaranteed minimum bandwidth. The sum of all values entered must not exceed 100.

Format

```
cos-queue min-bandwidth <bw-0> <bw-1> ... <bw-n>
```

Modes

Global Config

Interface Config (not MACH 4002 24G/48G)

<bw-n>

Enter the minimum bandwidth percentage for Queue n.
Valid range: n = 0 ...7.

■ no cos-queue min-bandwidth

This command restores the default for each queue's minimum bandwidth value.

Format

```
no cos-queue min-bandwidth
```

Modes

Global Config

Interface Config (not MACH 4002 24G/48G)

10.3.3 cos-queue strict

This command activates the strict priority scheduler mode for each specified queue. A queue cannot be a member of a queuing algorithm higher than its next higher priority queue. That is, any strict priority queue must start at class 7 and be consecutive.

Format

```
cos-queue strict <queue-id-1> [<queue-id-2> ...  
<queue-id-n>]
```

Modes

Global Config

Interface Config (not MACH 4002 24G/48G)

<queue-id-n>

Enter a Queue Id from 0 to 7.

■ no cos-queue strict

This command activates the weighted round robin (WRR) scheduler mode for each specified queue. A queue cannot be a member of a queuing algorithm lower than its next lowe priority queue. That is, any WRR queue must start at class 0 and be consecutive.

Format

```
no cos-queue strict <queue-id-1> [<queue-id-2> ...  
<queue-id-n>]
```

Modes

Global Config

Interface Config (not MACH 4002 24G/48G)

<queue-id-n>

Enter a Queue Id from 0 to 7.

10.3.4 traffic-shape

This command specifies the maximum transmission bandwidth limit for the interface as a whole. Also known as rate shaping, this has the effect of smoothing temporary traffic bursts over time so that the transmission traffic rate is bounded. A value from 0-100 (percentage of link rate) must be specified, with 0 indicating no traffic shaping is in effect. When interface shaping is enabled on a port which has some queues in WRR group, then the minimum bandwidth configuration of the weighted queues is not honored.

Format

```
traffic-shape <bw>
```

Modes

```
Global Config
```

```
Interface Config
```

<bw>

```
Enter the shaping bandwidth percentage from 0 to  
100 in increments of 5.
```

■ no traffic-shape

This command disables the traffic shaping.

Format

```
no traffic-shape
```

Modes

```
Global Config
```

```
Interface Config
```

10.3.5 show interfaces cos-queue

This command displays the class-of-service queue configuration for the specified interface. The slot/port parameter is optional. If specified, the class-

of-service queue configuration of the interface is displayed. If omitted, the most recent global configuration settings are displayed.

Format

```
show interfaces cos-queue [slot/port]
```

Mode

Privileged EXEC

Interface

This displays the slot/port of the interface. If displaying the global configuration, this line is replaced by a Global Configuration indication.

Intf Shaping Rate

The maximum transmission bandwidth limit for the interface as a whole. It is independent of any per-queue maximum bandwidth value(s) in effect for the interface. This is a configured value.

The following information is repeated for each queue on the interface.

Queue Id

An interface supports 8 queues numbered 0 to 7.

Minimum Bandwidth

The minimum transmission bandwidth guarantee for the queue, expressed as a percentage. A value of 0 means bandwidth is not guaranteed and the queue operates using best-effort. This is a configured value.

Maximum Bandwidth

The maximum transmission bandwidth limit for the queue, expressed as a percentage. A value of 0 means no upper limit is enforced, so the queue may use any or all of the available bandwidth of the interface. This is a configured value.

Scheduler Type

Indicates whether this queue is scheduled for transmission using a strict priority or a weighted scheme. This is a configured value.

11 Protocol-based VLAN Commands

This chapter provides a detailed explanation of the protocol-based VLAN commands.

11.1 Show Commands

11.1.1 show port protocol

This command displays the Protocol-Based VLAN information for either the entire system, or for the indicated Group.

Format

```
show port protocol {<groupid> | all}
```

Mode

Privileged EXEC

Group Name

This field displays the group name of an entry in the Protocol-based VLAN table.

Group ID

This field displays the group identifier of the protocol group.

Protocol(s)

This field indicates the type of protocol(s) for this group.

VLAN

This field indicates the VLAN associated with this Protocol Group.

Interface(s)

This field lists the slot/port interface(s) that are associated with this Protocol Group.

11.2 Configuration Commands

11.2.1 vlan protocol group

This command adds protocol-based VLAN group to the system. The *<groupName>* is a character string of 1 to 16 characters. When it is created, the protocol group will be assigned a unique number that will be used to identify the group in subsequent commands.

Format

```
vlan protocol group <groupname>
```

Mode

```
Global Config
```

11.2.2 vlan protocol group add protocol

This command adds the <protocol> to the protocol-based VLAN identified by <groupid>. A group may have more than one protocol associated with it. Each interface and protocol combination can only be associated with one group. If adding a protocol to a group causes any conflicts with interfaces currently associated with the group, this command will fail and the protocol will not be added to the group. The possible values for protocol are *ip*, *arp*, and *ipx*.

Default

none

Format

```
vlan protocol group add protocol <groupid> <protocol>
```

Mode

Global Config

■ no vlan protocol group add protocol

This command removes the <protocol> from this protocol-based VLAN group that is identified by this <groupid>. The possible values for protocol are *ip*, *arp*, and *ipx*.

Format

```
no vlan protocol group add protocol <groupid> <protocol>
```

Mode

Global Config

11.2.3 vlan protocol group remove

This command removes the protocol-based VLAN group that is identified by this <groupid>.

Format

```
vlan protocol group remove <groupid>
```

Mode

```
Global Config
```

11.2.4 protocol group

This command attaches a <vlanid> to the protocol-based VLAN identified by <groupid>. A group may only be associated with one VLAN at a time, however the VLAN association can be changed.

The referenced VLAN should be created prior to the creation of the protocol-based VLAN except when GVRP is expected to create the VLAN.

Default

```
none
```

Format

```
protocol group <groupid> <vlanid>
```

Mode

```
VLAN database
```

■ no protocol group

This command removes the <vlanid> from this protocol-based VLAN group that is identified by this <groupid>.

Format

```
no protocol group <groupid> <vlanid>
```

Mode

```
VLAN database
```

11.2.5 protocol vlan group

This command adds the physical <slot/port> interface to the protocol-based VLAN identified by <groupid>. A group may have more than one interface associated with it. Each interface and protocol combination can only be associated with one group. If adding an interface to a group causes any conflicts with protocols currently associated with the group, this command will fail and the interface(s) will not be added to the group.

The referenced VLAN should be created prior to the creation of the protocol-based VLAN except when GVRP is expected to create the VLAN.

Default

none

Format

```
protocol vlan group <groupid>
```

Mode

Interface Config

■ no protocol vlan group

This command removes the <interface> from this protocol-based VLAN group that is identified by this <groupid>. If <all> is selected, all ports will be removed from this protocol group.

Format

```
no protocol vlan group <groupid>
```

Mode

Interface Config

11.2.6 protocol vlan group all

This command adds all physical interfaces to the protocol-based VLAN identified by <groupid>. A group may have more than one interface associated with it. Each interface and protocol combination can only be associated with one group. If adding an interface to a group causes any conflicts with protocols currently associated with the group, this command will fail and the interface(s) will not be added to the group.

The referenced VLAN should be created prior to the creation of the protocol-based VLAN except when GVRP is expected to create the VLAN.

Default

none

Format

```
protocol vlan group all <groupid>
```

Mode

Global Config

■ no protocol vlan group all

This command removes all interfaces from this protocol-based VLAN group that is identified by this <groupid>.

Format

```
no protocol vlan group all <groupid>
```

Mode

Global Config

12 Index

Symbols

{deny|permit}

819

auto-negotiate all

197

auto-summary

727

Numerics

1583compatibility

678

A

access-list

825

access-list fragments

827

addport

191

address-conflict

309

adminmode

192

arc

479

area default-cost

678

area nssa

679

area nssa default-info-originate

679

area nssa no-redistribute (OSPF)

680

area nssa no-summary (OSPF)

680

area nssa translator-role (OSPF)

680

area nssa translator-stab-intv

681

area range

681

area stub

682

area stub summarylsa

683

area virtual-link

684

area virtual-link authentication

685

area virtual-link dead-interval

686

area virtual-link hello-interval

687

area virtual-link retransmit-interval

688

area virtual-link transmit-delay

689

areaid

36

ARP

aging

597

cache, displaying

598, 600

response time

594

retries

595

arp

590

arp cachesize

590, 592

arp dynamicrenew

593

arp purge

593

arp resptime

594

arp retries

595

arp selective-learning

596

arp timeout

597

authentication login

533

authorization network radius

535

auto-disable reason

193

auto-disable reset

195

auto-disable timer

195

auto-negotiate

196

B

boot skip-aca-on-boot

310, 310

bridge address-learning

118

bridge address-relearn detect operation

119

bridge address-relearn detect threshold

119

bridge aging-time

120

bridge duplex-mismatch-detect operation

121

bridge fast-link-detection

121

bridge framesize

70

bridge vlan-learning

122

broadcasts

broadcast storm recovery mode

274,

275, 277

broadcast storm trap

765, 798

C

cable-crossing

198

cablestatus

311

classofservice dot1p mapping

102

classofservice ip-dscp-mapping

103

classofservice trus

104

clear arp-cache

597

clear arp-table-switch

312

clear commands

clear arp-table-switch

312

clear config

313

clear pass

315

clear traplog

316, 317

clear vlan

317

clear config

313

clear config factory

313

clear counters

313

clear dot1x statistics

535

clear eventlog

311

clear hiper-ring

314

clear igmpsnooping

314

clear inlinpower

419

clear link-aggregation

316

clear lldp config all

357

clear mac-addr-table

315

clear pass

315

clear port-sec

506

clear radius statistics

536

clear ring-coupling

317

clear sfp-white-list

326

clear signal-contact

316

clear traplog	317	configuration reset	313
clear vlan	317	config-watchdog	318
Competence Center	877	copy	318
config commands		copy nvram clibanner	324
config arp agetime	597	copy nvram startup-config	326
config arp resptime	594	copy system bootcode	326
config arp retries	595	copy system image	326
config lags adminmode	212	copy system running-config	326
config lags linktrap	213	copy nvram capture	321
config lags name	214	copy nvram capture aca	
config loginsession	298	capture	321
config port admin-mode	267, 268	copy nvram clibanner	321
config port linktrap	269, 270, 271	copy nvram errorlog	322
config port physical-mode	273	copy nvram script	322
config switchconfig broadcast	274, 275, 277	copy nvram traplog	323
config switchconfig flowcontrol	278, 279	copy system running-config	323
config trapflags bcststorm	765, 798	copy tftp/// nvram httpscert	321
config users add	303, 304	cos-queue max-bandwidth	834
config users delete	302, 303, 304	cos-queue min-bandwidth	835
config users passwd	305	cos-queue strict	836
config vlan add	280		
config vlan delete	280	D	
config vlan garp jointime	214, 215, 216, 217, 218, 219, 220	debug tcpdump filter delete	99
config vlan garp leavealltime	222	debug tcpdump filter list	98
config vlan garp leavetime	221	debug tcpdump filter show	98
config vlan interface acceptframe	282, 283, 288	debug tcpdump help	96
config vlan name	285	debug tcpdump start cpu	96
config vlan participation	286, 287	debug tcpdump start cpu filter	97
config vlan ports ingressfilter	284, 289	debug tcpdump stop	97
config vlan ports pvid	290, 292	default-information originate (OSPF)	690, 728
config vlan ports tagging	291, 293	default-metric (OSPF)	691
config port autoneg	214	default-metric (RIP)	729
Config router ospf adminmode	676	deleteport	200
Config router ospf area externrouting	678	deleteport all	200
Config router rip adminmode	727, 730, 735, 737, 738	device configuration commands	201
Config router rip interface defaultmetric	726, 732, 733	device-status connection-error	327
Config router rip interface version receive	726	device-status monitor	328
Config router rip interface version send	734	DHCP server configuration example	512
config switchconfig flowcontrol	278, 279	dhcp-relay	508, 509
config users delete	302, 303, 304, 305	dhcp-server addr-probe	516
config users passwd	302, 303, 304, 305	dhcp-server operation	517
config vlan delete	280	dhcp-server pool add	517
config vlan ports acceptframe	292	dhcp-server pool delete	522
config vlan ports ingressfilter	283, 288, 289, 290, 842	dhcp-server pool disable	522
		dhcp-server pool enable	522
		dhcp-server pool modify hirschmann-device	521
		dhcp-server pool modify mode	518
		dhcp-server pool modify option	520
		dhcp-server pool modify leasetime	521
		digital-input	122
		digital-output	124
		dip-switch operation	201
		disable ip multicast mdebug mtrace	748

disconnect	298	inlinepower (Interface Config)	418
distance ospf	692	inlinepower budget slot	421
distance rip	730	inlinepower threshold slot	422
distribute-list out	693, 731	inlinepower trap slot	422
dot1x defaultlogin	536	Interface Config Mode	59
dot1x dynamic-vlan enable	537	inventory	244, 245, 246, 248, 249, 250, 252, 253, 533, 745, 746, 747, 748, 749, 752, 753, 754, 755, 756, 757, 758, 759, 760, 761, 763, 764, 766, 767, 768, 769, 770, 771, 772, 773, 775, 776, 777, 778, 779, 780, 781, 782, 784, 788, 790, 791, 792, 793, 794, 795, 796, 797, 829, 831, 832, 840
dot1x guest-vlan	538	ip access-group	828
dot1x initialize	539	ip address	605
dot1x login	539	ip dvmrp	763, 766
dot1x mac-auth-bypass	540	ip dvmrp metric	764
dot1x max-req	541	ip dvmrp trapflags	765
dot1x max-users	542	ip forwarding	612
dot1x port-control	543	ip http secure-port	575
dot1x port-control all	544	ip http secure-protocol	575
dot1x re-authenticate	545	ip http server	575
dot1x re-authentication	545	ip https certgen	578
dot1x safe-vlan	546	ip https port	578
dot1x system-auth-control	547	ip https server	577
dot1x timeout	547	ip igmp	773
dot1x user	551	ip igmp last-member-query-count	775
duplex settings	273	ip igmp last-member-query-interval	776
dvlan-tunnel ethertype	108	ip igmp query-interval	777
		ip igmp query-max-response-time	778
		ip igmp robustness	779
		ip igmp startup-query-count	780
		ip igmp startup-query-interval	781
		ip igmp version	774
		ip irdp	634
		ip irdp address	635
		ip irdp holdtime	636
		ip irdp maxadvertinterval	637
		ip irdp minadvertinterval	638
		ip irdp preference	639
		ip mcast boundary	744
		ip mtu	606
		ip multicast	745
		ip multicast staticroute	746
		ip multicast ttl-threshold	747
		ip netdirbcast	607
		ip ospf	677
		ip ospf areaid	696
		ip ospf authentication	697
		ip ospf cost	698
		ip ospf dead-interval	699
		ip ospf hello-interval	700
		ip ospf mtu-ignore	704
		ip ospf priority	701
		ip ospf retransmit-interval	702
E			
enable (OSPF)	676		
enable (RIP)	725		
ethernet-ip	135		
exit-overflow-interval	694		
external-lsdb-limit	695		
F			
fast-hiper-ring	490		
flow control	278, 279		
frame acceptance mode	282, 283, 288		
G			
Global Config Mode	58		
GVRP			
join time	214, 215, 216, 217, 218, 219, 220		
leave time	221		
H			
hiper-ring	484		
hiper-ring mode	484		
hiper-ring port primary	485		
hiper-ring port secondary	485		
hiper-ring recovery-delay	486		
hostroutesaccept	735		
I			
IEEE 802.1Q	282, 283, 288		
ingress filtering	284, 289		
inlinepower (Global Config)	417		

ip ospf transmit-delay	703	link-aggregation	211
ip pimdm	790	link-aggregation adminmode	212
ip pimdm hello-interval	793	link-aggregation linktrap	213
ip pimdm holdtimes	791	link-aggregation name	214
ip pimdm mode	792	link-aggregation staticcapability	112
ip pim-trapflags	798	lldp	353
ip proxy-arp	591	LLDP - Link Layer Discovery Protocol	341
ip rip	726	lldp admin-state	357
ip rip authentication	732	lldp chassis tx-interval	356
ip rip receive version	733	lldp config chassis admin-state	354
ip rip send version	734	lldp config chassis notification-interval	354
ip route default	610	lldp config chassis re-init-delay	355
ip route distance	611	lldp config chassis tx-delay	355
ip routing	604	lldp config chassis tx-hold-mult	356
ip ssh protocol	552	lldp fdb-mode	358
ip table-sizes	615	lldp hm-mode	358
ip table-sizes arp-entries	616	lldp max-neighbors	359
ip table-sizes multicast-routes	618	lldp med	360
ip table-sizes unicast-routes	617	lldp med al	361
ip vlan-single-mac	613	lldp med confignotification	361
ip vrrp	653, 656	lldp med confignotification all	362
ip vrrp advertisement-address	664	lldp med faststartrepeatcount	363
ip vrrp authentication	659	lldp med transmit-tlv	364
ip vrrp delay-preemption	661	lldp med transmit-tlv all	365
ip vrrp domain	667	lldp notification	366
ip vrrp domain send-member-advertisements	654	lldp tlv gmrp	369
ip vrrp ip	658	lldp tlv igmp	369
ip vrrp link-down-notification	665	lldp tlv link-aggregation	366
ip vrrp mode	657	lldp tlv mac-phy-config-state	366
ip vrrp preempt	660	lldp tlv max-frame-size	367
ip vrrp priority	662	lldp tlv mgmt-addr	367
ip vrrp tap	655	lldp tlv pnio	367
ip vrrp timers advertise	663	lldp tlv pnio-alias	368
ip vrrp timers advertise milliseconds	663	lldp tlv pnio-mrp	368
ip vrrp track	666	lldp tlv port-desc	368
ipaddr	36	lldp tlv portsec	370
		lldp tlv port-vlan	369
		lldp tlv protocol	370
		lldp tlv ptp	370
		lldp tlv sys-cap	371
		lldp tlv sys-desc	371
		lldp tlv sys-name	371
		lldp tlv vlan-name	372
		logging buffered	178
		logging buffered wrap	179
		logging cli-command	180
		logging console	181
		logging host	182
		logging host reconfigure	183
		logging host remove	183
		logging snmp-requests get operation	183
		logging snmp-requests get severity	184
		logging snmp-requests set operation	184
		logging snmp-requests set severity	185
J			
join time	214, 215, 216, 217, 218, 219, 220		
L			
LAGs			
enabling or disabling	212		
link traps	213		
name	214		
summary information	257		
leave time	221, 222		
Line Config Mode	59		
Link Aggregation(802.3ad) Commands	112		
link aggregations. See LAGs			
link traps			
interface	269, 270, 271		
LAG	213		

protocol vlan group all	845	reload	335
PTP - Precision Time Protocol	388	reset system command	333, 335
ptp clock-mode	394	response time	594
ptp operation	395	retries	595
ptp sync-lower-bound	395	ring-coupling	495
ptp sync-upper-bound	396	ring-coupling config	496
ptp v1 burst	402	ring-coupling net-coupling	497
ptp v1 operation	402	ring-coupling operation	497
ptp v1 preferred-master	396	ring-coupling port	498
ptp v1 re-initialize	397	ring-coupling redundancy-mode	498
ptp v1 subdomain-name	397	rmon-alarm add	214
ptp v1 sync-interval	398	rmon-alarm delete	215
ptp v2bc announce-interval	403	rmon-alarm disable	216
ptp v2bc announce-timeout	404	rmon-alarm enable	215
ptp v2bc asymmetry	406	rmon-alarm modify falling-event	219
ptp v2bc delay-mechanism	404	rmon-alarm modify interval	217
ptp v2bc domain	400	rmon-alarm modify mib-variable	216
ptp v2bc network-protocol	405	rmon-alarm modify rising-event	219
ptp v2bc operation	403	rmon-alarm modify sample-type	218
ptp v2bc pdelay-interval	405	rmon-alarm modify startup-alarm	218
ptp v2bc priority1	399	rmon-alarm modify thresholds	217
ptp v2bc priority2	399	Router Config RIP Mode	59
ptp v2bc sync-interval	404		
ptp v2bc utc-offset	400	router-id	704
ptp v2bc utc-offset-valid	400	routing	603
ptp v2bc v1-compatibility-mode	405		
ptp v2bc vlan	401	S	
ptp v2bc vlan-priority	401	Schulungsangebot	877
ptp v2tc asymmetry	406	script apply	187
ptp v2tc delay-mechanism	406	script delete	188
ptp v2tc management	407	script list	188
ptp v2tc multi-domain-mode	407	script show	189
ptp v2tc network-protocol	408	script validate	189
ptp v2tc operation	408	selftest ramtest	239
ptp v2tc pdelay-interval	409	selftest reboot-on-error	240
ptp v2tc power-tlv-check	411	serial timeout	143
ptp v2tc primary-domain	409	serviceshell	241
ptp v2tc profile	410	session-limit	117
ptp v2tc sync-local-clock	412	sessions	
ptp v2tc syntonization	410	closing	298, 329
ptp v2tc vlan	411	displaying	299
ptp v2tc vlan-priority	412	session-timeout	118
		set cli banner	337
R		set garp timer join	220
radius accounting mode	553	set garp timer leave	221
radius server host	553	set garp timer leaveall	222
radius server key	555	set gmrp adminmode	223
radius server msgauth	555	set gmrp forward-all-groups	226
radius server primary	556	set gmrp forward-unknown	227
radius server retransmit	557	set gmrp interfacemode	224, 225
radius server timeout	558	set igmp	228, 229
reboot	333	set igmp aging-time-unknown	229
redistribute	736	set igmp automatic-mode	230
redistribute (RIP)	705	set igmp forward-all	231

Index

set igmp forward-unknown	232	show switchconfig	258, 259, 260
set igmp groupmembershipinterval	233	show users	300
set igmp interfacemode	234	show vlan detailed	261
set igmp lookup-interval-unknown	235	show vlan interface	264
set igmp lookup-resp-time-unknown	235	show vlan summary	263
set igmp maxresponse	236	show config-watchdog	71
set igmp querier max-response-time	237	show device-status	71
set igmp querier protocol-version	237	show dhcp-relay	508, 510
set igmp querier status	238	show dhcp-server	514
set igmp querier tx-interval	238	show dhcp-server operation	515
set igmp query-ports-to-filter	239	show dhcp-server pool	516
set igmp static-query-port	232	show dhcp-server port	515
set pre-login-banner text	239	show digital-input	127, 130
set pro-login-banner banner	339	show digital-input all	129
set prompt	143	show digital-input config	128
show	66	show digital-output	131, 134
show access-lists	832	show digital-output all	133
show access-lists global	831	show digital-output config	132
show address-conflict	66	show dip-switch	244
show arc	480	show dot1x	562
show arp	598	show dot1x clients	568
show arp brief	600	show dot1x users	567
show arp switch	67, 73, 601	show dvlan-tunnel	111
show authentication	72, 561	show ethernet-ip	144, 147
show authentication users	562	show eventlog	73
show auto-disable brief	242	show fast-hiper-ring	488
show auto-disable reasons	243	show garp	245
show boot skip-aca-on-boot	310, 310	show gmrp configuration	245
show bridge address-learning	67	show hiper-ring	483
show bridge address-relearn-detect	68	show hiper-ring info	484
show bridge aging-time	68	show igmpsnooping	246
show bridge duplex-mismatch-detect	69	show inlinepower	413
show bridge fast-link-detection	69	show inlinepower port	414
show bridge framesize	69	show inlinepower slot	420
show bridge vlan-learning	70	show interface	74
show classofservice dot1pmapping	105	show interface ethernet	76
show classofservice ip-dscp-mapping	106	show interface switchport	83
show classofservice trust	107	show interface utilization	84
show commands		show interfaces cos-queue	837
show arp table	598, 600	show inventory	284
show inventory	244, 245, 246, 248, 249,	show ip access-lists	829
250, 252, 253, 533, 745, 746, 747,		show ip brief	614
748, 749, 752, 753, 754, 755, 756,		show ip dvmrp	767
757, 758, 759, 760, 761, 763, 764,		show ip dvmrp interface	768
766, 767, 768, 769, 770, 771, 772,		show ip dvmrp neighbor	769
773, 775, 776, 777, 778, 779, 780,		show ip dvmrp nexthop	770
781, 782, 784, 788, 790, 791, 792,		show ip dvmrp prune	771
793, 794, 795, 796, 797, 829, 831,		show ip dvmrp route	772
832, 840		show ip http	576
show lags summary	257	show ip https	579
show login session	299	show ip igmp	782
show port	256	show ip igmp groups	782
show stats switch detailed	74, 76, 82	show ip igmp interface	784
		show ip igmp interface stats	788

show ip interface	619	show lldp config port tlv	346
show ip interface brief	621	show lldp med	347
show ip irdp	639	show lldp med interface	348
show ip mcast	753	show lldp med local-device detail	349
show ip mcast boundary	754	show lldp med remote-device	350
show ip mcast interface	754	show lldp med remote-device detail	351
show ip mcast mroute	755	show lldp remote-data	351
show ip mcast mroute group	756	show logging	85
show ip mcast mroute source	757	show loginsession	299, 306
show ip mcast mroute static	758	show mac access-lists	822
show ip ospf	707	show mac notification	253
show ip ospf area	710	show mac-address-conflict	86
show ip ospf database	711	show mac-addr-table	87
show ip ospf interface	713	show mac-filter-table gmrp	248
show ip ospf interface brief	715	show mac-filter-table igmpsnooping	249
show ip ospf interface stats	716	show mac-filter-table multicast	250
show ip ospf neighbor	717	show mac-filter-table static	251
show ip ospf neighbor brief	720	show mac-filter-table staticfiltering	252
show ip ospf range	721	show mac-filter-table stats	253
show ip ospf stub table	722	show monitor session	255
show ip ospf virtual-link	723	show mrinfo	759
show ip ospf virtual-link brief	724	show mrp	474
show ip pimdm	794	show mrp current domain	475
show ip pimdm interface	795	show mstat	760
show ip pimdm interface stats	796	show mtrace	761
show ip pimdm neighbor	797	show network	120, 144
show ip rip	738	show network mgmt-access	146
show ip rip interface brief	740	show port	256, 278, 279
show ip route	622	show port protocol	840
show ip route bestroutes	623	show port-monitor	424, 424
show ip route entry	624	show port-monitor brief	426
show ip route preferences	625	show port-monitor crc-fragment	427
show ip route static	626	show port-monitor link-flap	427
show ip ssh	569	show port-monitor speed-duplex	429
show ip stats	627	show port-sec dynamic	499
show ip vlan	643	show port-sec mode	500
show ip vrrp	670	show port-sec port	501
show ip vrrp domain	671	show ptp	388
show ip vrrp interface	672	show ptp configuration	391
show ip vrrp interface brief	674	show ptp operation	391
show ip vrrp interface stats	668	show ptp port	392
show link-aggregation	257	show ptp status	393
show link-aggregation brief	113	show radius	570
show lldp	341	show radius accounting	558
show lldp chassis tx-interval	344	show radius statistics	571
show lldp config	341	show reboot	334
show lldp config chassis	342	show reload	336
show lldp config chassis admin-state	342	show ring-coupling	493
show lldp config chassis notification-interval	342	show rmon-alarm	258
show lldp config chassis re-init-delay	343	show router rip interface	741
show lldp config chassis tx-delay	343	show running-config	91
show lldp config chassis tx-hold-mult	343	show selftest	259
show lldp config port	345	show serial	147
		show serviceshell	259

Index

show signal-contact	88	snmp-server community mode	163
show slot	90	snmp-server community ro	164
show snmp sync	150	snmp-server community rw	164
show snmp-access	148	snmp-server contact	160
show snmpcommunity	149	snmp-server enable traps	165
show snmptrap	151	snmp-server enable traps linkmode	168
show snmp	373	snmp-server enable traps multiusers	169
show snmp anycast	375	snmp-server enable traps port-sec	170
show snmp client	375	snmp-server enable traps stpmode	171
show snmp operation	376	snmp-server location	164
show snmp server	377	snmp-server sysname	165
show snmp status	377	snmptrap	172
show snmp time	378	snmptrap ipaddr	173
show spanning-tree	439	snmptrap mode	174
show spanning-tree brief	440	snmptrap snmpversion	175
show spanning-tree interface	442	SNTP - Simple Network Time Protocol	373
show spanning-tree mst detailed	443	snmp anycast address	379
show spanning-tree mst port detailed	444	snmp anycast transmit-interval	379
show spanning-tree mst port summary	447	snmp anycast vlan	380
show spanning-tree mst summary	448	snmp client accept-broadcast	380
show spanning-tree summary	449	snmp client disable-after-sync	381
show spanning-tree vlan	450	snmp client offset	381
show storm-control	260	snmp client request-interval	382
show storm-control limiters port	260	snmp client server primary	383
show sub-ring	523	snmp client server secondary	384
show switchconfig	120	snmp client threshold	385
show sysinfo	92, 107, 108	snmp operation	386
show telnet	152	snmp server disable-if-local	387
show telnetcon	153	snmp time system	387
show temperature	95	spanning-tree	451
show track	647, 649	spanning-tree auto-edgeport	452
show track applications	651	spanning-tree bpduguard	453
show trapflags	154	spanning-tree bpdumigrationcheck	272
show users	300	spanning-tree configuration name	454
show users authentication	573	spanning-tree configuration revision	455
show vlan	261	spanning-tree edgeport	456
show vlan brief	263	spanning-tree forceversion	457
show vlan port	264	spanning-tree forward-time	458, 460
show voice vlan	265	spanning-tree guard loop	459
show voice vlan interface	266	spanning-tree guard none	460
shutdown	267	spanning-tree guard root	461
shutdown all	268	spanning-tree hello-time	462
signal-contact	331	spanning-tree hold-count	462
signal-contact connection-error	330	spanning-tree max-age	463
slot/port	36	spanning-tree max-hops	464
snmp sync community-to-v3	269	spanning-tree mst	465
snmp trap link-status	270	spanning-tree mst instance	469
snmp trap link-status all	271	spanning-tree mst priority	467
snmp-access global	155, 156	spanning-tree mst vlan	468
snmp-access version v3-encryption	156	spanning-tree port mode	470
snmp-server	96, 158	spanning-tree port mode all	471
snmp-server community	159	spanning-tree stp-mrp-mode	472
snmp-server community ipaddr	161	spanning-tree tcnguard	473
snmp-server community ipmask	162	speed	273

- speeds 273
- split-horizon 737
- statistics
 - switch, related commands 74, 76, 82
- storm-control broadcast 274
- storm-control broadcast (port-related) 276
- storm-control egress-limit 276
- storm-control egress-limiting 274
- storm-control flowcontrol 278
- storm-control flowcontrol per port 279
- storm-control ingress-limit 277
- storm-control ingress-limiting 275
- storm-control ingress-mode 275, 277
- sub-ring mode 525
- sub-ring mrp-domainID 529
- sub-ring operation 526
- sub-ring port 527
- sub-ring protocol 526
- sub-ring ring-name 527
- sub-ring vlan 528
- Sub-Ring Commands 523
- sub-ring delete-ring 530
- sub-ring new-ring 530
- switch
 - information, related commands 258, 259, 260
 - inventory 244, 245, 246, 248, 249, 250, 252, 253, 533, 745, 746, 747, 748, 749, 752, 753, 754, 755, 756, 757, 758, 759, 760, 761, 763, 764, 766, 767, 768, 769, 770, 771, 772, 773, 775, 776, 777, 778, 779, 780, 781, 782, 784, 788, 790, 791, 792, 793, 794, 795, 796, 797, 829, 831, 832, 840
 - resetting 333, 335
 - statistics, related commands 74, 76, 82
- System Information and Statistics Commands 100
- System Utilities 309, 533
- system utilities 309–330
- T**
- tagging 291, 293
- telnet 114
 - sessions, closing 298, 329
 - sessions, displaying 299
- telnetcon maxsessions 176
- telnetcon timeout 177
- temperature 332
- timeouts
 - ARP 597
- traceroute 312
- track interface 644
- track logical 645
- track mode 645
- track ping 646
- track trap 647
- traffic-shape 837
- transport input telnet 115
- transport output telnet 116
- trap flags
 - broadcast storm 765, 798
- trap log
 - clearing 316, 317
- trapflags 707
- trunks. See LAGs
- U**
- update module-configuration 241
- update-timer 738
- User Account Management Commands 298
- user account management commands 298
- User Exec Mode 58
- users
 - adding 303, 304
 - deleting 302, 303, 304
 - displaying 300
 - passwords 305, 315
- users access 303
- users defaultlogin 301
- users login 302, 574
- users name 304
- users passwd 305
- users snmpv3 accessmode 306
- users snmpv3 authentication 307
- users snmpv3 encryption 308
- utilization alarm-threshold 95
- V**
- vlan 280
 - vlan acceptframe 282, 283
 - vlan ingressfilter 284
 - VLAN Mode 58
 - vlan name 285
 - vlan participation 286
 - vlan participation all 287
 - vlan port acceptframe all 288
 - vlan port ingressfilter all 289
 - vlan port priority all 107
 - vlan port pvid all 290
 - vlan port tagging all 291
 - vlan priority 108
 - vlan protocol group 841
 - vlan protocol group add protocol 842
 - vlan protocol group remove 843

Index

vlan pvid	292
vlan routing	642
vlan tagging	293
vlan0-transparent-mode	281
VLANs	
adding	280
changing the name of	285
deleting	280
details	261
frame acceptance mode	282, 283, 288
IDs	290, 292
ingress filtering	284, 289
jointime	214, 215, 216, 217, 218, 219, 220
leave all time	222
leave time	221
participation in	286, 287
port information	264
resetting parameters	317
summary information	263
tagging	291, 293
voice vlan (Global Config Mode)	294
voice vlan (Interface Config Mode)	295
voice vlan auth	297
W	
Web connections, displaying	299

13 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 875 for more information.

A

ABR. See “Area Border Router” on page 860.

Access Control List. An ACL is a database that an Operating System uses to track each user’s access

rights to system objects (such as file directories and/or files).

ACL. See “Access Control List” on page 859.

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.

API. See “Application Programming Interface” on page 860.

Application Programming Interface. An API is an interface used by an programmer to interface with functions provided by an application.

Area Border Router. A router located on the border of one or more OSPF areas that connects those areas to the backbone network. ABRs are considered members of both the OSPF backbone and the attached areas. They therefore maintain routing tables describing both the backbone topology and the

topology of the other areas. (Cisco Systems Inc.)

ARP. See “Address Resolution Protocol” on page 860.

ASAM. See “ATM Subscriber Access Multiplexer” on page 860.

ASBR. See “Autonomous System Boundary Router” on page 860.

ATM Subscriber Access Multiplexer. A telephone central office multiplexer that supports SDL ports over a wide range of network interfaces. An ASAM sends and receives subscriber data (often Internet services) over existing copper telephone lines, concentrating all traffic onto a single high-speed trunk for transport to the Internet or the enterprise intranet. This device is similar to a DSLAM (different manufacturers use different terms for similar devices). (Cisco Systems Inc.)

Autonomous System Boundary Router. ABR located between an OSPF autonomous system and a non-OSPF network. ASBRs run both OSPF and another routing protocol, such as RIP. ASBRs must reside in a non-stub OSPF area. See also ABR, non-stub area, and OSPF. (Cisco Systems Inc.)

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 861.

BGP. See “Border Gateway Protocol” on page 861.

BootP. See “Bootstrap Protocol.” on page 861.

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.

Border Gateway Protocol. BGP is a protocol for exchanging routing information between gateway host (each with its own router) in a network of autonomous systems. BGP is often the protocol used between gateway hosts on the Internet. The routing table contains a list of known routers, the addresses they can reach, and a cost metric associated with the path to each router so that the best available route is chosen. Hosts using BGP communicate using the Transmission Control Protocol (TCP) and send updated router table information only when one host has detected a change. Only the affected part of the routing table is sent. BGP-4, the latest version, lets administrators configure cost

metrics based on policy statements. (BGP-4 is sometimes called BGP4, without the hyphen.) BGP communicates with autonomous (local) networks using Internal BGP (IBGP) since it doesn't work well with IGP. The routers inside the autonomous network thus maintain two routing tables: one for the interior gateway protocol and one for IBGP. BGP-4 makes it easy to use Classless Inter-Domain Routing (Classless Inter-Domain Routing), which is a way to have more addresses within the network than with the current IP address assignment scheme.

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

cards.h. A file that instructs the base code driver how to construct the driver.

card_db. A database that contains everything from port maps to module information.

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 862.

Command Line Interface. CLI is a line-item interface for configuring systems.

Common Open Policy Service Protocol. A proposed standard protocol for exchanging network policy information between a Policy Decision Point (PDP) in a network and Policy Enforcement Points (PEPs) as part of overall Quality of Service (QoS) - the allocation of network traffic resources according to desired priorities of service. The policy decision point might be a network server controlled directly by the network administrator who

enters policy statements about which kinds of traffic (voice, bulk data, video, teleconferencing, and so forth) should get the highest priority. The policy enforcement points might be router or layer 3 switches that implement the policy choices as traffic moves through the network. Currently, COPS is designed for use with the Resource Reservation Protocol (RSVP), which lets you allocate traffic priorities in advance for temporary high-bandwidth requirements (for example, video broadcasts or multicasts). It is possible that COPS will be extended to be a general policy communications protocol.

Complex Programmable Logic Device. CPLD is a programmable circuit on which a logic network can be programmed after its construction.

COPS. See “Common Open Policy Service Protocol.” on page 862.

CPLD. See “Complex Programmable Logic Device.” on page 862.

D

DAPI. See “Device Application Programming Interface” on page 862.

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 863.

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 863..

Distance-Vector Multicast Routing Protocol. DVMRP is a distance vector routing protocol used between routers in an intranet. This hop-based protocol describes a method of building multicast trees from the multicast source to all the receivers (or leaves) of the tree.

DVMRP. See “Distance-Vector Multicast Routing Protocol.” on page 863.

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 864.

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 874 for more information.

FIFO. First In First Out.

Flash Memory. See “EEPROM” on page 864.

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 865.

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 865.

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 864.

GMRP. See “GARP Multicast Registration Protocol” on page 864.

GPCM. See “General Purpose Chip-select Machine” on page 865.

GVD. GARP VLAN Database.

GVRP. See “GARP VLAN Registration Protocol.” on page 865.

H

.h file. Header file in C code. Contains function and coding definitions.

HAPI. See “Hardware Abstraction Programming Interface” on page 865.

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 866.

IGMP. See “Internet Group Management Protocol” on page 866.

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 866 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 866.

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 867.

L

LAN. See “Local Area Network” on page 868.

LDAP. See “Lightweight Directory Access Protocol” on page 867.

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 869.

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 868.

MOSPF. See “Multicast OSPF” on page 869.

MPLS. See “Multi-Protocol Label Switching” on page 869.

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 “OSPF” on page 871 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 869.

N

NAT. See “Network Address Translation” on page 870.

Network Address Translation.

Sometimes referred to as Transparent Proxying, IP Address Overloading, or IP Masquerading. Involves use of a device called a Network Address Translator, which assigns a contrived, or logical, IP address and port number to each node on an organization's internal network and passes packets using these assigned addresses.

NM. Network Module.

nm. Nanometer (1×10^9) meters.

non-stub area. Resource-intensive OSPF area that carries a default route, static routes, intra-area routes, interarea routes, and external routes. Non-stub areas are the only OSPF areas that can have virtual links configured across them, and are the only areas that can contain an ASBR. Compare with stub area. See also ASAM and OSPF. (Cisco Systems Inc.)

NP. Network Processor.

O

Open Shortest Path First. A link-state (algorithm used by the router to determine the current topology of a network), Interior Gateway (distributes routing information between routers belonging to a single Autonomous System) routing protocol. This protocol's algorithm determines the shortest path from its router to all the other routers in the network. This protocol is rapidly replacing RIP on the Internet.

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 871.

OSI. See “Open Systems Interconnection” on page 871.

OSPF. See “Open Shortest Path First” on page 871.

P

PDU. See “Protocol Data Unit” on page 872.

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.

PIM-DM. See “Protocol Independent Multicast – Dense Mode” on page 872.

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.

Protocol Independent Multicast – Dense Mode. Like DVMRP, PIM-DM uses a flood and prune protocol for building multicast trees. However, unlike DVMRP, PIM-DM uses existing unicast protocols for determining the route to the source.

Q

QoS. See “Quality of Service” on page 872.

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.

Resource Reservation Setup

Protocol. RSVP is a new Internet protocol being developed to enable the Internet to support specified Qualities-of-Service (QoS). Using RSVP, an application will be able to reserve resources along a route from source to destination. RSVP-enabled routers will then schedule and prioritize packets to meet the prioritization assigned by QoS. RSVP is a chief component of a new type of Internet being developed, known broadly as an integrated services Internet. The general idea is to enhance the Internet to support transmission of real-time data.

RFC. Request For Comment.

RIP. See “Routing Information Protocol” on page 872.

Routing Information Protocol.

RIP is the routing protocol used by the routed process on Berkeley-

derived UNIX systems. Many networks use RIP; it works well for small, isolated, and topologically simple networks.

RIPng. Routing Information Protocol, new generation.

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.

RSVP. See “Resource Reservation Setup Protocol” on page 872.

RTOS. See “Real-Time Operating System” on page 872.

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, 100SX 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 873.

SODIMM. Small Outline Dual Inline Memory Module.

SRAM. Static Random Access Memory.

STP. Spanning Tree Protocol. See "802.1D" on page 859 for more information.

stub area. OSPF area that carries a default route, intra-area routes, and interarea routes, but does not carry external routes. Virtual links cannot be configured across a stub area, and they cannot contain an ASBR. Compare with non-stub area. See also ASAM and OSPF. (Cisco Systems Inc.)

SX. See "SimpleX signaling" on page 874.

SYSAPI. See "Systems Application Programming Interface" on page 874.

Systems Application Programming Interface. SYSAPI is a module within the System Support software that provides system-wide routines for network and mbuf support and provides the interface into the system registry.

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 874.

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.

Virtual Router Redundancy

Protocol. VRRP specifies an election protocol that dynamically assigns responsibility for a virtual router to one of the VRRP routers on a LAN. The VRRP router controlling the IP address(es) associated with a virtual router is called the Master, and forwards packets sent to these IP addresses. The election process provides dynamic fail-over in the forwarding responsibility should the Master become unavailable. This allows any of the virtual router IP addresses on the LAN to be used as the default first hop router by end-hosts. The advantage gained from using VRRP is a higher availability default path without requiring configuration of dynamic routing or router discovery protocols on every end-host.

VLAN. See "Virtual Local Area Network" on page 875.

vMAN. Virtual Metropolitan Area Network.

VRRP. See "Virtual Router Redundancy Protocol" on page 875.

W

WAN. See “Wide Area Network” on page 876.

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

PowerMICE, MACH 104, MACH 1040, MACH 4000

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
3.1.5	Using the offline configurator	64
3.2	Saving settings	67
3.2.1	Saving locally (and on the ACA)	67
3.2.2	Saving in a binary file or a script file on a URL	69
3.2.3	Saving to a binary file on the PC	70
3.2.4	Saving as a script on the PC	70
3.2.5	Saving as an offline configuration file on the PC	71
3.3	Configuration Signature	72
4	Loading Software Updates	73
4.1	Loading the Software manually from the ACA	75
4.1.1	Selecting the software to be loaded	76
4.1.2	Starting the software	77
4.1.3	Performing a cold start	78
4.2	Automatic software update by ACA	79
4.3	Loading the software from the TFTP server	81
4.4	Loading the Software via File Selection	83
4.5	Bootcode Update via TFTP	84
4.5.1	Updating the Bootcode file	84
5	Configuring the Ports	87
6	Assistance in the Protection from Unauthorized Access	93
6.1	Protecting the device	94
6.2	Password for SNMP access	95
6.2.1	Description of password for SNMP access	95
6.2.2	Entering the password for SNMP access	96
6.3	Telnet/internet/SSH access	100
6.3.1	Description of Telnet Access	100
6.3.2	Description of Web Access (http)	100
6.3.3	Description of SSH Access	101
6.3.4	Switching Telnet/Internet/SSH access on/off	102
6.3.5	Web access through HTTPS	103
6.4	Restricted Management Access	106
6.5	HiDiscovery Access	109
6.5.1	Description of the HiDiscovery Protocol	109
6.5.2	Enabling/disabling the HiDiscovery function	109

6.6	Port access control	110
6.6.1	Description of the port access control	110
6.6.2	Application Example for Port Access Control	111
6.7	Port Authentication IEEE 802.1X	113
6.7.1	Description of Port Authentication according to IEEE 802.1X	113
6.7.2	Authentication Process according to IEEE 802.1X	114
6.7.3	Preparing the Device for the IEEE 802.1X Port Authentication	114
6.7.4	IEEE 802.1X Settings	115
6.8	Access Control Lists (ACL)	116
6.8.1	Description of prioritizing with ACLs	117
6.8.2	Description of IP-based ACLs	118
6.8.3	Description of MAC-based ACLs	119
6.8.4	Configuring IP ACLs	121
6.8.5	Configuring MAC ACLs	123
6.8.6	Configuring Priorities with IP ACLs	123
6.8.7	Specifying the Sequence of the Rules	125
6.8.8	ACLs for Layer 4 fragments	126
6.9	Login Banner	128
6.10	CLI Banner	129
7	Synchronizing the System Time in the Network	131
7.1	Setting the time	132
7.2	SNTP	134
7.2.1	Description of SNTP	134
7.2.2	Preparing the SNTP Configuration	135
7.2.3	Configuring SNTP	136
7.3	Precision Time Protocol	139
7.3.1	Description of PTP Functions	139
7.3.2	Preparing the PTP Configuration	145
7.3.3	Application Example	147
7.4	Interaction of PTP and SNTP	152
8	Network Load Control	155
8.1	Direct Packet Distribution	156
8.1.1	Store and Forward	156
8.1.2	Multi-Address Capability	156
8.1.3	Aging of learned MAC addresses	157
8.1.4	Entering Static Addresses	158
8.1.5	Disabling the Direct Packet Distribution	159

8.2	Multicast Application	161
8.2.1	Description of the Multicast Application	161
8.2.2	Example of a Multicast Application	162
8.2.3	Description of IGMP Snooping	163
8.2.4	Setting IGMP Snooping	164
8.2.5	Description of GMRP	169
8.2.6	Setting GMRP	171
8.3	Rate Limiter	173
8.3.1	Description of the Rate Limiter	173
8.3.2	Rate limiter settings	174
8.4	QoS/Priority	175
8.4.1	Description of Prioritization	175
8.4.2	VLAN tagging	176
8.4.3	IP ToS / DiffServ	178
8.4.4	Management prioritization	181
8.4.5	Handling of Received Priority Information	181
8.4.6	Handling of traffic classes	182
8.4.7	Setting prioritization	184
8.5	Flow Control	191
8.5.1	Description of Flow Control	191
8.5.2	Setting the Flow Control	193
8.6	VLANs	194
8.6.1	VLAN Description	194
8.6.2	Examples of VLANs	195
8.6.3	Double VLAN Tagging	208
9	Operation Diagnosis	213
9.1	Sending Traps	214
9.1.1	List of SNMP traps	215
9.1.2	SNMP Traps when Booting	216
9.1.3	Configuring Traps	217
9.2	Monitoring the Device Status	219
9.2.1	Configuring the Device Status	220
9.2.2	Displaying the Device Status	221
9.3	Out-of-band Signaling	222
9.3.1	Controlling the Signal Contact	223
9.3.2	Monitoring the Device Status via the Signal Contact	224
9.3.3	Monitoring the Device Functions via the Signal Contact	224
9.3.4	Monitoring the Fan	225
9.4	Port Status Indication	228

9.5	Event Counter at Port Level	230
9.5.1	Detecting Non-matching Duplex Modes	231
9.5.2	TP Cable Diagnosis	233
9.5.3	Port Monitor	235
9.5.4	Auto Disable	238
9.6	Displaying the SFP Status	240
9.7	Topology Discovery	241
9.7.1	Description of Topology-Detection	241
9.7.2	Displaying the Topology Discovery Results	242
9.8	Detecting IP Address Conflicts	244
9.8.1	Description of IP Address Conflicts	244
9.8.2	Configuring ACD	245
9.8.3	Displaying ACD	245
9.9	Detecting Loops	246
9.10	Reports	247
9.11	Monitoring Data Traffic on the Ports (Port Mirroring)	249
9.12	Syslog	253
9.13	Trap log	256
9.14	MAC Notification	257
A	Setting up the Configuration Environment	259
A.1	Setting up a DHCP/BOOTP Server	260
A.2	Setting up a DHCP Server with Option 82	266
A.3	TFTP Server for Software Updates	270
A.3.1	Setting up the TFTP Process	271
A.3.2	Software Access Rights	274
A.4	Preparing access via SSH	275
A.4.1	Generating a key	275
A.4.2	Loading a key onto the device	277
A.4.3	Access through an SSH	277
A.5	HTTPS Certificate	280
A.6	Service Shell	281

B	General Information	283
B.1	Management Information Base (MIB)	284
B.2	Abbreviations used	287
B.3	Technical Data	288
B.4	Readers' Comments	289
C	Index	291
D	Further Support	295

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 “Routing Configuration User Manual” document contains the information you need to start operating the routing function. It takes you step-by-step from a small router application through to the router configuration of a complex network.

The manual enables you to configure your router by following the examples.

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) as well as Telnet or SSH (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)
- ▶ SSH (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.

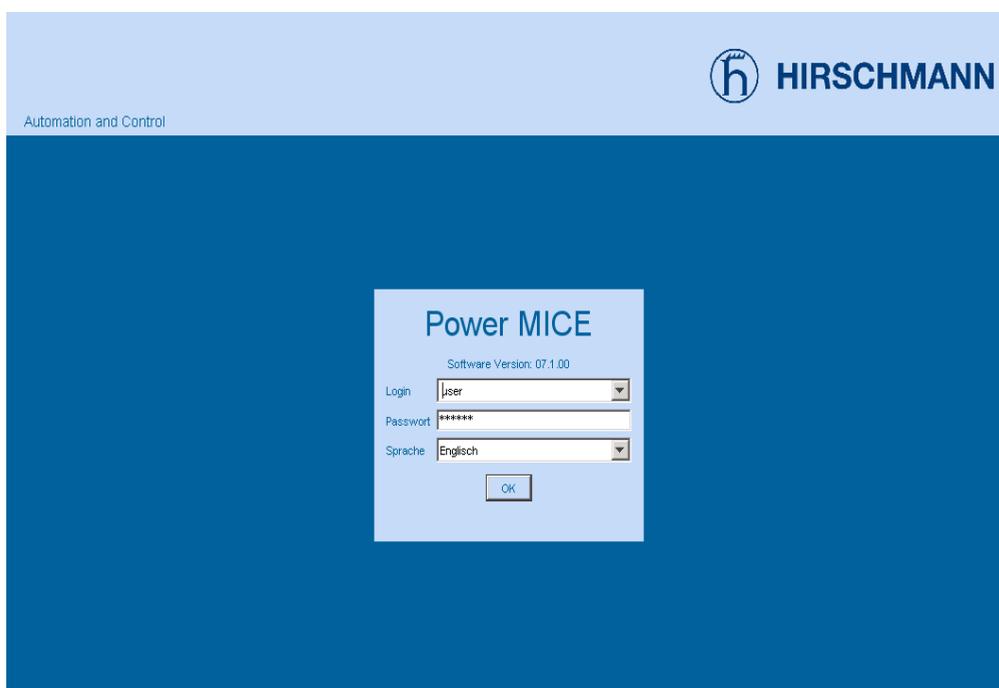


Figure 5: Login window

- 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

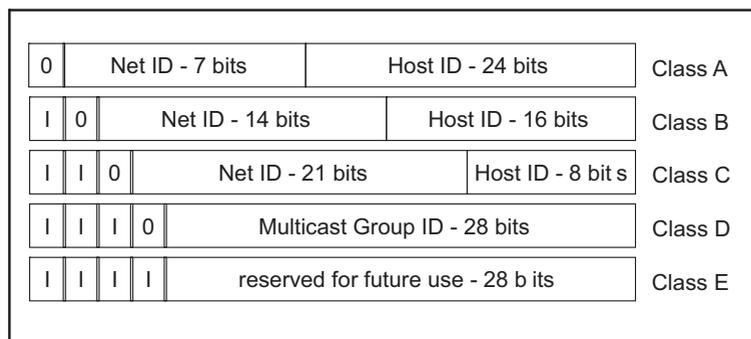


Figure 6: Bit representation of the IP address

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).

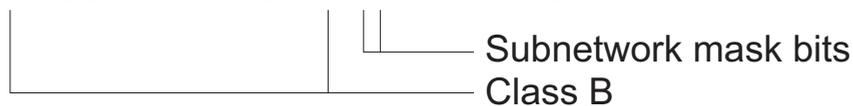
Example of a netmask:

Decimal notation

255.255.192.0

Binary notation

11111111.11111111.11000000.00000000

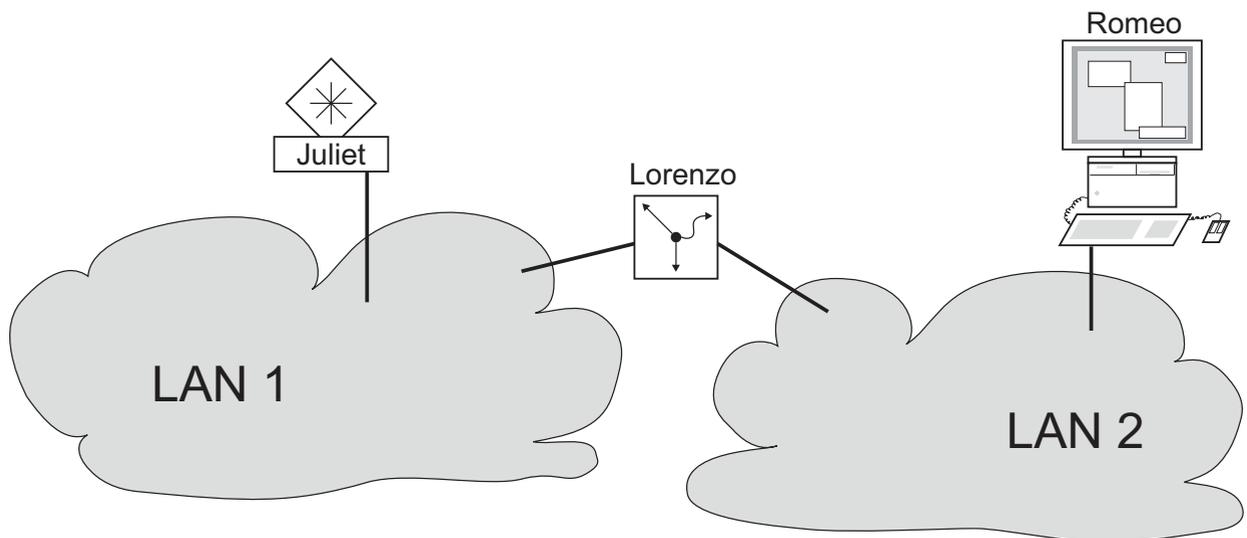


Example of IP addresses with subnetwork assignment when the above subnet mask is applied:



### ■ 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 |
|                                 |                       | ----- 25 mask bits -----            |
| CIDR notation: 149.218.112.0/25 |                       |                                     |
|                                 |                       | ----- Mask bits -----               |

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.

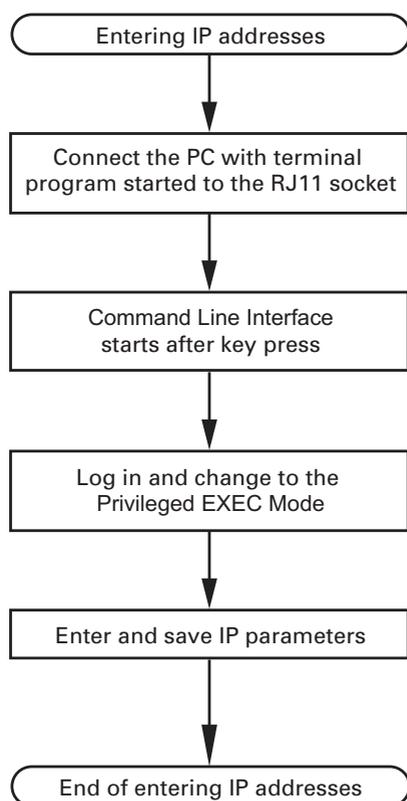


Figure 8: Flow chart for entering IP addresses

**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 67 “Saving locally \(and on the ACA\)”](#).

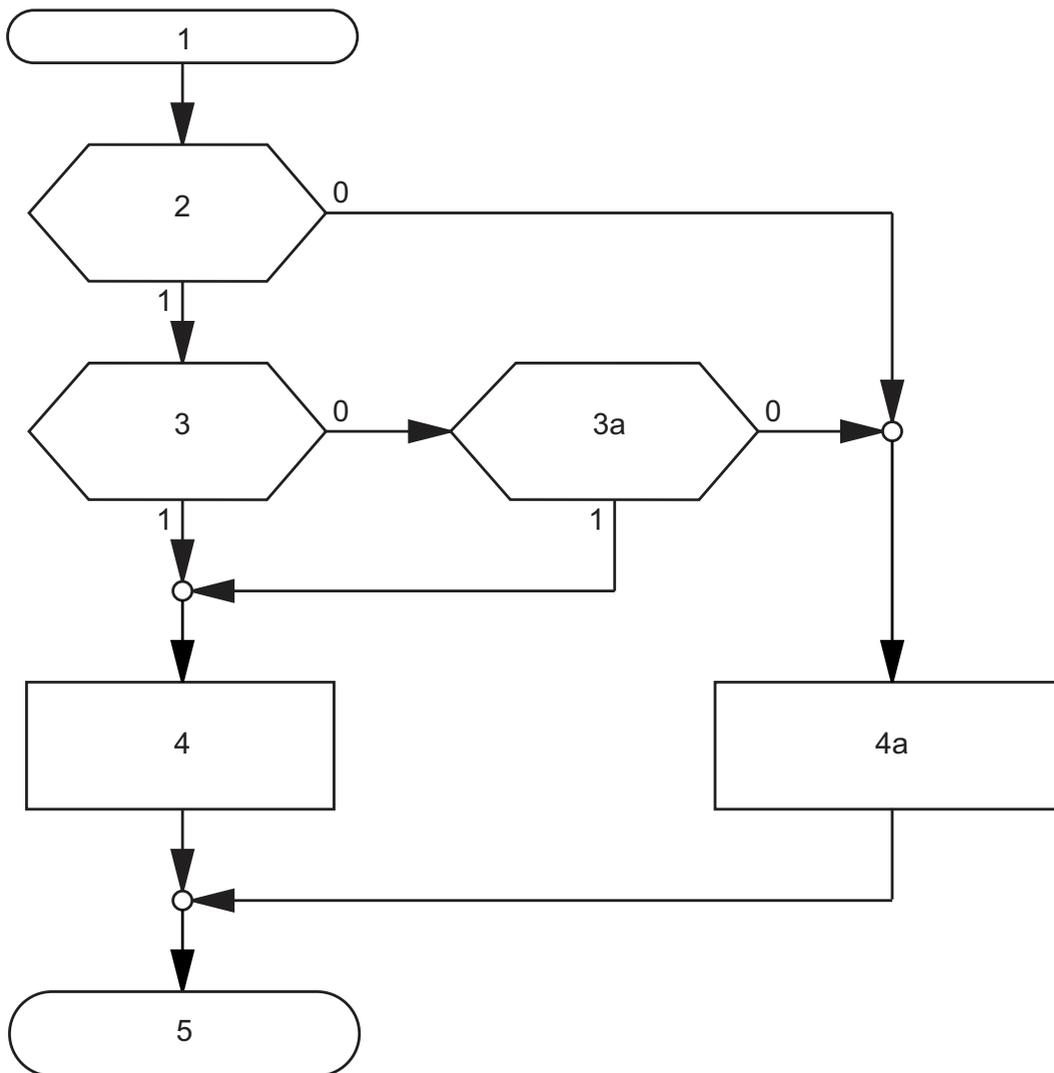


Figure 9: Flow chart of loading configuration data from the ACA

- 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 260.](#)

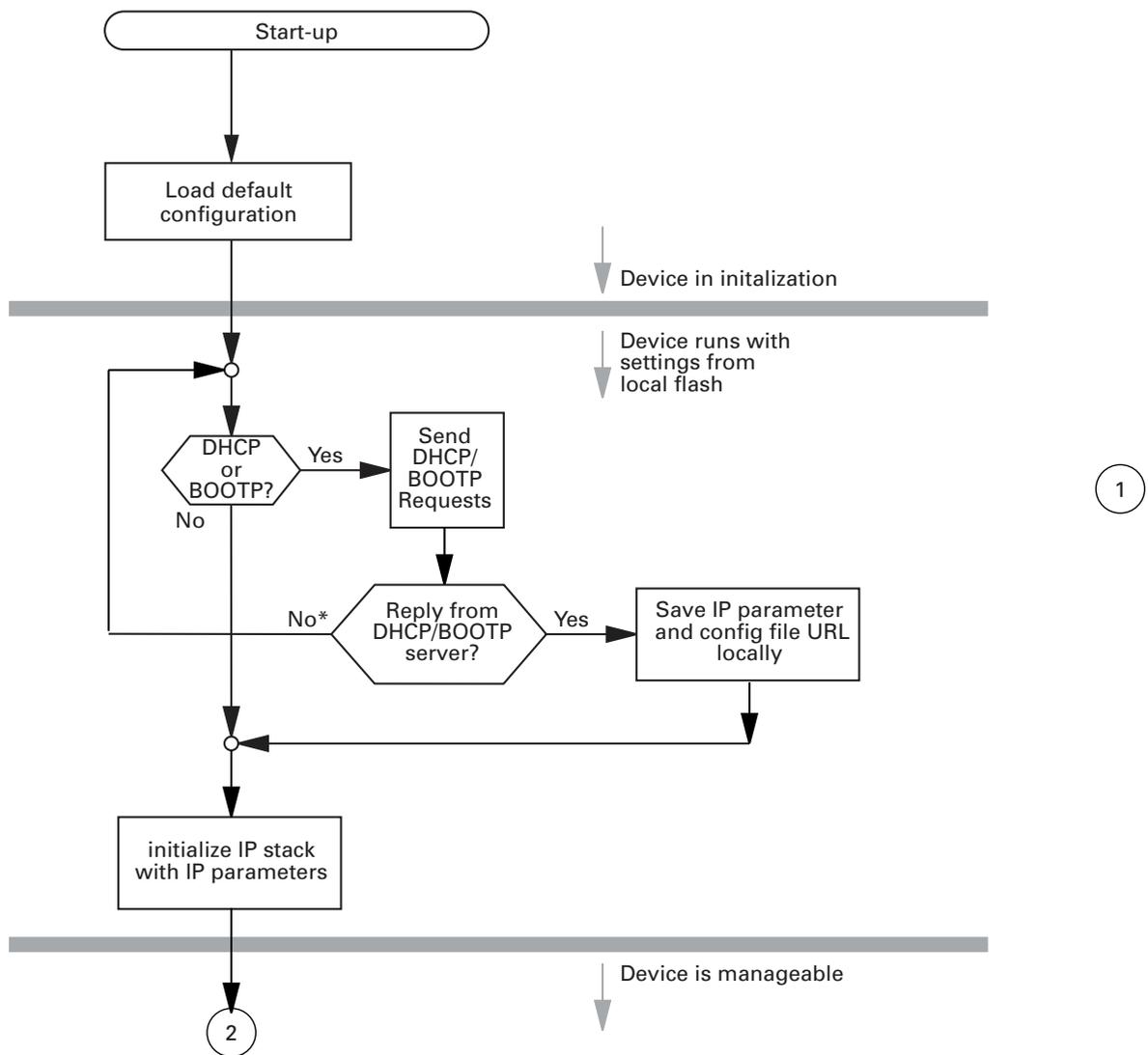


Figure 10: Flow chart for the BOOTP/DHCP process, part 1  
 \* see note [figure 11](#)

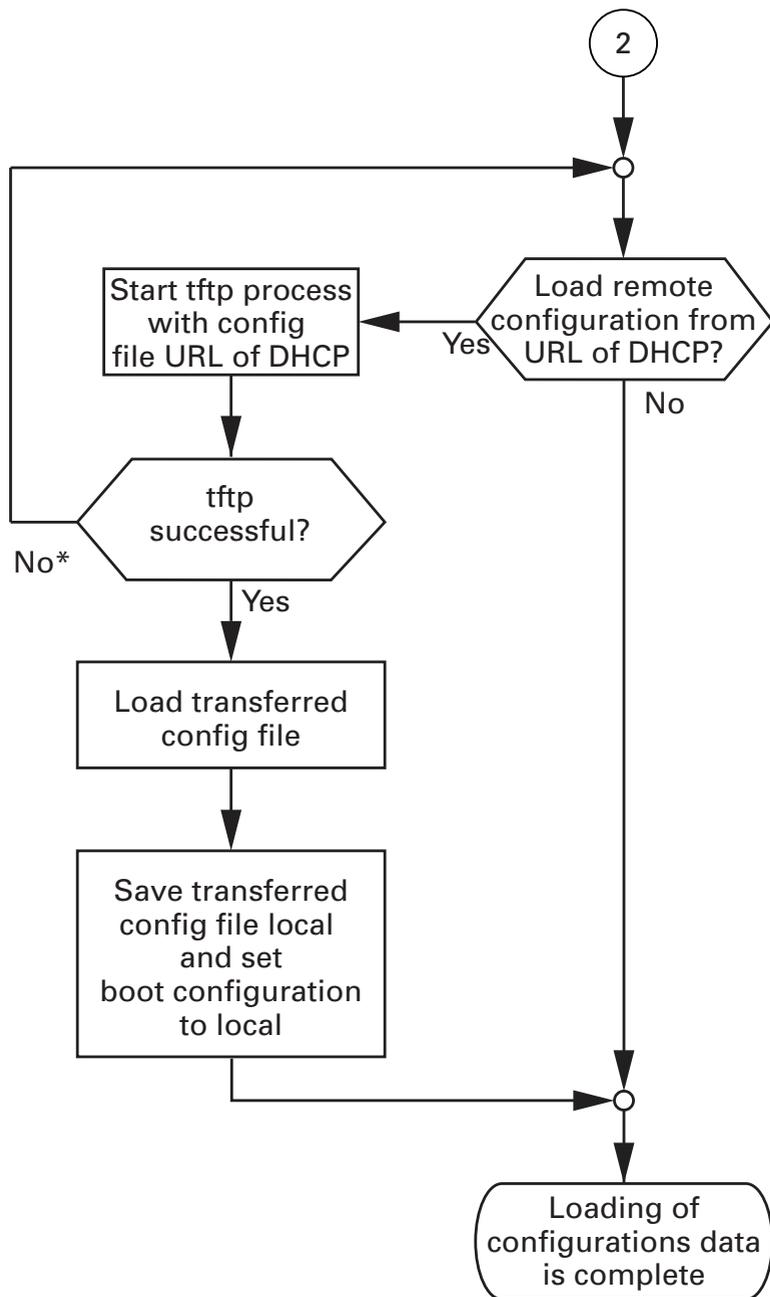


Figure 11: Flow chart for the BOOTP/DHCP process, part 2

**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 260 “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 266.

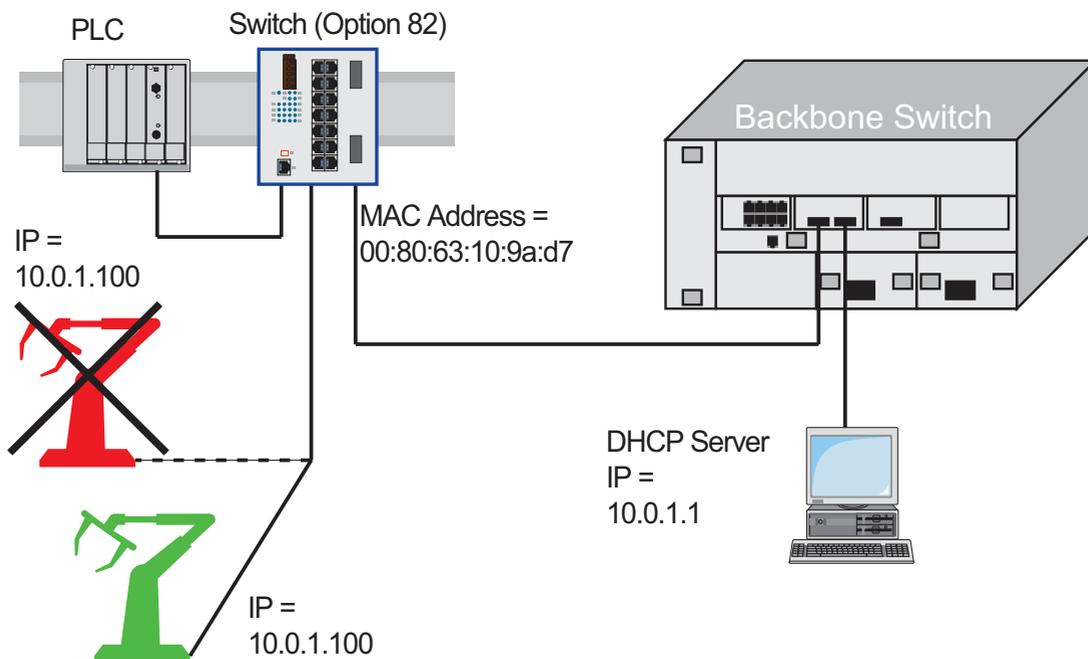


Figure 12: Application example of using Option 82

## 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 260.](#)
  - ▶ 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 266.](#)
  - ▶ 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 266 “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.

**Note:** If you want to access the device via SSH, you also need an SSH key. To transfer the SSH key of the old device to the new one, you have the following options:

- If you have already created the key and saved it outside the device (e.g. on your administration workstation), load the saved key onto the new device ([see on page 277 “Loading a key onto the device”](#)).
- Otherwise create a new SSH key and load it onto the new device ([see on page 275 “Preparing access via SSH”](#)). Note that the new device now identifies itself by means of another key.



## 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.
- ▶ from a script file of the AutoConfiguration Adapter. If an ACA is connected to the device, the device automatically loads its configuration from the script file of the ACA during the boot procedure ([see on page 63 “Loading a script from the ACA”](#)).

**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 or an editable and readable script on the PC 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 69 “Saving in a binary file or a script 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 67](#) describes how you can save a configuration file on an ACA.

#### ■ Loading a script from the ACA

If the ACA contains a script file, the device automatically loads its configuration from the script file on the ACA during the boot procedure.

The prerequisites for this are:

- ▶ The ACA is connected during the boot procedure.
- ▶ There is no binary configuration in the main directory of the ACA.
- ▶ The main directory of the ACA contains a file with the name “autoupdate.txt”.
- ▶ The file “autoupdate.txt” is a text file and contains a line whose content has the format `script=<file_name>`. Here `<file_name>` stands for the name of the script file to be loaded, e.g. `custom.cli`.
- ▶ The file specified using `script=<file_name>`, e.g. `custom.cli`, is located in the main directory of the ACA and is a valid script file.

If the local non-volatile memory of the device contains a configuration, the device ignores this.

After applying the script, the device updates the configuration in the local non-volatile memory with the configuration from the script.

In the process, it also writes the current binary configuration to the ACA.

**Note:** During the boot procedure, a binary configuration on the ACA has priority over a script on the ACA.

The chapter [“Saving locally \(and on the ACA\)”](#) describes how you can save a script 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 217 “Configuring Traps”](#)),
- ▶ update the device status ([see on page 220 “Configuring the Device Status”](#)),
- ▶ update the status of the signal contacts ([see on page 223 “Controlling the Signal Contact”](#)).

## **3.1.5 Using the offline configurator**

The offline configurator allows you to create configurations for devices in advance. You create the configuration virtually on your PC and load it onto your device in a 2nd step.

In this way you can prepare and manage the device configuration efficiently, thus saving time and effort both when creating the configuration and loading it to the devices.

For more details on using the offline configurator, see the chapter “Loading a configuration from the offline configurator” in the “GUI” Reference Manual.

### ■ **Example of using the offline configurator**

An IT employee already creates the configuration files for the devices of a production cell during the planning phase. In doing so, he uses existing configuration files for a similar production cell and modifies these.

He makes the offline configuration files available to the field service employee, who mounts the devices on site and then loads the configuration to the devices. All that is required for this is for the devices to be reachable and have received an IP address, e.g. via HiDiscovery.

### ■ **Data format**

The offline configurator reads and writes configuration data in an XML-based format. The file name extension of these files is “.ocf” (Offline Configurator Format).

You can use the graphical user interface of the devices to load these files and thus configure your devices very quickly.

The XML format also allows you to use other tools to create, edit and manage the offline configuration files and thus optimize your administration processes.

### ■ **Installation and operating requirements**

A requirement for the installation is a PC with a Windows™ XP operating system (with Service Pack 3) or higher.

You install the offline configurator from the product CD included with the device. To do so, start the “Setup.exe” installation file from the “ocf\_setup” folder.

The offline configurator - like the graphical user interface - uses Java software 6 (“Java™ Runtime Environment (JRE) Version 1.6.x”). Install the software from [www.java.com](http://www.java.com).

### ■ **Using the offline configurator**

Start the offline configurator by double-clicking the “Offline Management” desktop symbol.

For more details on using the offline configurator, see the chapter “Loading a configuration from the offline configurator” in the “GUI” Reference Manual.

## 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, or as an editable and readable script,
- ▶ save the current configuration in binary form or as an editable and readable CLI script 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 217 “Configuring Traps”),
- ▶ update the device status (see on page 220 “Configuring the Device Status”),
- ▶ update the status of the signal contacts (see on page 223 “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 or a script 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, choose "to URL (binary)" to create a binary file, or "to URL (script)" to create an editable and readable script 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
copy nvram:script
 tftp://10.0.1.159/switch/
 config.txt
```

Switch to the privileged EXEC mode.

The device saves the configuration data in a binary file on a tftp server in the connected network

The device saves the configuration data in a script file on a tftp server in the connected network.

**Note:** 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 loading script files, these are only intended for overwriting the default setting of the configuration.

### 3.2.3 Saving to a binary file on the PC

The device allows you to save the current configuration data in a binary file on your PC.

- Select the  
Basics: Load/Save dialog.
- In the "Save" frame, click "on the PC (binary)".
- In the save dialog, enter the name of the file in which you want the device to save the configuration file.
- Click "Save".

### 3.2.4 Saving as a script on the PC

The device allows you to save the current configuration data in an editable and readable file on your PC.

- Select the `Basics: Load/Save` dialog.
- In the “Save” frame, click “to PC (script)”.
- In the save dialog, enter the name of the file in which you want the device to save the configuration file.
- Click "Save".

### 3.2.5 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 75](#).

- 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 keeps a backup of the existing software in the non-volatile memory.
  - 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 270 “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.

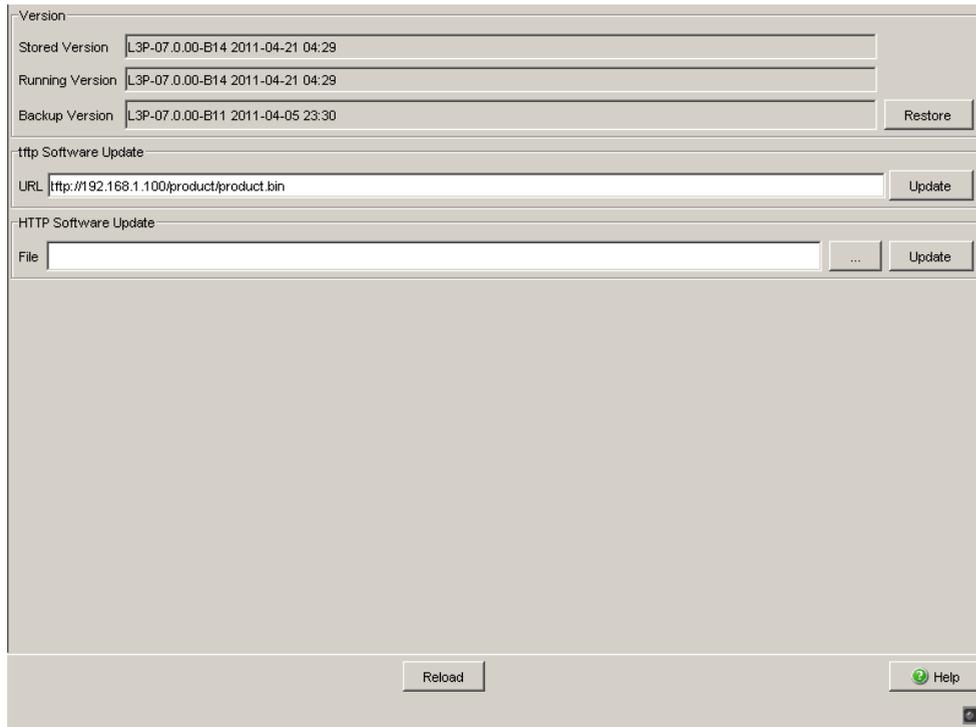


Figure 16: Software update dialog

- 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**

If the device is equipped with PoE media modules, it will then allow you to supply current to devices such as IP phones via the twisted-pair cable. PoE media modules support Power over ETHERNET according to IEEE 802.3af.

On delivery, the Power over ETHERNET function is activated globally and on all PoE-capable ports.

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 MACH 4000:

The device provides the nominal power for the sum of all PoE ports plus a surplus. Should the connected devices require more PoE power than is provided, the device then switches PoE off at the ports. Initially, the device switches PoE off at the ports with the lowest PoE priority. If multiple ports have the same priority, the device first switches PoE off at the ports with the higher port number.

### **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.
- In the “Priority” column (MACH 4000), set the PoE priority of the port to “low”, “high” or “critical”.
- 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 214 “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/SSH access can be switched off
- ▶ Restricted Management access
- ▶ HiDiscovery-Function can be switched off
- ▶ Port access control by IP or MAC address
- ▶ IEEE 802.1X standard port authentication
- ▶ Access Control Lists (ACL)
- ▶ 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 96 “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.  
If necessary, deactivate SSH access.  
[See “Switching Telnet/Internet/SSH access on/off” on page 102.](#)
- 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.
- The "Accept only encrypted requests" function encrypts the data of the Web-based management that is transferred between your PC and the device with SNMPv3. You can set the function differently for access with a read password and access with a read/write password.
- When you activate the "Synchronize password to v1/v2 community" function, when the password is changed the device synchronizes the corresponding community name.
  - When you change the password for the read/write access, the device updates the readWrite community for the SNMPv1/v2 access to the same value.
  - When you change the password for the read access, the device updates the readOnly community for the SNMPv1/v2 access to the same value.

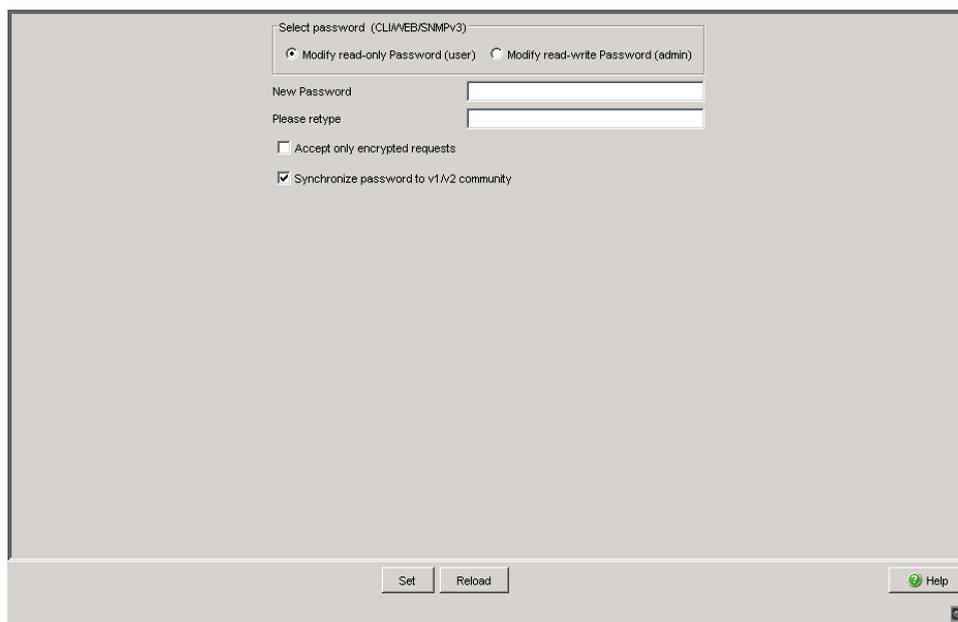


Figure 18: Password/SNMP Access dialog

**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.

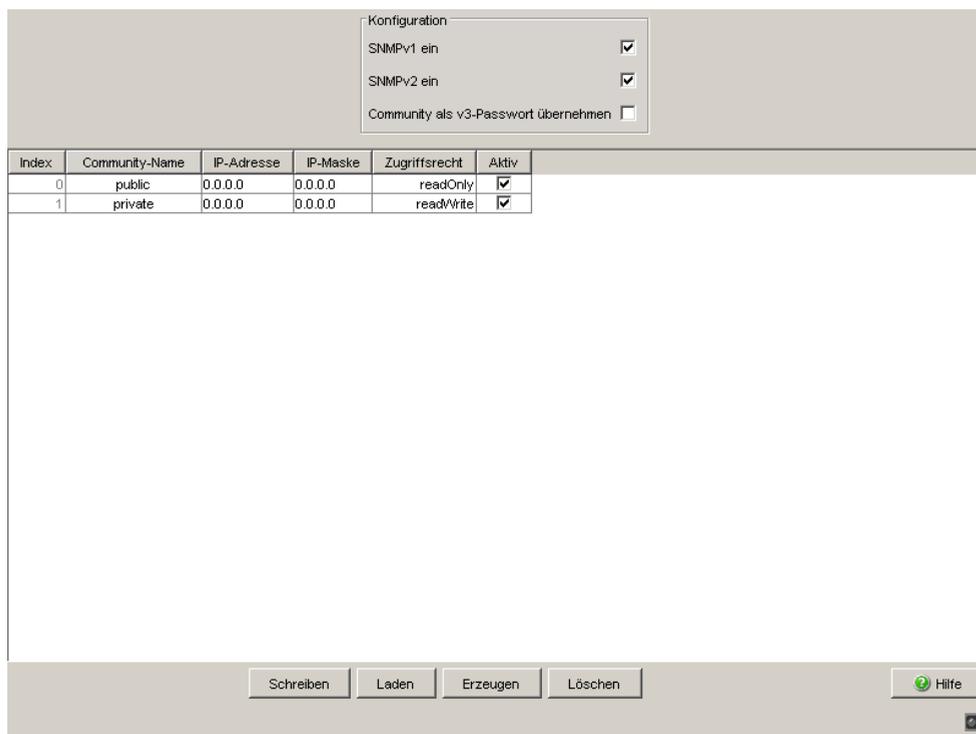
If you select SNMPv1 or SNMPv2, you can specify in the table via which IP addresses the device may be accessed, and what kinds of passwords are to be used.

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 image shows a configuration dialog for SNMPv1/v2 access. It features 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 columns: Index, Community-Name, IP-Adresse, IP-Maske, Zugriffsrecht, and Aktiv. The table contains two rows: index 0 with 'public' community, IP 0.0.0.0, mask 0.0.0.0, 'readOnly' rights, and 'Aktiv' checked; and index 1 with 'private' community, IP 0.0.0.0, mask 0.0.0.0, 'readWrite' rights, and 'Aktiv' checked. At the bottom, there are buttons for 'Schreiben', 'Laden', 'Erzeugen', 'Löschen', and 'Hilfe'.

| 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"/> |

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”.

## 6.3 Telnet/internet/SSH access

### 6.3.1 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.

### 6.3.2 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.

### 6.3.3 Description of SSH Access

The device's SSH server allows you to configure the device using the Command Line Interface (in-band). You can deactivate the SSH server to prevent SSH access to the device.

The server is deactivated in its default setting.

After the SSH server has been deactivated, you will no longer be able to access the device via a new SSH connection. If an SSH 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 SSH server.

**Note:** To be able to access the device via SSH, you require a key that has to be installed on the device. See [“Preparing access via SSH” on page 275](#).

The device supports SSH version 1 and version 2. You have the option to define the protocol to be used.

- Open the `Security:Telnet/Web/SSH Access` dialog.
- Select the protocol to be used in the "Configuration" frame, "SSH Version" field.

|                     |                                           |
|---------------------|-------------------------------------------|
| enable              | Change to the privileged EXEC mode.       |
| no ip ssh           | Deactivates the SSH server.               |
| ip ssh protocol 2   | The SSH server uses SSH version 2.        |
| ip ssh protocol 1   | The SSH server uses SSH version 1.        |
| ip ssh protocol 1 2 | The SSH server uses SSH versions 1 and 2. |
| ip ssh              | Activates the SSH server.                 |

### 6.3.4 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/SSH access` dialog.
- Disable the server to which you want to refuse access.

|                           |                                           |
|---------------------------|-------------------------------------------|
| enable                    | Switch to the privileged EXEC mode.       |
| configure                 | Switch to the Configuration mode.         |
| lineconfig                | Switch to the configuration mode for CLI. |
| transport input telnet    | Enable Telnet server.                     |
| no transport input telnet | Disable Telnet server.                    |
| exit                      | Switch to the Configuration mode.         |
| exit                      | Switch to the privileged EXEC mode.       |
| ip http server            | Enable Web server.                        |
| no ip http server         | Disable Web server.                       |
| ip ssh                    | Enable SSH function on Switch             |
| no ip ssh                 | Disable SSH function on Switch            |

### 6.3.5 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:httpscert`
- 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/SSH 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.

## 6.4 Restricted Management Access

The device allows you to differentiate the management access to the device based on IP address ranges, and to differentiate these in turn based on management services (http, snmp, telnet, ssh). You thus have the option to set finely differentiated management access rights.

If you only want the device, which is located, for example, in a production plant, to be managed from the network of the IT department via the Web interface, but also want the administrator to be able to access it remotely via SSH, you can achieve this with the “Restricted management access” function.

You can configure this function using the graphical user interface or the CLI. The graphical user interface provides you with an easy configuration option. Make sure you do not unintentionally block your access to the device. The CLI access to the device via V.24 provided at all times is excluded from the function and cannot be restricted.

In the following example, the IT network has the address range 192.168.1.0/24 and the remote access is from a mobile phone network with the IP address range 109.237.176.0 - 109.237.176.255.

The device is already prepared for the SSH access ([see on page 275 “Preparing access via SSH”](#)) and the SSH client application already knows the fingerprint of the host key on the device.

| Parameter                 | IT network    | Mobile phone network |
|---------------------------|---------------|----------------------|
| Network address           | 192.168.1.0   | 109.237.176.0        |
| Netmask                   | 255.255.255.0 | 255.255.255.0        |
| Desired management access | http, snmp    | ssh                  |

Table 4: Example parameter for the restricted management access

Select the `Security:Restricted Management Access` dialog.

- Leave the existing entry unchanged and use the “Create” button to create a new entry for the IT network.
- Enter the IP address 192.168.1.0.
- Enter the netmask 255.255.255.0.
- Leave the HTTP and SNMP management services activated and deactivate the Telnet and SSH services by removing the checkmarks from the respective boxes.
- Use the “Create” button to create a new entry for the mobile phone network.
- Enter the IP address 109.237.176.0.
- Enter the netmask 255.255.255.0.
- Deactivate the HTTP, SNMP and Telnet services and leave SSH activated.
- Make sure you have CLI access to the device via V.24.
- Deactivate the preset entry, because this allows everything and would cause your subsequent entries to have no effect.
- Activate the function.
- Click on “Write” to temporarily save the data.
- If your current management station is also located in the IT network, you continue to have access to the graphical user interface. Otherwise the device ignores operations via the graphical user interface, and it also rejects a restart of the graphical user interface.
- Check whether you can access the device from the IT network via http and snmp: Open the graphical user interface of the device in a browser, login on the start screen, and check whether you can read data (as user “user”) or read and write data (as user “admin”). Check whether the device rejects connections via telnet and ssh.
- Check whether you can access the device from the mobile phone network via ssh: Open an SSH client, make a connection to the device, login, and check whether you can read data, or read and write data. Check whether the device rejects connections via http, snmp and telnet.
- When you have successfully completed both tests, save the settings in the non-volatile memory. Otherwise check your configuration. If the device rejects access with the graphical user interface, use the CLI of the device to initially deactivate the function via V.24.

|                                                       |                                                                                             |
|-------------------------------------------------------|---------------------------------------------------------------------------------------------|
| enable                                                | Switch to the privileged EXEC mode.                                                         |
| show network mgmt-access                              | Display the current configuration.                                                          |
| network mgmt-access add                               | Create an entry for the IT network. This is given the smallest free ID - in the example, 2. |
| network mgmt-access modify 2<br>ip 192.168.1.0        | Set the IP address of the entry for the IT network.                                         |
| network mgmt-access modify 2<br>netmask 255.255.255.0 | Set the netmask of the entry for the IT network.                                            |
| network mgmt-access modify 2<br>telnet disable        | Deactivate telnet for the entry of the IT network.                                          |
| network mgmt-access modify 2<br>ssh disable           | Deactivate SSH for the entry of the IT network.                                             |
| network mgmt-access add                               | Create an entry for the mobile phone network. In the example, this is given the ID 3.       |
| network mgmt-access modify 3<br>ip 109.237.176.0      | Set the IP address of the entry for the mobile phone network.                               |
| network mgmt-access modify 3<br>netmask 255.255.255.0 | Set the netmask of the entry for the mobile phone network.                                  |
| network mgmt-access modify 3<br>http disable          | Deactivate http for the entry of the mobile phone network.                                  |
| network mgmt-access modify 3<br>snmp disable          | Deactivate snmp for the entry of the mobile phone network.                                  |
| network mgmt-access modify 3<br>telnet disable        | Deactivate telnet for the entry of the mobile phone network.                                |
| network mgmt-access status 1<br>disable               | Deactivate the <b>preset</b> entry.                                                         |
| network mgmt-access<br>operation enable               | Activate the function <b>immediately</b> .                                                  |
| show network mgmt-access                              | Display the current configuration of the function.                                          |
| copy system:running-config<br>nvram:startup-config    | Save the entire configuration in the non-volatile memory.                                   |

## 6.5 HiDiscovery Access

### 6.5.1 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.

### 6.5.2 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 network protocol hidiscovery off network protocol hidiscovery read-only network protocol hidiscovery read-write</pre> | <p>Switch to the privileged EXEC mode.<br/>Disable HiDiscovery function.</p> <p>Enable HiDiscovery function with “read-only” access</p> <p>Enable HiDiscovery function with “read-write” access</p> |
|-----------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

## 6.6 Port access control

### 6.6.1 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.

## 6.6.2 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 87 “Configuring the Ports”</a> ) and send an alarm |

Prerequisites for further configuration:

- ▶ The port for the LAN connection is enabled and configured correctly ([see on page 87 “Configuring the Ports”](#))
- ▶ Prerequisites for the device to be able to send an alarm (trap) ([see on page 217 “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.

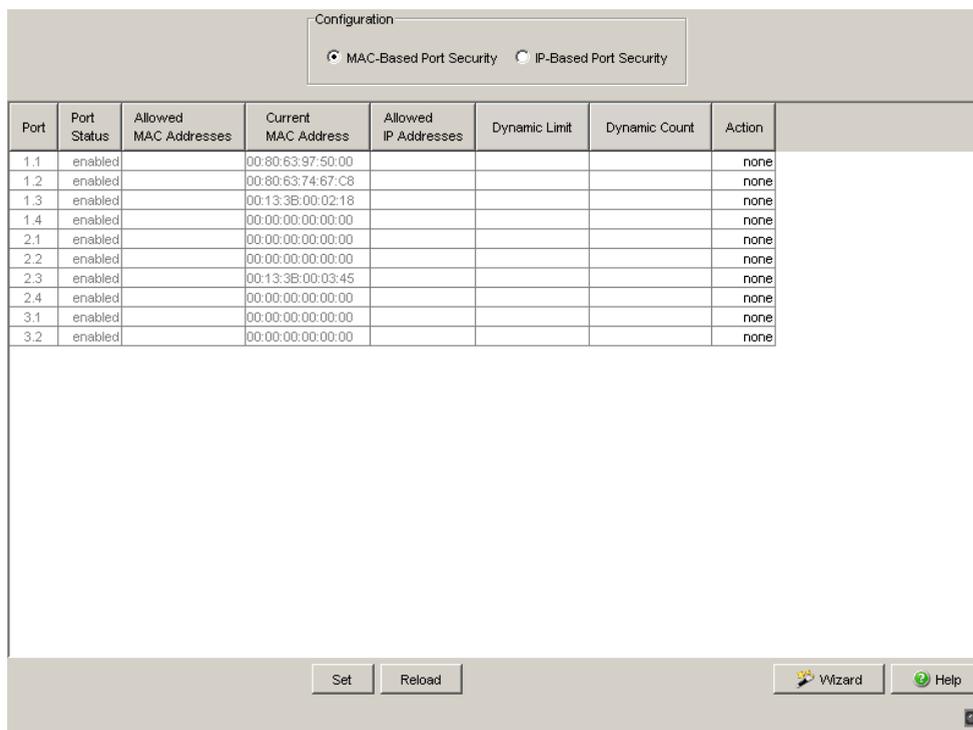


Figure 20: Port Security dialog

- 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.

## 6.7 Port Authentication IEEE 802.1X

### 6.7.1 Description of Port Authentication according to IEEE 802.1X

The port-based network access control is a method described in norm IEEE 802.1X to help protect IEEE 802 networks from unauthorized access. The protocol controls the access to this port by authenticating and authorizing a terminal device that is connected to one of the device's ports.

The authentication and authorization is carried out by the authenticator, in this case the device. The device authenticates the supplicant (the querying device, e.g. a PC, etc.), which means that it permits the access to the services it provides (e.g. access to the network to which the device is connected) or denies it. In the process, the device accesses an external authentication server (RADIUS server), which checks the authentication data of the supplicant. The device exchanges the authentication data with the supplicant via the Extensible Authentication Protocol over LANs (EAPOL), and with the RADIUS server via the RADIUS protocol.



Figure 21: Radius server connection

## **6.7.2 Authentication Process according to IEEE 802.1X**

A supplicant attempts to communicate via a device port.

- ▶ The device requests authentication from the supplicant. At this time, only EAPOL traffic is allowed between the supplicant and the device.
- ▶ The supplicant replies with its identification data.
- ▶ The device forwards the identification data to the authentication server.
- ▶ The authentication server responds to the request in accordance with the access rights.
- ▶ The device evaluates this response and provides the supplicant with access to this port (or leaves the port in the blocked state).

## **6.7.3 Preparing the Device for the IEEE 802.1X Port Authentication**

- Configure your own IP parameters (for the device).
- Globally enable the 802.1X port authentication function.
- Set the 802.1X port control to "auto". The default setting is "force-authorized".
- Enter the "shared secret" between the authenticator and the Radius server. The shared secret is a text string specified by the RADIUS server administrator.
- Enter the IP address and the port of the RADIUS server. The default UDP port of the RADIUS server is port 1812.

## 6.7.4 IEEE 802.1X Settings

### ■ Configuring the RADIUS Server

- Select the `Security:802.1x Port Authentication:RADIUS Server` dialog.

This dialog allows you to enter the data for 1, 2 or 3 RADIUS servers.

- Click "Create entry" to open the dialog window for entering the IP address of a RADIUS server.
- Confirm the IP address entered using "OK".  
You thus create a new row in the table for this RADIUS server.
- In the "Shared secret" column you enter the character string which you get as a key from the administrator of your RADIUS server.
- With "Primary server" you name this server as the first server which the device should contact for port authentication queries. If this server is not available, the device contacts the next server in the table.
- "Selected server" shows which server the device actually sends its queries to.
- With "Delete entry" you delete the selected row in the table.

### ■ Selecting Ports

- Select the `Security:802.1x Port Authentication:Port Configuration` dialog.
- In the "Port control" column you select "auto" for the ports for which you want to activate the port-related network access control.

### ■ Activating Access Control

- Select the `Security:802.1x Port Authentication:Global` dialog.
- With "Function" you enable the function.

## 6.8 Access Control Lists (ACL)

You can use Access Control Lists (ACL) to filter out, forward, divert or prioritize data packets as they are received. The device provides

- ▶ MAC-based ACLs and
- ▶ IP-based ACLs.

The device considers the ACLs when it receives a package. This is why the lists are called Ingress ACLs.

You configure Access Control Lists via the Command Line Interface. You will find details on this in the document “Reference Manual Command Line Interface”.

The device provides the following ACL capabilities:

- ▶ Up to 100 ACLs
- ▶ 10 rules per ACL,
- ▶ Up to 100 rules per interface,
- ▶ Up to 1000 rules on all interfaces combined
- ▶ Possible actions:
  - permit and deny,
  - in combination with permit: assign queue and redirect - i.e. if a rule applies, the packet is forwarded to the specific interface.
- ▶ “Deny everything” is always the (invisible) final rule. It comes into effect if no other rules apply to this interface.

The configuration of ACLs consists of the following steps:

- First define ACL and then
- attach the ACL to one or all interfaces.  
You can attach ACLs to all physical ports and to all link aggregation interfaces.

**Note:** You configure Access Control Lists via the Command Line Interface. You will find details on this in the document “Reference Manual Command Line Interface”.

The sequence used in defining the rules of a list and the sequence in which these lists are connected to an interface determines the sequence in which the rules and lists are used ([see on page 125 “Specifying the Sequence of the Rules”](#)).

**Note:** With PowerMICE and MACH 4000, you can use either MAC-based or IP-based ACLs for each interface. With MACH 4002-24G/48G, you can use both MAC-based and IP-based ACLs for each interface.

### 6.8.1 Description of prioritizing with ACLs

Prioritizing with ACLs provides you with an extension of the prioritizing function. Using the “assign queue” ACL action, you can perform extended prioritizing using protocols, source and destination addresses, VLAN ID, and so on ([see on page 118 “Description of IP-based ACLs”](#)), ([see on page 119 “Description of MAC-based ACLs”](#)).

If an ACL rule containing an assign queue action applies to a packet received, the device modifies the priority information in the data packet ([see on page 175 “QoS/Priority”](#)) according to the specified ([see table 5](#)) assign queue parameter. This procedure is known as ACL remarking. The device sends the data packets with the modified priority information.

| Assign queue parameter | VLAN priority | DSCP     |
|------------------------|---------------|----------|
| 0                      | 0             | CS0 (0)  |
| 1                      | 1             | CS1 (8)  |
| 2                      | 2             | CS2 (16) |
| 3                      | 3             | CS3 (24) |
| 4                      | 4             | CS4 (32) |
| 5                      | 5             | CS5 (40) |
| 6                      | 6             | CS6 (48) |
| 7                      | 7             | CS7 (56) |

Table 5: Assigning the assign queue parameters to the modified VLAN priority and to the modified DSCP value

## 6.8.2 Description of IP-based ACLs

The device differentiates between standard and extended IP-based ACLs. ACLs with an ID number (ACL ID)

- ▶ 1 to 99 are standard IP-based ACLs and
- ▶ 100 to 199 are extended IP-based ACLs.

Standard IP-based ACLs provide the following criteria for filtering:

- ▶ IP source address with netmask
- ▶ All data packets (match any)

Extended IP-based ACLs provide the following criteria for filtering:

- ▶ All data packets (every)
- ▶ Protocol number or protocol (IP, ICMP, IGMP, TCP, UDP)
- ▶ IP source address with netmask or all IP source addresses (any)
- ▶ Layer 4 protocol port number of the source (UDP port, TCP port)
- ▶ IP destination address with netmask or all IP destination addresses (any)
- ▶ Layer 4 protocol port number of the destination (UDP port, TCP port)
- ▶ ToS field with mask

- ▶ DSCP field
- ▶ IP precedence field

**Note:** If you are using IP ACLs at ports which are located in the HIPER-Ring or which participate in the Ring/network coupling, you add the following rule to the ACLs:

- ▶ PERMIT
- ▶ Protocol: UDP
- ▶ Source IP: ANY
- ▶ Destination IP: 0.0.0.0/32
- ▶ Source port: 0
- ▶ Destination port: 0
- ▶ CLI command (1xx stands for 100..199):

```
access-list 1xx permit udp any eq 0
0.0.0.0 0.0.0.0 eq 0
```

**Note:** IP address masks in the rules of ACLs are inverse. This means that if you want to mask a single IP address, you select the netmask 0.0.0.0.

### 6.8.3 Description of MAC-based ACLs

While you use an ID number to identify IP-based ACLs, you use a unique name of your choice to identify MAC-based ACLs.

MAC-based ACLs provide the following criteria for filtering:

- ▶ Source MAC address with masks or all sources (any)
- ▶ Destination MAC address or all destinations (any)
- ▶ Ethernet type

- ▶ VLAN ID
- ▶ VLAN priority (COS)
- ▶ Secondary VLAN ID
- ▶ Secondary VLAN priority

**Note:** If you are using MAC ACLs at ports which are located in the HIPER-Ring or which participate in the Ring/network coupling, you add the following rule to the ACLs:

- ▶ PERMIT
- ▶ Source MAC: ANY
- ▶ Destination MAC: 00:80:63:00:00:00
- ▶ Destination MAC mask: 01:00:00:ff:ff:ff
- ▶ CLI command in Config-mac-access mode:  

```
permit any 00:80:63:00:00:00 01:00:00:ff:ff:ff
```

**Note:** If you are using MAC ACLs at ports located in the MRP-Ring, you add the following rule to the ACLs:

- ▶ PERMIT
- ▶ Source MAC: ANY
- ▶ Destination MAC: 01:15:4E:00:00:00
- ▶ Destination MAC mask: 00:00:00:00:00:03
- ▶ CLI command in the Config-mac-access mode:  

```
permit any 01:15:4E:00:00:00 00:00:00:00:00:03
```

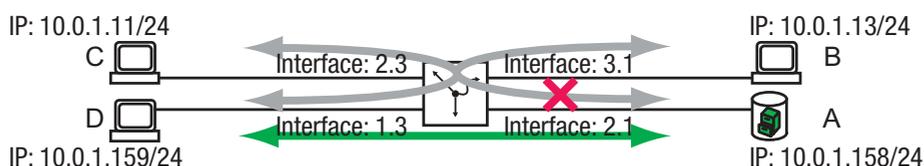
**Note:** MAC address masks in the rules of ACLs are inverse.

This means that if you want to mask a single MAC address, you select the network mask 00:00:00:00:00:00.

If you want to mask MAC addresses in the range from 00:80:63:00:00:00 to 00:80:63:FF:FF:FF, you select the network mask 00:00:00:FF:FF:FF.

## 6.8.4 Configuring IP ACLs

Example: Extended ACL



B and C are not allowed to communicate with A.

```
enable
configure
access-list 100 deny ip
 10.0.1.11 0.0.0.0
 10.0.1.158 0.0.0.0
access-list 100 permit
ip any any

access-list 110 deny ip
 10.0.1.13 0.0.0.0
 10.0.1.158 0.0.0.0
access-list 110 permit
ip any any

exit
show ip access-lists 100
```

Change to the privileged EXEC mode.

Change to the Configuration mode.

Erzeugt die erweiterte ACL 100 mit der 1. Regel. Diese verweigert den Datenverkehr von der IP-Quelladresse 10.0.1.11 zur IP-Zieladresse 10.0.1.158.

Fügt der ACL 100 eine weitere Regel hinzu. Diese erlaubt den Datenverkehr von jeder IP-Quelladresse zu jeder IP-Zieladresse.

Erzeugt die erweiterte ACL 110 mit der 1. Regel. Diese verweigert den Datenverkehr von der IP-Quelladresse 10.0.1.13 zur IP-Zieladresse 10.0.1.158.

Fügt der ACL 110 eine weitere Regel hinzu. Diese erlaubt den Datenverkehr von jeder IP-Quelladresse zu jeder IP-Zieladresse.

Change to the privileged EXEC mode.

Zeigt die Regeln von ACL 100 an.

ACL ID: 100

Rule Number: 1

```
Action..... deny
Match All..... FALSE
Protocol..... 255(ip)
Source IP Address..... 10.0.1.11
Source IP Mask..... 0.0.0.0
Destination IP Address..... 10.0.1.158
Destination IP Mask..... 0.0.0.0
```

Rule Number: 2

```
Action..... permit
Match All..... TRUE
```

```
configure Change to the Configuration mode.
interface 2/3 Change to the Interface Configuration mode of
 interface 2/3.
ip access-group 100 in Bindet die ACL 100 für empfangene Daten an das
 Interface 2.3.
exit Change to the Configuration mode.
interface 3/1 Wechsel in den Interface-Konfigurationsmodus
 von Interface 3.1.
ip access-group 110 in Bindet die ACL 110 für empfangene Daten an das
 Interface 3.1.
exit Change to the Configuration mode.
exit Change to the privileged EXEC mode.
```

show access-lists interface 2/3 in

| ACL Type | ACL ID | Sequence Number |
|----------|--------|-----------------|
| IP       | 100    | 1               |

## 6.8.5 Configuring MAC ACLs

Example: MAC ACL

Filtering AppleTalk and IPX from the entire network.

| <pre>enable configure mac access-list extended ipx-apple   deny any any ipx   deny any any appletalk   permit any any exit  mac access-group ipx-apple in exit  show mac access-lists</pre> | <p>Switch to the privileged EXEC mode.</p> <p>Switch to the Configuration mode.</p> <p>Create the extended ACL "ipx-apple".</p> <p>Add the rule "deny IPX" to the list.</p> <p>Add the rule "deny AppleTalk" to the list.</p> <p>Add the rule "permit all other data" to the list.</p> <p>Switch to the Configuration mode.</p> |                                         |                 |              |   |         |                                         |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------|-----------------|--------------|---|---------|-----------------------------------------|
| <pre>show mac access-lists</pre>                                                                                                                                                            | <p>Attach the ACL "ipx-apple" to all interfaces.</p> <p>Switch to the privileged EXEC mode.</p> <p>Display the ACLs..</p>                                                                                                                                                                                                       |                                         |                 |              |   |         |                                         |
| <pre>MAC ACL Name</pre> <hr/> <pre>ipx-apple</pre>                                                                                                                                          | <table border="0"> <thead> <tr> <th style="text-align: left;">Rules</th> <th style="text-align: left;">Direction</th> <th style="text-align: left;">Interface(s)</th> </tr> </thead> <tbody> <tr> <td>3</td> <td>inbound</td> <td>1/1,1/2,1/3,1/4,2/1,2/2,2/3,2/4,3/1,3/2</td> </tr> </tbody> </table>                          | Rules                                   | Direction       | Interface(s) | 3 | inbound | 1/1,1/2,1/3,1/4,2/1,2/2,2/3,2/4,3/1,3/2 |
| Rules                                                                                                                                                                                       | Direction                                                                                                                                                                                                                                                                                                                       | Interface(s)                            |                 |              |   |         |                                         |
| 3                                                                                                                                                                                           | inbound                                                                                                                                                                                                                                                                                                                         | 1/1,1/2,1/3,1/4,2/1,2/2,2/3,2/4,3/1,3/2 |                 |              |   |         |                                         |
| <pre>show access-lists interface 1/1 in</pre>                                                                                                                                               | <p>Display the ACLs of interface 1.1.</p>                                                                                                                                                                                                                                                                                       |                                         |                 |              |   |         |                                         |
| <pre>ACL Type</pre> <hr/> <pre>MAC</pre>                                                                                                                                                    | <table border="0"> <thead> <tr> <th style="text-align: left;">ACL ID</th> <th style="text-align: left;">Sequence Number</th> </tr> </thead> <tbody> <tr> <td>ipx-apple</td> <td>1</td> </tr> </tbody> </table>                                                                                                                  | ACL ID                                  | Sequence Number | ipx-apple    | 1 |         |                                         |
| ACL ID                                                                                                                                                                                      | Sequence Number                                                                                                                                                                                                                                                                                                                 |                                         |                 |              |   |         |                                         |
| ipx-apple                                                                                                                                                                                   | 1                                                                                                                                                                                                                                                                                                                               |                                         |                 |              |   |         |                                         |

## 6.8.6 Configuring Priorities with IP ACLs

Example: Prioritizing Multicast streams.

- ▶ Assign priority 6 to the Multicast streams with the IP Multicast destination addresses 239.1.1.1 to 239.1.1.255 and
- ▶ Assign priority 5 to the Multicast streams with the IP Multicast destination addresses 237.1.1.1 to 237.1.1.255 and

```

enable
configure
access-list 102 permit ip
 any 239.1.1.1 0.0.0.255
 assign-queue 6
access-list 102 permit ip
 any 237.1.1.1 0.0.0.255
 assign-queue 5

exit
show ip access-lists 102
ACL ID: 102

Rule Number: 1
Action..... permit
Match All..... FALSE
Protocol..... 255 (ip)
Destination IP Address..... 239.1.1.1
Destination IP Mask..... 0.0.0.255
Assign Queue..... 6

Rule Number: 2
Action..... permit
Match All..... FALSE
Protocol..... 255 (ip)
Destination IP Address..... 237.1.1.1
Destination IP Mask..... 0.0.0.255
Assign Queue..... 5

```

Switch to the privileged EXEC mode.  
 Switch to the Configuration mode.  
 Create the extended ACL 102 with the first rule. This rule assigns priority 6 to the IP Multicast destination addresses 239.1.1.1 with the mask 0.0.0.255.  
 Add another rule to the ACL 102. This rule assigns priority 5 to the IP Multicast destination addresses 237.1.1.1 with the mask 0.0.0.255.  
 Switch to the privileged EXEC mode.  
 Displays the rules of ACL 102.

**Example: Extended ACL with prioritizing using the Simple Network Management Protocol (SNMP, Layer 4)**

```

enable
configure
access-list 104 permit udp
 any any eq snmp
 assign-queue 5

exit
show ip access-lists 104

```

Change to the privileged EXEC mode.  
 Change to the Configuration mode.  
 Create the extended ACL 104 with the first rule. This rule assigns priority 5 to all SNMP packets with the UDP destination port (=161). This rule overwrites any priority contained in a VLAN tag with the value 5, and also overwrites the IP-DSCP value with cs5.  
 Change to the privileged EXEC mode.  
 Displays the rules of ACL 104.

```

ACL ID: 104

Rule Number: 1
Action..... permit
Match All..... FALSE
Protocol..... 17 (udp)
Destination L4 Port Keyword..... 161 (snmp)
Assign Queue..... 5

configure Change to the Configuration mode.
interface 2/1 Switch to the Interface Configuration mode of
 interface 2/1.
ip access-group 104 in Attaches ACL 104 to interface 2.1.
exit Change to the Configuration mode.
exit Change to the privileged EXEC mode.

show access-lists interface 2/1 in Display the ACLs attached to interface 2.1
 forreceived data packets.

ACL Type ACL ID Sequence Number

IP 100 1
IP 102 3
IP 104 4

```

ACL 100 contains the rule “permit all” at the end. Thus the ACLs 102 and 104 are never applied. You can use the sequence number to alter the sequence for processing the ACLs ([see on page 125 “Specifying the Sequence of the Rules”](#)).

### 6.8.7 Specifying the Sequence of the Rules

The sequence of the ACLs determines their usage. The first list that applies is used, and all subsequent rules are ignored. You can influence the sequence by assigning the sequence number. A small sequence number has precedence over a higher one.

```

enable
configure
ip access-group 100 in 30
ip access-group 102 in 10
ip access-group 104 in 20
exit
show access-lists interface 2/1 in

```

Switch to the privileged EXEC mode.  
 Switch to the Configuration mode.  
 Assign sequence number 30 to ACL 100.  
 Assign sequence number 10 to ACL 102.  
 Assign sequence number 20 to ACL 104.  
 Switch to the privileged EXEC mode.  
 Display the ACLs attached to interface 2.1 for received data packets.

| ACL Type | ACL ID | Sequence Number |
|----------|--------|-----------------|
| IP       | 100    | 30              |
| IP       | 104    | 20              |
| IP       | 102    | 10              |

### 6.8.8 ACLs for Layer 4 fragments

Splitting a long data packet into a number of shorter data packets is known as fragmenting. For example, some transferring routers fragment a Layer 4 data packet into a number of Layer 3 data packets if the length of the data packet is greater than the MTU (Maximum Transmission Unit) of the transferring interface.

Only the first Layer 3 data packet contains the Layer 4 header, e.g. TCP or UDP. The following data packets with the Layer 4 fragments do not contain any Layer 4 headers that can be evaluated. Therefore, ACLs drop these data packets. The MACH104, MACH1040 and MACH4002 24G/48G devices process Layer 4 fragments and allow you to forward these data packets also.

When you set up an ACL for Layer 4, the device uses the user-defined rule to automatically create a second rule for the fragments:

- ▶ The user-defined rule processes the data packet with the first Layer 4 fragment.
- ▶ The automatically created rule processes the data packets with the following Layer 4 fragments.

Therefore, when the fragment processing is activated, the maximum possible number of ACLs in the device is reduced.

You activate the processing of Layer 4 fragments globally in the device:

|                             |                                                 |
|-----------------------------|-------------------------------------------------|
| enable                      | Change to the privileged EXEC mode.             |
| configure                   | Change to the Configuration mode.               |
| access-list fragments       | Activate the fragment processing in the device. |
| exit                        | Change to the privileged EXEC mode.             |
| show access-lists global    | Display the global ACL settings of the device.  |
| L4 Fragment Processing..... | Enabled                                         |

## 6.9 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.

## 6.10 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 136 “Configuring SNTP”](#)), ([see on page 147 “Application Example”](#)).

The device is equipped with a buffered hardware clock. This keeps the current time

- ▶ if the power supply fails or
- ▶ if you disconnect the device from the power supply.

Thus the current time is available to you again, e.g. for log entries, when the device is started.

The hardware clock bridges a power supply downtime of 1 hour. The prerequisite is that the power supply of the device has been connected continually for at least 5 minutes beforehand.

**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.

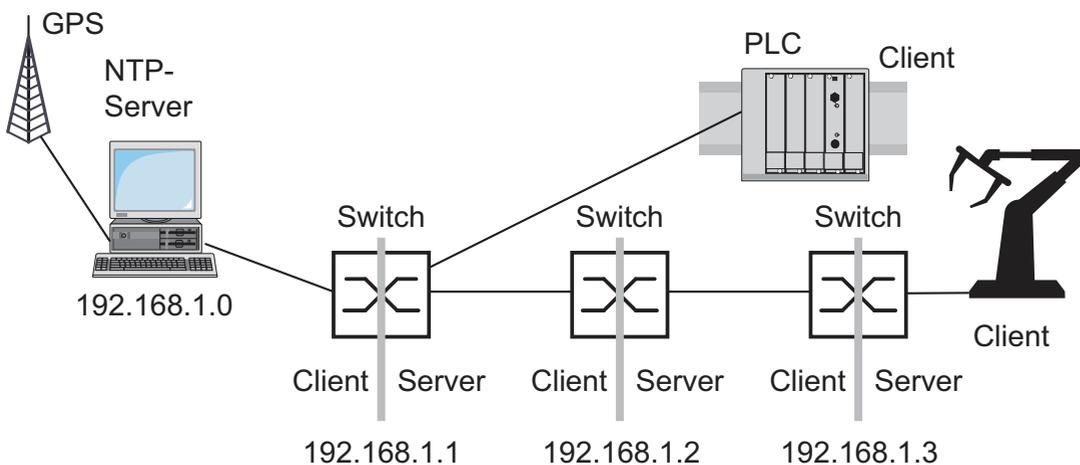


Figure 22: SNTP cascade

## 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.

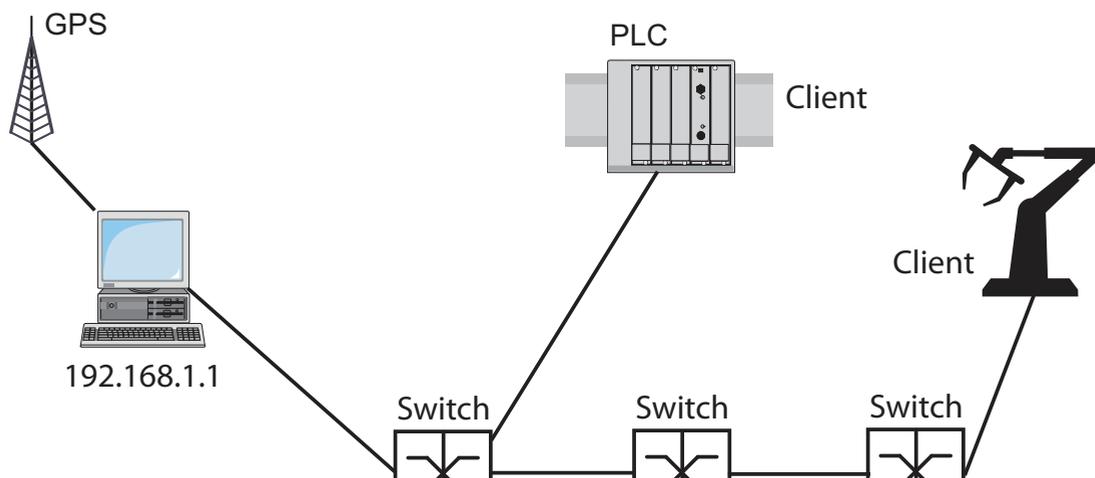


Figure 23: Example of SNTP cascade

- 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 6).
- 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 6: Destination address classes for SNTP and NTP packets

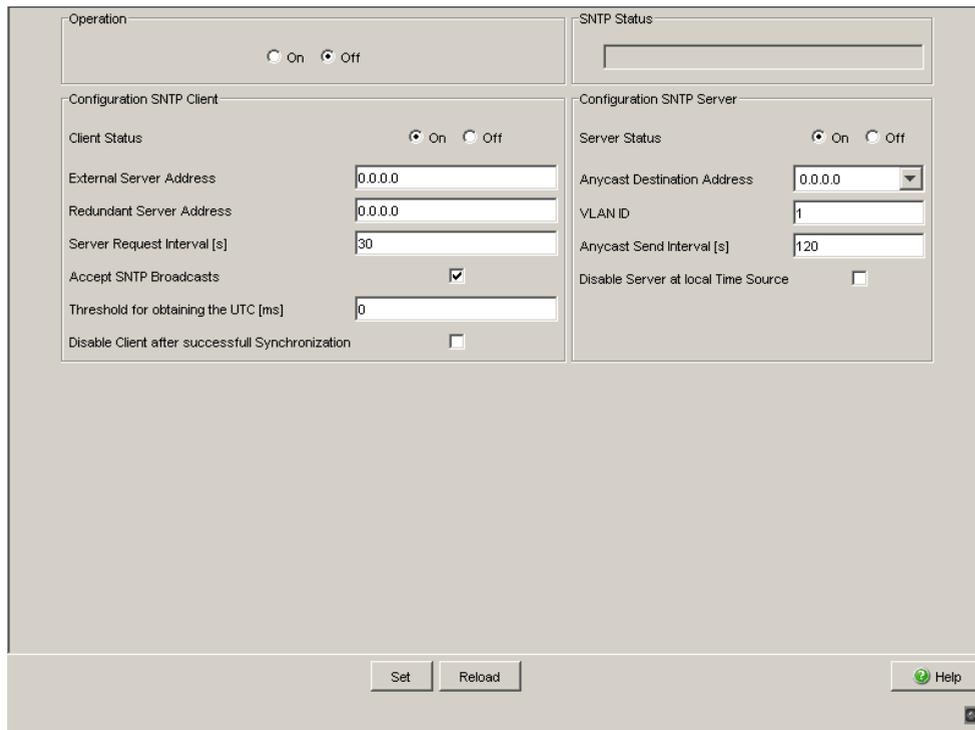


Figure 24: SNTP Dialog

| 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 7: Settings for the example (see figure 23)

## 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.

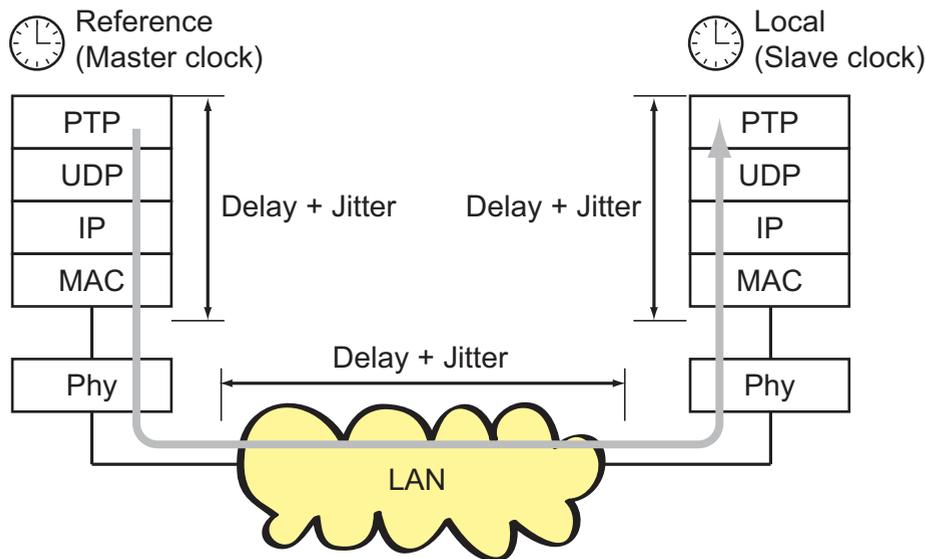
| PTPv1<br>Stratum<br>number | PTPv2<br>Clock class | Specification                                                                                                                                                                                                                                                                                                  |
|----------------------------|----------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 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 8: 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 8: *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 Datagram Protocol (Transport Layer)  
 IP Internet Protocol (Network Layer)  
 MAC Media Access Control  
 Phy Physical Layer

*Figure 25: Delay and jitter for clock synchronization*

To get around the delay and jitter in the protocol stack, IEEE 1588 recommends inserting a special hardware time stamp unit between the MAC and Phy layers.

Devices/modules with the “-RT” suffix in their names are equipped with this time stamp unit and support PTP version 1. Media modules MM23 and MM33 support PTP version 1 and PTP version 2.

The delay and jitter in the LAN increase in the media and transmission devices along the transmission path.

With the introduction of PTP version 2, two procedures are available for the delay measurement:

▶ End-to-End (E2E)

E2E corresponds to the procedure used by PTP version 1. Every slave clock measures only the delay to its master clock.

▶ Peer-to-Peer (P2P)

With P2P, like in E2E, every slave clock measures the delay to its master clock. In addition, in P2P every master clock measures the delay to the slave clock. For example, if a redundant ring is interrupted, the slave clock can become the master clock and the master clock can become the slave clock. This switch in the synchronization direction takes place without any loss of precision, as with P2P the delay in the other direction is already known.

The cable delays are relatively constant. Changes occur very slowly. IEEE 1588 takes this fact into account by regularly making measurements and calculations.

IEEE 1588 eliminates the inaccuracy caused by delays and jitter by defining boundary clocks. Boundary clocks are clocks integrated into devices. These clocks are synchronized on the one side of the signal path, and on the other side of the signal path they are used to synchronize the subsequent clocks (ordinary clocks).

PTP version 2 also defines what are known as transparent clocks. A transparent clock cannot itself be a reference clock, nor can it synchronize itself with a reference clock. However, it corrects the PTP messages it transmits by its own delay time and thus removes the jitter caused by the transmission. When cascading multiple clocks in particular, you can use transparent clocks to achieve greater time precision for the connected terminal devices than with boundary clocks

The Power Profile TLV Check is available on Mice, PowerMICE, MACH1040, MACH104 devices. When enabled this function checks for the presents of Power TLVs. Use the following worksteps to enable the device to check for announce messages containing Power Profile TLVs and use the TLVs for syntonization:

- Open the `Time:PTP:Version 2(TC):Global` dialog.
- Select the "Power TLV Check" checkbox
- Select the "Syntonize" checkbox

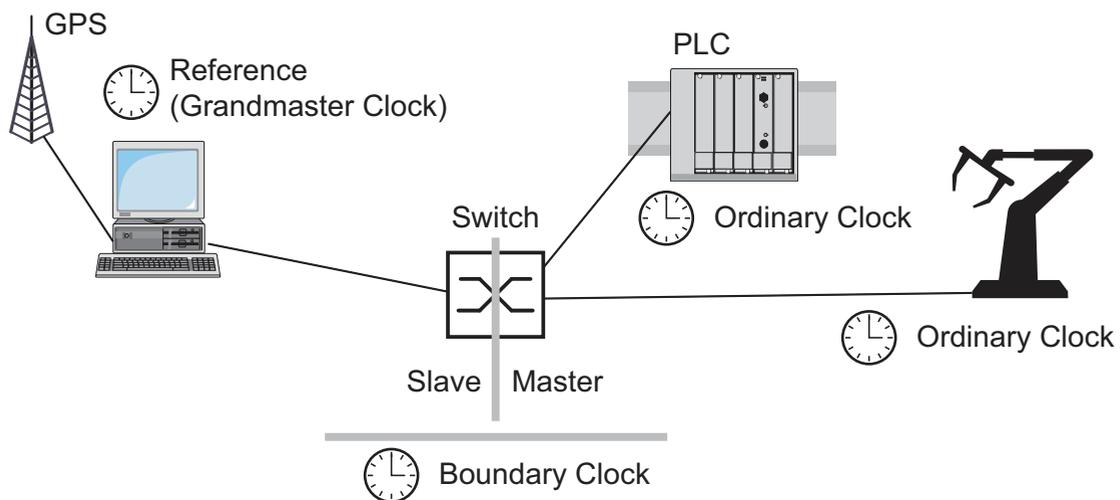


Figure 26: Position of the boundary clock in a network

Irrespective of the physical communication paths, the PTP allocates logical communication paths which you define by setting up PTP subdomains. The purpose of subdomains is to form groups of clocks which are chronologically independent from the other domains. The clocks in one group typically use the same communication paths as other clocks.

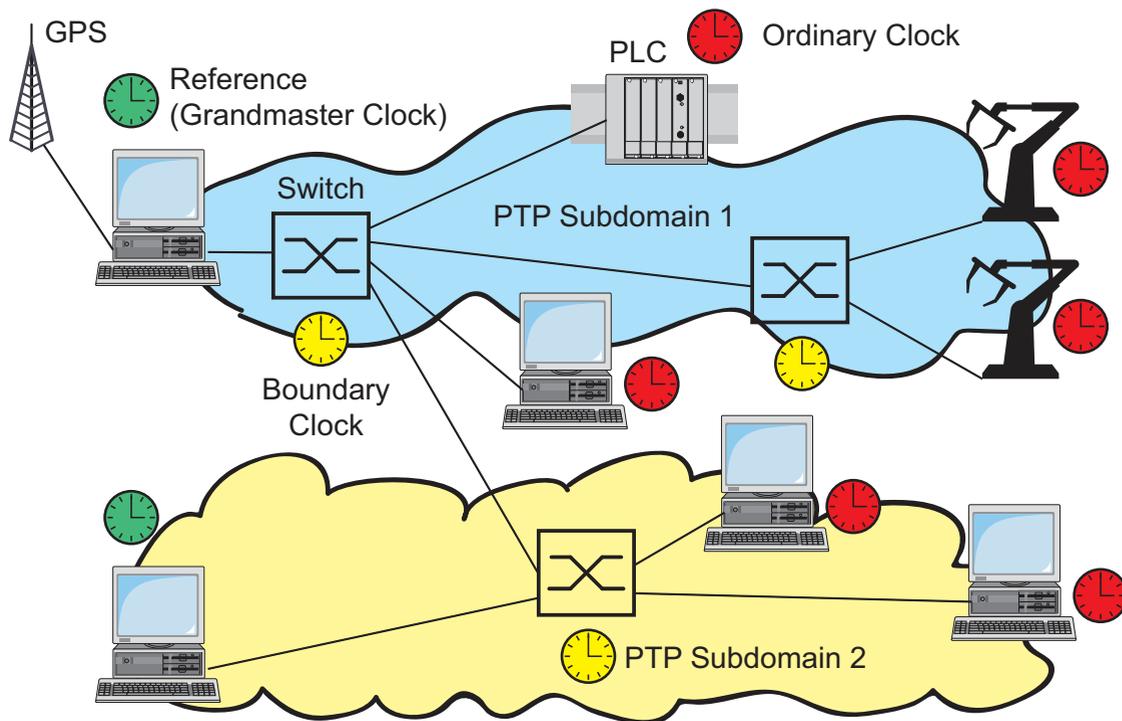


Figure 27: PTP subdomains

### 7.3.2 Preparing the PTP Configuration

After the function is activated, the PTP takes over the configuration automatically.

- To gain an overview of the distribution of clocks, draw a network plan with the devices involved in PTP.

**Note:** Connect all the connections you need to distribute the PTP information to connections with an integrated time stamp unit (RT modules). Devices without a time stamp unit take the information from the PTP and use it to set their clocks. They are not involved in the protocol.

- Enable the PTP function on devices whose time you want to synchronize using PTP.
- Select the PTP version and the PTP mode. Select the same PTP version for all the devices that you want to synchronize.

| PTP mode                  | Application                                                                                                                                                                 |
|---------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| v1-simple-mode            | Support for PTPv1 without special hardware. The device synchronizes itself with received PTPv1 messages. Select this mode for devices without a timestamp unit (RT module). |
| v1-boundary-clock         | Boundary Clock function based on IEEE 1588-2002 (PTPv1).                                                                                                                    |
| v2-boundary-clock-onestep | Boundary Clock function based on IEEE 1588-2008 (PTPv2) for devices with MM23 and MM33 media modules. The one-step mode determines the precise PTP time with one message.   |
| v2-boundary-clock-twostep | Boundary Clock function based on IEEE 1588-2008 (PTPv2) for devices with RT modules. The two-step mode determines the precise PTP time with two messages.                   |

*Table 9: Selecting a PTP mode*

---

| PTP mode             | Application                                                                                                                                                                 |
|----------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| v2-simple-mode       | Support for PTPv2 without special hardware. The device synchronizes itself with received PTPv2 messages. Select this mode for devices without a timestamp unit (RT module). |
| v2-transparent-clock | Transparent Clock (one-step) function based on IEEE 1588-2008 (PTPv2) for devices with MM23 and MM33 media modules.                                                         |

*Table 9: Selecting a PTP mode*

- If no reference clock is available, you specify a device as the reference clock and set its system time as accurately as possible.

### 7.3.3 Application Example

PTP is used to synchronize the time in the network. As an SNTP client, the left device (see figure 28) gets the time from the NTP server via SNTP. The device assigns PTP clock stratum 2 (PTPv1) or clock class 6 (PTPv2) to the time received from an NTP server. Thus the left device becomes the reference clock for the PTP synchronization and is the “preferred master”. The “preferred master” forwards the exact time signal via its connections to the RT module. The device with the RT module receives the exact time signal at a connection of its RT module and thus has the clock mode “v1-boundary-clock”. The devices without an RT module have the clock mode “v1-simple-mode”.

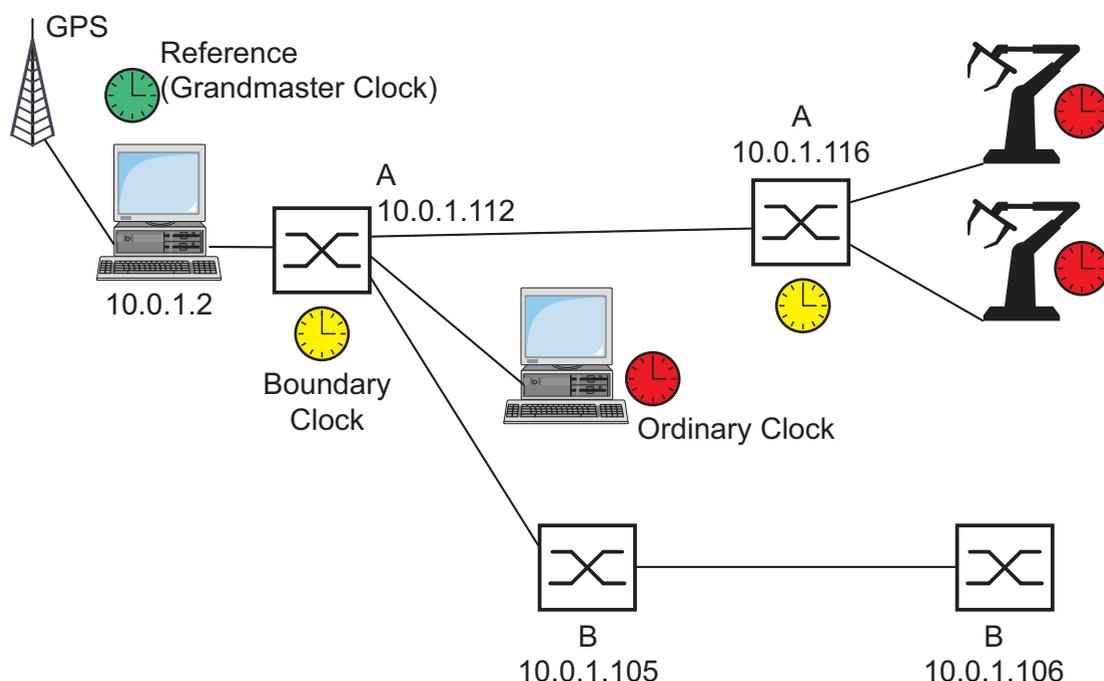


Figure 28: Example of PTP synchronization

A: Device with RT module

B: Device without RT module:

| Device                      | 10.0.1.112        | 10.0.1.116        | 10.0.1.105     | 10.0.1.106     |
|-----------------------------|-------------------|-------------------|----------------|----------------|
| <b>PTP Global</b>           |                   |                   |                |                |
| Operation                   | on                | on                | on             | on             |
| Clock Mode                  | v1-boundary-clock | v1-boundary-clock | v1-simple-mode | v1-simple-mode |
| Preferred Master            | true              | false             | false          | false          |
| <b>SNTP</b>                 |                   |                   |                |                |
| Operation                   | on                | off               | off            | off            |
| Client Status               | on                | off               | off            | off            |
| External server address     | 10.0.1.2          | 0.0.0.0           | 0.0.0.0        | 0.0.0.0        |
| Server request interval     | 30                | any               | any            | any            |
| Accept SNTP Broadcasts      | No                | any               | any            | any            |
| Server status               | on                | off               | off            | off            |
| Anycast destination address | 0.0.0.0           | 0.0.0.0           | 0.0.0.0        | 0.0.0.0        |
| VLAN ID                     | 1                 | 1                 | 1              | 1              |

Table 10: Settings for the example (see figure 28)

The following configuration steps apply to the device with the IP address 10.0.1.112. Configure the other devices in the same way with the values from the table above.

Enter the SNTP parameters.

- Select the `Time:SNTP` dialog.
- Activate SNTP globally in the “Operation” frame.
- Activate the SNTP client (client status) in the “Configuration SNTP Client” frame.
- In the “Configuration SNTP Client” frame, enter:
  - “External server address”: 10.0.1.2
  - “Request interval”: 30
  - “Accept SNTP Broadcasts”: No

- Activate the SNTP server (server status) in the “Configuration SNTP Server” frame.
- In the “Configuration SNTP Server” frame, enter:
  - “Anycast destination address”: 0.0.0.0
  - “VLAN ID”: 1
- Click "Set" to save the changes temporarily.

|                                        |                                                                     |
|----------------------------------------|---------------------------------------------------------------------|
| enable                                 | Change to the privileged EXEC mode.                                 |
| configure                              | Change to the Configuration mode.                                   |
| sntp operation on                      | Switch on SNTP globally.                                            |
| sntp operation client on               | Switch on SNTP client.                                              |
| sntp client server primary<br>10.0.1.2 | Enter the IP address of the external SNTP server<br>10.0.1.2.       |
| sntp client request-interval<br>30     | Enter the value 30 seconds for the SNTP server<br>request interval. |
| sntp client accept-broadcast<br>off    | Deactivate “Accept SNTP Broadcasts”.                                |
| sntp operation server on               | Switch on SNTP server.                                              |
| sntp anycast address 0.0.0.0           | Enter the SNTP server Anycast destination<br>address 0.0.0.0.       |
| sntp anycast vlan 1                    | Enter the SNTP server VLAN ID 1.                                    |

- Enter the global PTP parameters.

- Select the `Time:PTP:Global` dialog.
- Activate the function in the “Operation IEEE 1588 / PTP” frame.
- Select `v1-boundary-clock` for “PTP version mode”.
- Click "Set" to save the changes temporarily.

|                                      |                                    |
|--------------------------------------|------------------------------------|
| ptp operation enable                 | Switch on PTP globally.            |
| ptp clock-mode v1-boundary-<br>clock | Select PTP version and clock mode. |

- In this example, you have chosen the device with the IP address 10.0.1.112 as the PTP reference clock. You thus define this device as the “Preferred Master”.

- Select the `Time:PTP:Version1:Global` dialog.
- In the “Operation IEEE 1588 / PTP” frame, select `true` for the “Preferred Master”.
- Click "Set" to save the changes temporarily.

```
ptp v1 preferred-master true
```

 Define this device as the “Preferred Master”.

- Get PTP to apply the parameters.

- In the `Time:PTP:Version1:Global` dialog, click on “Reinitialize” so that PTP applies the parameters entered.

```
ptp v1 re-initialize
```

 Apply PTP parameters.

- Save the settings in the non-volatile memory.

- 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.

```
copy system:running-config
nvram:startup-config
```

Save the current configuration to the non-volatile memory.

## 7.4 Interaction of PTP and SNTP

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

**Note:** Configure the devices so that each device only receives the time from one source.

If the device gets its time via PTP, you enter the “External server address” 0.0.0.0 in the SNTP client configuration and do not accept SNTP Broadcasts. If the device gets its time via SNTP, make sure that the “best” clock is connected to the SNTP server. Then both protocols will get the time from the same server. The example (see figure 29) shows such an application.

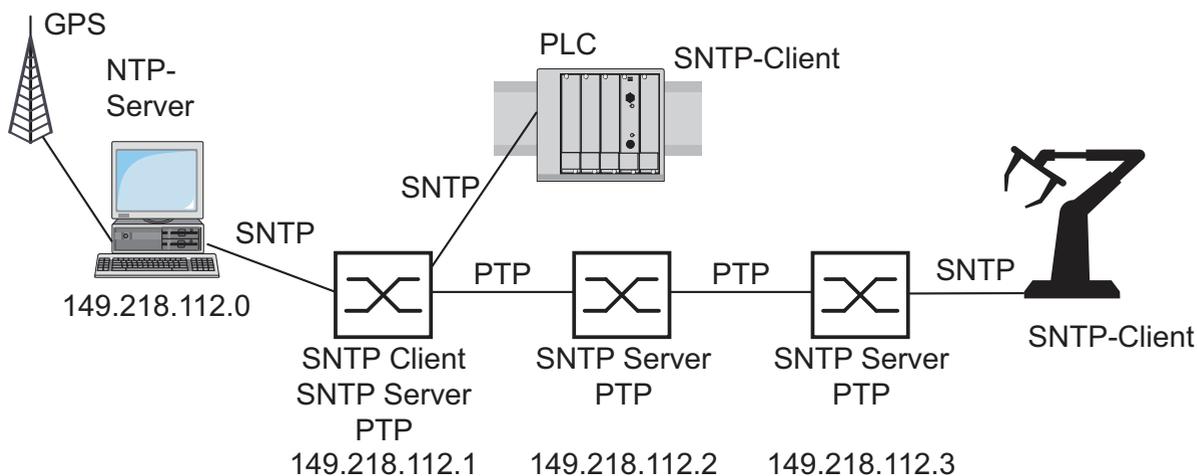


Figure 29: Example of the coexistence of PTP and SNTP

### ■ Application Example

The requirements with regard to the accuracy of the time in the network are quite high, but the terminal devices only support SNTP (see figure 29).

| Device                      | 149.218.112.1     | 149.218.112.2     | 149.218.112.3     |
|-----------------------------|-------------------|-------------------|-------------------|
| PTP                         |                   |                   |                   |
| Operation                   | on                | on                | on                |
| Clock Mode                  | v1-boundary-clock | v1-boundary-clock | v1-boundary-clock |
| Preferred Master            | false             | false             | false             |
| SNTP                        |                   |                   |                   |
| Operation                   | on                | on                | on                |
| Client Status               | on                | off               | off               |
| External server address     | 149.218.112.0     | 0.0.0.0           | 0.0.0.0           |
| Server request interval     | any               | any               | any               |
| Accept SNTP Broadcasts      | No                | No                | No                |
| Server status               | on                | on                | on                |
| Anycast destination address | 224.0.1.1         | 224.0.1.1         | 224.0.1.1         |
| VLAN ID                     | 1                 | 1                 | 1                 |
| Anycast send interval       | 30                | 30                | 30                |

*Table 11: Settings for the example*

In the example, the left device, as an SNTP client, gets the time from the NTP server via SNTP. The device assigns PTP clock stratum 2 (PTPv1) or clock class 6 (PTPv2) to the time received from an NTP server. Thus the left device becomes the reference clock for the PTP synchronization. PTP is active for all 3 devices, thus enabling precise time synchronization between them. As the connectable terminal devices in the example only support SNTP, all 3 devices act as SNTP servers.



## 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 158 “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 156 “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 67 "Saving settings")
- ▶ `invalid`: With this status you delete a manually created filter.
- ▶ `gmrp`: The filter was created by GMRP.
- ▶ `gmrp/permanent`: GMRP added further port markings to the filter after it was created by the administrator. The port markings added by the GMRP are deleted by a restart.
- ▶ `igmp`: The filter was created by IGMP 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.

To prevent all the video data from slowing down the entire network, the device uses the GMRP to distribute the Multicast address information. As a result, the image data with a Multicast address is only distributed to those ports that are connected to the associated monitors for surveillance.

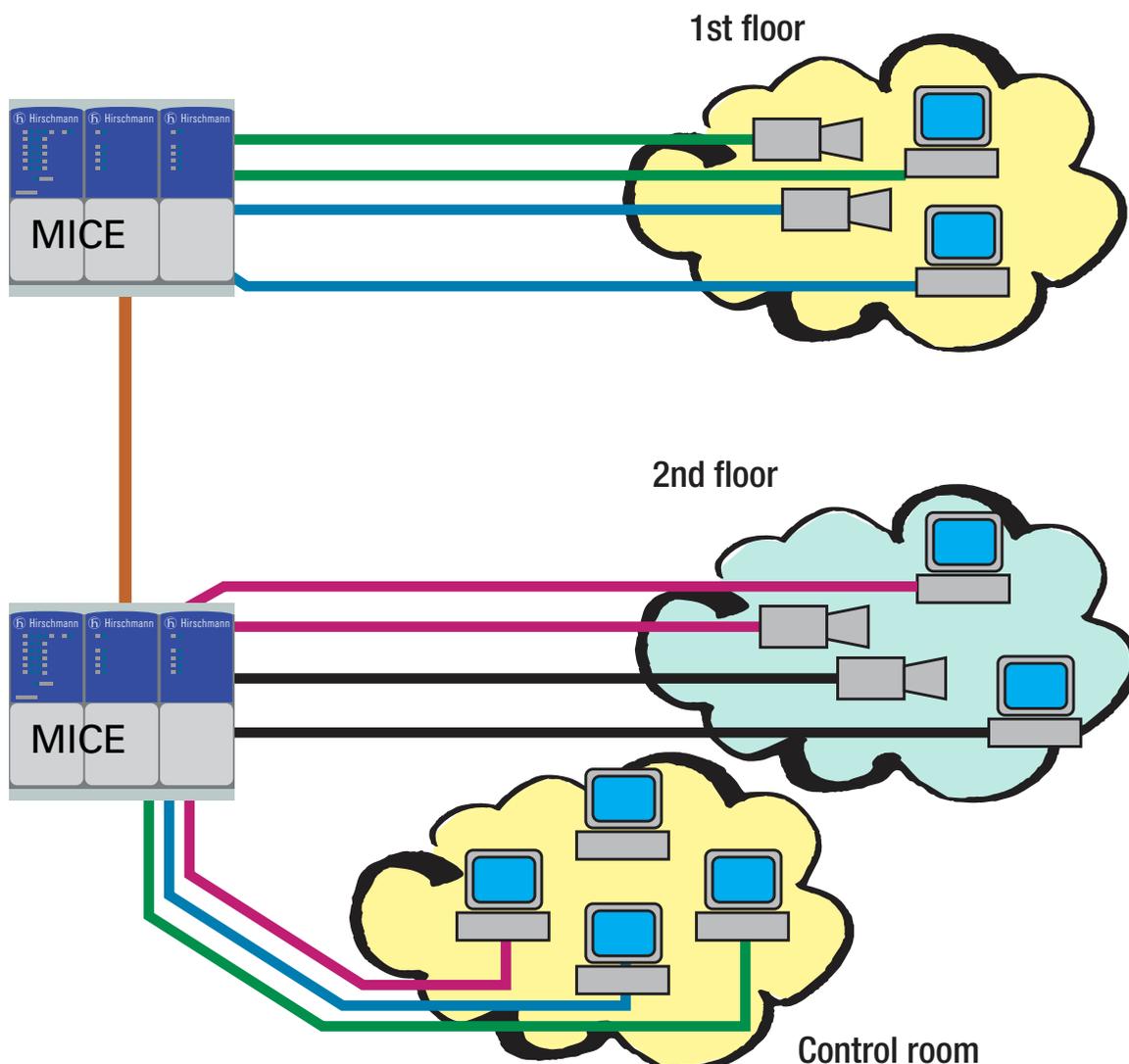


Figure 30: Example: Video surveillance in machine rooms

### 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 165 “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 165 “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 165 “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 12: 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.

| 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 31: IGMP Snooping dialog

### 8.2.5 Description of GMRP

The GARP Multicast Registration Protocol (GMRP) describes the distribution of data packets with a multicast address as the destination address on Layer 2.

Devices that want to receive data packets with a multicast address as the destination address use the GMRP to perform the registration of the multicast address. For a switch, registration involves entering the multicast addresses in the filter table. When you enter a multicast address in the filter table, the switch sends this information in a GMRP packet to the ports. As a result, the connected switches forward the multicast address entered in the filter table to this switch. The GMRP sends packets with a Multicast address in the destination address field to the ports entered.

The feature is available on MS, RS, MACH102, MACH1020/30, Octopus, RSR and MACH1040, MACH104 devices. Depending on the configuration, the switch either discards unknown multicast addresses, or sends the data packets with unknown multicast addresses to the ports.

Default setting: "Off".

## 8.2.6 Setting GMRP

- Select the `Switching:Multicasts:GMRP` dialog.

### ■ Operation

The "Operation" frame allows you to enable GMRP globally for the entire device.

If GMRP is disabled, then

- ▶ the device does not generate any GMRP packets,
- ▶ does not evaluate any GMRP packets received, and
- ▶ sends (floods) received data packets to all ports.

The device is transparent for received GMRP packets, regardless of the GMRP setting.

### ■ Multicasts

The "Multicasts" frame allows you to configure GMRP to discard multicasts addresses or send them to the ports.

Enable GMRP, then:

- ▶ when you select "Discard", the device deletes unknown multicasts
- ▶ when you select "Send To All Ports", the device evaluates the GMRP packets received, and sends (floods) received data packets to the ports.

## ■ Settings per Port (Table)

- ▶ „GMRP”  
This table column enables you to enable/disable the GMRP for each port when the GMRP is enabled globally. When you switch off the GMRP at a port, no registrations can be made for this port, and GMRP packets cannot be forwarded at this port.
- ▶ “GMRP Service Requirement”  
Devices that do not support GMRP can be integrated into the Multicast addressing by means of
  - ▶ a static filter address entry on the connecting port.
  - ▶ selecting “Forward all groups” in the table column “GMRP Service Requirement”.  
The device enters ports with the selection “Forward all groups” in all Multicast filter entries learned via GMRP.

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

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

Operation:  On  Off

Multicasts: Unknown Multicasts  Discard  Send To All Ports

| Port | GMRP                                | GMRP Service Requirement        |
|------|-------------------------------------|---------------------------------|
| 1.1  | <input checked="" type="checkbox"/> | Forward all unregistered groups |
| 1.2  | <input checked="" type="checkbox"/> | Forward all unregistered groups |
| 1.3  | <input checked="" type="checkbox"/> | Forward all unregistered groups |
| 1.4  | <input checked="" type="checkbox"/> | Forward all unregistered groups |
| 1.5  | <input checked="" type="checkbox"/> | Forward all unregistered groups |
| 1.6  | <input checked="" type="checkbox"/> | Forward all unregistered groups |
| 1.7  | <input checked="" type="checkbox"/> | Forward all unregistered groups |
| 1.8  | <input checked="" type="checkbox"/> | Forward all unregistered groups |
| 1.9  | <input checked="" type="checkbox"/> | Forward all unregistered groups |
| 1.10 | <input checked="" type="checkbox"/> | Forward all unregistered groups |
| 1.11 | <input checked="" type="checkbox"/> | Forward all unregistered groups |
| 1.12 | <input checked="" type="checkbox"/> | Forward all unregistered groups |
| 1.13 | <input checked="" type="checkbox"/> | Forward all unregistered groups |
| 1.14 | <input checked="" type="checkbox"/> | Forward all unregistered groups |
| 1.15 | <input checked="" type="checkbox"/> | Forward all unregistered groups |
| 1.16 | <input checked="" type="checkbox"/> | Forward all unregistered groups |

Buttons: Set, Reload, Help

Figure 32: Multicasts 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 ingress limiter function for all ports and to select the ingress limitation on all ports (either broadcast packets only or broadcast packets and Multicast packets).
- ▶ "Egress Limiter (Pkt/s)" allows you to enable or disable the egress limiter function for broadcasts on all ports.

Setting options per port:

- ▶ Ingress Limiter Rate for the packet type selected in the Ingress Limiter frame:
  - ▶ = 0, no ingress limit at this port.
  - ▶ > 0, maximum ingress traffic rate in kbit/s that can be sent at this port.
- ▶ Egress Limiter Rate for broadcast packets:
  - ▶ = 0, no rate limit for egress broadcast packets at this port.
  - ▶ > 0, maximum number of egress broadcasts per second sent at this port.

| Module | Port | Ingress Limiter Rate (kbit/s) | Egress Limit (Pkt/s) Packet Type: BC |
|--------|------|-------------------------------|--------------------------------------|
| 1      | 1    | 0                             | 0                                    |
| 1      | 2    | 0                             | 0                                    |
| 1      | 3    | 0                             | 0                                    |
| 1      | 4    | 0                             | 0                                    |
| 2      | 1    | 0                             | 0                                    |
| 2      | 2    | 0                             | 0                                    |
| 2      | 3    | 0                             | 0                                    |
| 2      | 4    | 0                             | 0                                    |
| 3      | 1    | 0                             | 0                                    |
| 3      | 2    | 0                             | 0                                    |

Figure 33: Rate Limiter dialog

---

## 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 8 priority queues (IEEE 802.1D standard traffic classes). Received data packets are assigned to these classes by

- ▶ Access Control Lists, MAC- or IP-based ACLs ([see on page 116 “Access Control Lists \(ACL\)”](#)).
- ▶ 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 87 “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. This means that the Access-Control Lists always take priority over the following mechanisms. AccessControl Lists can classify the data packets relative to Layer 2, Layer 3 and Layer 4 (e.g. MAC addresses, IP addresses, protocols, TCP/UDP ports).

Data packets can contain prioritizing/QoS information:

- ▶ VLAN priority based on IEEE 802.1Q/ 802.1D (Layer 2)
- ▶ Type of Service (ToS) or DiffServ (DSCP) for IP packets (Layer 3)

## 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                | 2                               | Best effort (default)                                   |
| 1                | 0                               | Background                                              |
| 2                | 1                               | Standard                                                |
| 3                | 3                               | Excellent effort (business critical)                    |
| 4                | 4                               | Controlled load<br>(streaming multimedia)               |
| 5                | 5                               | Video, less than 100 milliseconds of latency and jitter |
| 6                | 6                               | Voice, less than 10 milliseconds of latency and jitter  |
| 7                | 7                               | Network control reserved traffic                        |

*Table 13: Assignment of the priority entered in the tag to the traffic classes*

**Note:** Network protocols and redundancy mechanisms use the highest traffic class 7. Therefore, select other traffic classes for application data.

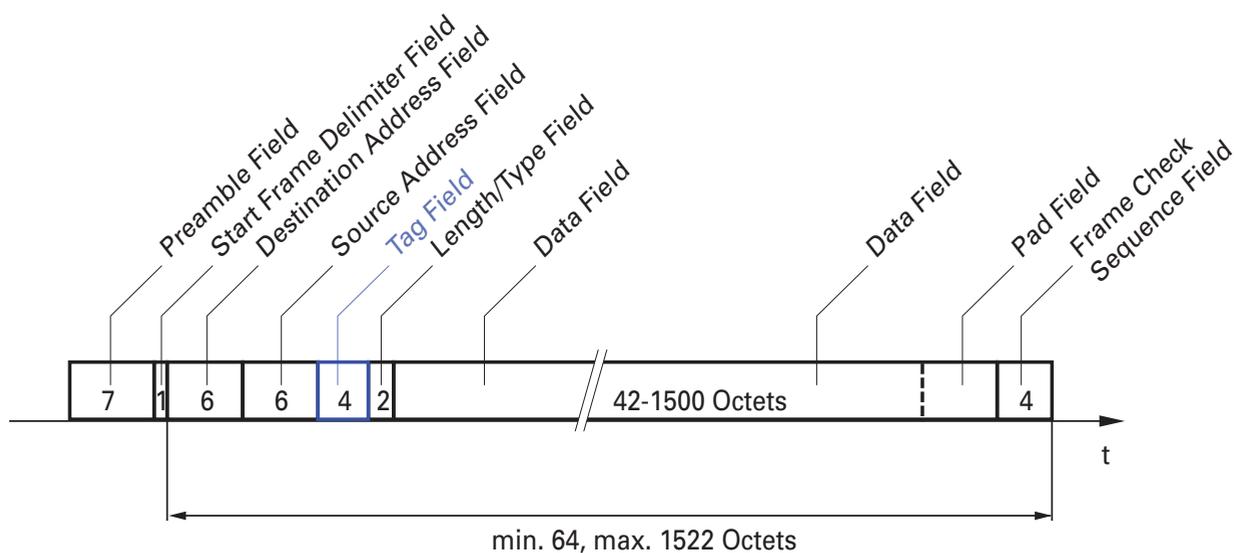


Figure 34: Ethernet data packet with tag

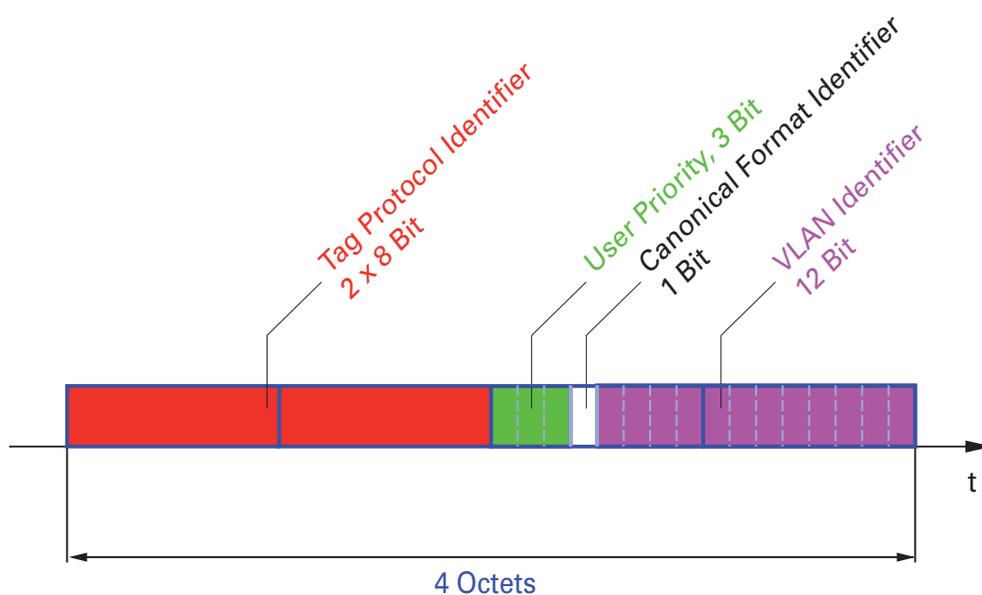


Figure 35: Tag format

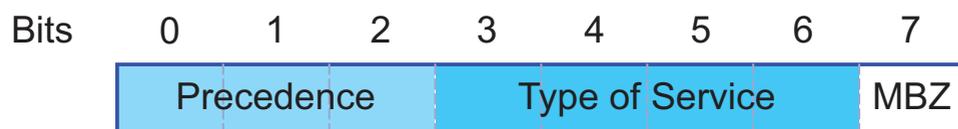
When using VLAN prioritizing, note the following special features:

- ▶ 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 14) 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 14: 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 14: ToS field in the IP header

## ■ Differentiated Services

The Differentiated Services field in the IP header (see figure 36) 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.

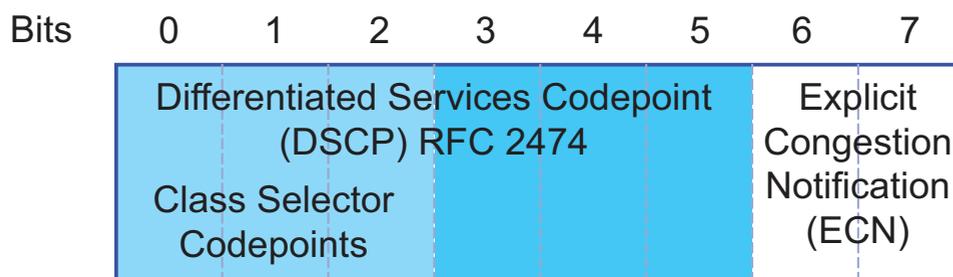


Figure 36: Differentiated Services field in the IP header

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)  |
| Immidiate            | 010              | CS2 (010000)  |
| Priority             | 001              | CS1 (001000)  |
| Routine              | 000              | CS0 (000000)  |

Table 15: Assigning the IP precedence values to the DSCP value

| DSCP value        | DSCP name        | Traffic Class (default setting) |
|-------------------|------------------|---------------------------------|
| 0                 | Best Effort /CS0 | 2                               |
| 1-7               |                  | 2                               |
| 8                 | CS1              | 0                               |
| 9,11,13,15        |                  | 0                               |
| 10,12,14          | AF11,AF12,AF13   | 0                               |
| 16                | CS2              | 1                               |
| 17,19,21,23       |                  | 1                               |
| 18,20,22          | AF21,AF22,AF23   | 1                               |
| 24                | CS3              | 3                               |
| 25,27,29,31       |                  | 3                               |
| 26,28,30          | AF31,AF32,AF33   | 3                               |
| 32                | CS4              | 4                               |
| 33,35,37,39       |                  | 4                               |
| 34,36,38          | AF41,AF42,AF43   | 4                               |
| 40                | CS5              | 5                               |
| 41,42,43,44,45,47 |                  | 5                               |
| 46                | EF               | 5                               |
| 48                | CS6              | 6                               |
| 49-55             |                  | 6                               |
| 56                | CS7              | 7                               |
| 57-63             |                  | 7                               |

Table 16: Mapping the DSCP values onto the traffic classes

### 8.4.4 Management prioritization

To have full access to the management of the device, even in situations of high network load, the device enables you to prioritize management packets. In prioritizing management packets (SNMP, SSH, etc.), the device sends the management packets with priority information.

- ▶ On Layer 2 the device modifies the VLAN priority in the VLAN tag. For this function to be useful, the configuration of the corresponding ports must permit the sending of packets with a VLAN tag.
- ▶ On Layer 3 the device modifies the IP-DSCP value.

### 8.4.5 Handling of Received Priority Information

The device offers the following options for evaluating this priority information:

- ▶ `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 176 “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 16](#)). You can modify this assignment.  
The device prioritizes non-IP packets according to the port priority.

## 8.4.6 Handling of traffic classes

For the handling of traffic classes, the device provides:

- ▶ Strict Priority
- ▶ Weighted Fair Queuing
- ▶ Strict Priority combined with Weighted Fair Queuing

Default setting: 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 applications that are time- or latency-critical, such as VoIP or video, Strict Priority enables high-priority data to be sent immediately([see on page 183 “Maximum bandwidth”](#)).

### ■ Description of Weighted Fair Queuing

With Waited Fair Queuing, also called WeightedRoundRobin (WRR), the user assigns a minimum or reserved bandwidth to each traffic class. This ensures that data packets with a lower priority are also sent when the network is very busy.

The weighting values range from 0% to 100% of the available bandwidth, in steps of 5%.

- ▶ A weighting of 0 is equivalent to a "no bandwidth" setting.
- ▶ The sum of the individual bandwidths may add up to 100%.

If you assign Weighted Fair Queuing to every traffic class, the entire bandwidth for the corresponding port is available to you.

When you combine Weighted Fair Queuing with Strict Priority, make sure that the highest traffic class of Weighted Fair Queuing is smaller than the lowest traffic class of Strict Priority.

In this case, a high Strict Priority network load can significantly reduce the bandwidth available for Weighted Fair Queuing.

### ■ **Maximum bandwidth**

By entering a maximum bandwidth you can limit the bandwidth for each traffic class to a maximum value, regardless of whether you selected “Weighted Fair Queuing” or “Strict Priority”.

- ▶ Weighted Fair Queuing (see on page 182 “Description of Weighted Fair Queuing”) requires that the maximum bandwidth is at least as big as the minimum bandwidth.
- ▶ With “Strict Priority”, individual high-priority packets with low latency are processed (see on page 182 “Description of Strict Priority”). If the maximum bandwidth is configured to a value less than 100%, even data packets with lower traffic classes can be sent in periods of high-priority overloading.  
The weighting values range from 0% to 100% of the available bandwidth, in steps of 5%.

### ■ **Description of Traffic Shaping**

With Traffic Shaping you have the option of restricting the maximum bandwidth of an interface.

The values for the bandwidth restriction range from 0% to 95%, in steps of 5%.

- ▶ The value "0" is equivalent to a "no bandwidth restriction" setting.
- ▶ The value "95" means that 95% of the bandwidth is available.

If the bandwidth set is temporarily exceeded, the device saves the data and sends it when the bandwidth load has decreased again. Traffic Shaping thus smooths out any overload situations.

If Traffic Shaping is active on an interface, the device ignores the bandwidths reserved for Weighted Fair Queuing.

## 8.4.7 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 device uses to assign a traffic class to received data packets (see on page 175 “Description of Prioritization”).

**Note:** If you have set up VLANs, pay attention to the “VLAN 0 Transparent mode” (see `Switching:VLAN:Global`)

|                              |                                                              |
|------------------------------|--------------------------------------------------------------|
| <code>enable</code>          | Switch to the privileged EXEC mode.                          |
| <code>configure</code>       | Switch to the Configuration mode.                            |
| <code>interface 1/1</code>   | Switch to the Interface Configuration mode of interface 1/1. |
| <code>vlan priority 3</code> | Assigns port priority 3 to interface 1/1.                    |
| <code>exit</code>            | 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.

|                                                |                                                 |
|------------------------------------------------|-------------------------------------------------|
| <code>enable</code>                            | Switch to the privileged EXEC mode.             |
| <code>configure</code>                         | Switch to the Configuration mode.               |
| <code>classofservice dot1p-mapping 0 2</code>  | Assign traffic class 2 to VLAN priority 0.      |
| <code>classofservice dot1p-mapping 1 2</code>  | Also assign traffic class 2 to VLAN priority 1. |
| <code>exit</code>                              | Switch to the privileged EXEC mode.             |
| <code>show classofservice dot1p-mapping</code> | Display the assignment.                         |

| User Priority | Traffic Class |
|---------------|---------------|
| -----         | -----         |
| 0             | 2             |
| 1             | 2             |
| 2             | 0             |
| 3             | 1             |
| 4             | 2             |
| 5             | 2             |
| 6             | 3             |
| 7             | 3             |

### ■ Always assign port priority to received data packets (PowerMICE, MACH 104, MACH 1040 and MACH 4000)

|                                        |                                                              |
|----------------------------------------|--------------------------------------------------------------|
| <code>enable</code>                    | Switch to the privileged EXEC mode.                          |
| <code>configure</code>                 | Switch to the Configuration mode.                            |
| <code>interface 1/1</code>             | Switch to the Interface Configuration mode of interface 1/1. |
| <code>no classofservice trust</code>   | Assign the "no trust" mode to the interface.                 |
| <code>  vlan priority 1</code>         | Set the port priority to 1.                                  |
| <code>exit</code>                      | Switch to the Configuration mode.                            |
| <code>exit</code>                      | Switch to the privileged EXEC mode.                          |
| <code>show classofservice trust</code> | Display the trust mode on interface 1/1.                     |
| <code>  1/1</code>                     |                                                              |
| Class of Service Trust Mode: Untrusted |                                                              |
| Untrusted Traffic Class: 4             |                                                              |

### ■ Assigning the traffic class to a DSCP

- Select the QoS/Priority:IP DSCP Mapping dialog.
- In the "Traffic Class" column, enter the desired values.

|                                      |                                     |
|--------------------------------------|-------------------------------------|
| <code>enable</code>                  | Switch to the privileged EXEC mode. |
| <code>configure</code>               | Switch to the Configuration mode.   |
| <code>classofservice</code>          | Assign traffic class 1 to DSCP CS1. |
| <code>  ip-dscp-mapping cs1 1</code> |                                     |

```
show classofservice ip-dscp-mapping
```

| IP DSCP    | Traffic Class |
|------------|---------------|
| 0 (be/cs0) | 2             |
| 1          | 2             |
| .          |               |
| .          |               |
| 8 (cs1)    | 1             |
| .          |               |

### ■ Always assign DSCP priority per interface to received IP data packets (PowerMICE, MACH 104, MACH 1040 and MACH 4000)

|                                      |                                                              |
|--------------------------------------|--------------------------------------------------------------|
| enable                               | Switch to the privileged EXEC mode.                          |
| configure                            | Switch to the Configuration mode.                            |
| interface 6/1                        | Switch to the interface configuration mode of interface 6/1. |
| classofservice trust ip-dscp         | Assign the "trust ip-dscp" mode to the interface.            |
| exit                                 | Switch to the Configuration mode.                            |
| exit                                 | Switch to the privileged EXEC mode.                          |
| show classofservice trust 6/1        | Display the trust mode on interface 6/1.                     |
| Class of Service Trust Mode: IP DSCP |                                                              |
| Non-IP Traffic Class: 2              |                                                              |

### ■ 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                               | Switch to the privileged EXEC mode.       |
| configure                            | Switch to the Configuration mode.         |
| classofservice trust ip-dscp         | Assign the "trust ip-dscp" mode globally. |
| exit                                 | Switch to the Configuration mode.         |
| exit                                 | Switch to the privileged EXEC mode.       |
| show classofservice trust            | Display the trust mode.                   |
| Class of Service Trust Mode: IP DSCP |                                           |

## ■ Configuration of Weighted Fair Queuing and Traffic Shaping

| <pre>enable configure no cos-queue strict 0 1 2 3 4 5  cos-queue min-bandwidth 10 10 15 15 20 30 0 0  cos-queue max-bandwidth 20 20 20 20 20 30 30 30  exit show interfaces cos-queue</pre>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | <p>Switch to the privileged EXEC mode.</p> <p>Switch to the Configuration mode.</p> <p>Switches off Strict Priority for traffic classes 0 to 5 and thus switches on Weighted Fair Queuing. Traffic classes 6 and 7 remain in Strict Priority mode.</p> <p>Assigns the weighting to the Weighted Fair Queuing traffic classes. In the case of Strict Priority, because the device first transmits all the data packets with a high priority, you can enter the weighting 0 for the Strict Priority traffic classes and distribute 100% among the remaining traffic classes. The device distributes the remaining bandwidth in accordance with the percentage weighting.</p> <p>Assign a maximum bandwidth to all traffic classes (Shaping). Because the two Strict Priority traffic classes are limited to a maximum of 30%, the remaining queues have at least 40% of the bandwidth at their disposal. The device immediately sends Strict Priority data up to a maximum bandwidth of 30%.</p> <p>Switch to the privileged EXEC mode.</p> <p>Display the configuration.</p> |                |                |                |                |       |       |       |       |   |    |    |          |   |    |    |          |   |    |    |          |   |    |    |          |   |    |    |          |   |    |    |          |   |   |    |        |   |   |    |        |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------|----------------|----------------|----------------|-------|-------|-------|-------|---|----|----|----------|---|----|----|----------|---|----|----|----------|---|----|----|----------|---|----|----|----------|---|----|----|----------|---|---|----|--------|---|---|----|--------|
| <pre>Global Configuration Interface Shaping Rate..... 0</pre>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |                |                |                |                |       |       |       |       |   |    |    |          |   |    |    |          |   |    |    |          |   |    |    |          |   |    |    |          |   |    |    |          |   |   |    |        |   |   |    |        |
| <table border="0"> <thead> <tr> <th style="text-align: left;">Queue Id</th> <th style="text-align: left;">Min. Bandwidth</th> <th style="text-align: left;">Max. Bandwidth</th> <th style="text-align: left;">Scheduler Type</th> </tr> <tr> <th style="text-align: left;">-----</th> <th style="text-align: left;">-----</th> <th style="text-align: left;">-----</th> <th style="text-align: left;">-----</th> </tr> </thead> <tbody> <tr> <td>0</td> <td>10</td> <td>20</td> <td>Weighted</td> </tr> <tr> <td>1</td> <td>10</td> <td>20</td> <td>Weighted</td> </tr> <tr> <td>2</td> <td>15</td> <td>20</td> <td>Weighted</td> </tr> <tr> <td>3</td> <td>15</td> <td>20</td> <td>Weighted</td> </tr> <tr> <td>4</td> <td>20</td> <td>20</td> <td>Weighted</td> </tr> <tr> <td>5</td> <td>30</td> <td>30</td> <td>Weighted</td> </tr> <tr> <td>6</td> <td>0</td> <td>30</td> <td>Strict</td> </tr> <tr> <td>7</td> <td>0</td> <td>30</td> <td>Strict</td> </tr> </tbody> </table> |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | Queue Id       | Min. Bandwidth | Max. Bandwidth | Scheduler Type | ----- | ----- | ----- | ----- | 0 | 10 | 20 | Weighted | 1 | 10 | 20 | Weighted | 2 | 15 | 20 | Weighted | 3 | 15 | 20 | Weighted | 4 | 20 | 20 | Weighted | 5 | 30 | 30 | Weighted | 6 | 0 | 30 | Strict | 7 | 0 | 30 | Strict |
| Queue Id                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | Min. Bandwidth                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | Max. Bandwidth | Scheduler Type |                |                |       |       |       |       |   |    |    |          |   |    |    |          |   |    |    |          |   |    |    |          |   |    |    |          |   |    |    |          |   |   |    |        |   |   |    |        |
| -----                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | -----                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | -----          | -----          |                |                |       |       |       |       |   |    |    |          |   |    |    |          |   |    |    |          |   |    |    |          |   |    |    |          |   |    |    |          |   |   |    |        |   |   |    |        |
| 0                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | 10                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | 20             | Weighted       |                |                |       |       |       |       |   |    |    |          |   |    |    |          |   |    |    |          |   |    |    |          |   |    |    |          |   |    |    |          |   |   |    |        |   |   |    |        |
| 1                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | 10                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | 20             | Weighted       |                |                |       |       |       |       |   |    |    |          |   |    |    |          |   |    |    |          |   |    |    |          |   |    |    |          |   |    |    |          |   |   |    |        |   |   |    |        |
| 2                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | 15                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | 20             | Weighted       |                |                |       |       |       |       |   |    |    |          |   |    |    |          |   |    |    |          |   |    |    |          |   |    |    |          |   |    |    |          |   |   |    |        |   |   |    |        |
| 3                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | 15                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | 20             | Weighted       |                |                |       |       |       |       |   |    |    |          |   |    |    |          |   |    |    |          |   |    |    |          |   |    |    |          |   |    |    |          |   |   |    |        |   |   |    |        |
| 4                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | 20                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | 20             | Weighted       |                |                |       |       |       |       |   |    |    |          |   |    |    |          |   |    |    |          |   |    |    |          |   |    |    |          |   |    |    |          |   |   |    |        |   |   |    |        |
| 5                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | 30                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | 30             | Weighted       |                |                |       |       |       |       |   |    |    |          |   |    |    |          |   |    |    |          |   |    |    |          |   |    |    |          |   |    |    |          |   |   |    |        |   |   |    |        |
| 6                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | 0                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | 30             | Strict         |                |                |       |       |       |       |   |    |    |          |   |    |    |          |   |    |    |          |   |    |    |          |   |    |    |          |   |    |    |          |   |   |    |        |   |   |    |        |
| 7                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | 0                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | 30             | Strict         |                |                |       |       |       |       |   |    |    |          |   |    |    |          |   |    |    |          |   |    |    |          |   |    |    |          |   |    |    |          |   |   |    |        |   |   |    |        |

## ■ Configuring Traffic Shaping on a port

|                                           |                                                                                                                                                     |
|-------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------|
| <pre>enable configure interface 1/2</pre> | <p>Switch to the privileged EXEC mode.</p> <p>Switch to the Configuration mode.</p> <p>Switch to the interface configuration mode for port 1.2.</p> |
|-------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------|

```

traffic-shape 50 Restricts the maximum bandwidth of
 interface 1/2 to 50%.
exit Switch to the Configuration mode.
exit Switch to the privileged EXEC mode.
show interfaces cos-queue Display the configuration of interface 1/2.
 1/2

Interface..... 1/2
Interface Shaping Rate..... 50

Queue Id Min. Bandwidth Max. Bandwidth Scheduler Type

0 10 20 Weighted
1 10 20 Weighted
2 15 20 Weighted
3 15 20 Weighted
4 20 20 Weighted
5 30 30 Weighted
6 0 30 Strict
7 0 30 Strict

enable Switch to the privileged EXEC mode.
configure Switch to the Configuration mode.
interface 1/2 Switch to the interface configuration mode for
 port 1.2.
traffic-shape 50 Restricts the maximum bandwidth of
 interface 1/2 to 50%.
exit Switch to the Configuration mode.
exit Switch to the privileged EXEC mode.
show interfaces cos-queue Display the configuration of interface 1/2.
 1/2

Interface..... 1/2
Interface Shaping Rate..... 50

Queue Id Min. Bandwidth Max. Bandwidth Scheduler Type

0 10 20 Weighted
1 10 20 Weighted
2 15 20 Weighted
3 15 20 Weighted
4 20 20 Weighted
5 30 30 Weighted
6 0 30 Strict
7 0 30 Strict

```

**■ 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 195 “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 37](#)) 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.

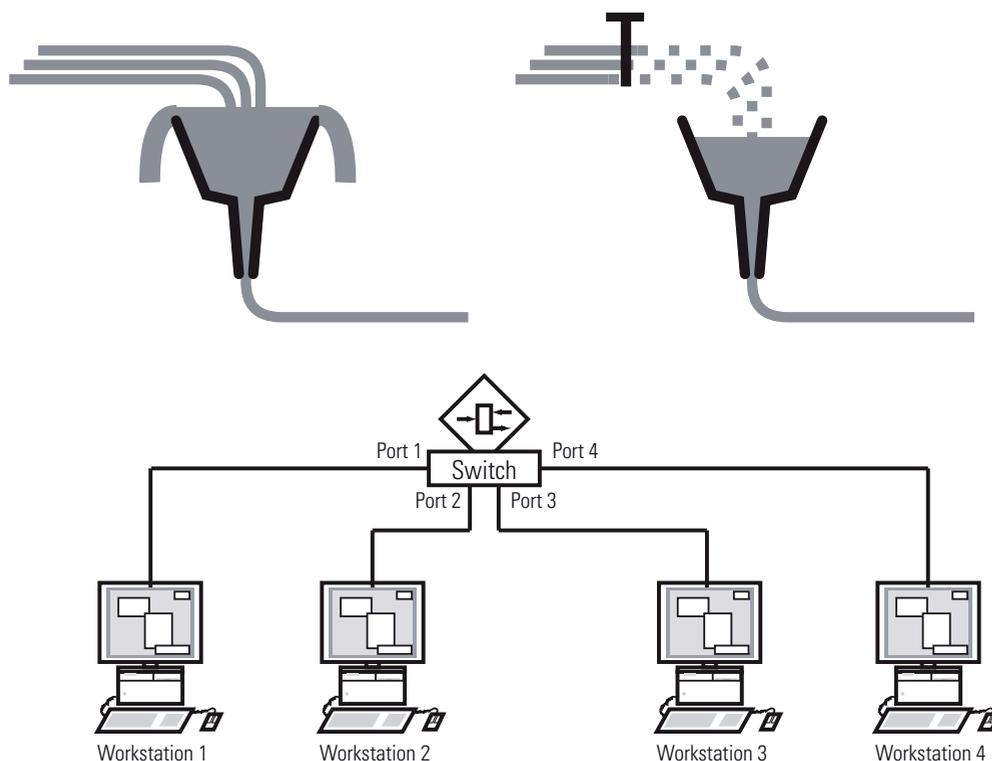


Figure 37: Example of flow control

### ■ Flow Control with a full duplex link

In the example (see [figure 37](#)) 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 37](#)) 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

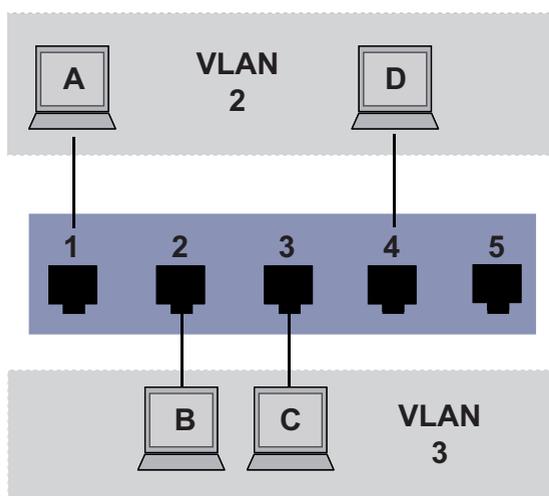


Figure 38: Example of a simple port-based VLAN

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 17: Ingress table

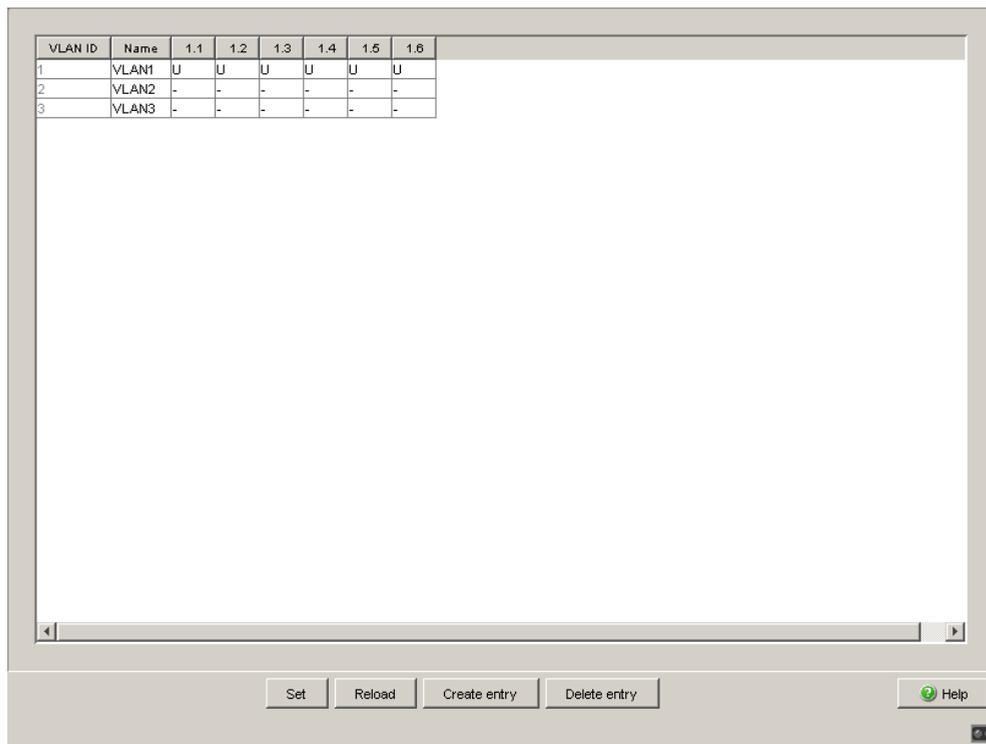
| VLANID | Port |   |   |   |   |
|--------|------|---|---|---|---|
|        | 1    | 2 | 3 | 4 | 5 |
| 1      |      |   |   |   | U |
| 2      | U    |   |   | U |   |
| 3      |      | U | U |   |   |

Table 18: Egress table

Proceed as follows to perform the example configuration:

Configure VLAN

Open the `Switching:VLAN:Static` dialog.



*Figure 39: 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

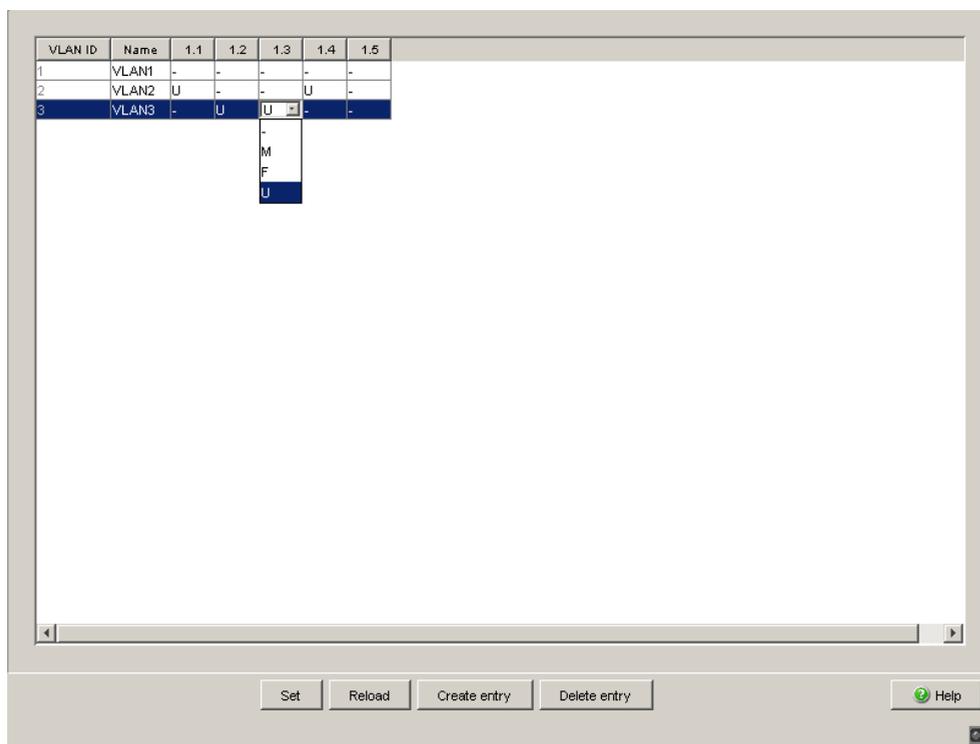


Figure 40: Defining the VLAN membership of the ports.

- 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        | GVRP                                |
|------|--------------|------------------------|--------------------------|-------------------------------------|
| 1.1  | 1            | admitAll               | <input type="checkbox"/> | <input checked="" type="checkbox"/> |
| 1.2  | 1            | admitAll               | <input type="checkbox"/> | <input checked="" type="checkbox"/> |
| 1.3  | 1            | admitAll               | <input type="checkbox"/> | <input checked="" type="checkbox"/> |
| 1.4  | 1            | admitAll               | <input type="checkbox"/> | <input checked="" type="checkbox"/> |
| 2.1  | 1            | admitAll               | <input type="checkbox"/> | <input checked="" type="checkbox"/> |
| 2.2  | 1            | admitOnlyVlanTag       | <input type="checkbox"/> | <input checked="" type="checkbox"/> |
| 2.3  | 1            | admitAll               | <input type="checkbox"/> | <input checked="" type="checkbox"/> |
| 2.4  | 1            | admitAll               | <input type="checkbox"/> | <input checked="" type="checkbox"/> |
| 3.1  | 1            | admitAll               | <input type="checkbox"/> | <input checked="" type="checkbox"/> |
| 3.2  | 1            | admitAll               | <input type="checkbox"/> | <input checked="" type="checkbox"/> |

*Figure 41: 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 settings for `GVRP` and `Ingress Filter` do 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

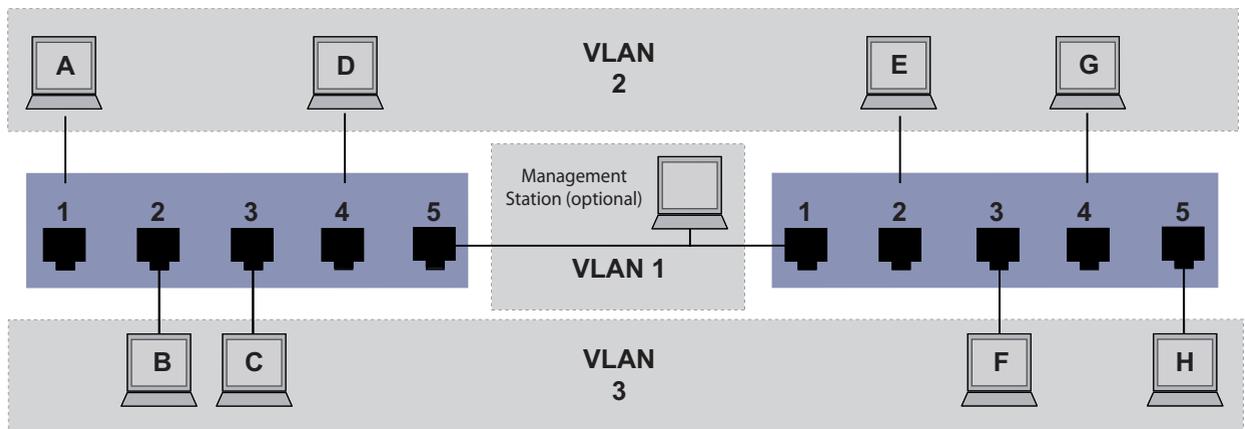


Figure 42: Example of a more complex VLAN configuration

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 19: 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 20: 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 21: Egress table for device on left

| VLAN ID | Port |   |   |   |   |
|---------|------|---|---|---|---|
|         | 1    | 2 | 3 | 4 | 5 |
| 1       | U    |   |   |   |   |

Table 22: Egress table for device on right

| VLAN ID | Port |   |   |
|---------|------|---|---|
| 2       | T    | U | U |
| 3       | T    | U | U |

Table 22: 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.

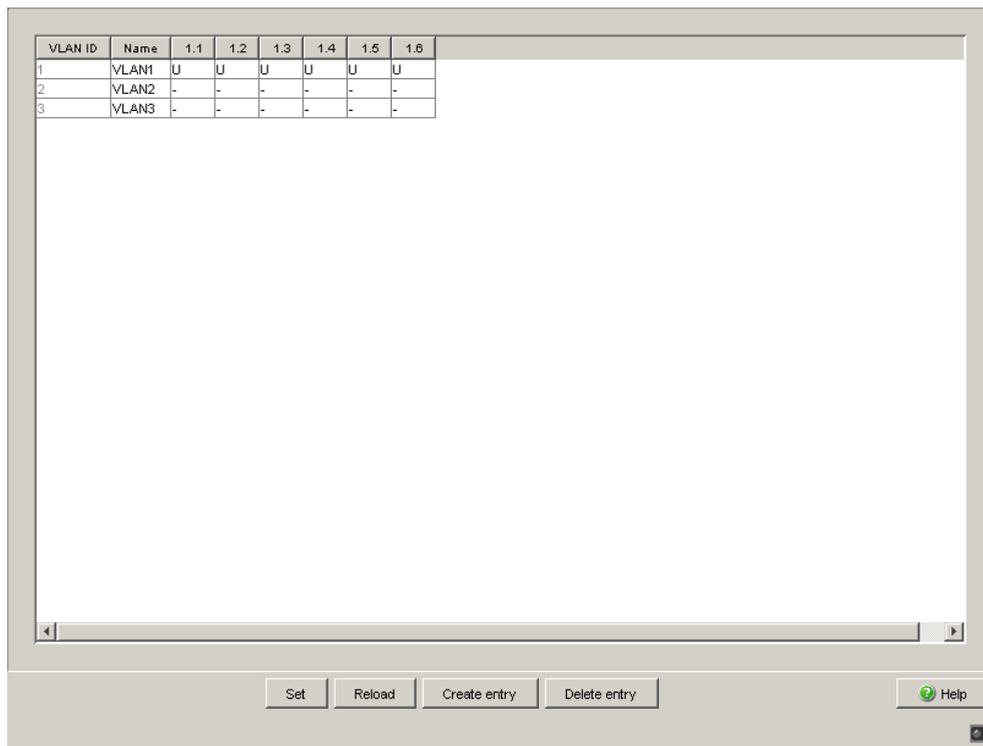
Here, VLAN tagging (IEEE 801.1Q) is used within the VLAN with the ID 1 (Uplink). You can see this from the letter  $\mathbb{T}$  in the egress table of the ports.

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 43: 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.

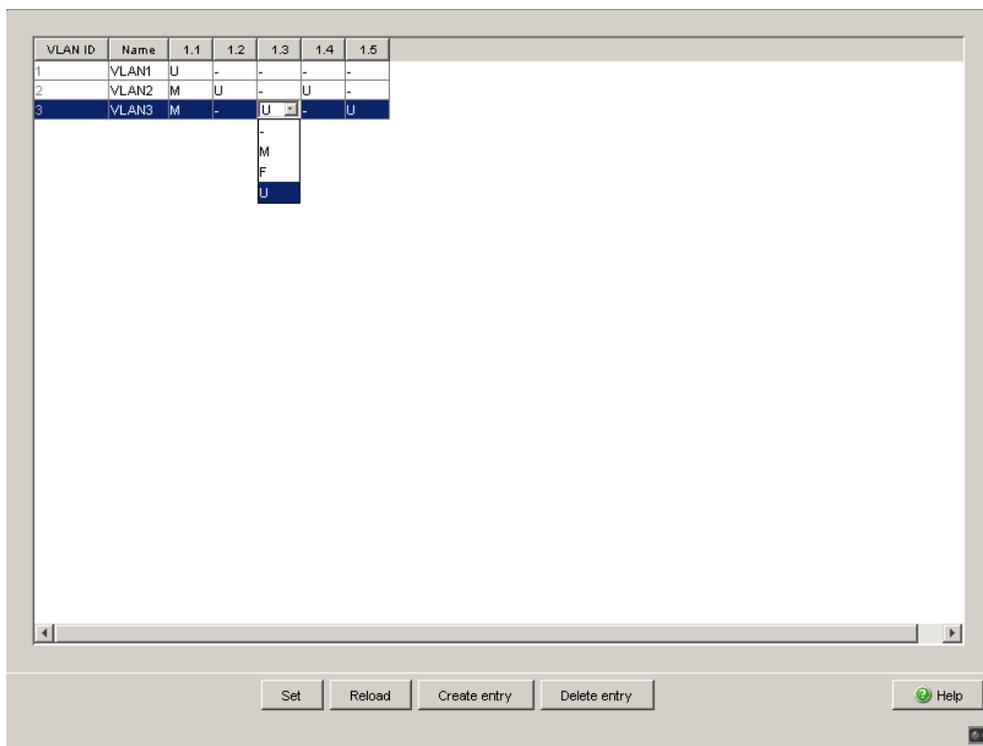
```

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 44: 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        | GVRP                                |
|------|--------------|------------------------|--------------------------|-------------------------------------|
| 1.1  | 1            | admitAll               | <input type="checkbox"/> | <input checked="" type="checkbox"/> |
| 1.2  | 1            | admitAll               | <input type="checkbox"/> | <input checked="" type="checkbox"/> |
| 1.3  | 1            | admitAll               | <input type="checkbox"/> | <input checked="" type="checkbox"/> |
| 1.4  | 1            | admitAll               | <input type="checkbox"/> | <input checked="" type="checkbox"/> |
| 2.1  | 1            | admitAll               | <input type="checkbox"/> | <input checked="" type="checkbox"/> |
| 2.2  | 1            | admitOnlyVlanTag       | <input type="checkbox"/> | <input checked="" type="checkbox"/> |
| 2.3  | 1            | admitAll               | <input type="checkbox"/> | <input checked="" type="checkbox"/> |
| 2.4  | 1            | admitAll               | <input type="checkbox"/> | <input checked="" type="checkbox"/> |
| 3.1  | 1            | admitAll               | <input type="checkbox"/> | <input checked="" type="checkbox"/> |
| 3.2  | 1            | admitAll               | <input type="checkbox"/> | <input checked="" type="checkbox"/> |

*Figure 45: 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.

### 8.6.3 Double VLAN Tagging

**For the devices MACH 1040 and MACH 4002-24G/48G.**

Double VLAN tagging (VLAN tunneling) enables you to transmit from traffic to layer 2. Double VLAN tagging allows you to avoid conflicts between the VLAN IDs of the incoming traffic and the VLANs already set up your network. You leave existing VLANs in your network unchanged and thus minimize your configuration work. This applies to:

- ▶ frames without VLAN tags,
- ▶ frames with priority tags, and
- ▶ frames with VLAN tags with any VLAN ID, including those which you are already employing for other purposes in your network.

Applications include:

- ▶ tunneling from any client traffic to layer 2,
- ▶ bypassing restrictions to the number of VLAN IDs,
- ▶ summarizing VLANs per port.

You can set up several tunnels with different VLAN IDs and thereby freely select the Ethertype of the inserted tunnel tags for your network.

The ports participating in this VLAN tunnel are either:

- ▶ Access ports on which your network receives and sends external traffic, or
- ▶ Core ports which are all located inside your network and are connected with another core port.

To construct a VLAN tunnel, set up a selectable VLAN on your devices and put the access and core ports in this tunnel VLAN. Access ports are untagged members in your tunnel VLAN and have the tunnel VLAN ID as their port VLAN ID. Core ports are tagged members in all tunnel VLANs and do not need a port VLAN ID. Also, increase the maximum size for frames on all switches with core ports to 1,552 bytes.

### How the VLAN tunnel works

- ▶ The device assigns the port VLAN ID to the frame when a frame is received at an access port. This is the tunnel VLAN ID. This also applies to frames which have already been tagged.
- ▶ Core ports are tagged members in all tunnel VLANs and send out the frame with the tunnel tag.
- ▶ The core ports transmit traffic with the tunnel VLAN ID.
- ▶ Access ports are untagged members only in their tunnel VLAN. The device removes the tunnel tag at the sending access port and sends out the original frame.

Default setting: Double VLAN tagging is deactivated at all ports. The presetting for the Ethertype of the tunnel tag is 8100Hex.

### ■ Example of Double VLAN Tagging

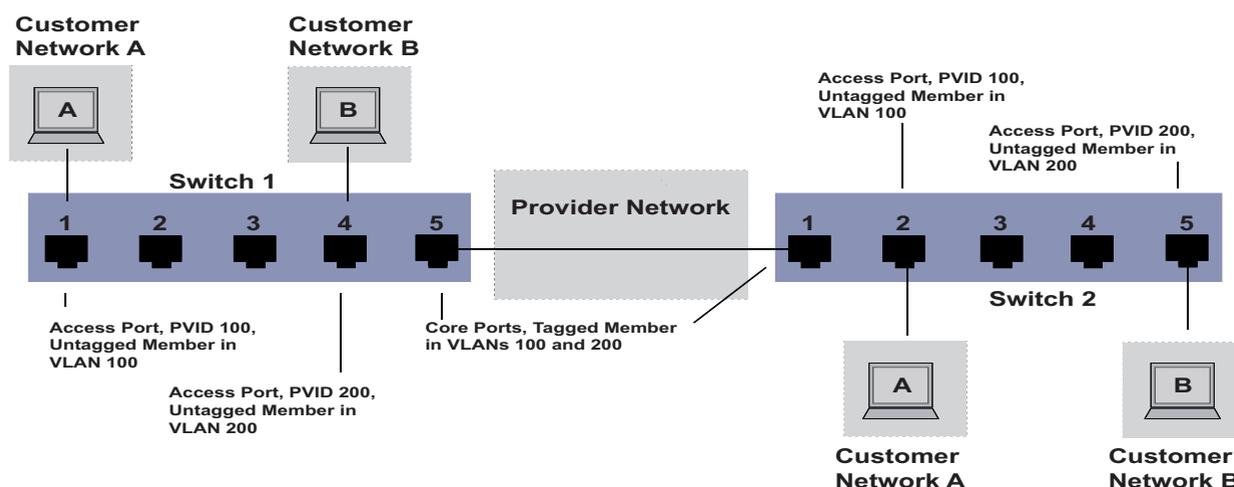


Figure 46: Example of a VLAN tunnel through use of double VLAN tagging

This example shows a provider network, the data from two client networks, A and B, transported to layer 2 through 2 VLAN tunnels. The traffic received from the client network is not subject to any restrictions with regard to VLAN IDs. The frames received can be without VLAN tags, or provided with VLAN tags or only priority tags.

VLAN-IDs 100 and 200 are not yet used on the provider network. You decide to assign the new VLAN 100 service to Client A, and the VLAN 200 service to Client B. The VLANs for the device are defined as follows:

| Client | Service VLAN ID |
|--------|-----------------|
| A      | 100             |
| B      | 200             |

Table 23: Assignment of client networks to service VLANs (VLAN tunnels)

On Switch 1, ports 1 and 4 are access ports, and port 5 is a core port (port within the provider network). On switch 2, ports 2 and 5 are access ports and port 1 is a core port. All ports are located on module 1 of the related Switch. The port settings are defined as follows:

| Switch | Port | Port role | Participant in VLAN (Tagging) | PVID |
|--------|------|-----------|-------------------------------|------|
| 1      | 1/1  | Access    | 100 (U)                       | 100  |
|        | 1/4  | Access    | 200 (U)                       | 200  |
|        | 1/5  | Core      | 100 (T), 200 (T)              | -    |
| 2      | 1/1  | Core      | 100 (T), 200 (T)              | -    |
|        | 1/2  | Access    | 100 (U)                       | 100  |
|        | 1/5  | Access    | 200 (U)                       | 200  |

Table 24: Port settings for VLAN tunnel

Set the sample configuration with the CLI:

### Switch 1:

```
enable
vlan database
vlan 100
vlan name 100 KUNDE_A

vlan 200
vlan name 200 KUNDE_B

exit
configure
bridge framesize 1552

interface 1/1

vlan pvid 100
vlan participation include
100
```

Switch to the privileged EXEC mode.  
Switch to the VLAN configuration mode.  
Create a new VLAN with the VLAN ID 100.  
Give the VLAN with the VLAN ID 100 the name CLIENT\_A.  
Create a new VLAN with the VLAN ID 200.  
Give the VLAN with the VLAN ID 200 the name CLIENT\_B.  
Switch to the privileged EXEC mode.  
Switch to the Configuration mode.  
Set the permissible frame size to 1,522 bytes.  
Switch to the Interface Configuration mode of interface 1/1.  
Port 1.1 is given the port VLAN ID 100.  
Port 1.1 becomes a member of VLAN 100.

```

no vlan tagging

mode dvlan-tunnel access
exit

interface 1/4

vlan pvid 200
vlan participation include
 200
no vlan tagging

mode dvlan-tunnel access
exit

interface 1/5

vlan participation include
 100
vlan participation include
 200
vlan tagging
mode dvlan-tunnel core
exit

```

Port 1.1 becomes an untagged member (`no vlan tagging is default`)

Port 1.1 becomes an access port  
Switch to the Configuration mode.

Switch to the interface configuration mode of interface 1/4.

Port 1.4 is given the port VLAN ID 200.

Port 1.4 becomes a member of VLAN 200.

Port 1.4 becomes an untagged member (`no vlan tagging is default`)

Port 1.4 becomes an access port  
Switch to the Configuration mode.

Switch to the interface configuration mode for port 1.5.

Port 1.5 becomes a member of VLAN 100.

Port 1.5 becomes a member of VLAN 200.

Port 1.5 becomes a tagged member

Port 1.5 becomes a core port  
Switch to the Configuration mode.

## Switch 2:

```

enable
vlan database
vlan 100
vlan name 100 KUNDE_A

vlan 200
vlan name 200 KUNDE_B

exit
configure
bridge framesize 1552

interface 1/1

vlan participation include
 100
vlan participation include
 200
vlan tagging
mode dvlan-tunnel core

```

Switch to the privileged EXEC mode.

Switch to the VLAN configuration mode.

Create a new VLAN with the VLAN ID 100.

Give the VLAN with the VLAN ID 100 the name CLIENT\_A.

Create a new VLAN with the VLAN ID 200.

Give the VLAN with the VLAN ID 200 the name CLIENT\_B.

Switch to the privileged EXEC mode.

Switch to the Configuration mode.

Set the permissible frame size to 1,522 bytes.

Switch to the Interface Configuration mode of interface 1/1.

Port 1.1 becomes a member of VLAN 100.

Port 1.1 becomes a member of VLAN 200.

Port 1.1 becomes a tagged member

Port 1.1 becomes a core port

---

|                                             |                                                                                 |
|---------------------------------------------|---------------------------------------------------------------------------------|
| <code>exit</code>                           | Switch to the Configuration mode.                                               |
| <code>interface 1/2</code>                  | Switch to the interface configuration mode for port 1.2.                        |
| <code>vlan pvid 100</code>                  | Port 1.2 is given the port VLAN ID 100.                                         |
| <code>vlan participation include 100</code> | Port 1.2 becomes a member of VLAN 100.                                          |
| <code>no vlan tagging</code>                | Port 1.2 becomes an untagged member ( <code>no vlan tagging is default</code> ) |
| <code>mode dvlan-tunnel access</code>       | Port 1.2 becomes an access port                                                 |
| <code>exit</code>                           | Switch to the Configuration mode.                                               |
| <code>interface 1/5</code>                  | Switch to the interface configuration mode for port 1.5.                        |
| <code>vlan participation include 200</code> | Port 1.5 becomes a member of VLAN 200.                                          |
| <code>no vlan tagging</code>                | Port 1.5 becomes an untagged member ( <code>no vlan tagging is default</code> ) |
| <code>mode dvlan-tunnel access</code>       | Port 1.5 becomes an access port                                                 |
| <code>exit</code>                           | Switch to the Configuration mode.                                               |

## 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
- ▶ TP cable diagnosis
- ▶ 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.                                                                                                                                             |
| vrrpTrapNewMaster        | this is sent if another router becomes the master router for an interface or a virtual address.                                                                                                            |
| vrrpTrapAuthFailure      | this is sent if the router receives a packet with an invalid authentication from another VRRP router.                                                                                                      |
| hmConfigurationSavedTrap | this is sent after the device has successfully saved its configuration locally.                                                                                                                            |

Table 25: Possible traps

---

| Trap name                  | Meaning                                                                                                                                                                                                     |
|----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| hmConfigurationChangedTrap | this is sent if you change the configuration of the device after saving locally for the first time.                                                                                                         |
| 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 25: 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.

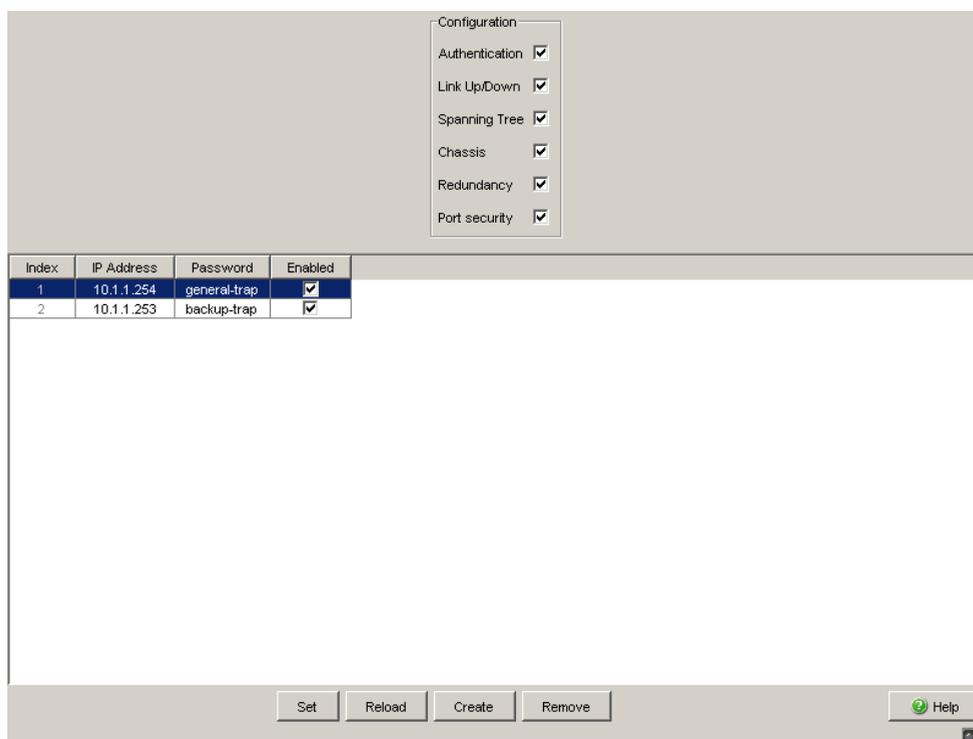


Figure 47: Alarms dialog

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        | Summarizes the following events: <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> To take this event into account, you activate “Create trap when status changes” in the <code>Diagnostics:Signal Contact 1/2</code> dialog. <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> |
|                | 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 26: 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 224 “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 88 “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
- ▶ Failure of a fan (MACH 4000).

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 224 “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.

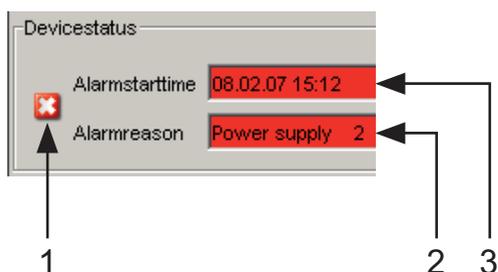
```
enable
configure
device-status monitor all
error
device-status trap enable
```

Change to the privileged EXEC mode.  
Change to the Configuration mode.  
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 48: 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 88 “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
- ▶ Failure of a fan (MACH 4000).

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 224 "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.

|                                           |                                                      |
|-------------------------------------------|------------------------------------------------------|
| <code>enable</code>                       | Switch to the privileged EXEC mode.                  |
| <code>configure</code>                    | Switch to the Configuration mode.                    |
| <code>signal-contact 1 mode manual</code> | Select the manual setting mode for signal contact 1. |
| <code>signal-contact 1 state open</code>  | Open signal contact 1.                               |
| <code>signal-contact 1 state close</code> | 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 224 "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.

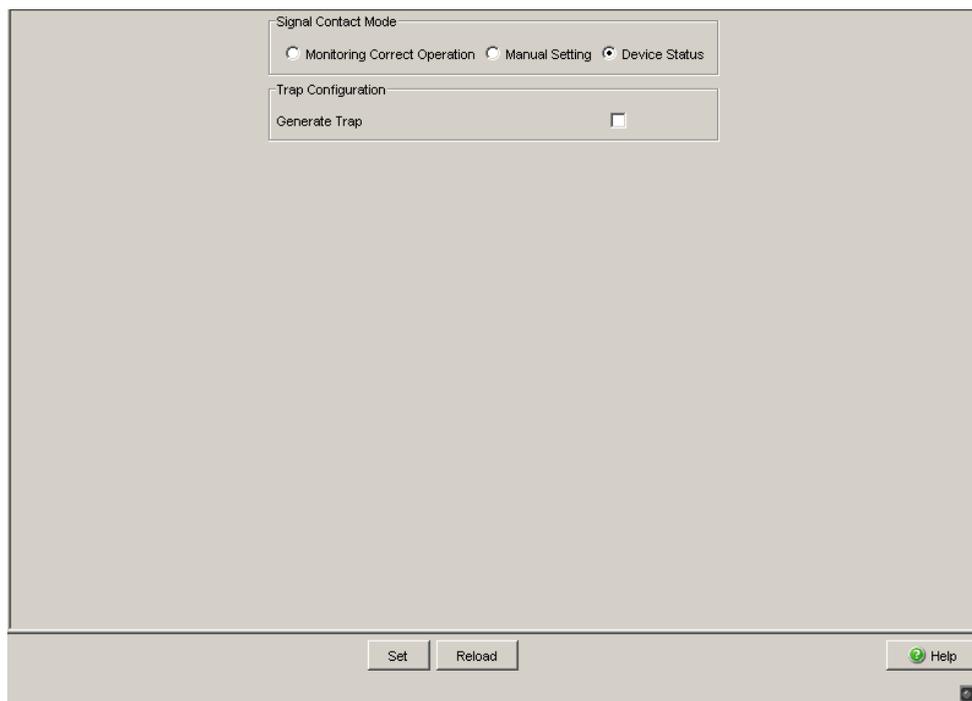


Figure 49: Signal Contact dialog

```
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.

### 9.3.4 Monitoring the Fan

Devices in the Mach 4000 family have a replaceable plug-in fan unit. This plug-in fan helps considerably in reducing the internal temperature of the device.

Fans are subject to natural wear. The failure of one or more fans in the plug-in fan can have a negative effect on the operation and life span of the device, or can lead to a total failure of the device.

The device enables you

- ▶ to signal changes to the status of the plug-in fan out-of-band (outside the data flow) via a signal contact ([see on page 224 “Monitoring the Device Status via the Signal Contact”](#))
- ▶ to signal changes to the status of the plug-in fan by sending a trap when the device status changes
- ▶ to detect status changes to the plug-in fan in the Web-based interface on the system side and
- ▶ to query changes to the status of the plug-in fan in the Command Line Interface.

Proceed as follows to signal changes to the fan status via a signal contact and with an alarm message:

- Select the `Diagnostics:Signal Contact` dialog.
- Select the signal contact you want to use (in the example, signal contact 1) in the corresponding tab page “Signal contact 1” or “Signal contact 2”.
- In the “Signal contact mode” frame, select “Function monitoring”.
- In the “Function monitoring” frame, select the fan monitoring.
- 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.

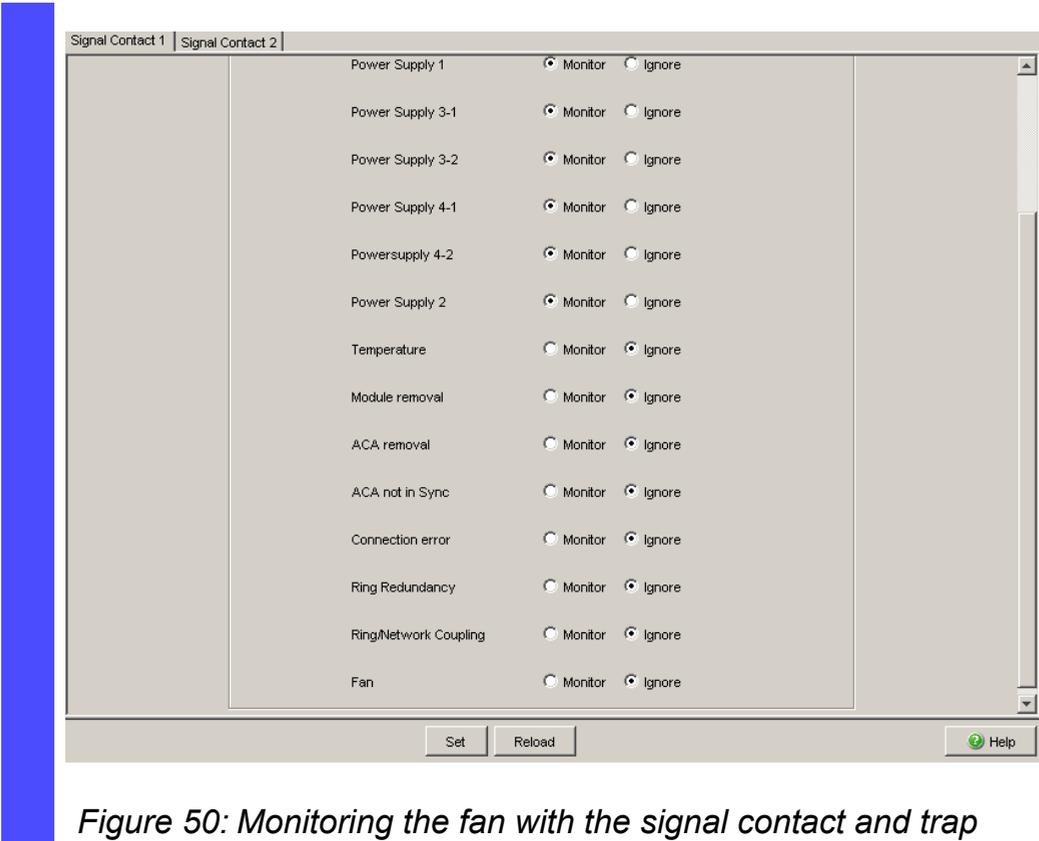
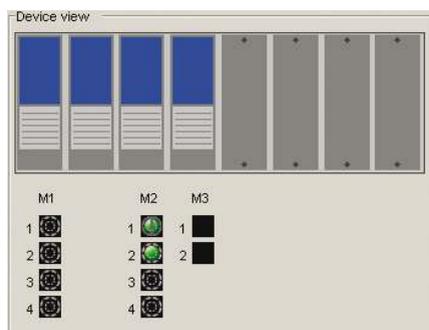


Figure 50: Monitoring the fan with the signal contact and trap

## 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 51: 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 27: 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 52 shows a screenshot of the 'Port Statistics dialog' window. The window contains a table with 10 columns: Port, Transmitted Packets, Transmitted Unicast Packets, Transmitted Non Unicast Packets, Received Packets, Received Octets, Received Fragments, Detected CRC errors, Detected Collisions, and Detected Late Collisions. The table lists statistics for 12 ports (1.1 to 3.2). Below the table is a horizontal scrollbar and a 'Reload' button. A 'Help' button is located in the bottom right corner of the dialog.

Figure 52: 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 ( $\geq 10$ 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 28: Evaluation of non-matching of the duplex mode

| No. | Automatic configuration | Current duplex mode | Detected error events ( $\geq 10$ 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 28: 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).

```
enable
```

```
configure
```

```
bridge duplex-mismatch-detect
operation enable
```

```
bridge duplex-mismatch-detect
operation disable
```

Change to the privileged EXEC mode.

Change to the Configuration mode.

Activates the detection and reporting of non-matching duplex modes.

Deactivates the detection and reporting of non-matching duplex modes.

## 9.5.2 TP Cable Diagnosis

The TP cable diagnosis allows you to check the connected cables for short-circuits or interruptions.

**Note:** While the check is running, the data traffic at this port is suspended.

The check takes a few seconds. After the check, the "Result" row contains the result of the cable diagnosis. If the result of the check shows a cable problem, then the "Distance" row contains the cable problem location's distance from the port.

| Result        | Meaning                                                      |
|---------------|--------------------------------------------------------------|
| normal        | The cable is okay.                                           |
| open          | The cable is interrupted.                                    |
| short circuit | There is a short-circuit in the cable.                       |
| unknown       | No cable check was performed yet, or it is currently running |

*Table 29: Meaning of the possible results*

Prerequisites for correct TP cable diagnosis:

- ▶ 1000BASE-T port, connected to a 1000BASE-T port via 8-core cable or
- ▶ 10BASE-T/100BASE-TX port, connected to a 10BASE-T/100BASE-TX port.

### 9.5.3 Port Monitor

When you enable this feature the device monitors the port states. The device offers you the ability to disable individual ports or send a trap when user-defined conditions occur.

Definable port conditions are:

- ▶ Link Flap
- ▶ CRC/Fragments
- ▶ Overload Detection
- ▶ Speed and duplex combination

In the Global dialog, you activate the configurations defined in the "Link Flap", "CRC/Fragments" and "Overload Detection" tabs. The device detects these conditions when you activate the functions. If the device detects the user defined condition on a port, it produces the response defined for that port.

Link Flapping occurs when a link alternately advertises its link state as up and down. You configure the device to detect this condition and then define whether to send a trap or shut the port off.

Using the Cyclical Redundancy Check (CRC) the device detects data packets modified during the transmission based on the checksum. The device detects the total number of packets received that were less than 64 octets in length, excluding framing bits, but including FCS octets, and had either a FCS error or an Alignment Error.

- ▶ A FCS error is a bad Frame Check Sequence (FCS) with an integral number of octets.
- ▶ An Alignment Error is a bad FCS with a non-integral number of octets.

The device monitors both criteria if you enable the function in the "Global" tab. If the number of occurred CRC/fragment errors exceeds the specified threshold, the device executes the user-specified action.

Overload Detection prevents a broadcast, multicast, or unicast storm from disrupting traffic on a port. The Overload Detection function monitors packets passing from a port to the switching bus to determine if the packet is unicast, multicast, or broadcast. The switch counts the number of user-defined packets received within the "Sampling Interval" and compares the measurement with a user-defined threshold. The port blocks traffic after reaching the "Upper Threshold". When you activate the recovery function for Overload Detection, the port remains blocked until the traffic rate drops below the "Lower Threshold" and then forwards traffic as normal.

The device allows you to define which duplex mode is allowed for which speed for a specific port. The monitoring of the combination of speed and duplex mode prevents any undesired connections.

- Open the `Diagnositics:Ports:Port Monitor` dialog.
- Open the "Link Flap" tab.
- Define the number of times that a port cycles between link up and link down before the function disables the port, in the "Link Flap Count" text box, in the "Parameter" frame.
- Define the elapse time in the "Sample Interval [s]" text box in the "Parameter" frame.
  
- Open the "CRC/Fragments" tab.
- Define the number of packets received containing changes in raw data or fragment packets received before the function disables the port, in the "CRC/Fragments count [ppm]" text box, in the "Parameter" frame.
- Define the elapse time in the "Sample Interval [s]" text box in the "Parameter" frame.
  
- Open the "Overload Detection" tab.
- Define the elapse time in the "Sample Interval [s]" text box in the "Parameter" frame.
- For each port, define the type of traffic to monitor in the "Traffic Type" column.
- For each port, define the type of threshold to use in the "Threshold Type" column.
- For each port, define the threshold at which the device enables the port in the "Lower Threshold" column.
- For each port, define the threshold at which the device disables the port in the "Upper Threshold" column.
  
- Open the "Speed Duplex" tab.

- You define for each port which duplex mode is allowed for which speed.
  - "hdx" = half duplex
  - "fdx" = full duplex
  - "10" = 10 Mbit/s
  - "100" = 100 Mbit/s
  - etc.
- Open the "Global" tab.
- In the "Port Monitor on" column of the "Global" tab, select the ports to monitor.
- To activate the Port Monitor function, click On in the "Operation" frame.

## 9.5.4 Auto Disable

If the configuration shows a port as enabled, but the device detects an error, the software shuts down that port. In other words, the device software disables the port because of a detected error condition.

When a port is auto-disabled, the device effectively shuts down the port and the port blocks traffic. The port LED blinks green 3 times per period and identifies the reason for the shutdown. In addition, the device generates a log entry listing the reason for the auto-disable. When you enable the port after a timeout by auto-disable, the device generates a log entry.

This feature provides a recovery function which automatically enables an auto-disabled port after a user-defined time. When this function enables a port, the device sends a trap with the port number and an empty "Reason" entry.

The auto-disable function serves the following purposes:

- ▶ It assists the network administrator in port analysis.
- ▶ It eliminates the possibility that this port causes other ports on the module (or the entire module) to shut down.

**Note:** The "Reset" button allows you to enable the port before the "Reset Timer [s]" counts down.

So that the device enables the ports again that were disabled because of a detected error state, complete the following steps:

- Open the `Diagnostics:Ports:Auto Disable` dialog.
- To enable ports again that the device has disabled due to link flaps, in the "Configuration" frame mark the "Link Flap" checkbox. You define the parameters that cause the ports to be disabled due to link flaps in the `Diagnostics:Ports:Port Monitor` dialog, on the "Link Flap" tab.

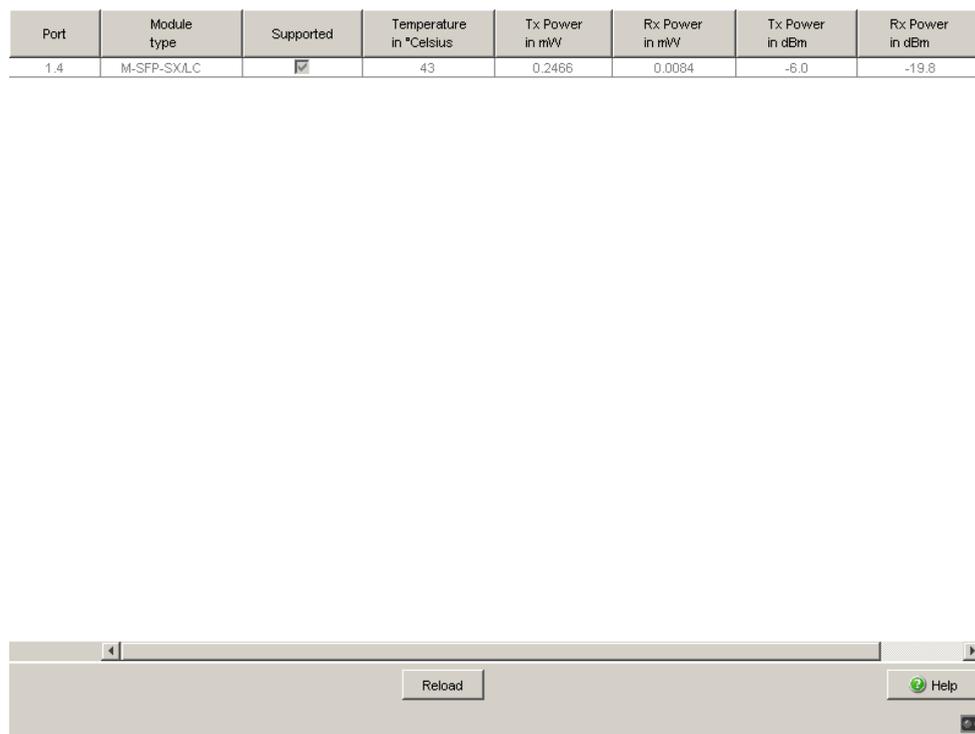
- To enable ports again that the device has disabled due to CRC or fragment errors, on the "Configuration" frame mark the "CRC Error" checkbox.  
You define the parameters that cause the ports to be disabled due to CRC or fragment errors in the `Diagnostics:Ports:Port Monitor` dialog, on the "CRC/Fragments" tab.
- To enable ports again that the device has disabled due to an overload, in the "Configuration" frame mark the "Overload Detection" checkbox.  
You define the parameters that cause the ports to be disabled due to an overload in the `Diagnostics:Ports:Port Monitor` dialog, on the "Overload Detection" tab.
- To enable ports again that the device disabled due to an incorrect speed and duplex combination, in the "Configuration" frame mark the "Speed Duplex" checkbox.  
You define the parameters that cause the ports to be disabled due to an incorrect speed and duplex combination in the `Diagnostics:Ports:Port Monitor` dialog, on the "Speed Duplex" tab.
- To enable ports again that the device disabled due to an unauthorized access to the port, in the "Configuration" frame you mark the "Port Security" checkbox.  
You define the parameters that cause the ports to be disabled due to unauthorized access in the `Security:Port Security` dialog.
- You define the time until each port is automatically enabled again in the "Reset Timer [s]" column in the table.

## 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 53: 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 158 “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. 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 30: 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 30).

## 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.

| Timestamp | IP Address | MAC address |
|-----------|------------|-------------|
|-----------|------------|-------------|

Figure 54: 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 Monitoring Data Traffic on the Ports (Port Mirroring)

The MACH4002 24/48 + 4G and the Power MICE support up to 8 ports.

The port mirroring function enables you to review the data traffic from a group of ports on the device for diagnostic purposes (N:1). The device forwards (mirrors) the data for these ports to another port. This process is port mirroring.

The ports from which the device copies the traffic are source ports. The port on which you review the data is the destination port. You use physical ports as source or destination ports.

In port mirroring, the device copies valid data packets of the source port to the destination port. The device does not affect the data traffic on the source ports during port mirroring.

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

When selecting "RX" as the monitoring direction on a source port, only frames received on the source port will be copied/mirrored to the destination port ( monitoring ingress).

When selecting "TX" as the monitoring direction on a source port, only frames transmitted on the source port will be copied/mirrored to the destination port (monitoring egress).

With port mirroring active, the device copies the traffic received and/or forwarded on a source port to the destination port.

The PowerMICE and MACH4000 devices use the destination port for the port mirroring task exclusively. The source port forwards and receives traffic as normal.

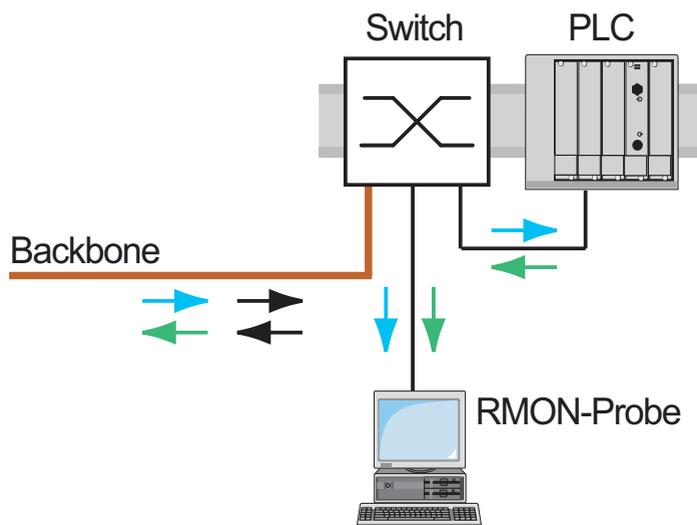


Figure 55: Port mirroring

- Select the `Diagnostics:Port Mirroring` dialog.

This dialog allows you to configure and activate the port mirroring function of the device.

- Select the source ports whose data traffic you want to review from the physical ports list by checkmarking the relevant boxes. The device displays the "Source Port" currently used as the "Destination Port" as grayed out in the table. Default setting: no source ports.
- Select the destination port to which you have connected your management tool from the drop-down menu in the "Destination Port" frame. Selecting a destination port is mandatory for a valid port mirroring configuration. The drop-down menu displays available ports exclusively, for example, the list excludes the ports currently in use as source ports. Default setting: port – (no destination port).
- To select the monitoring traffic direction, checkmark the relevant "RX" and "TX" boxes for ingress and egress monitoring directions.
- To switch on the function, select `On` in the "Operation" frame. Default setting: `Off`.

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

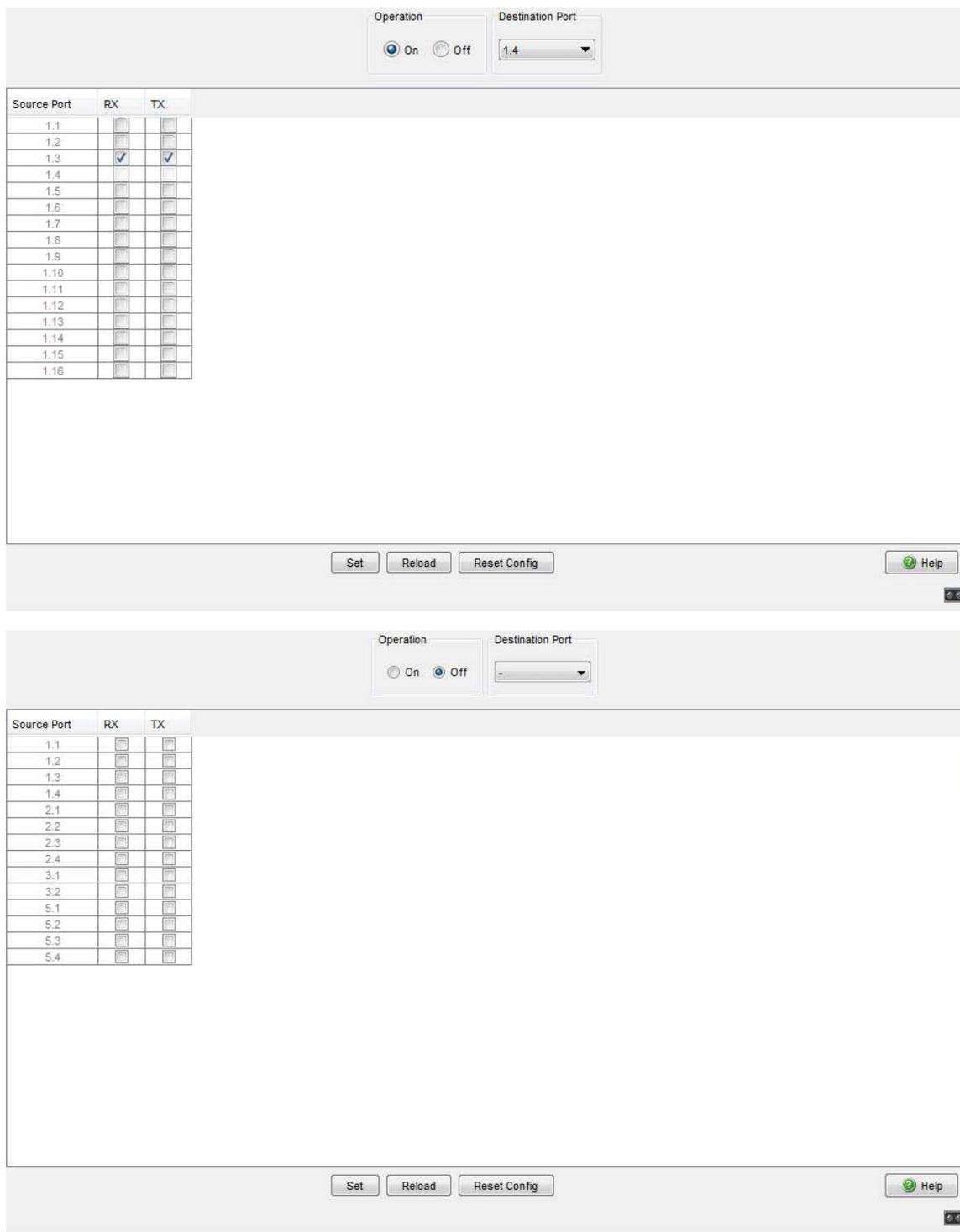


Figure 56: Port Mirroring dialog

## 9.12 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 256 “Trap log”) and in the log file (see on page 247 “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.

```
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

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
```

Switch to the privileged EXEC mode.  
Switch to the Configuration mode.  
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”.  
Enable the Syslog function.  
Switch to the privileged EXEC mode.  
Display the syslog host settings.

Switch to the privileged EXEC mode.  
Switch to the Configuration mode.  
Create log events from reading SNMP requests.  
The “5” indicates the seriousness of the message that the device allocates to messages from reading SNMP requests. “5” means “note”.  
Create log events from writing SNMP requests.  
The “5” indicates the seriousness of the message that the device allocates to messages from writing SNMP requests. “5” means “note”.  
Switch to the privileged EXEC mode.  
Display the SNMP logging settings.

```
Log SNMP SET requests : enabled
Log SNMP SET severity : notice
Log SNMP GET requests : enabled
Log SNMP GET severity : notice
```

## 9.13 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 253 “Syslog”](#)).

## 9.14 MAC Notification

MAC notification, also known as MAC address change notification, tracks users on a network by storing the MAC address change activity. When the switch learns or removes a MAC address, the device sends an SNMP trap to a configured trap destination. The device generates MAC address change notifications for dynamic unicast MAC addresses.

The device buffer contains up to 20 addresses. If the buffer is full before the user -defined interval expires, then the device sends a trap to the management station.

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

- Open the `Diagnositics:MAC Notification` dialog.
- Select the activity for which the device sends a trap in the "Mode"column.
- To select the ports for which the device sends a trap, activate the checkbox in the "Enabled" column.
- Define the number of seconds between trap transmissions in the "Interval [s]" textbox.
- To enable the function, click `On` in the "Operation" frame.

|                                           |                                                             |
|-------------------------------------------|-------------------------------------------------------------|
| <code>enable</code>                       | Change to the privileged EXEC mode.                         |
| <code>configure</code>                    | Change to the Configuration mode.                           |
| <code>mac notification interval 20</code> | Set MAC notification interval to 20 seconds.                |
| <code>interface 1/1</code>                | Change to the Interface Configuration mode of port 1/1.     |
| <code>mac notification mode</code>        | Set the mode for which the device sends a MAC notification. |
| <code>mac notification operation</code>   | Enable sending of MAC notification traps for this port.     |
| <code>exit</code>                         | Change to the Configuration mode.                           |
| <code>mac notification operation</code>   | Enable the MAC notification function globally.              |



# **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 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.

- 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`.

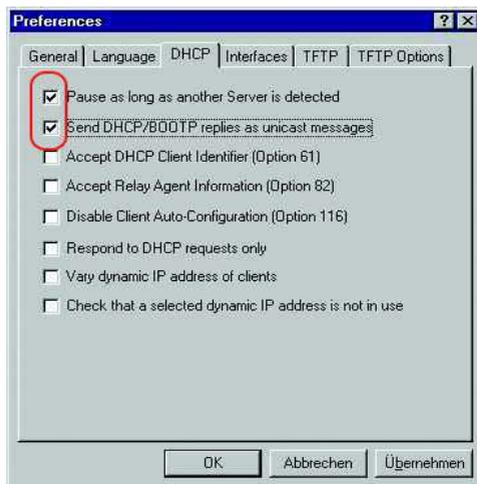


Figure 58: DHCP setting

- To enter the configuration profiles, select `Options: Configuration Profiles` in the menu bar.
- Enter the name of the new configuration profile and click `Add`.

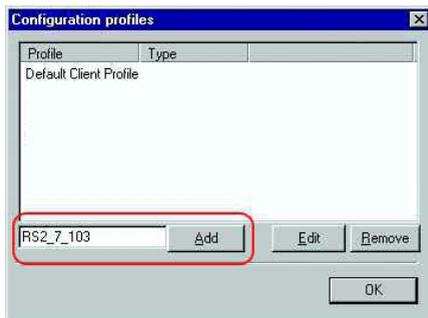


Figure 59: Adding configuration profiles

- Enter the netmask and click `Apply`.

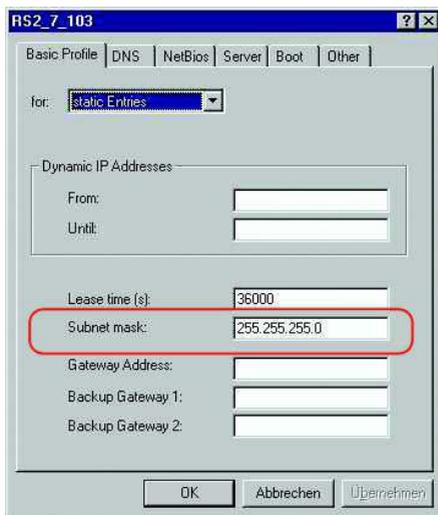


Figure 60: Netmask in the configuration profile

- 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`.

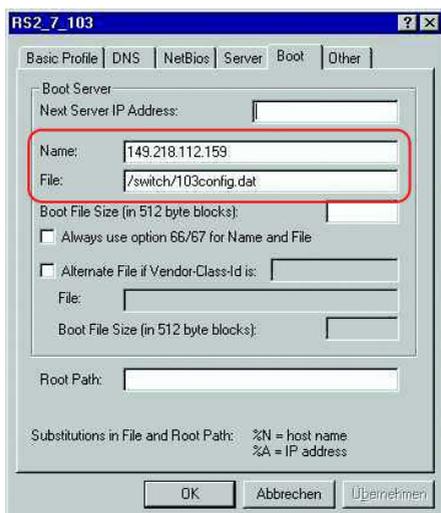


Figure 61: Configuration file on the tftp server

- 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**.

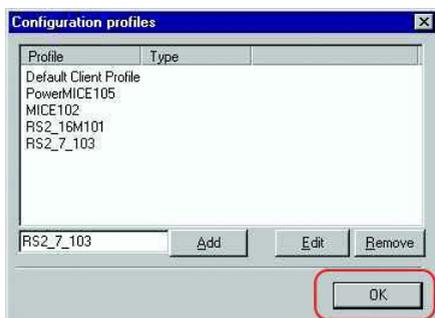


Figure 62: Managing configuration profiles

- To enter the static addresses, click `Static` in the main window.



Figure 63: Static address input

- Click New.



Figure 64: 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.

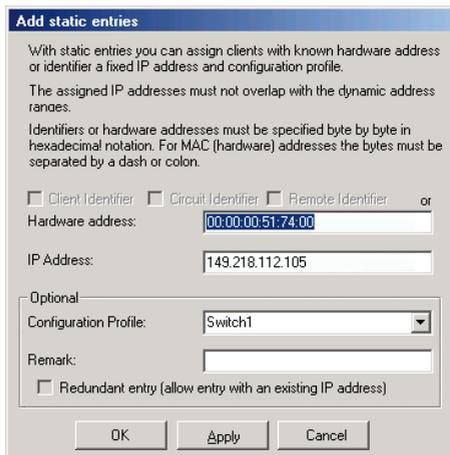


Figure 65: Entries for static addresses

- Add an entry for each device that will get its parameters from the DHCP server.

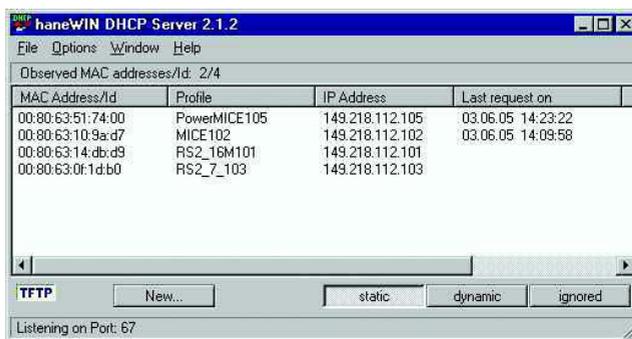


Figure 66: DHCP server with entries

## 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 67: 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.

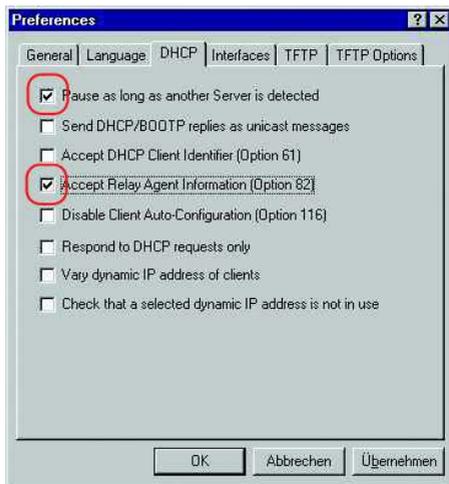


Figure 68: DHCP setting

- To enter the static addresses, click `New`.



Figure 69: Adding static addresses

- Select `Circuit Identifier` and **Remote Identifier**.

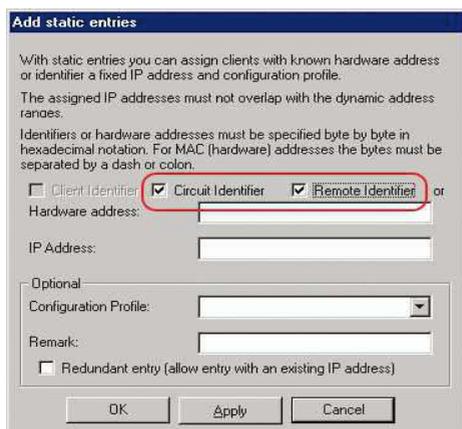


Figure 70: Default setting for the fixed address assignment

- 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:

`ciclhvsvvssmmpprirlxxxxxxxxxxxx`

- ▶ `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.

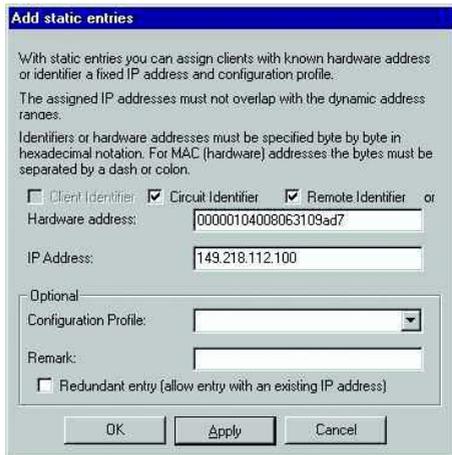


Figure 71: Entering the addresses

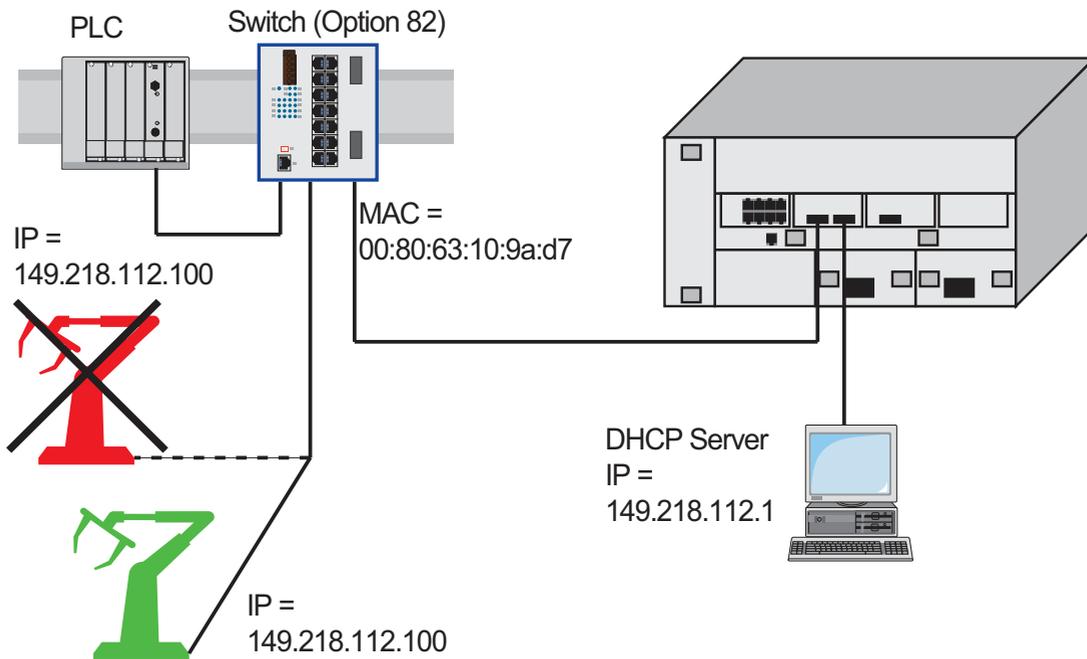


Figure 72: Application example of using Option 82

## 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 73](#)) 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.

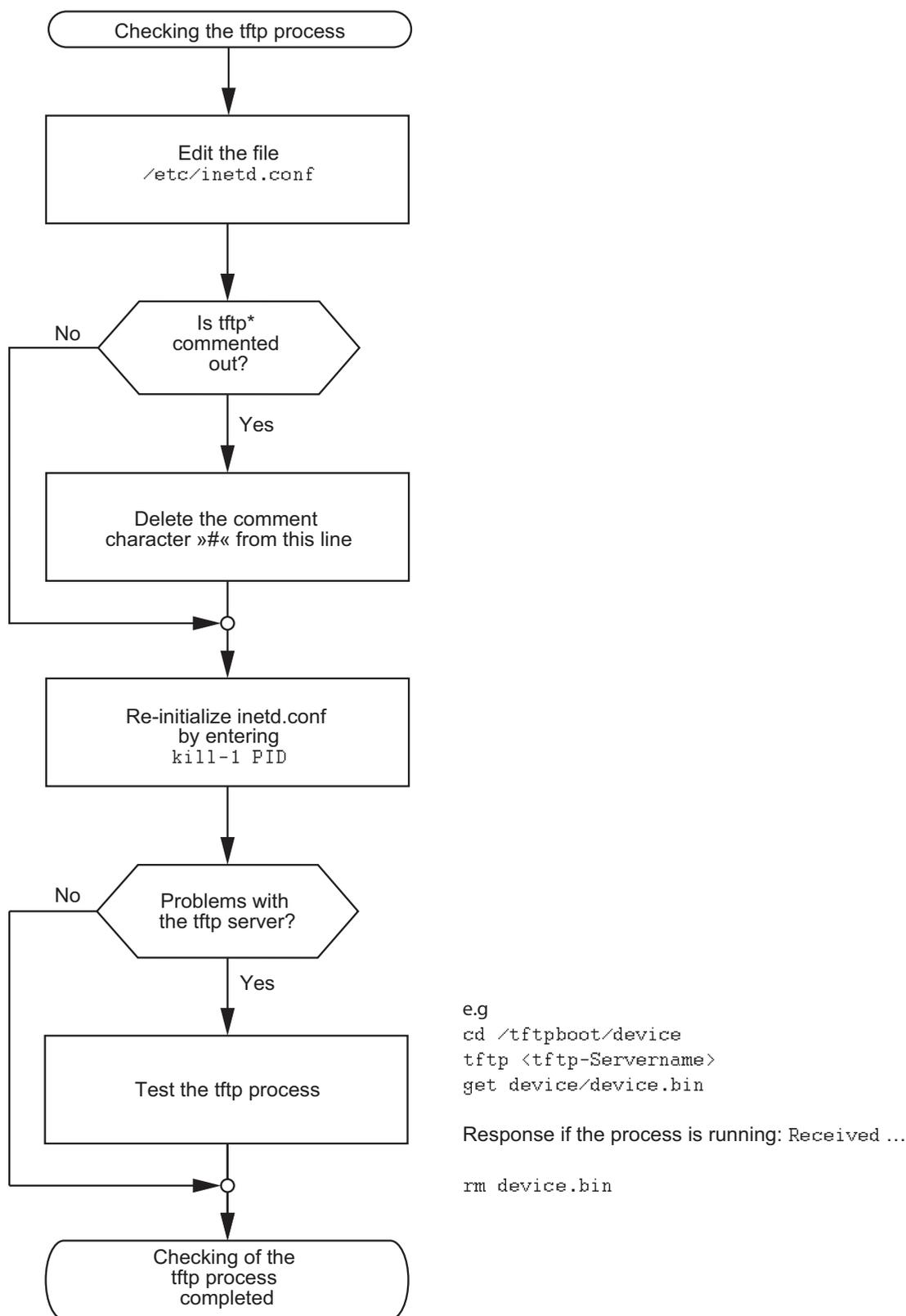
For example:

```
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 73: 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 31: 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 Preparing access via SSH

To be able to access the device via SSH, perform the following steps:

- ▶ Generate a key (SSH host key).
- ▶ Install the key on the device.
- ▶ Enable access via SSH on the device.
- ▶ Install a program for executing the SSH protocol (SSH client) on your computer.

### A.4.1 Generating a key

The device gives you the option to use your own self-generated keys for the SSH server. If there is no SSH key on the device, the device generates the required keys automatically when the SSH server is switched on for the first time.

The PuTTYgen program allows you to generate the key. This program is located on the product CD.

- Start the program by double-clicking on it.
- In the "Parameters" frame you select the type of key to be generated.
  - To generate a key for SSH version 2, you select "SSH-2 (RSA)" or "SSH-2 (DSA)".
  - To generate a key for SSH version 1, you select "SSH-1 (RSA)".
- Make sure that the field "Number of bits in a generated key" in the "Parameters" frame is showing the value 1024.
- In the "Actions" box, click on "Generate". Move the mouse pointer over the PuTTYgen-window, so that PuTTYgen can create the key using random numbers.
- Leave the "Key passphrase" and "Confirm passphrase" input boxes empty.

- Save the key:
  - To save a key for SSH version 2, click the `Conversions:Export` OpenSSH key menu.
  - To save a key for SSH version 1, click the "Save private key" button in the "Actions" frame.
- Answer the question about saving the key without a passphrase with "Yes".
- Select the Save location and enter a file name for the key file.
- Note down the key fingerprint, so that you can check it when establishing a connection.
- You should also store the key in a location separate from the device so that, if the device is being replaced, the key can be transferred to the new device.

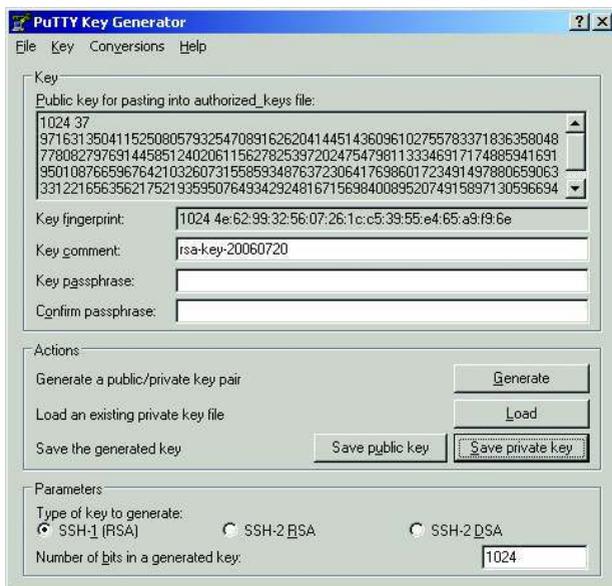


Figure 74: PuTTY key generator

For experienced network administrators, another way of creating the key is with the OpenSSH Suite. To generate the key, enter the following command:

```
ssh-keygen(.exe) -q -t rsa1 -f rsa1.key -C '' -N ''
```

## A.4.2 Loading a key onto the device

You load the SSH key onto the device with the Command Line Interface via TFTP.

SSH version 1 works with an RSA key. However, SSH version 2 works with an RSA key and a DSA key. For SSH version 2, you always load both keys to the device.

- Store the keys on your tftp server.
- Load the keys from the tftp server onto the device.

```
enable
no ip ssh
copy tftp://ip/filepath/key
 nvram:sshkey-rsa2
copy tftp://ip/filepath/key
 nvram:sshkey-dsa
copy tftp://ip/filepath/key
 nvram:sshkey-rsa1
ip ssh
```

Switch to the privileged EXEC mode.

Deactivates the SSH server.

Loads the key to the non-volatile memory of the device.

▶ `nvram:sshkey-rsa2` is the storage location of the RSA key for SSH version 2.

▶ `nvram:sshkey-dsa` is the storage location of the DSA key for SSH version 2.

▶ `nvram:sshkey-rsa1` is the storage location of the RSA key for SSH version 1.

Activates the SSH server.

## A.4.3 Access through an SSH

One way of accessing your device through an SSH is by using the PuTTY program. This program is provided on the product-CD.

- Start the program by double-clicking on it.
- Enter the IP address of your device.
- Select "SSH".
- Click on "Open" to set up the connection to your device.

Depending on the device and the time at which SSH was configured, it can take up to a minute to set up the connection.

Just before the connection is established, the PuTTY program displays a security alarm message and gives you the option of checking the key fingerprint.



Figure 75: Security alert prompt for the fingerprint

- Check the fingerprint of the key to ensure that you have actually connected to the desired device. You will find the fingerprint of your key in the "Key fingerprint" field of the PuTTY key generator.
- If the fingerprint matches your key, click on "Yes".

PuTTY also displays another security alarm message at the defined warning threshold.



Figure 76: Security query at the defined warning threshold

- Click on "Yes" in the security alarm message.

To suppress this message when establishing subsequent connections, select "SSH" in the "Category" box in the PuTTY program before opening the connection. In the "Encryption options" box, select "DES" and click on "Up" until "DES" comes above the line "-- warn below here --". In the "Category" box, switch back to "Session" and establish the connection as usual.

For experienced network administrators, another way of accessing your device through an SSH is by using the OpenSSH Suite. To open the connection, enter the following command:

```
ssh admin@10.0.112.53 -cdes
```

- ▶ `admin` for the user name.
- ▶ `10.0.112.53` is the IP address of your device.
- ▶ `-cdes` sets the encryption type for SSHv1.

## A.5 HTTPS Certificate

The encryption of HTTPS connections requires an X.509 certificate. The device allows you to use your own X.509 certificate. If there is no X.509 certificate on the device, the device generates this automatically when the HTTPS server is switched on for the first time.

You load your own X.509 certificate onto the device with the Command Line Interface via TFTP.

- Store the certificate on your tftp server.
- Load the certificate from the tftp server onto the device.

```
enable
no ip https
```

```
copy tftp://ip/filepath/cert
nvram:httpscert
```

```
ip https
```

Change to the privileged EXEC mode.

Deactivates the HTTPS function before transferring the certificate to the device.

Loads the certificate to the non-volatile memory of the device.

`nvram:httpscert` is the storage location of the X.509 certificate.

Activates the HTTPS function after transferring the certificate to the device.

## A.6 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.                                 |

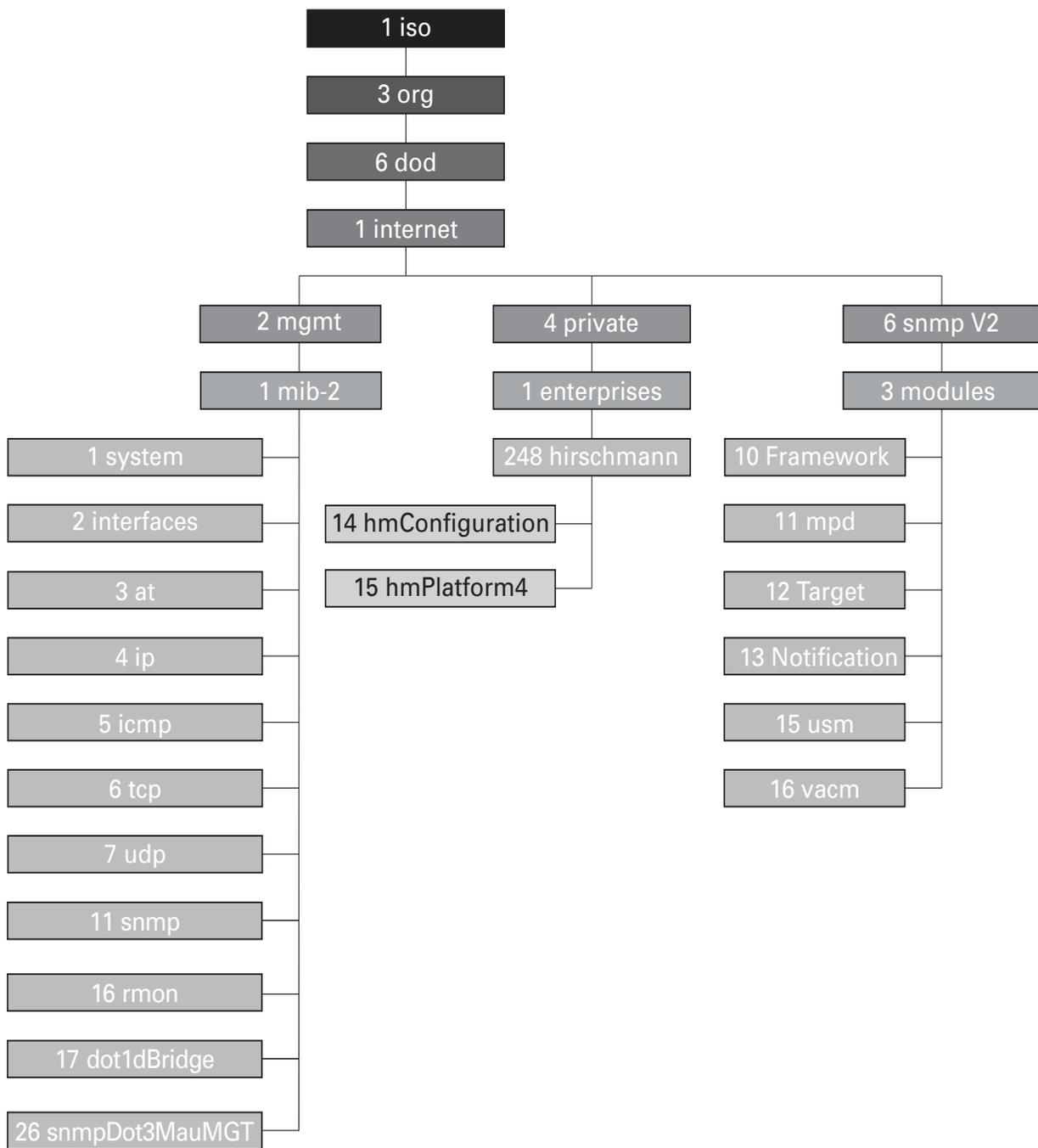


Figure 77: Tree structure of the Hirschmann MIB

A complete description of the MIB can be found on the product CD provided with the device.

---

## B.2 Abbreviations used

|       |                                         |
|-------|-----------------------------------------|
| ACA   | AutoConfiguration Adapter               |
| ACL   | Access Control List                     |
| 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>                       |                 | <b>D</b>                         |                         |
| ACA                            | 58, 75, 77, 218 | Data transfer parameters         | 18                      |
| ACA31                          | 41              | Destination address              | 156, 158, 159, 169      |
| ACD                            | 244             | Device Status                    | 219                     |
| ACL                            | 175             | DHCP                             | 27, 48, 51              |
| Access                         | 218             | DHCP Client                      | 48                      |
| Access Control List            | 175             | DHCP Option 82                   | 51                      |
| Access rights                  | 69, 95          | DHCP server                      | 132, 260, 266           |
| Access security                | 87              | Differentiated management access | 106                     |
| Address Conflict Detection     | 244             | Differentiated Services          | 179                     |
| Address table                  | 157             | DiffServ                         | 175                     |
| AF                             | 179             | DiffServ codepoint               | 179                     |
| Aging Time                     | 157, 163, 163   | Double VLAN tagging              | 208                     |
| Alarm                          | 217             | DSCP                             | 176, 179, 181, 186, 186 |
| Alarm messages                 | 214             | DVLAN tagging                    | 208                     |
| APNIC                          | 29              | Dynamic                          | 158                     |
| ARIN                           | 29              | <b>E</b>                         |                         |
| ARP                            | 34              | E2E                              | 142                     |
| ASF Finder                     | 58              | EF                               | 179                     |
| Assured Forwarding             | 179             | End-to-End                       | 142                     |
| Authentication                 | 218             | Event Log                        | 256                     |
| AutoConfiguration Adapter      | 41, 218         | Expedited Forwarding             | 179                     |
| Automatic Configuration        | 87              | <b>F</b>                         |                         |
| <b>B</b>                       |                 | FAQ                              | 295                     |
| Bandwidth                      | 161, 191        | Fan                              | 225                     |
| Bandwidth restriction          | 183             | Faulty device replacement        | 55                      |
| BOOTP                          | 27              | FDB                              | 158                     |
| Booting                        | 19              | Filter                           | 158                     |
| Boundary clock                 | 142             | Filter table                     | 158, 169                |
| Broadcast                      | 156, 158, 161   | First installation               | 27                      |
| <b>C</b>                       |                 | Flash memory                     | 62, 77                  |
| CD-ROM                         | 260, 266        | Flow control                     | 191                     |
| CIDR                           | 34              | Forwarding database              | 158                     |
| CLI Banner                     | 129             | <b>G</b>                         |                         |
| Classless Inter-Domain Routing | 34              | Gateway                          | 30, 38                  |
| Class Selector                 | 179             | Generic object classes           | 284                     |
| Clock                          | 139             | GMRP                             | 161, 169                |
| Clock synchronization          | 141             | GMRP per port                    | 172                     |
| Closed circuit                 | 222             | Grandmaster                      | 139                     |
| Cold start                     | 78              | <b>H</b>                         |                         |
| Command Line Interface         | 21              | HaneWin                          | 260, 266                |
| Configuration                  | 62              | Hardware address                 | 44                      |
| Configuration changes          | 214             | Hardware clock (buffered)        | 132                     |
| Configuration data             | 43, 51, 60, 67  | Hardware reset                   | 214                     |
| Configuration file             | 48, 63, 64      | HIPER-Ring (source for alarms)   | 218                     |
| Connection error               | 88              |                                  |                         |

|                                                      |                     |                                           |                    |
|------------------------------------------------------|---------------------|-------------------------------------------|--------------------|
| HiDiscovery                                          | 39, 109             | <b>O</b>                                  |                    |
| HiView                                               | 24                  | Object classes                            | 284                |
| Host address                                         | 30                  | Object description                        | 284                |
|                                                      |                     | Object ID                                 | 284                |
| <b>I</b>                                             |                     | Offline configuration                     | 64                 |
| IANA                                                 | 29                  | Operation monitoring                      | 222                |
| IEEE 1588 time                                       | 133                 | Option 82                                 | 28, 51, 266        |
| IEEE 802.1 Q                                         | 176                 | Ordinary clock                            | 142                |
| IEEE MAC Address                                     | 242                 | Out-of-band                               | 21                 |
| IGMP                                                 | 163                 | Overload protection                       | 191                |
| IGMP Querier                                         | 164                 |                                           |                    |
| IGMP Snooping                                        | 161, 163            | <b>P</b>                                  |                    |
| Industrial HiVision                                  | 12, 49              | P2P                                       | 142                |
| Industry Protocols                                   | 11                  | Password                                  | 22, 69, 96, 97     |
| Instantiation                                        | 284                 | Peer-to-Peer                              | 142                |
| Internet Assigned Numbers Authority                  | 29                  | PHB                                       | 179                |
| Internet service provider                            | 29                  | Phy                                       | 141                |
| In-band                                              | 21                  | Polling                                   | 214                |
| IP Address                                           | 29, 37, 44, 48, 244 | Port authentication                       | 113                |
| IP header                                            | 175, 178, 179       | Port Configuration                        | 87                 |
| IP Parameter                                         | 27                  | Port Mirroring                            | 249                |
| ISO/OSI layer model                                  | 34                  | Port Priority                             | 181, 185           |
|                                                      |                     | PROFINET IO                               | 11                 |
| <b>J</b>                                             |                     | Precedence                                | 179                |
| Java Runtime Environment                             | 65                  | Precision Time Protocol                   | 139                |
| JRE                                                  | 65                  | Priority                                  | 176, 181           |
|                                                      |                     | Priority Queues                           | 175                |
| <b>L</b>                                             |                     | Priority tagged frames                    | 176                |
| LACNIC                                               | 29                  | Protocol stack                            | 141                |
| Leave                                                | 163                 | PTP                                       | 131, 133, 139      |
| Link monitoring                                      | 219, 222            | PTP Subdomains                            | 143                |
| Loading a script file from the ACA                   | 63                  |                                           |                    |
| Local clock                                          | 140                 | <b>Q</b>                                  |                    |
| Login banner                                         | 128                 | QoS                                       | 176                |
| Login window                                         | 25                  | Query                                     | 163                |
|                                                      |                     | Query function                            | 164                |
| <b>M</b>                                             |                     | Queue                                     | 182                |
| MAC                                                  | 141                 |                                           |                    |
| MAC destination address                              | 34                  | <b>R</b>                                  |                    |
| Maximum bandwidth                                    | 183                 | Rate Limiter Settings                     | 174                |
| Media module for modular devices (source for alarms) | 218                 | Real time                                 | 131, 175           |
| Message                                              | 214                 | Reboot                                    | 78                 |
| Mode                                                 | 87                  | Receiver power status (source for alarms) | 218                |
| Multicast                                            | 136, 158, 161, 163  | Receiving port                            | 159                |
| Multicast address                                    | 169                 | Redundancy                                | 11                 |
|                                                      |                     | Reference clock                           | 132, 135, 139, 146 |
| <b>N</b>                                             |                     | Relay contact                             | 222                |
| Netmask                                              | 30, 38              | Release                                   | 73                 |
| Network address                                      | 29                  | Remote diagnostics                        | 222                |
| Network Management                                   | 49                  | Report                                    | 163, 247           |
| Network management station                           | 242                 | Request interval (SNTP)                   | 136                |
| Network topology                                     | 51                  | Reset                                     | 78                 |
|                                                      |                     | Restart                                   | 78                 |

# Index

---

|                                           |             |                                   |                    |
|-------------------------------------------|-------------|-----------------------------------|--------------------|
| RIPE NCC                                  | 29          | ToS                               | 175, 176, 178, 179 |
| Ring manager                              | 158         | TP cable diagnosis                | 233                |
| Ring/Network coupling (source for alarms) | 218         | Traffic Classes                   | 175, 182, 185      |
|                                           | 218         | Traffic Shaping                   | 183, 187, 187      |
| RMON probe                                | 249         | Training Courses                  | 295                |
| Router                                    | 12, 30      | Transmission reliability          | 214                |
|                                           |             | Transparent Clock                 | 142                |
| <b>S</b>                                  |             | Trap                              | 214, 217           |
| Segmentation                              | 214         | Trap target table                 | 214                |
| Service                                   | 247         | Trivial File Transfer Protocol    | 270                |
| Service provider                          | 29          | Trust dot1p                       | 181                |
| Service shell reactivation                | 281         | Trust ip-dscp                     | 181                |
| SFP Module (source for alarms)            | 218         | Type Field                        | 176                |
| SFP module                                | 240         | Type of Service                   | 178                |
| SFP status display                        | 240         |                                   |                    |
| Signal contact                            | 88, 222     | <b>U</b>                          |                    |
| Signal contact (source for alarm)         | 218         | UDP                               | 124                |
| Signal runtime                            | 135         | Unicast                           | 161                |
| SNMP                                      | 24, 95, 214 | Untrusted                         | 181                |
| SNTP                                      | 131, 136    | Update                            | 18                 |
| SNTP client                               | 136         | USB stick                         | 75                 |
| SNTP server                               | 152         | User name                         | 22                 |
| Software                                  | 274         | UTC                               | 133                |
| Software release                          | 73          |                                   |                    |
| Source address                            | 156         | <b>V</b>                          |                    |
| SSH                                       | 21          | Video                             | 182                |
| Starting the graphical user interface     | 24          | VLAN                              | 176, 181, 194      |
| State on delivery                         | 62, 62, 95  | VLAN 0                            | 53                 |
| Static                                    | 158         | VLAN ID (network parameter)       | 52                 |
| Strict Priority                           | 182         | VLAN priority                     | 184                |
| Subdomains                                | 143         | VLAN tag                          | 176, 194           |
| Subidentifier                             | 284         | VLAN tunnel                       | 208                |
| Subnet                                    | 38, 157     | VoIP                              | 182                |
| Summer time                               | 132         | V.24                              | 21                 |
| Supply voltage                            | 218         |                                   |                    |
| Symbol                                    | 13          | <b>W</b>                          |                    |
| System Monitor                            | 18          | Web-based Interface               | 24                 |
| System Name                               | 48          | Weighted Fair Queuing             | 182, 183, 187      |
| System requirements (GUI)                 | 24          | Weighted Round Robin              | 182                |
| System time                               | 135, 136    | Winter time                       | 132                |
|                                           |             |                                   |                    |
| <b>T</b>                                  |             | <b>X</b>                          |                    |
| TAI                                       | 133         | XML (Offline Configurator Format) | 65                 |
| Target table                              | 214         |                                   |                    |
| TCP/IP stack                              | 271         |                                   |                    |
| Technical Questions                       | 295         |                                   |                    |
| Telnet                                    | 21          |                                   |                    |
| TFTP                                      | 270         |                                   |                    |
| TFTP Update                               | 81          |                                   |                    |
| Time difference                           | 133         |                                   |                    |
| Time Management                           | 139         |                                   |                    |
| Time Stamp Unit                           | 141, 145    |                                   |                    |
| Time zone                                 | 132         |                                   |                    |
| Topology                                  | 51          |                                   |                    |



## 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.

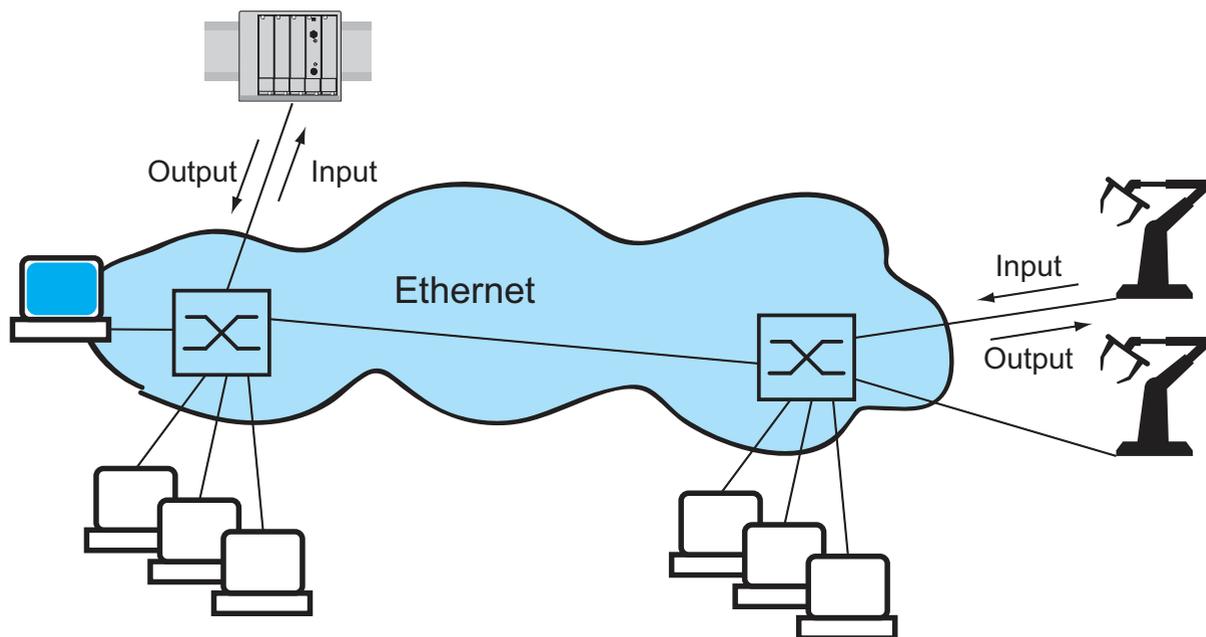


Figure 1: Example of communication.

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.

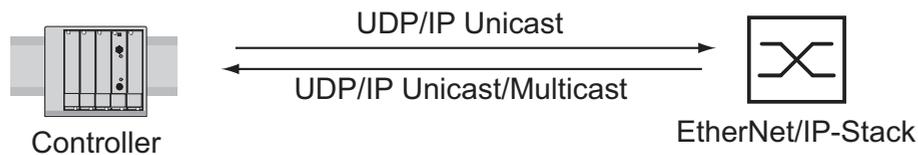
| Parameter          | Dialog                                             | Action                                                  |
|--------------------|----------------------------------------------------|---------------------------------------------------------|
| PROFINET IO        | Advanced:Industrial<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.

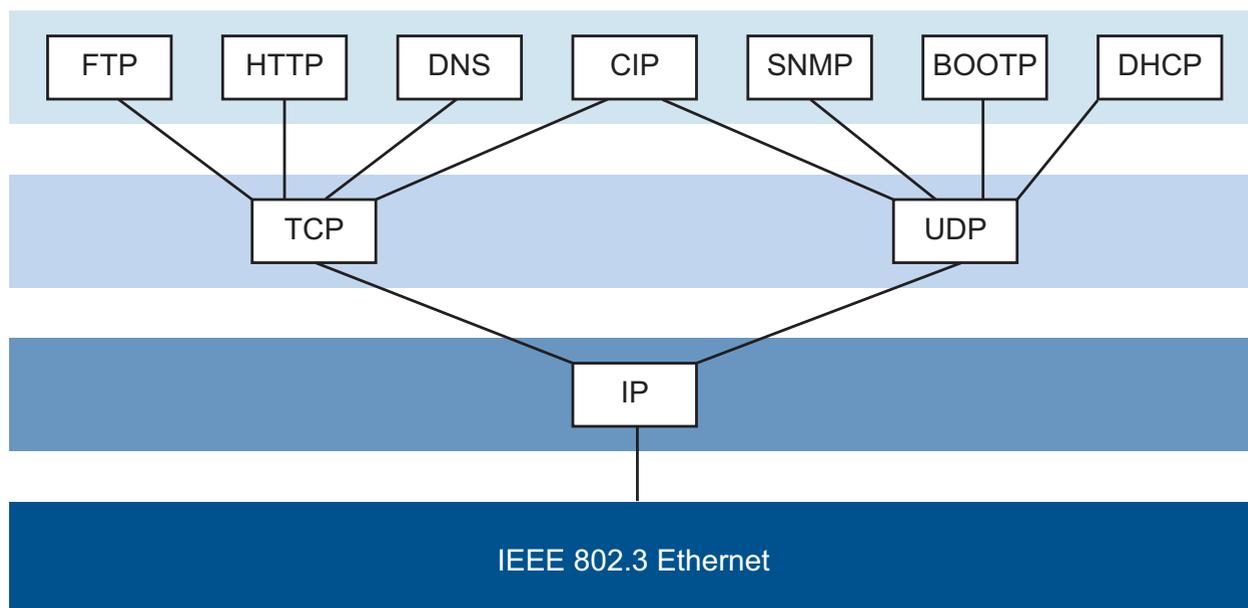


Figure 3: EtherNet/IP (CIP) in the ISO/OSI reference model

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*

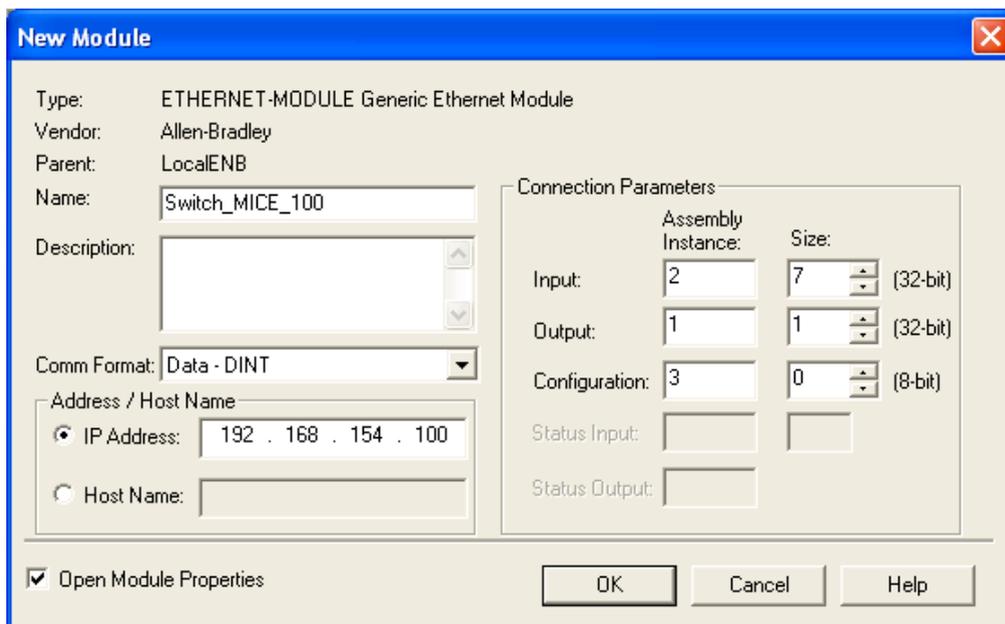


Figure 4: Integrating a new module into Logix 5000

- In the module properties, enter a value of at least 100 ms for the Request Packet Interval (RPI).

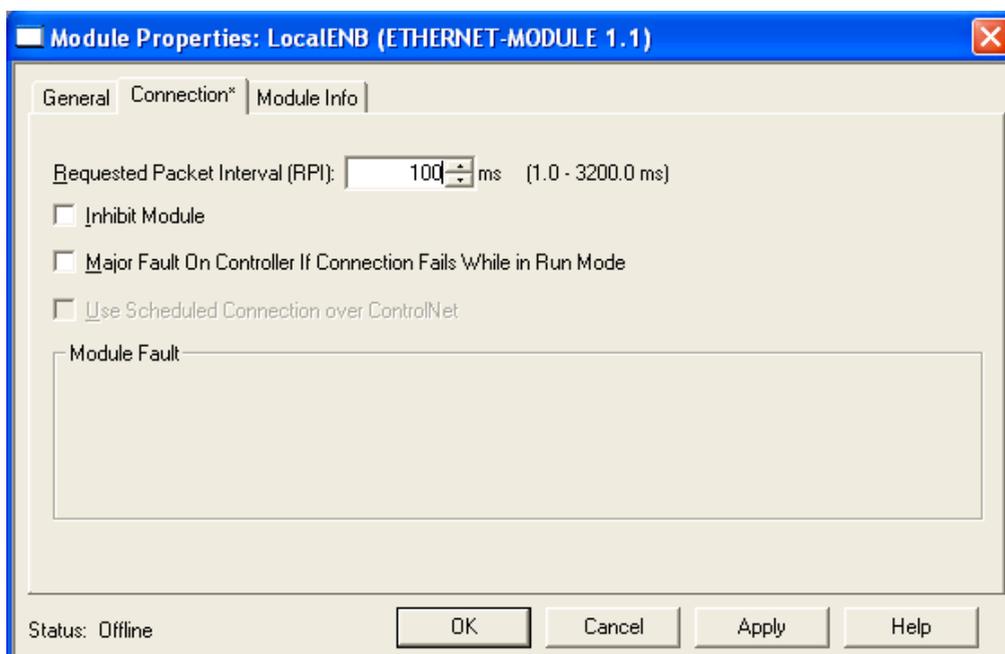


Figure 5: Module properties for the Request Packet Interval (RPI)

**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 (95<sub>H</sub>) 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

| Id  | Attribute               | Access rule | Data type                                                                                                                                    | Description                                                                                                    |
|-----|-------------------------|-------------|----------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------|
| 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<br>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 Interface 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.

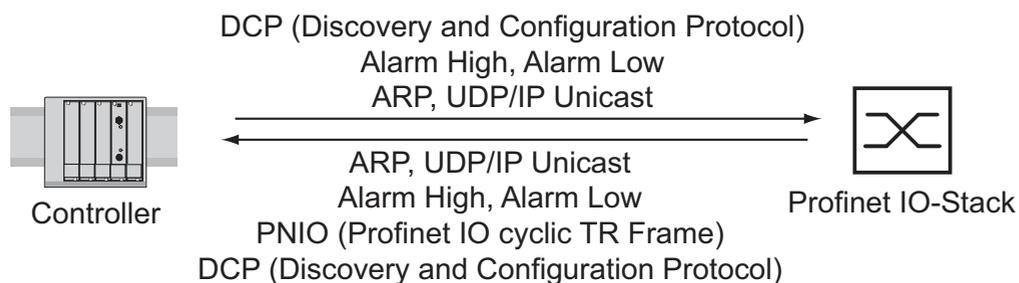


Figure 6: Communication between the Controller and the Switch

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.

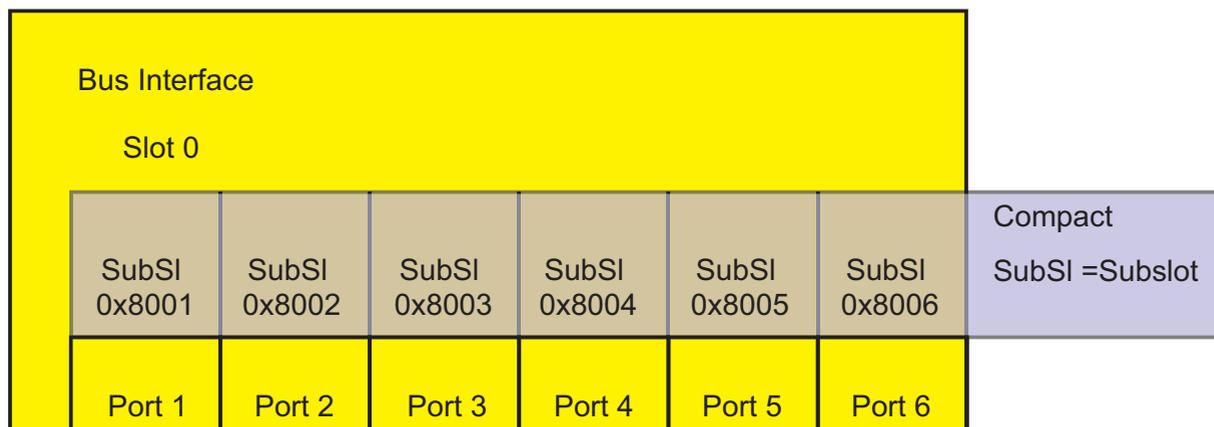


Figure 7: Compact Switch

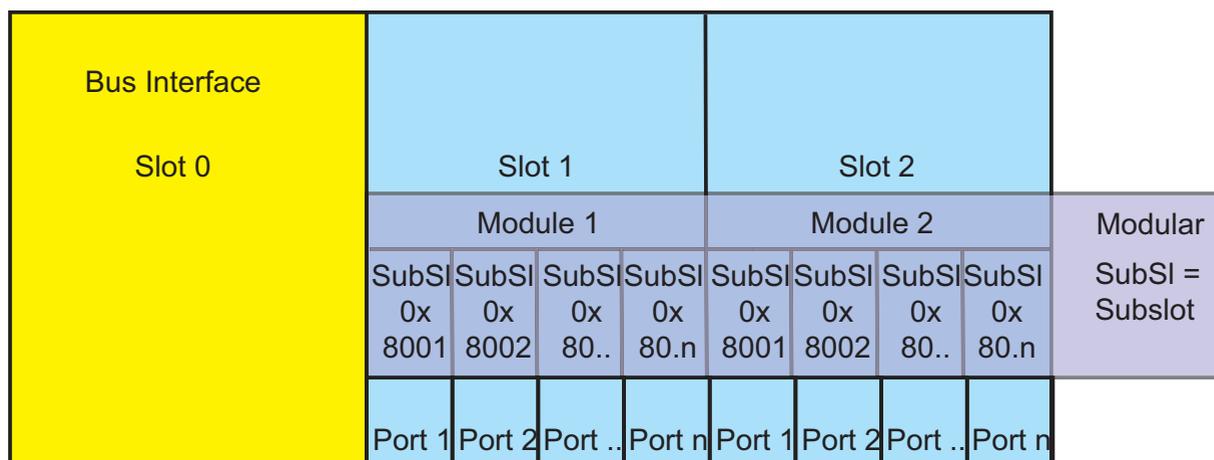


Figure 8: Modular Switch

## ■ **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.

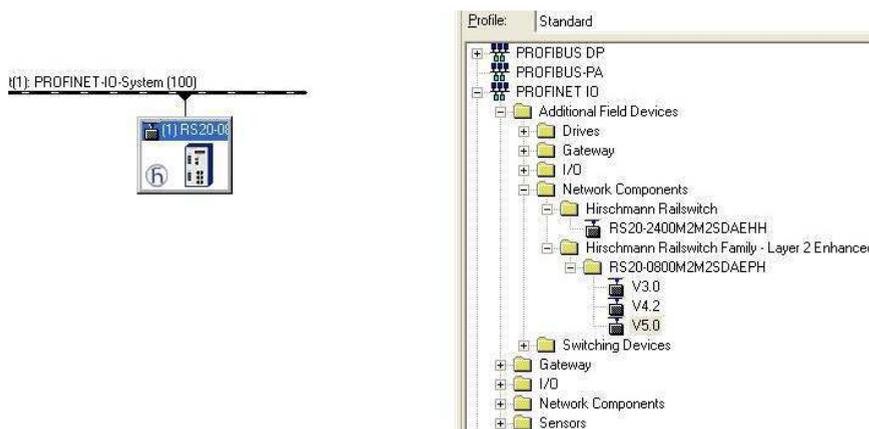


Figure 9: Adding a Switch from the Simatic S7 library

- To give the Switch its name, select the Switch and in the menu bar choose Target System:Ethernet>Edit Ethernet Participants...

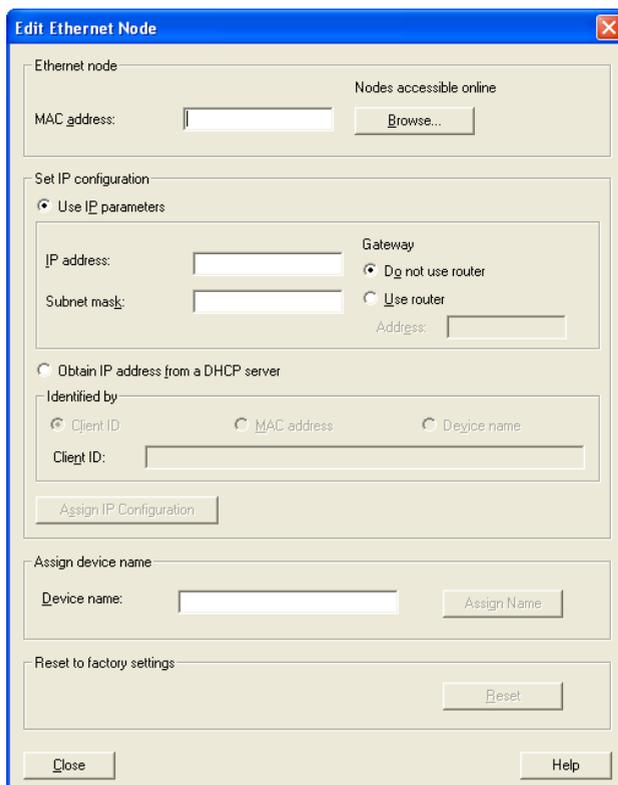
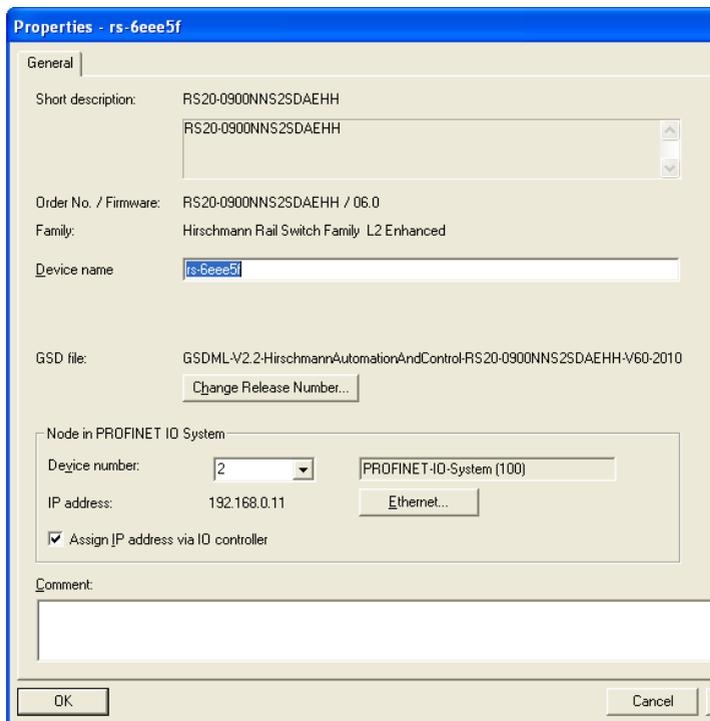


Figure 10: Dialog for entering the Switch name

- 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.

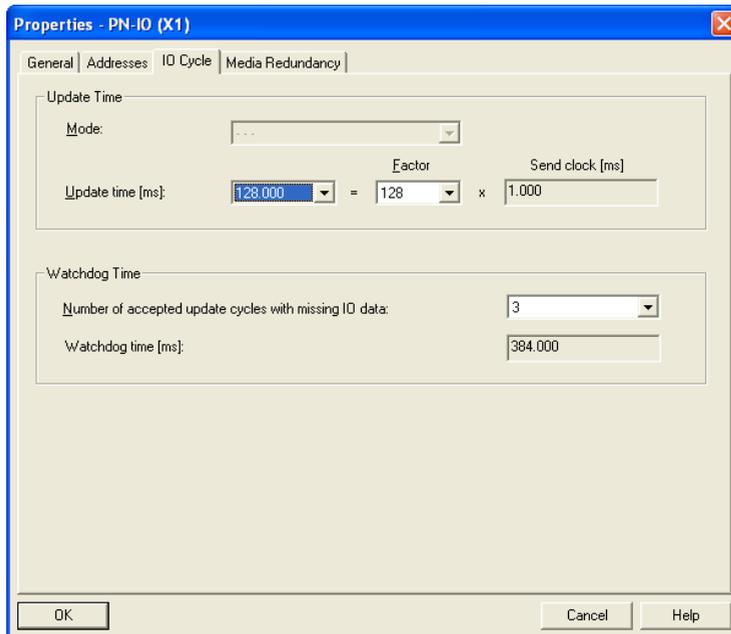


Figure 12: Dialog for entering the IO Cycle

- 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.

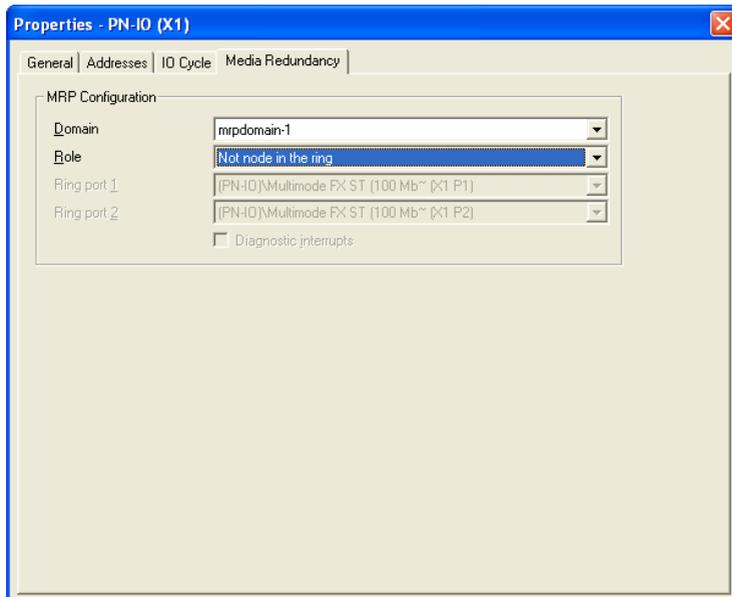


Figure 13: Dialog for entering the Media redundancy

- 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.

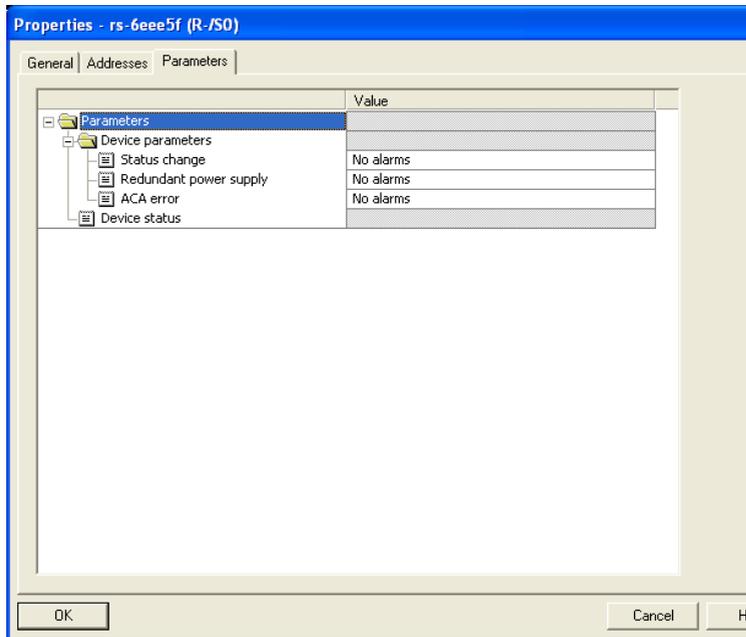


Figure 14: Configuring device alarms for e.g. RS20/RS30.

## ■ 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).

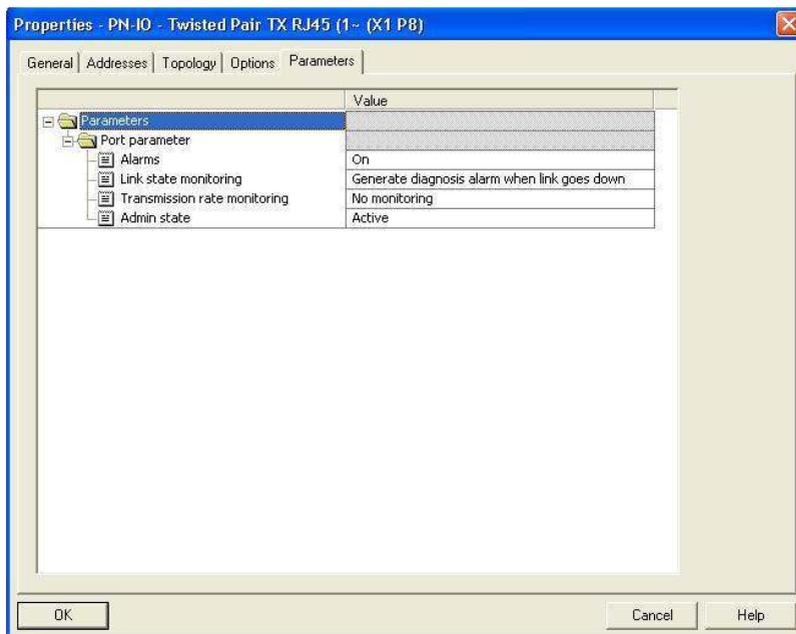


Figure 15: Port properties

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`.

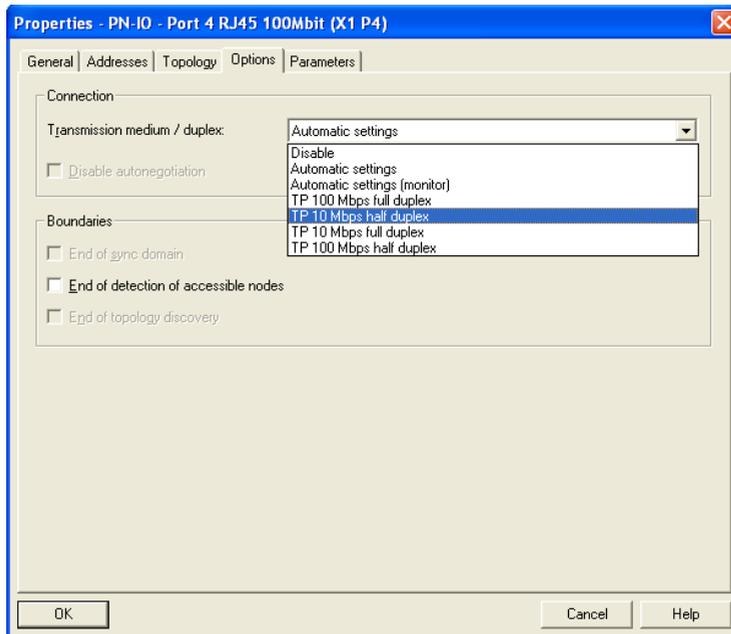


Figure 16: Dialog for entering the connection options

- 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`.

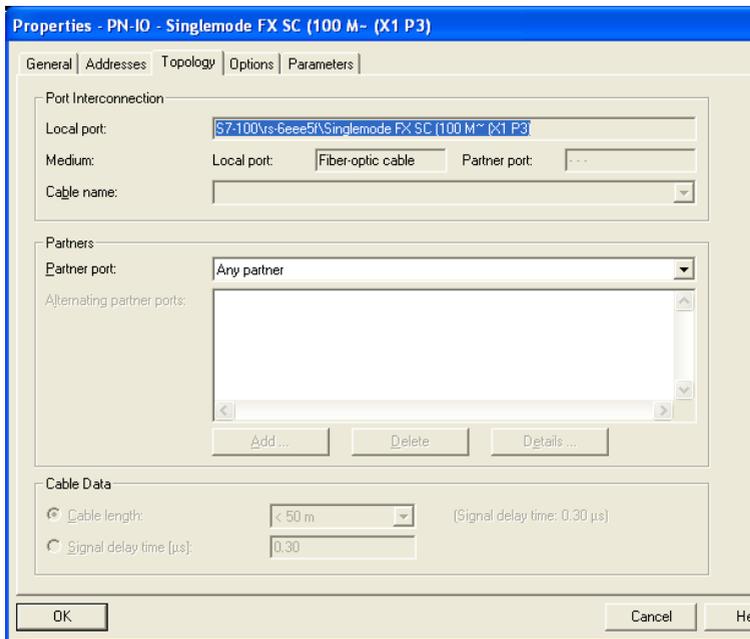


Figure 17: Dialog for entering the topology

- 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.

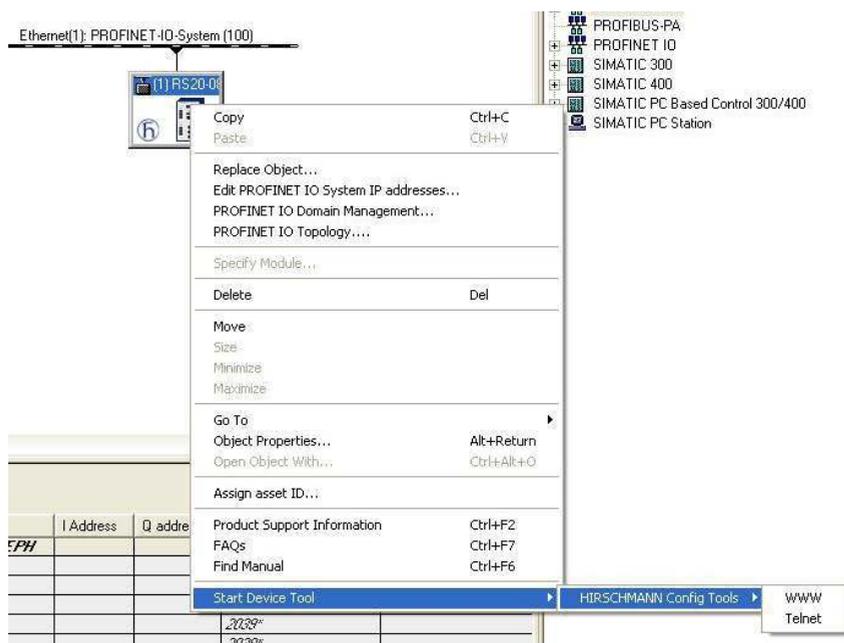


Figure 18: Call up the Hirschmann operating program

### 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.

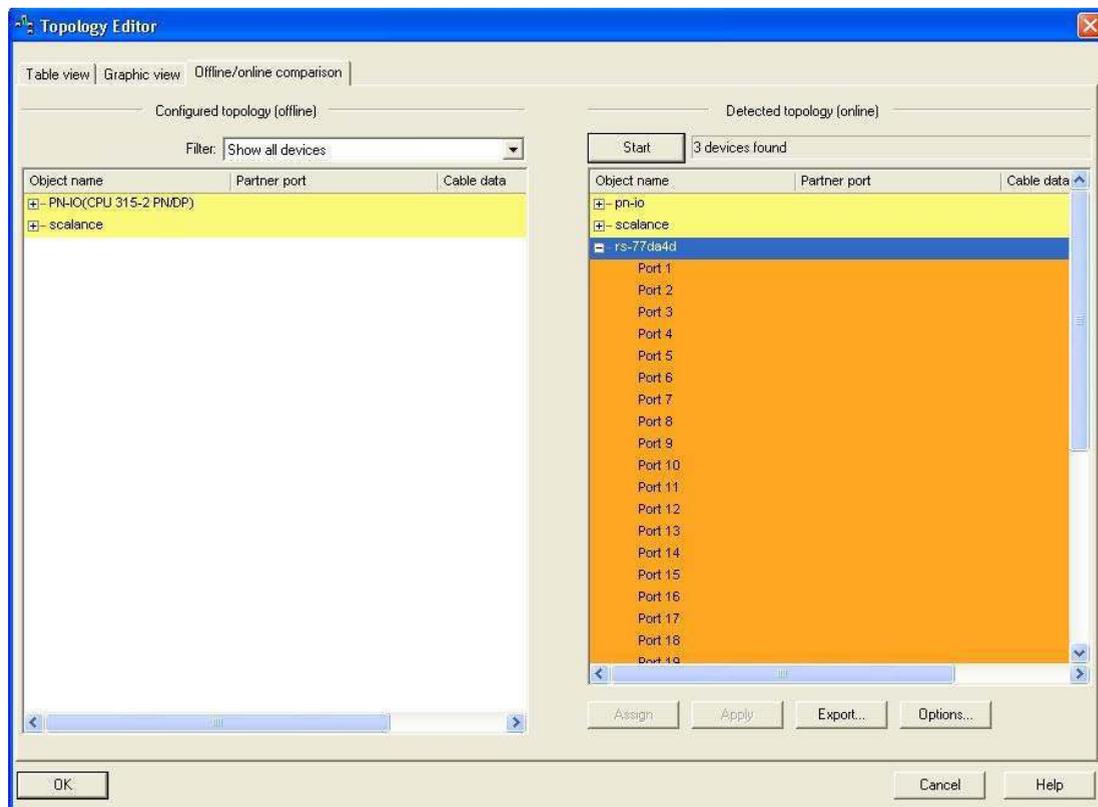


Figure 19: Topology Discovery

### ■ 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.

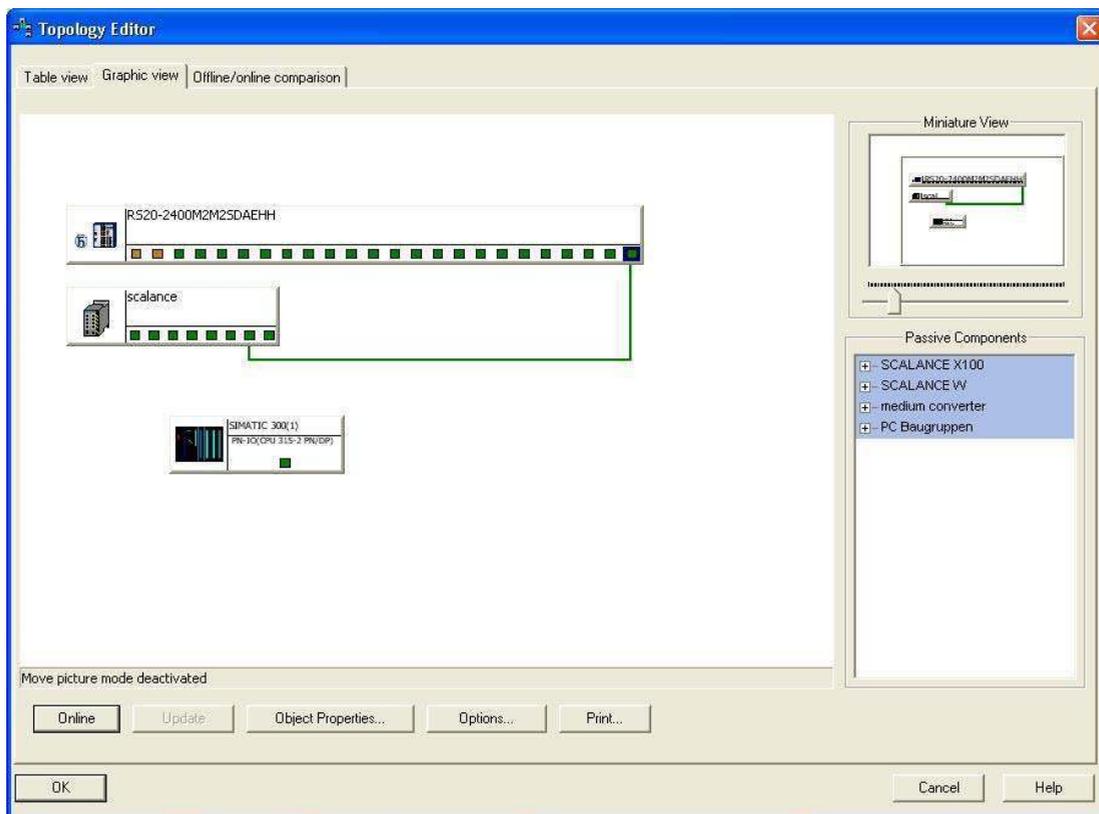


Figure 20: Configuring the topology

## ■ Communication diagnosis

Simatic S7 monitors the communication quality and outputs messages relating to communication problems.

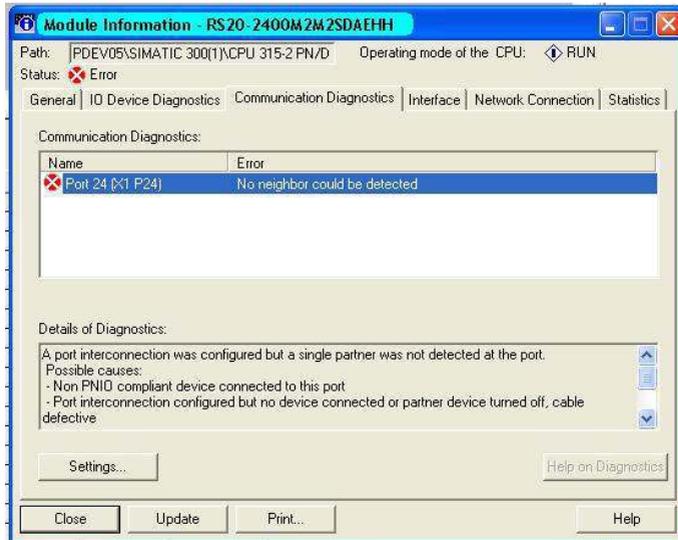
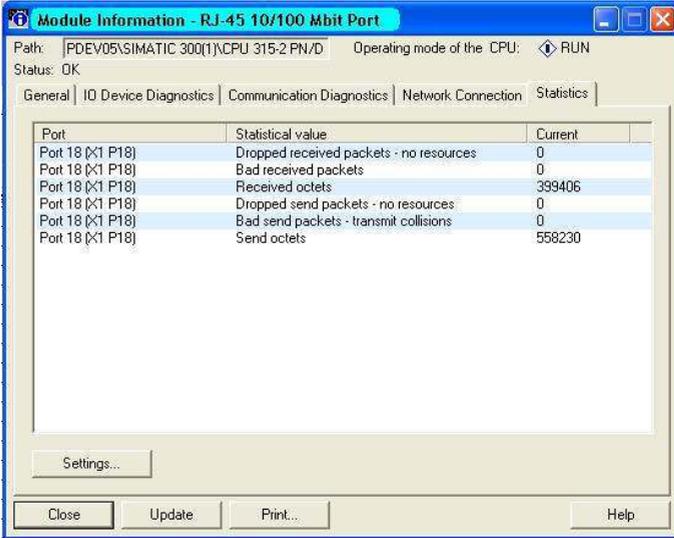


Figure 21: Diagnosis messages for the communication between the Switches and IO devices

### ■ 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 path is "PDEV05\SIMATIC 300(1)\CPU 315-2 PN/D" and the operating mode of the CPU is "RUN". The status is "OK". The window has tabs for "General", "IO Device Diagnostics", "Communication Diagnostics", "Network Connection", and "Statistics". The "Statistics" tab is active, displaying a table with the following data:

| 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    | 7                             | Not used              |  |
|           |      |                               | 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   |  |
| Input     | 2    | 6                             | Power supply unit 7   |  |
|           |      | 7                             | Power supply unit 8   |  |
|           |      |                               | Supply voltage status |  |
|           |      | 0                             | HIPER-Ring            |  |
|           |      | 1                             | Ring/Network coupling |  |
|           |      | 2                             | Connection error      |  |
|           |      | 3                             | Not used              |  |
|           |      | 4                             | Not used              |  |
| Output    |      | 5                             | Not used              |  |
|           |      | 6                             | Not used              |  |
|           |      | 7                             | Not used              |  |
|           |      |                               | 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.

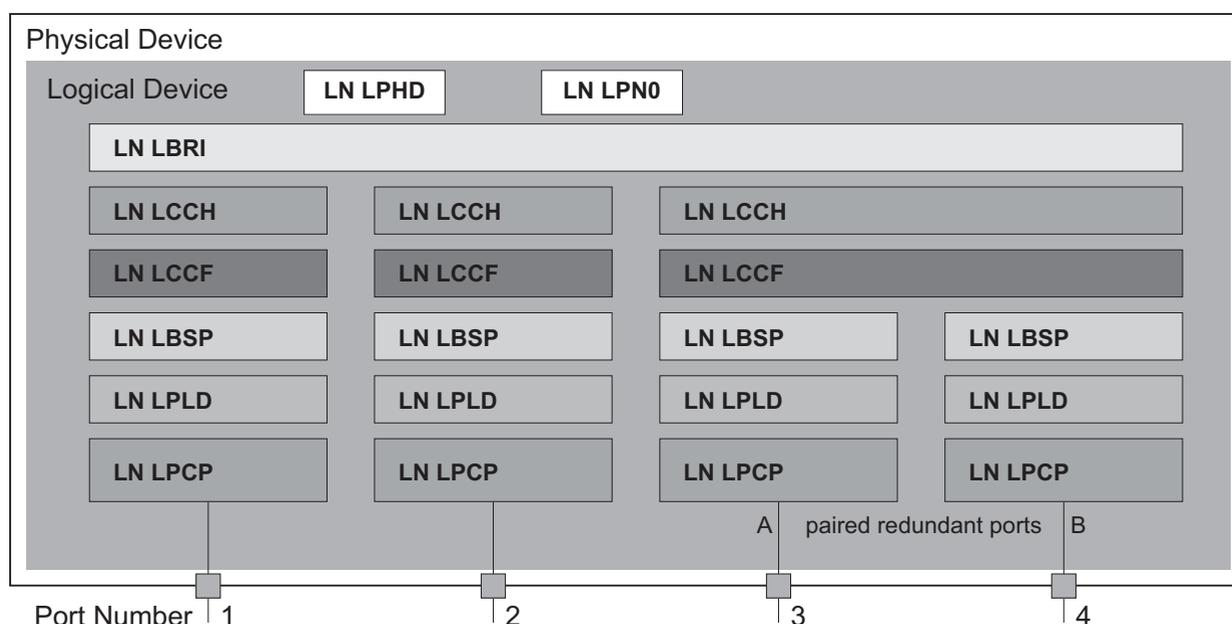


Figure 23: Bridge model based on Technical Report IEC 61850 90-4

| 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**

**PowerMICE, MACH 104, MACH 1040, MACH 4000**

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>7</b>  |
|          | <b>About this Manual</b>                            | <b>9</b>  |
|          | <b>Key</b>                                          | <b>11</b> |
| <b>1</b> | <b>Introduction</b>                                 | <b>13</b> |
| 1.1      | Overview of Redundancy Topologies                   | 14        |
| 1.2      | Overview of Redundancy Protocols                    | 16        |
| <b>2</b> | <b>Link Aggregation</b>                             | <b>19</b> |
| 2.1      | Example of link aggregation                         | 20        |
|          | 2.1.1 Creating and configuring the link aggregation | 21        |
| 2.2      | HIPER-Ring and Link Aggregation                     | 26        |
| <b>3</b> | <b>Ring Redundancy</b>                              | <b>29</b> |
| 3.1      | Example of a HIPER-Ring                             | 31        |
|          | 3.1.1 Setting up and configuring the HIPER-Ring     | 33        |
| 3.2      | Example of a MRP-Ring                               | 37        |
| <b>4</b> | <b>Multiple Rings</b>                               | <b>43</b> |
| 4.1      | Sub-Ring                                            | 44        |
|          | 4.1.1 Sub-Ring description                          | 44        |
|          | 4.1.2 Sub-Ring example                              | 48        |
|          | 4.1.3 Sub-Ring example configuration                | 51        |
| <b>5</b> | <b>Ring/Network Coupling</b>                        | <b>55</b> |
| 5.1      | Variants of the ring/network coupling               | 56        |
| 5.2      | Preparing a Ring/Network Coupling                   | 58        |
|          | 5.2.1 STAND-BY switch                               | 58        |
|          | 5.2.2 One-Switch coupling                           | 61        |
|          | 5.2.3 Two-Switch coupling                           | 67        |
|          | 5.2.4 Two-Switch Coupling with Control Line         | 75        |

|          |                                                         |            |
|----------|---------------------------------------------------------|------------|
| <b>6</b> | <b>Spanning Tree</b>                                    | <b>83</b>  |
| 6.1      | The Spanning Tree Protocol                              | 85         |
| 6.1.1    | The tasks of the STP                                    | 85         |
| 6.1.2    | Bridge parameters                                       | 86         |
| 6.1.3    | Bridge Identifier                                       | 86         |
| 6.1.4    | Root Path Cost                                          | 87         |
| 6.1.5    | Port Identifier                                         | 89         |
| 6.2      | Rules for Creating the Tree Structure                   | 90         |
| 6.2.1    | Bridge information                                      | 90         |
| 6.2.2    | Setting up the tree structure                           | 90         |
| 6.3      | Example of determining the root path                    | 93         |
| 6.4      | Example of manipulating the root path                   | 95         |
| 6.5      | Example of manipulating the tree structure              | 97         |
| 6.6      | The Rapid Spanning Tree Protocol                        | 98         |
| 6.6.1    | Port roles                                              | 98         |
| 6.6.2    | Port states                                             | 101        |
| 6.6.3    | Spanning Tree Priority Vector                           | 102        |
| 6.6.4    | Fast reconfiguration                                    | 102        |
| 6.6.5    | Configuring the Rapid Spanning Tree                     | 103        |
| 6.7      | Combining RSTP and MRP                                  | 112        |
| 6.7.1    | Application example for the combination of RSTP and MRP | 114        |
| <b>7</b> | <b>VRRP/HiVRRP</b>                                      | <b>117</b> |
| 7.1      | VRRP/HiVRRP Configuration                               | 118        |
| 7.1.1    | General settings                                        | 118        |
| 7.1.2    | VRRP instance settings                                  | 119        |
| 7.1.3    | Setting up the VRRP router instance                     | 121        |
| 7.1.4    | Configuring the VRRP router instance                    | 122        |
| 7.1.5    | Deleting a VRRP router instance                         | 122        |
| 7.2      | HiVRRP Domains                                          | 123        |
| 7.2.1    | Displaying HiVRRP domains                               | 123        |
| 7.2.2    | HiVRRP domain instances at different ports              | 124        |
| 7.3      | Statistics                                              | 125        |
| 7.3.1    | VRRP statistic for all ports                            | 125        |
| 7.3.2    | VRRP statistics per port                                | 125        |
| 7.4      | Tracking                                                | 127        |
| 7.4.1    | Deleting a tracking object                              | 128        |

|          |                          |            |
|----------|--------------------------|------------|
| <b>A</b> | <b>Readers' Comments</b> | <b>129</b> |
| <b>B</b> | <b>Index</b>             | <b>131</b> |
| <b>C</b> | <b>Further Support</b>   | <b>133</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 “Routing Configuration User Manual” document contains the information you need to start operating the routing function. The manual enables you to configure your router by following the examples.

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:

- ▶ Link Aggregation
- ▶ HIPER-Ring
- ▶ MRP-Ring
- ▶ Sub-Ring (RSR20, RSR30 and MACH 1000)
- ▶ Ring/Network coupling
- ▶ Rapid Spanning Tree Algorithm (RSTP)
- ▶ VRRP/HiVRRP

# 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<br>Sub-Ring (RSR20, RSR30, PowerMICE, MACH 1000 and MACH 4000)                  | Ring redundancy: a Basis-Ring with a Sub-Ring or an MRP-Ring with an RSTP-Ring.                                                                                                 |
| Topology with 3 non-nested loops          | RSTP<br>Ring Redundancy<br>Sub-Ring (RSR20, RSR30, PowerMICE, MACH 1000 and MACH 4000)<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 |
| Topology with nested loops                | RSTP<br>Sub-Ring (RSR20, RSR30, PowerMICE, MACH 1000 and MACH 4000)<br>Ring coupling                    | Ring coupling only couples non-nested rings, though these can couple local Sub-Rings.                                                                                           |

*Table 1: Overview of Redundancy Topologies*

The Ring Redundancy Protocol MRP has particular properties to offer:

- ▶ You have the option of nesting MRP-Rings. A coupled ring is known as a Sub-Ring ([see on page 44 “Sub-Ring”](#)).
- ▶ You have the option of coupling to MRP-Rings other ring structures that work with RSTP ([see on page 112 “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 83 “Spanning Tree”</a> ).                                    |
| HIPER-Ring                                                  | Ring                                                                                                      | typically 80 ms, up to < 500 ms or < 300 ms (selectable)<br>- 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)<br>- 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 83 “Spanning Tree”</a> ). |
| Sub-Ring (RSR20, RSR30, PowerMICE, MACH 1000 and MACH 4000) | Ring segment coupled to a primary ring                                                                    | typically 80 ms, up to < 500 ms or < 200 ms (selectable)<br>- the number of switches has a minimal effect on the switch over time                                                                                                                                                   |
| Link Aggregation                                            | Coupling of network segments via parallel active lines with dynamic load distribution and line redundancy |                                                                                                                                                                                                                                                                                     |
| VRRP/HiVRRP                                                 | Any structure; provides terminal devices with redundancy for default gateway                              | < 400 ms with HiVRRP                                                                                                                                                                                                                                                                |

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 Link Aggregation

The LACP (Link Aggregation Control Protocol based on IEEE 802.3ad) is a network protocol for dynamically bundling physical network connections. The added bandwidth of all connection lines is available for data transmission. In the case of a connection breaking down, the remaining connections take over the entire data transmission (redundancy). The load distribution between the connection lines is performed automatically.

You configure a link aggregation by combining at least 2 existing parallel redundant connection lines (known as a trunk) between two devices into one logical connection. You can use link aggregation to combine up to 8 (optimally up to 4) connection lines between devices into a trunk.

Any combination of twisted pair and F/O cables can be used as the connection lines of a trunk. Configure the connections so that the data rates and the duplex settings of the related ports are matching.

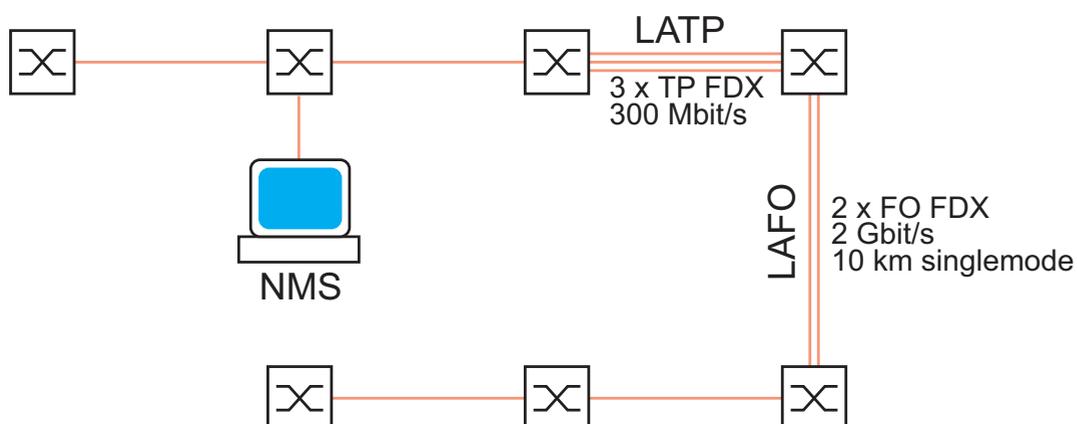
The maximum that can exit a device are

- 2 trunks for rail devices with 4 ports,
- 4 trunks for rail and MICE devices with 8-10 ports,
- 7 trunks for all other devices.

## 2.1 Example of link aggregation

In a network consisting of seven devices in a line topology, there are two segments with a particularly large amount of data traffic. You therefore decide to set up link aggregations in these segments. As well as dividing the load over several lines, you also get increased reliability in these segments through the redundant lines.

The link aggregation LATP (Link Aggregation Twisted Pair) consists of 3 twisted pair lines, and the link aggregation LAFO (Link Aggregation Fiber Optic) consists of 2 glass fiber lines.



*Figure 1: Example of link aggregation*  
*NMS = Network Management Station*  
*LATP = Link Aggregation Twisted Pair*  
*LAFO = Link Aggregation Fiber Optic*

The following example describes the configuration of the LATP link aggregation. For this link aggregation, you provide three free twisted pair ports at each of the two participating devices. (Connection: Module1 Port1 to Port3).

## 2.1.1 Creating and configuring the link aggregation

**Note:** A link aggregation connects exactly 2 devices.

You configure the link aggregation on each of the 2 devices involved. During the configuration phase, you connect only one single connection line between the devices. This is to avoid loops.

- Under `Basic Settings:Port Configuration`, you configure all three connections so that the transmission rate and the duplex settings of the participating ports on both devices are matching.
- Among the devices involved in a link aggregation, you define that device that has the most devices between itself and the device to which the configuration PC/(NMS network management station) is connected. You begin the configuration at this device, otherwise the Link Aggregation Control Protocol (LACP) can block ports and disconnect devices from the network, so that they cannot be configured any more.
- In the example below (see figure 2), you configure the link aggregation first on device 3, then on device 2. If you accidentally disconnect device 3 from the network, you can access it again by selecting “Allow static link aggregation” in the `Redundancy: Link Aggregation` dialog, or by activating this option via the CLI.

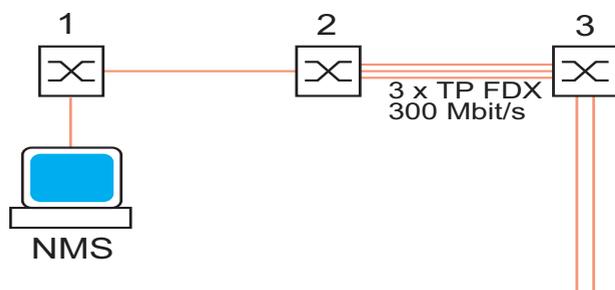


Figure 2: Example: “Defining the first device”  
NMS = Network Management Station

- Proceed as follows to configure a link aggregation from 3 twisted pair lines on device 3:

- Select the Redundancy:Link Aggregation (see figure 3) dialog.

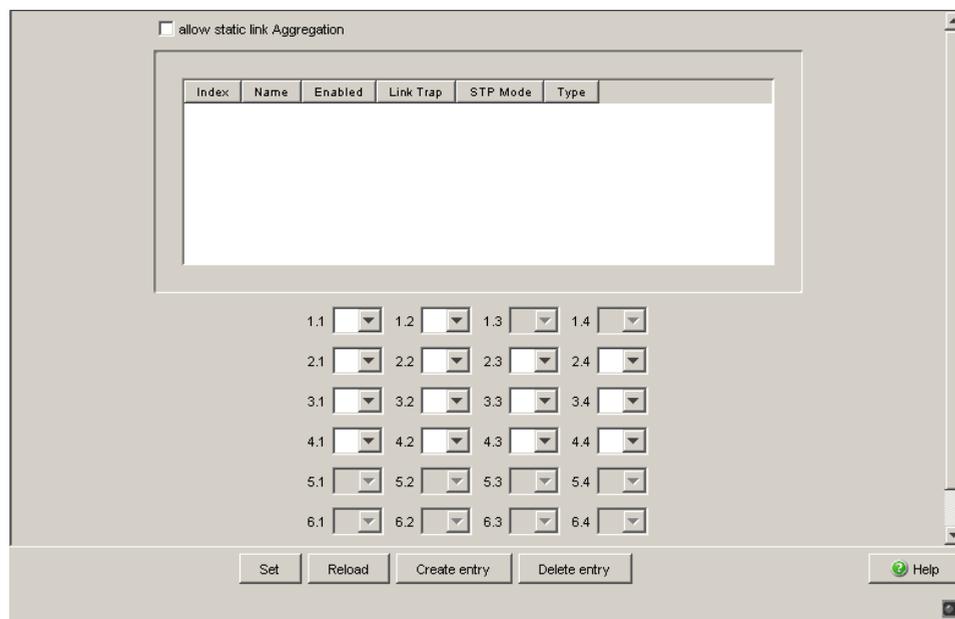


Figure 3: Creating the link aggregation

- Select Allow static link aggregation if the partner device does not support the Link Aggregation Control Protocol (LACP) (e.g. MACH 3000).
- Click “Create entry” to create a new link aggregation.
- The `Index` column shows you the ID under which the device uses a link aggregation (a trunk) as a virtual port. The device creates the port in module 8, which does not physically exist, and the first link aggregation then has the ID 8.1.
- The `Name` column allows you to give this connection any name you want. In this example, you give the new link aggregation the name “LAPT”.
- The `Enabled` column allows you to enable/disable a link aggregation that has been set up. Leave the checkmark in the “Enabled” column while you are using the link aggregation.

- Leave the checkmark in the `Link Trap` column if you want the device to generate an alarm if all the connections of the link aggregation are interrupted.
  - In the “STP Mode” column, you select `on` if the link aggregation connection is connected to a Spanning Tree, `off` if no Spanning Tree is active, or if the link aggregation is a segment of a HIPER-Ring.
  - “Type” shows whether you created this link aggregation manually (Allow static link aggregation is selected), or whether it was created dynamically using LACP (Allow static link aggregation is not selected).
- Note:** If there are multiple connections between devices that support LACP, and if Allow static link aggregation is nevertheless selected, `dynamic` is still displayed, because in this case the devices automatically switch to dynamic.

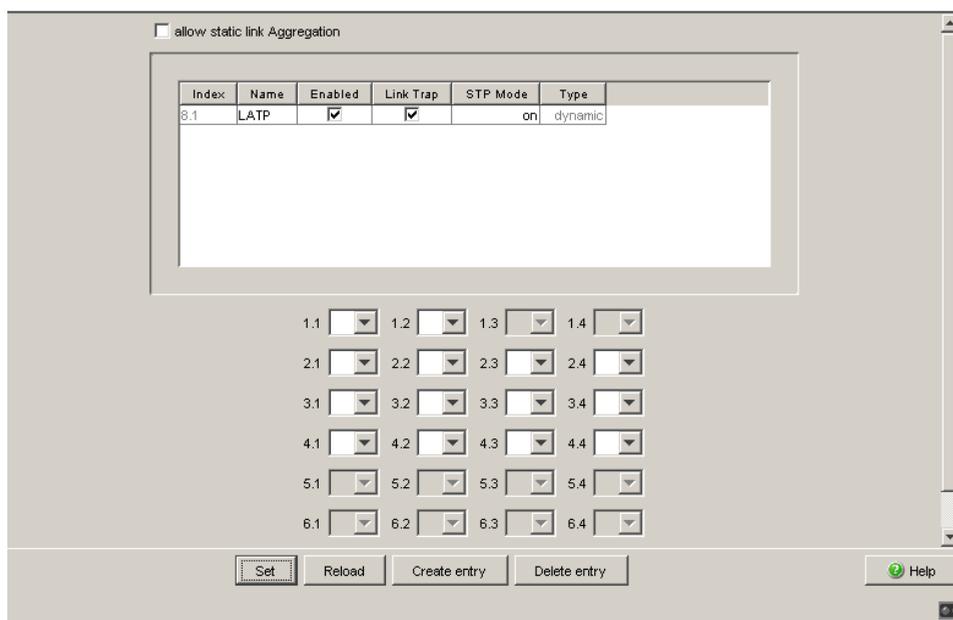


Figure 4: Link aggregation created and named.

- Now assign to the ports participating in the link aggregation (ports 1.1, 1.2 and 1.3) the index of the link aggregation connection LAPT (8.1). (see figure 5).

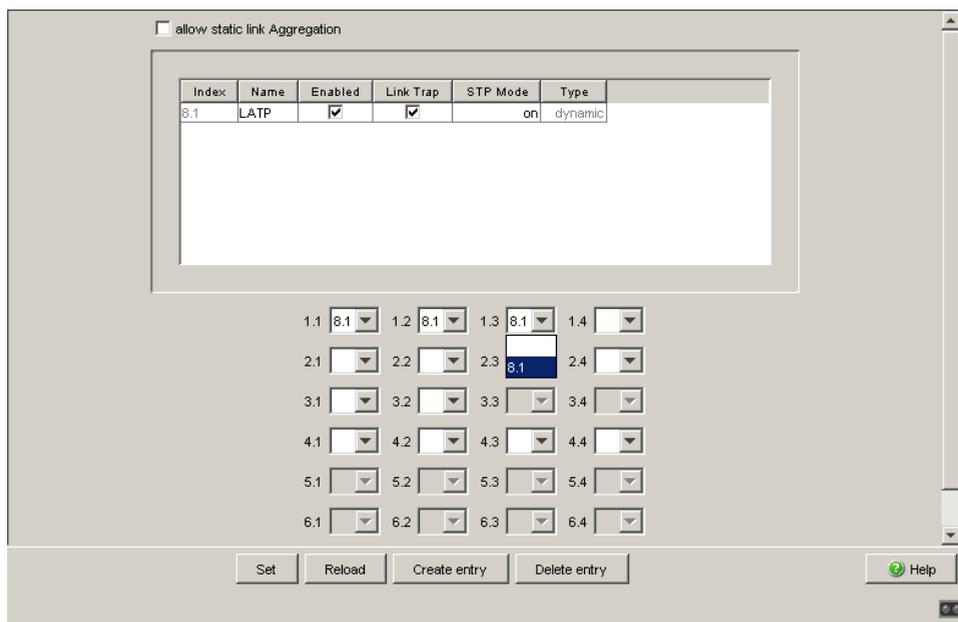


Figure 5: Assigning ports to link aggregation

```

enable
configure
link-aggregation LATP

New link aggregation created. Slot/port is 8.1.
Interface 1/1
addport 8/1
Interface 1/2
addport 8/1
Interface 1/3
addport 8/1
exit
show link-aggregation brief

Max. num. of LAGs: 7
Slot no. for LAGs: 8
Static Capability: Disabled
Logical Link-Aggr.
Interface Name Link State Mbr Ports Active Ports

8/1 LATP Down 1/1,1/2, 1/3

```

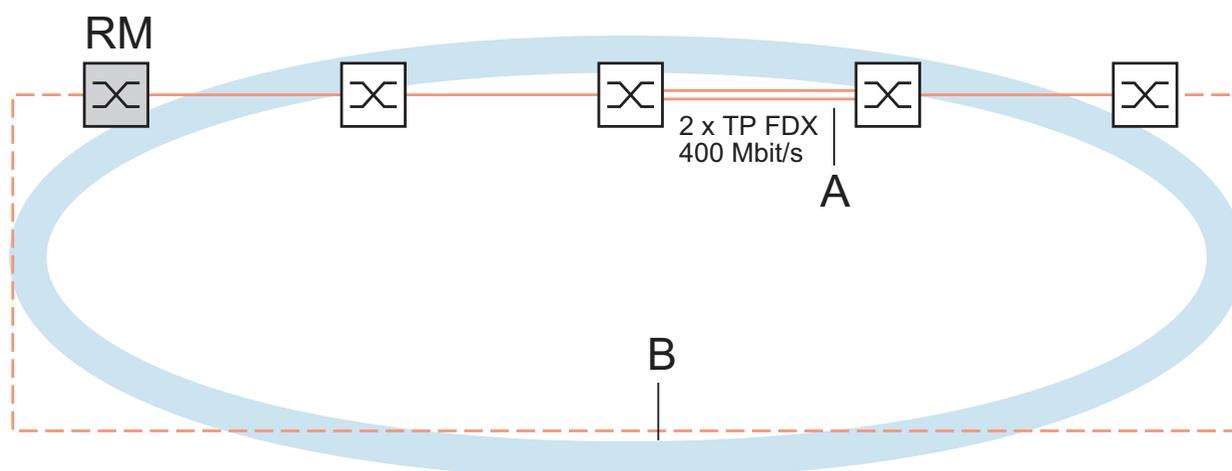
- Now you configure the partner device (device 2) in the same way.
- After the configuration, you connect the other connection line(s) between the devices.

**Note:** Exclude the combination of a link aggregation with the following redundancy procedures:

- ▶ Network/Ring coupling
- ▶ MRP-Ring
- ▶ Sub-Ring

## 2.2 HIPER-Ring and Link Aggregation

To increase the availability on particularly important connections, you can combine the HIPER-Ring (see on page 29 “Ring Redundancy”) and link aggregation redundancy functions.



*Figure 6: Example of a HIPER-Ring / link aggregation combination*  
RM = Ring Manager  
A = link aggregation  
B = HIPER-Ring

The above example shows a HIPER-Ring. One link aggregation forms a segment of the ring. When all the connection lines of the link aggregation are interrupted, the HIPER-Ring function activates the redundant line of the ring.

**Note:** If you want to use a link aggregation in a HIPER-Ring, you first configure the link aggregation, then the HIPER-Ring. In the HIPER-Ring dialog, you enter the index of the desired link aggregation as the value for the module and the port (8.x). Ascertain that the respective ring port belongs to the selected link aggregation.

**Note:** Deactivate RSTP when link aggregations are segments of a HIPER-Ring.



### 3 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.

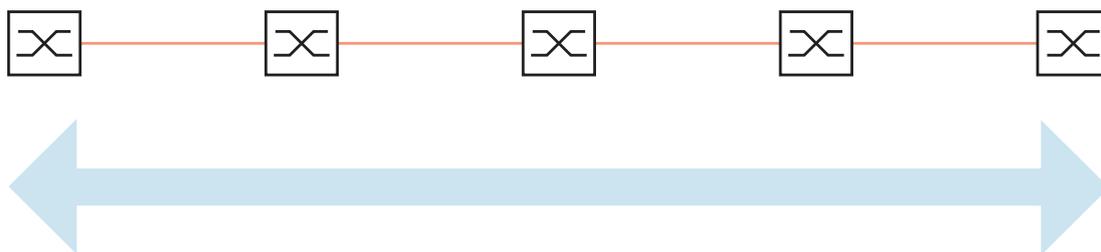


Figure 7: Line structure

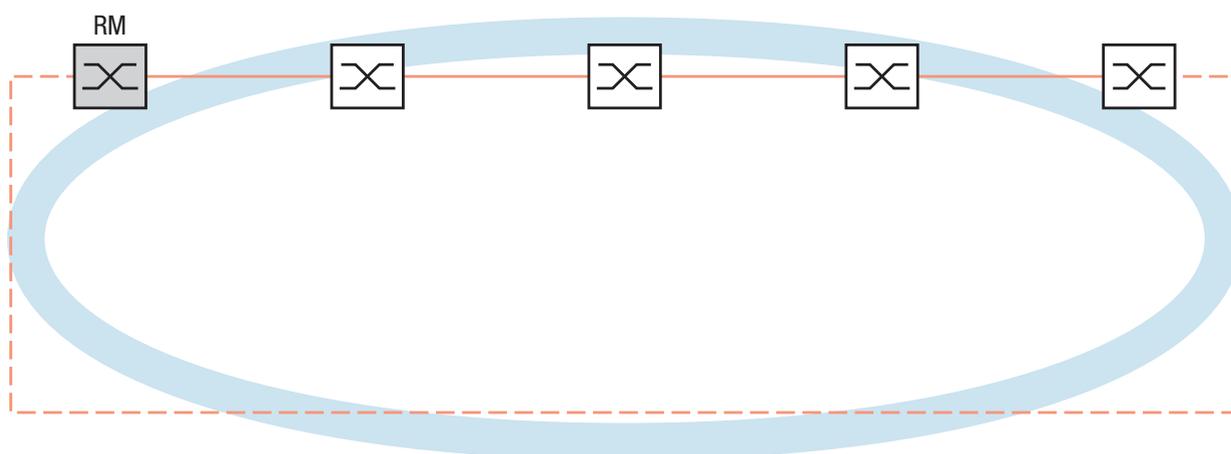


Figure 8: Redundant ring structure

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 (**M**edia **R**edundancy **P**rotocol) Ring (IEC 62439) of up to 50 devices typically transforms back to a line structure within 80 ms (adjustable to max. 200 ms/500 ms).

Devices with HIPER-Ring function capability:

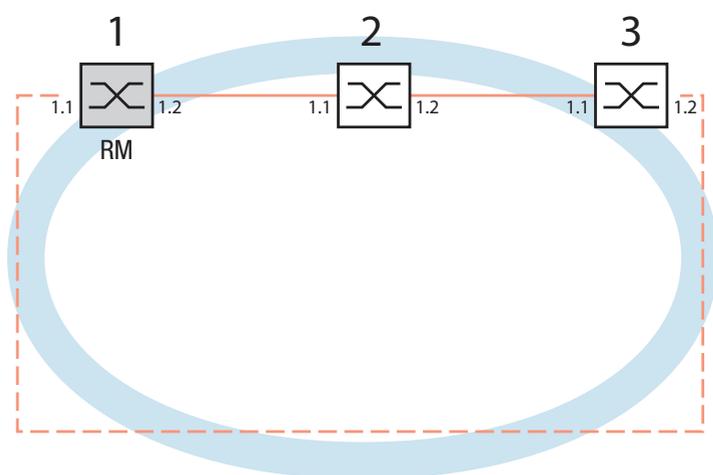
- ▶ Within a HIPER-Ring, you can use any combination of the following devices:
  - RS1
  - RS2-./.
  - RS2-16M
  - RS2-4R
  - RS20, RS30, RS40
  - RSR20, RSR30
  - OCTOPUS
  - MICE
  - MS20, MS30
  - PowerMICE
  - MACH 100
  - MACH 1000
  - MACH 1040
  - MACH 3000
  - MACH 4000
- ▶ Within an MRP-Ring, 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.

## 3.1 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 9: 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 the RS20/30/40, MS20/30 and PowerMICE Switches, 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.

### 3.1.1 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           | -                            |
| Optical   | 10 Gbit/s  | -                                               | on           | 10 Gbit/s full duplex (FDX)  |

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 10: 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.

## 3.2 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.

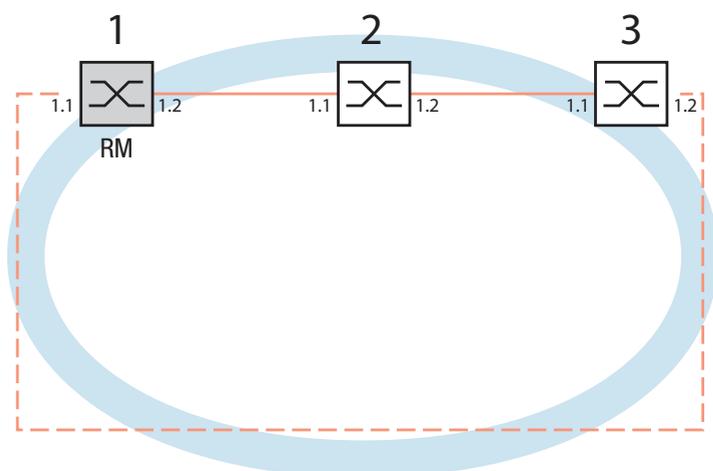


Figure 11: Example of MRP-Ring  
RM = Ring Manager  
— main line  
- - - redundant line

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           | -                            |
| Optical   | 10 Gbit/s  | -                                               | on           | 10 Gbit/s full duplex (FDX)  |

*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 12: 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 ( $\mathbb{T}$ ) in the static VLAN table for all ring ports in this MRP-Ring.

**Note:** If you want to use the RSTP ([see on page 83 “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.

## 4 Multiple Rings

The device allows you to set up multiple rings with different redundancy protocols:

- ▶ You have the option of nesting MRP-Rings. A coupled ring is known as a Sub-Ring ([see on page 44 “Sub-Ring”](#)).
- ▶ You have the option of coupling to MRP-Rings other ring structures that work with RSTP ([see on page 112 “Combining RSTP and MRP”](#)).

## 4.1 Sub-Ring

### 4.1.1 Sub-Ring description

**For the devices PowerMICE, MACH 1040 und MACH 4000.**

The Sub-Ring concept enables you to easily couple new network segments to suitable devices in existing redundancy rings (primary rings). The devices of the primary ring to which the new Sub-Ring is being coupled are referred to as Sub-Ring Managers (SRMs).

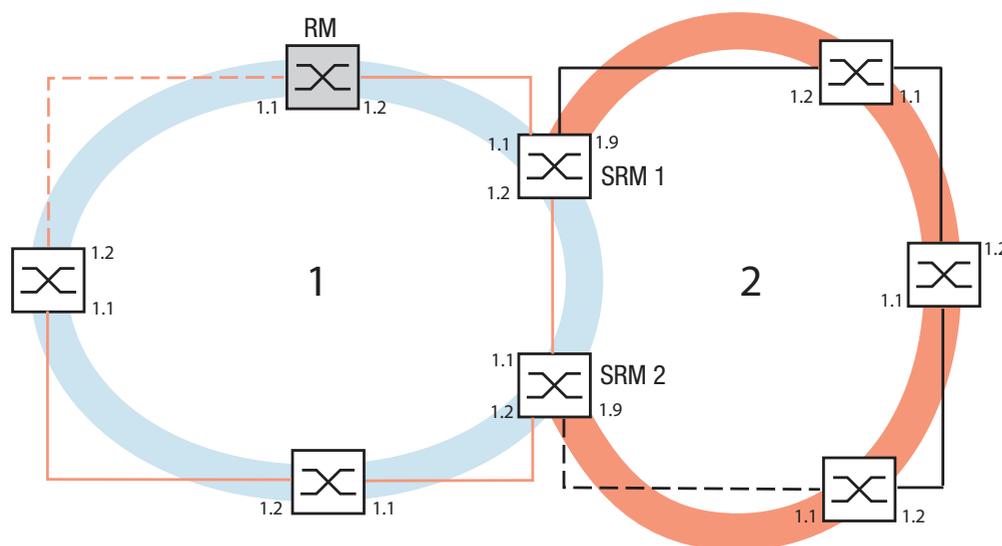


Figure 13: Example of a Sub-Ring structure

1 blue ring = basis ring

2 orange ring = Sub-Ring

SRM = Sub-Ring Manager

RM = Ring Manager

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

- MACH 1040
- MACH 4000
- PowerMICE

The SRM-capable devices support up to 4 SRM instances (MACH 1040 up to 16) and can thus be the Sub-Ring manager for up to 4 Sub-Rings at the same time (MACH 1040 for up to 16).

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

Each Sub Ring may consist of up to 200 participants. The SRMs themselves and the switches placed in the Base Ring between the SRMs do not count here.

Setting up Sub-Rings has the following advantages:

- ▶ Through the coupling process, you include the new network segment in the redundancy concept.
- ▶ You can easily integrate new company areas into existing networks.
- ▶ You easily map the organizational structure of a company in the network topology.
- ▶ As an MRP-Ring, the switching times of the Sub-Ring in redundancy cases are typically < 100 ms.

The following graphics show examples of possible Sub-Ring topologies:

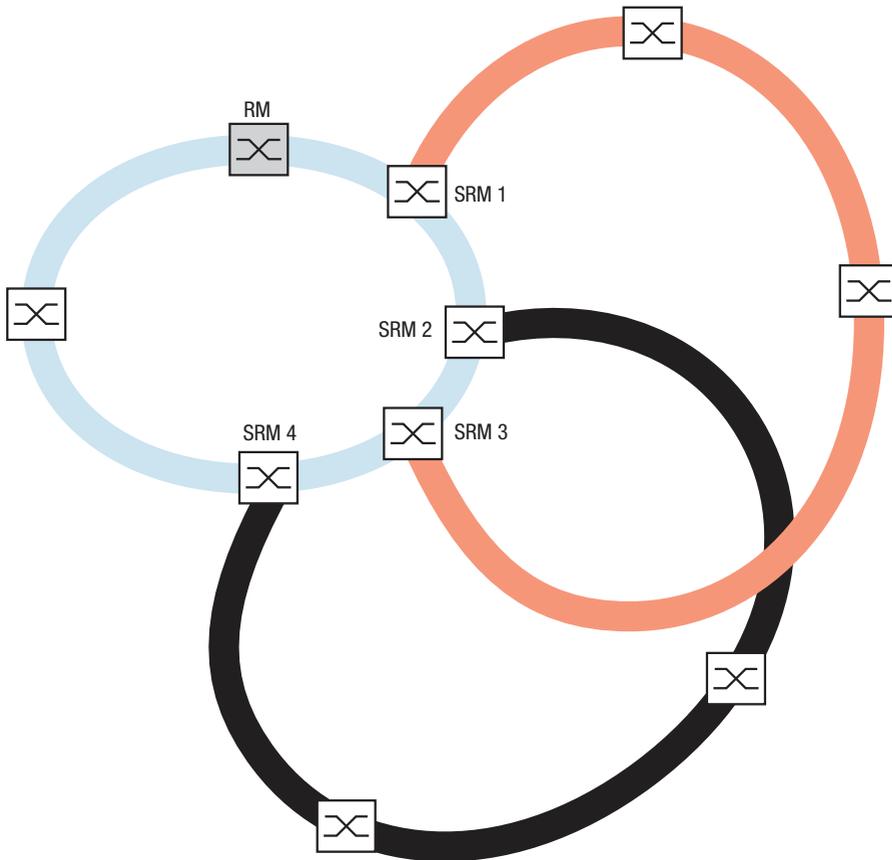
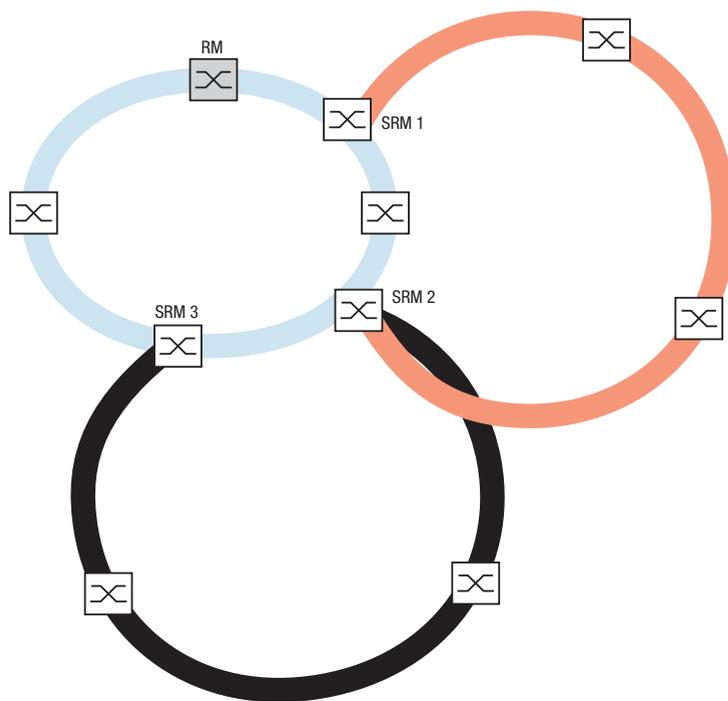
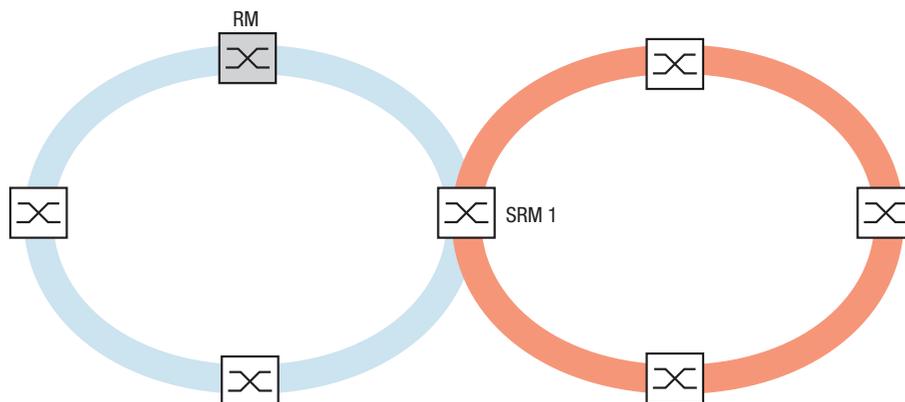


Figure 14: Example of an overlapping Sub-Ring structure



*Figure 15: Special case: a Sub-Ring Manager manages 2 Sub-Rings (2 instances). Depending on the device type, you can configure additional instances.*



*Figure 16: Special case: a Sub-Ring Manager manages both ends of a Sub-Ring at different ports (Single Sub-Ring Manager).*

**Note:** Connect Sub-Rings only to existing primary rings. Do not cascade Sub-Rings (i.e., a new Sub-Ring must not be connected to an existing Sub-Ring).

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

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

## 4.1.2 Sub-Ring example

You want to couple a new network segment with 3 devices to an existing redundant ring with the HIPER-Ring protocol. If you couple the network at both ends instead of only one end, this provides increased availability with the corresponding configuration.

The new network segment is connected as a Sub-Ring. The connection is made to existing devices of the basis ring with the following types:

- MACH 4000
- PowerMICE

Configure these devices as Sub-Ring Managers.

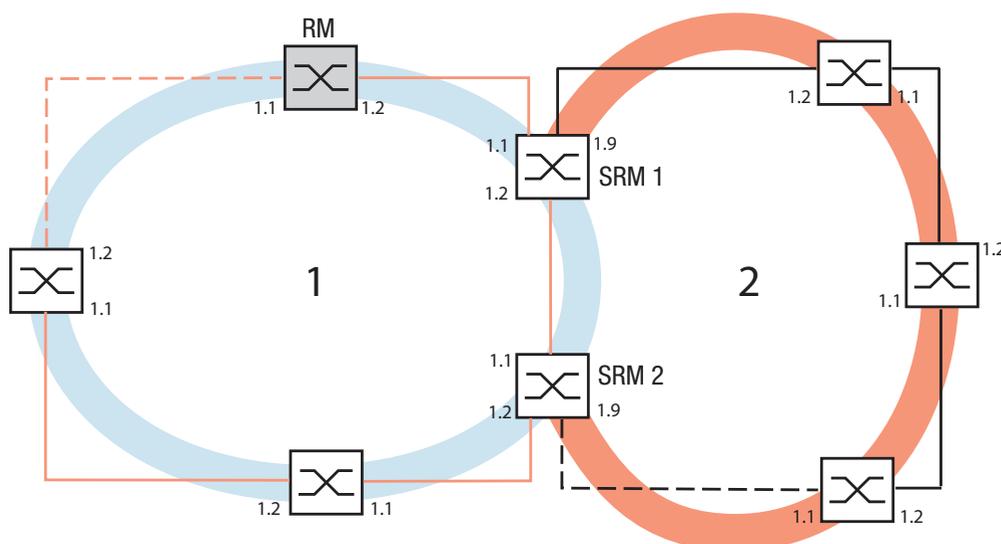


Figure 17: Example of a Sub-Ring structure

1 blue ring = basis ring

2 orange ring = Sub-Ring

SRM = Sub-Ring Manager

RM = Ring Manager

Proceed as follows to configure a Sub-Ring:

- Configure the three devices of the new network segment as participants in an MRP-Ring. This means:
  - Configure the transmission rate and the duplex mode for all the ring ports in accordance with 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           | -                            |
| Optical   | 10 Gbit/s  | -                                               | on           | 10 Gbit/s full duplex (FDX)  |

Table 5: Port settings for ring ports

□ Other settings:

- Define a different VLAN membership for the Primary Ring and the Sub-Ring even if the basis ring is using the MRP protocol, e.g. VLAN ID 1 for the Primary Ring and VLAN ID 2 for the Sub-Ring.
- For all ring ports in the Sub-Ring, select this VLAN ID and the VLAN membership Tagged (T) in the static VLAN table.
- Switch the MRP-Ring function on for all devices.
- In the Ring Redundancy dialog, under MRP-Ring, configure for all devices the two ring ports used in the Sub-Ring.
- Switch the Ring Manager function off for all devices.
- Do not configure link aggregation.
- Switch RSTP off for the MRP Ring ports used in the Sub-Ring.

**Note:** The MRP domain ID is a sequence of 16 numbers (range 0 to 255). The default domain (in the CLI: “default-domain“) is the MRP domain ID of 255 255 255 255 255 255 255 255 255 255 255 255 255 255 255 255. A MRP domain ID consisting entirely of zeroes is invalid.

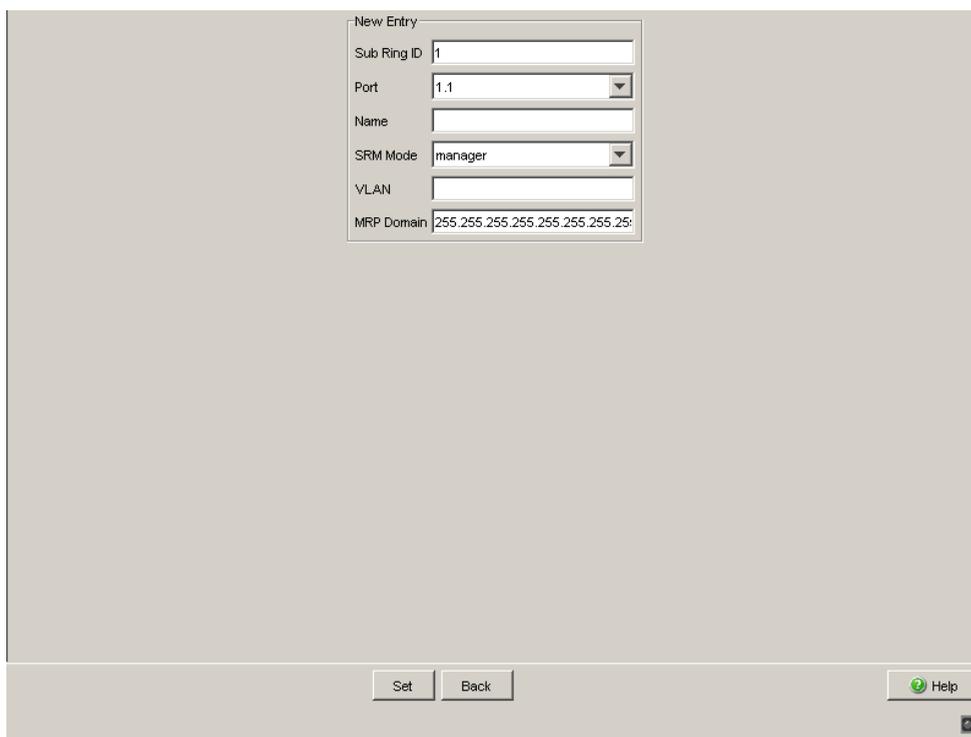
If you need to adjust the MRP domain ID, open the Command Line Interface (CLI) and proceed as follows:

|                                                                                                                                            |                                                                                                                                                                                          |
|--------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <pre>enable configure mrp delete-domain   current-domain</pre>                                                                             | <p>Change to the privileged EXEC mode.</p> <p>Change to the Configuration mode.</p> <p>Deletes the current MRP domain. If no MRP domain exists, the device outputs an error message.</p> |
| <pre>MRP current domain deleted: Domain ID:   255.255.255.255.255.255.255.255.255.255.255.255.255.255.255.255   (Default MRP domain)</pre> |                                                                                                                                                                                          |
| <pre>mrp new-domain   0.0.1.1.2.2.3.4.4.111.   222.123.0.0.66.99</pre>                                                                     | <p>Creates a new MRP domain with the specified MRP domain ID. You can subsequently access this domain with “current-domain”.</p>                                                         |
| <pre>MRP domain created: Domain ID: 0.0.1.1.2.2.3.4.5.111.222.123.0.0.66.99</pre>                                                          |                                                                                                                                                                                          |

### 4.1.3 Sub-Ring example configuration

Proceed as follows to configure the 2 Sub-Ring Managers in the example:

- Select the `Redundancy: Sub-Ring` dialog.
- Click the button "New".



The screenshot shows a 'New Entry' dialog box with the following fields and values:

| Field       | Value                       |
|-------------|-----------------------------|
| Sub Ring ID | 1                           |
| Port        | 1.1                         |
| Name        |                             |
| SRM Mode    | manager                     |
| VLAN        |                             |
| MRP Domain  | 255.255.255.255.255.255.255 |

Buttons at the bottom: Set, Back, Help.

*Figure 18: Sub-Ring – New Entry dialog*

- Enter the value "1" as the ring ID of this Sub-Ring.
- In the Module.Port field, enter the ID of the port (in the form X.X) that connects the device to the Sub-Ring (in the example, 1.9). For the connection port, you can use all the available ports that you have not already configured as ring ports of the basis ring.
- You have the option of entering a name for the Sub-Ring (in the example, "Test").

- Select the Sub-Ring Manager mode (SRM mode). You thus specify which connection between the primary ring and the Sub-Ring becomes the redundant line.

The options for the connection are:

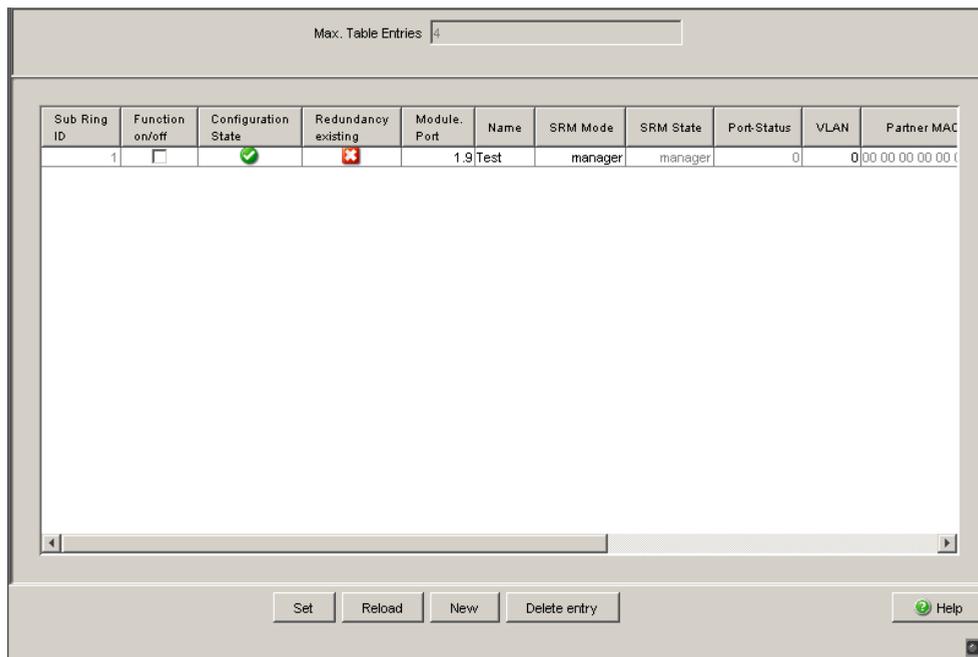
- ▶ Both Sub-Ring Managers have the same setting (default `manager`): - the device with the higher MAC address manages the redundant line.
- ▶ In the SRM Mode field, a device is selected to be the `redundant manager`: - this device manages the redundancy line as long as you have configured the other Sub-Ring Manager as a `manager`, otherwise the higher MAC address applies.

Configure Sub-Ring Manager 1 as the “manager” and Sub-Ring Manager 2 as the manager of the redundant line with “redundant manager”, in accordance with the overview drawing for this example.

- Leave the fields VLAN ID (default 0) and MRP Domain (default 255.255.255.255.255.255.255.255.255.255.255.255.255.255) as they are. The example configuration does not require any change here.
- Click "Set" to save the changes temporarily.
- Click “Back” to return to the Sub-Ring dialog.

|                                        |                                                            |
|----------------------------------------|------------------------------------------------------------|
| <code>enable</code>                    | Change to the privileged EXEC mode.                        |
| <code>configure</code>                 | Change to the Configuration mode.                          |
| <code>sub-ring new-ring 1</code>       | Creates a new Sub-Ring with the Sub-Ring ID 1.             |
| Sub-Ring ID created:ID: 1              |                                                            |
| <code>sub-ring 1 port 1/9</code>       | Defines port 9 in module 1 as the Sub-Ring port.           |
| Port set to 1/9                        |                                                            |
| <code>sub-ring 1 ring-name Test</code> | Assigns the name “Test” to Sub-Ring 1                      |
| Sub-Ring Ring name set to "Test"       |                                                            |
| <code>sub-ring 1 mode manager</code>   | Configures the mode of this Sub-Ring Manager as “manager”. |
| Mode of Switch set to manager          |                                                            |

- Click “Reload” to update the Sub-Ring overview and check all the entries.



*Figure 19: Completely configured Sub-Ring Manager*

- Configure the 2nd Sub-Ring Manager in the same way. If you have explicitly assigned SRM 1 the SRM mode `manager`, you configure SRM 2 as `redundant manager`. Otherwise, the assignment is performed automatically via the higher MAC address (see above)
- Switch the two Sub-Ring Managers on under “Function on/off” in the overview of the Sub-Ring dialog.
- Click "Set" to save the changes temporarily.
- 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.

```
enable
configure
sub-ring 1 operation enable
Operation set to Enabled
exit
show sub-ring
```

Change to the privileged EXEC mode.

Change to the Configuration mode.

Switches on the Sub-Ring with the Sub-Ring ID 1.

Change to the privileged EXEC mode.

Displays the state for all Sub-Rings on this device.



## 5 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

## 5.1 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 21). 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 27).

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 6).

|              | 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 6: 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 6](#)).

## 5.2 Preparing a Ring/Network Coupling

### 5.2.1 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 7: 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 | <p>According to the option selected</p> <ul style="list-style-type: none"> <li>- on "STAND-BY" DIP switch or in the</li> <li>- Redundancy:Ring/Network Coupling dialog, by making selection in "Select configuration".</li> </ul> <p><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.</p> |
| Software switch                   | In the Redundancy:Ring/Network Coupling dialog                                                                                                                                                                                                                                                                                                                                                                                                                  |

*Table 8: 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 20).

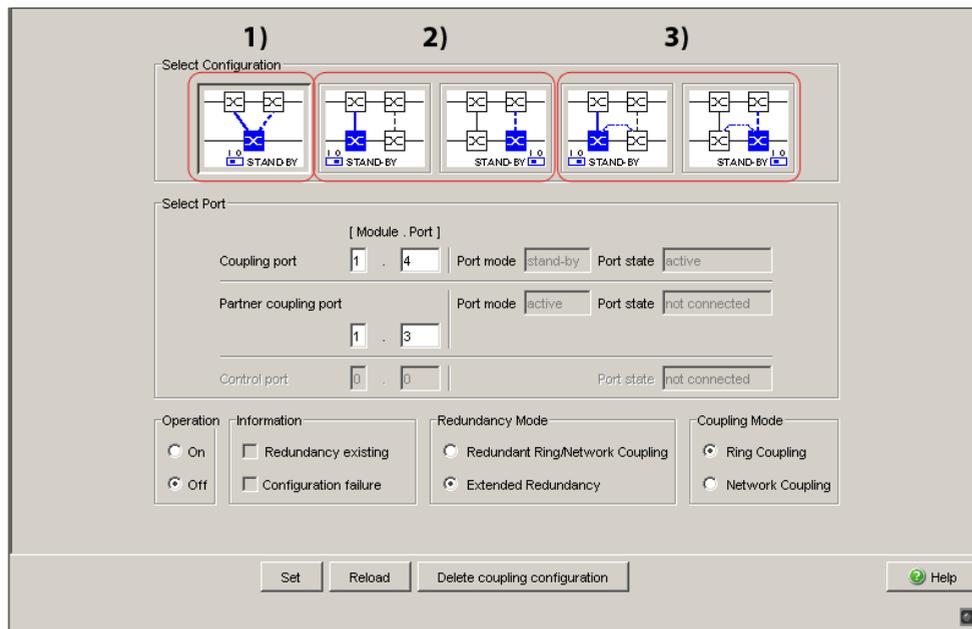


Figure 20: Choosing the ring coupling configuration (when the DIP switch is off, or for devices without a DIP switch)

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

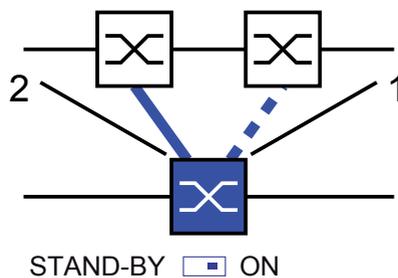
If the DIP switches are activated and you want to use the software to select one of the configurations that are not possible (grayed-out), you put the DIP switches on the device into another position and reload the dialog.

**Note:** Refrain from combining Rapid Spanning Tree and Ring/Network Coupling. Competing redundancy functions are ineligible.



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 22).



*Figure 22: 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 23).  
 .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 9](#).

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 9: 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 9: 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 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 9.

**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.

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.

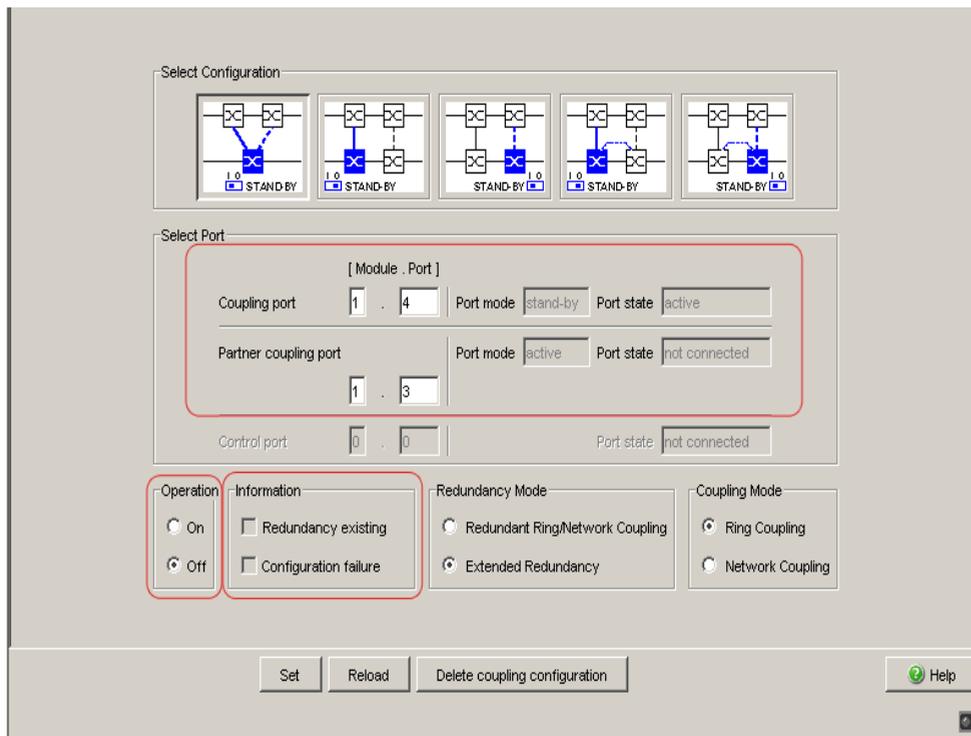


Figure 23: One-Switch coupling: Selecting the port and enabling/disabling operation

**Note:** The following settings are required for the coupling ports (you select the Basic Settings:Port Configuration dialog):  
See table 3 on page 33.

**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 24)
  - “Redundant Ring/Network Coupling” or
  - “Extended Redundancy”.

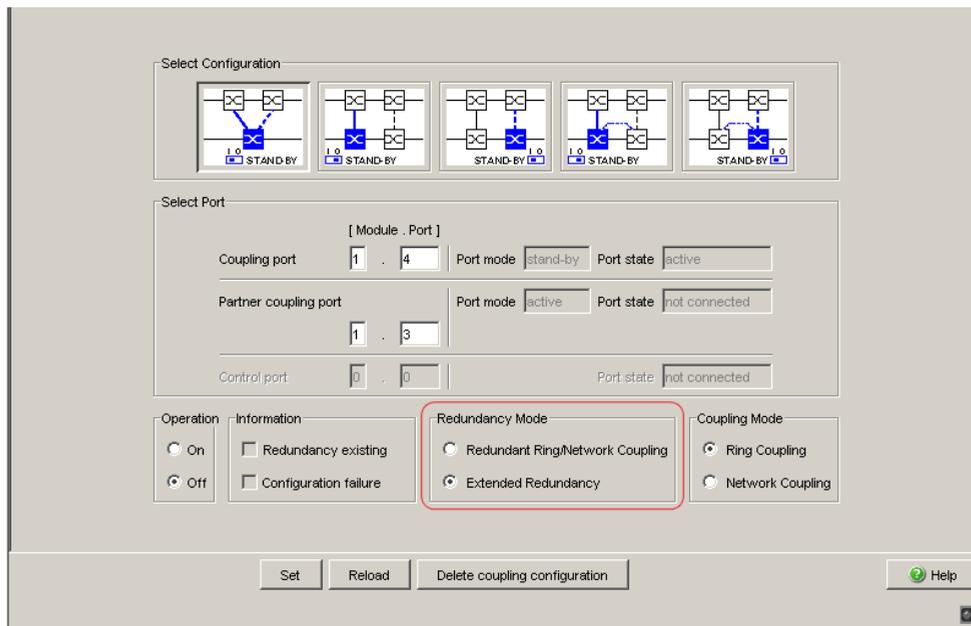


Figure 24: One-Switch coupling: Selecting the redundancy mode

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 25). During the reconfiguration period, packet duplications may occur. Therefore, select this setting only if your application detects package duplications.

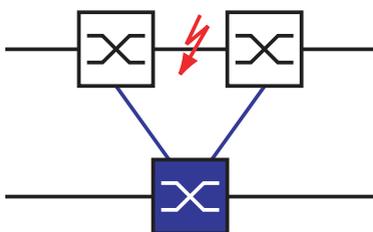


Figure 25: Extended redundancy

## Coupling mode

The coupling mode indicates the type of the connected network.

- In the “Coupling Mode” frame, select (see figure 26)
  - “Ring Coupling” or
  - “Network Coupling”

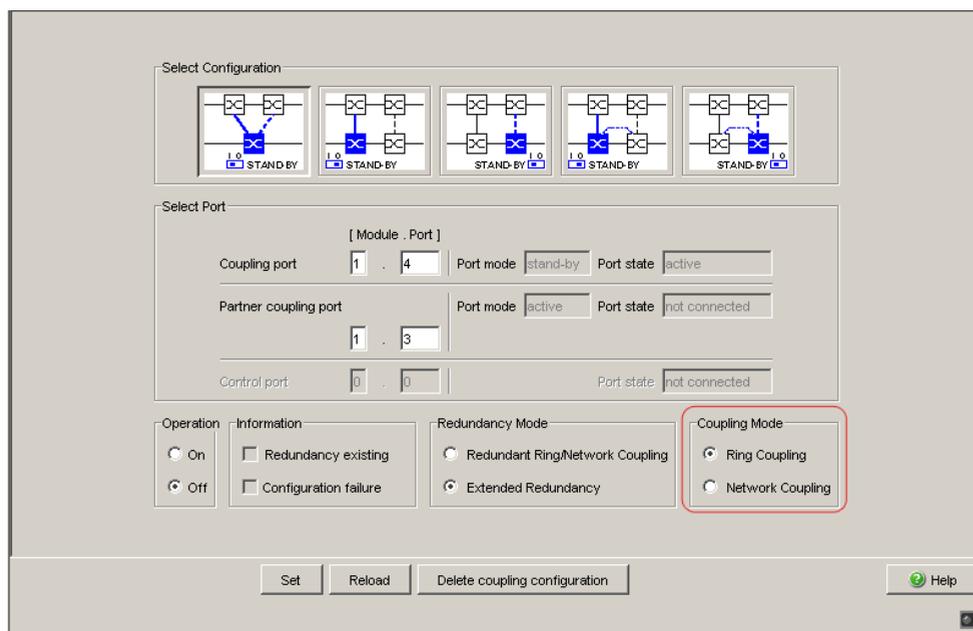


Figure 26: One-Switch coupling: Selecting the coupling mode

- 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.

### 5.2.3 Two-Switch coupling

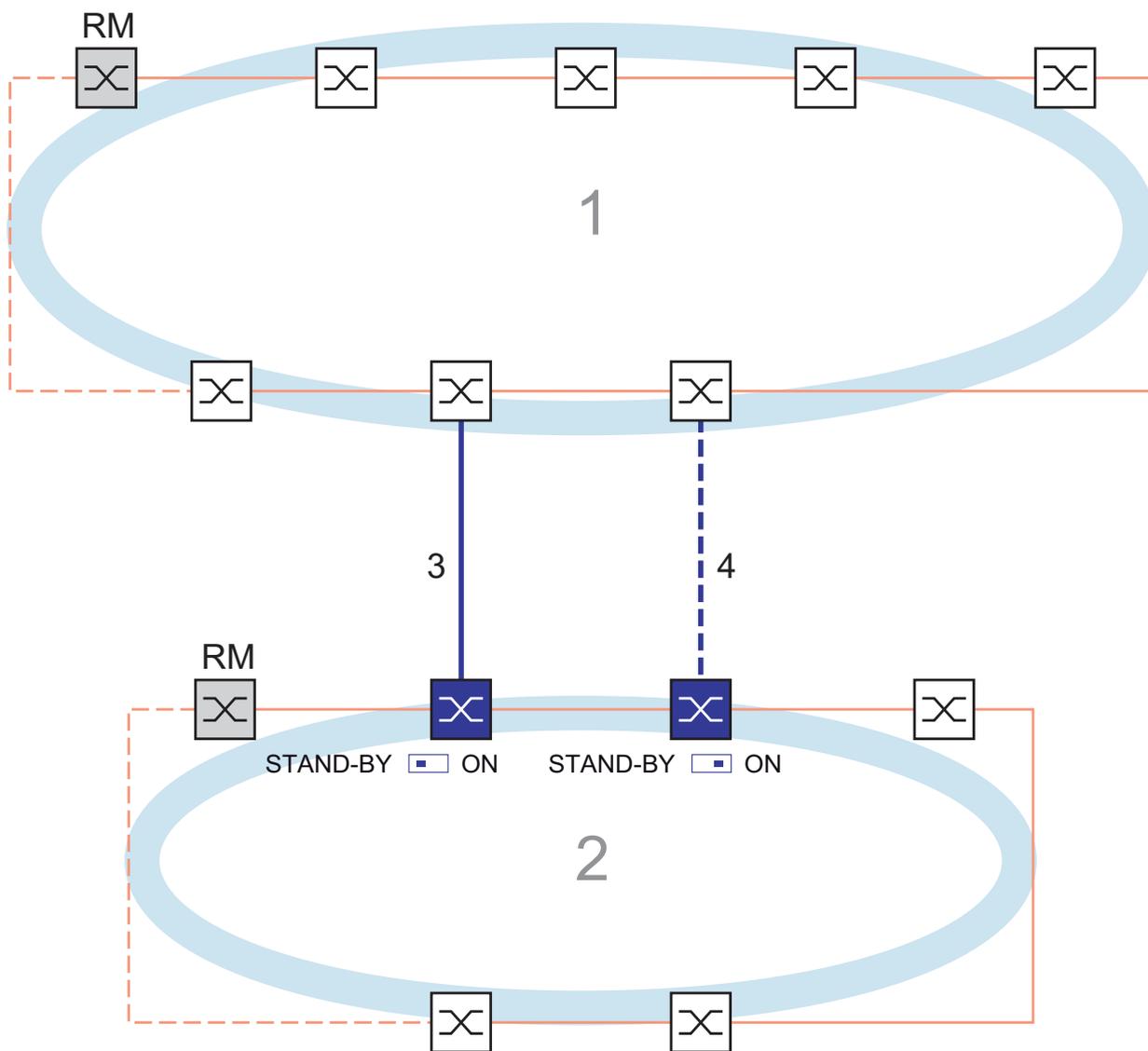


Figure 27: Example of two-Switch coupling

- 1: Backbone
- 2: Ring
- 3: Main line
- 4: Redundant line

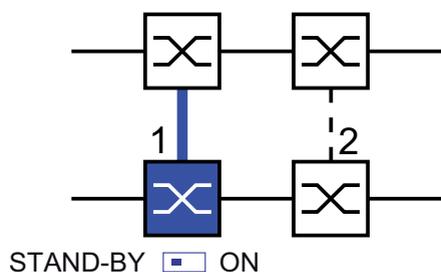
The coupling between 2 networks is performed by the main line (solid blue line). If the main line or one of the adjacent Switches becomes inoperable, the redundant line (dashed black line) takes over coupling the 2 networks. The coupling is performed by two Switches.

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 28).



*Figure 28: 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 29).  
 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.

| 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 10: 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 29](#))
- Now connect the redundant line.

The displays in the “Select port” frame mean:

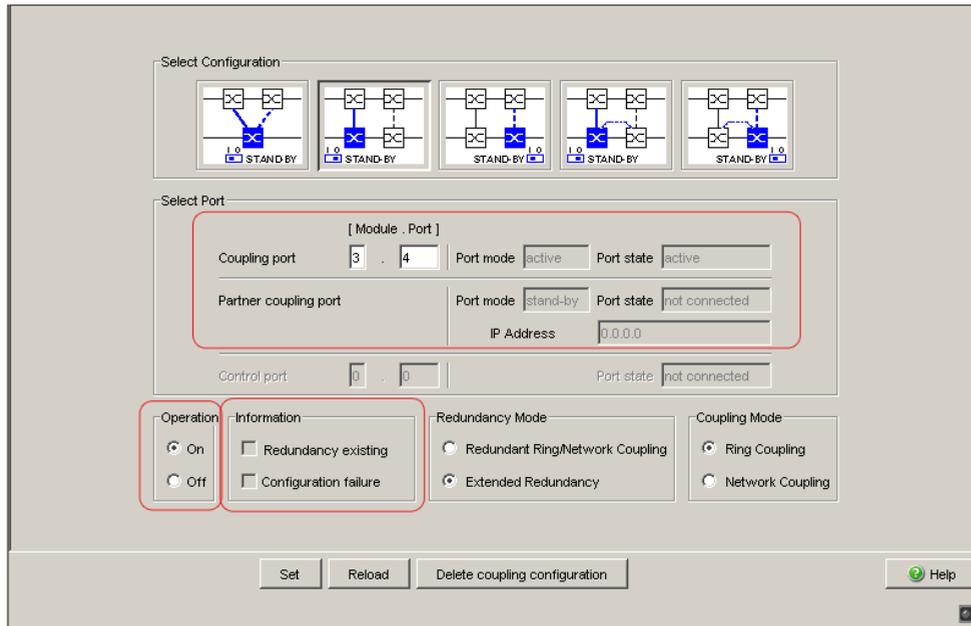
- “Port mode”: The port is either active or in stand-by mode.
- “Port state”: The port is either active, in stand-by mode or not connected.
- “IP Address”: The IP address of the partner, if the partner is already operating in the network.

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 29: 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):

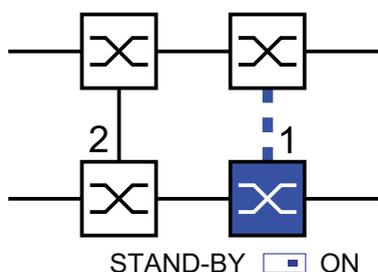
See [table 3 on page 33](#).

**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 30).



*Figure 30: 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 29).  
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.

**Note:** Configure the coupling port and the redundancy ring ports on different ports.

- Activate the function in the "Operation" frame (see figure 29)

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 33.](#)

**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 31](#))
  - “Redundant Ring/Network Coupling” or
  - “Extended Redundancy”.

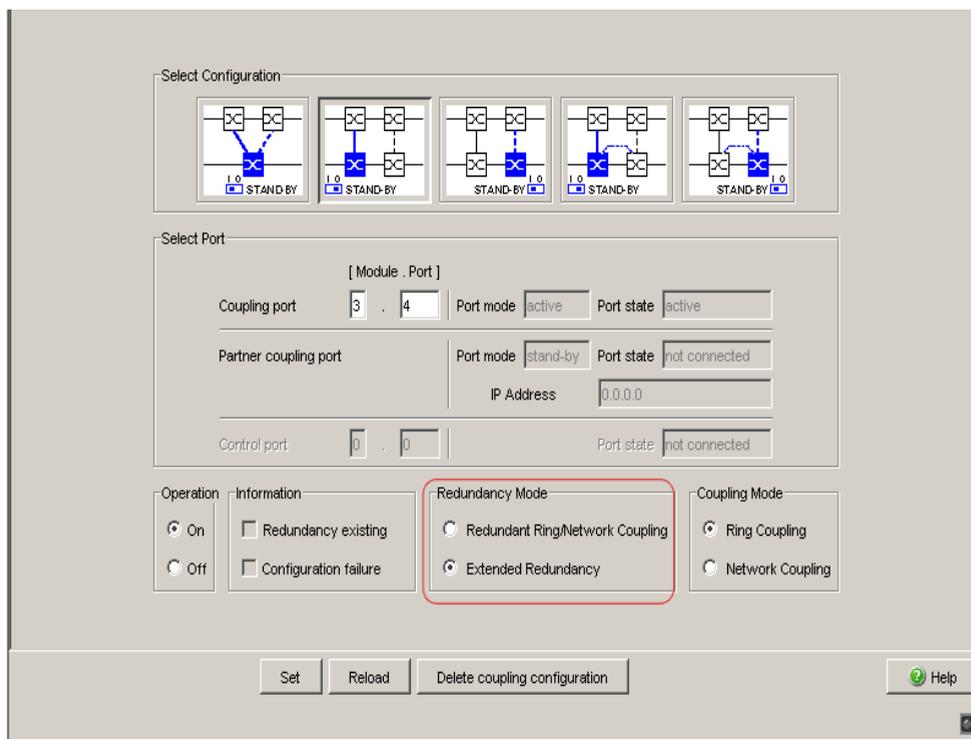


Figure 31: Two-Switch coupling: Selecting the redundancy mode

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 25). During the reconfiguration period, package duplications may occur. Therefore, only select this setting if your application detects package duplications.

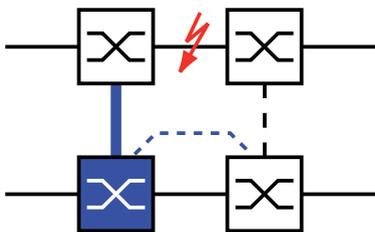


Figure 32: Extended redundancy

### Coupling mode

The coupling mode indicates the type of the connected network.

- In the “Coupling Mode” frame, select (see figure 33)
  - “Ring Coupling” or
  - “Network Coupling”

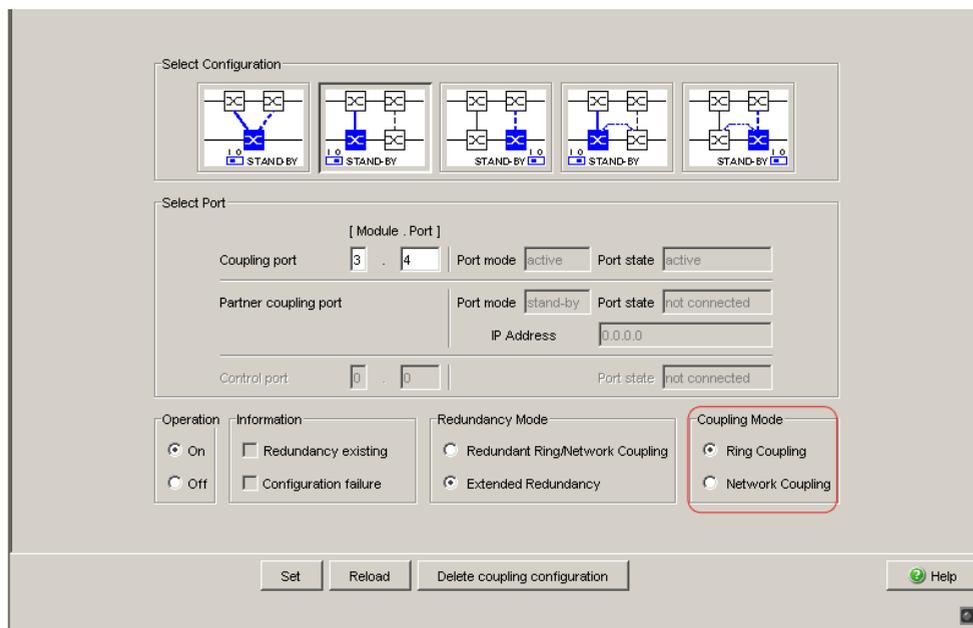


Figure 33: Two-Switch coupling: Selecting the coupling mode

- 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.

### 5.2.4 Two-Switch Coupling with Control Line

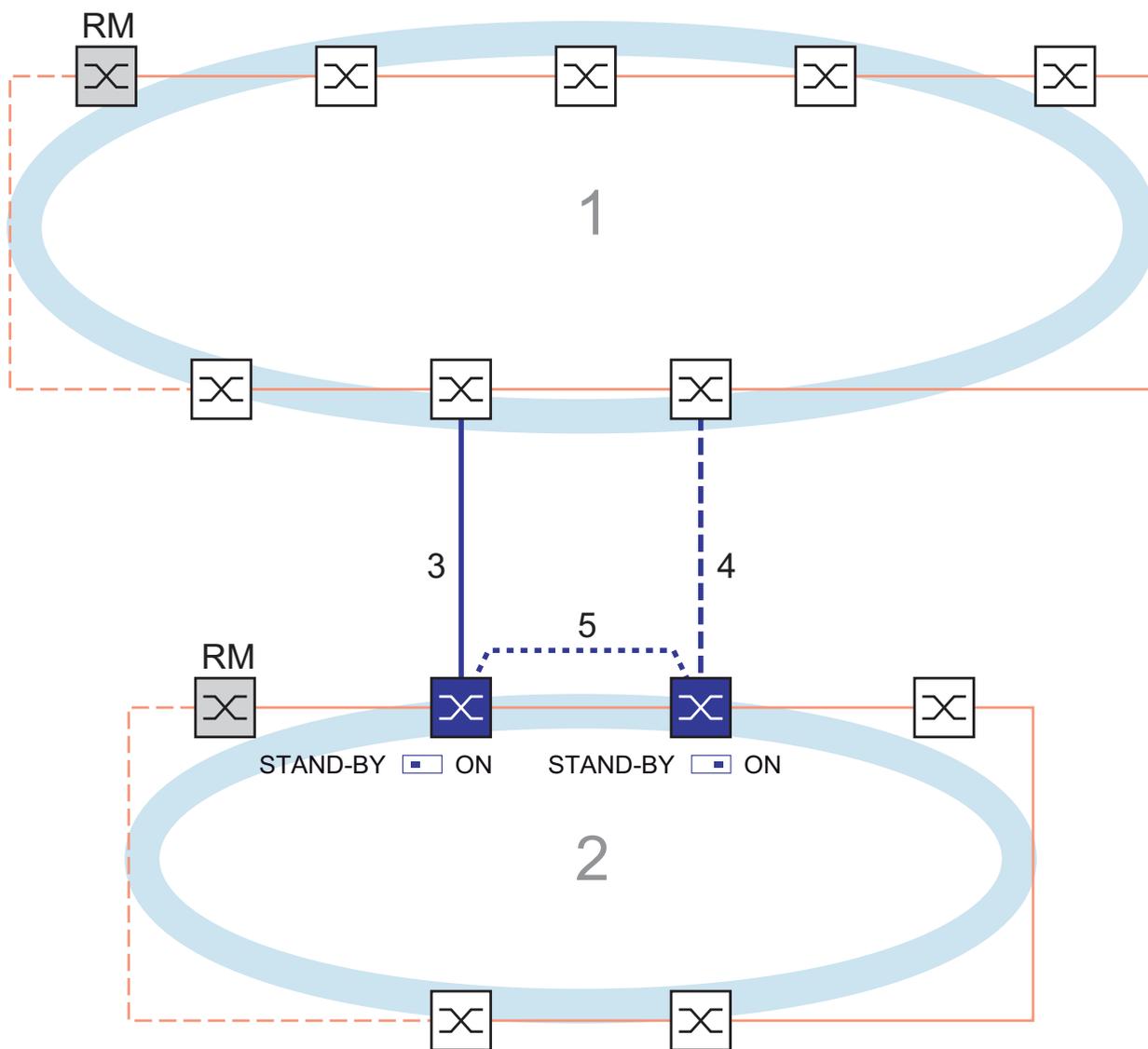


Figure 34: Example of Two-Switch coupling with control line

- 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 35).

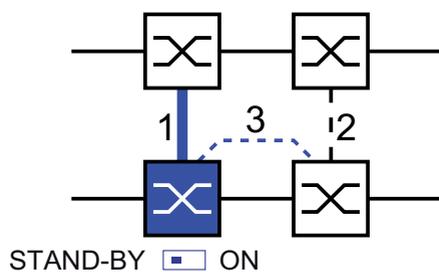


Figure 35: Two-Switch coupling with control line

- 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 36).  
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 11.
- 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 36)  
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 11.

| 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 11: 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 36)
- 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.

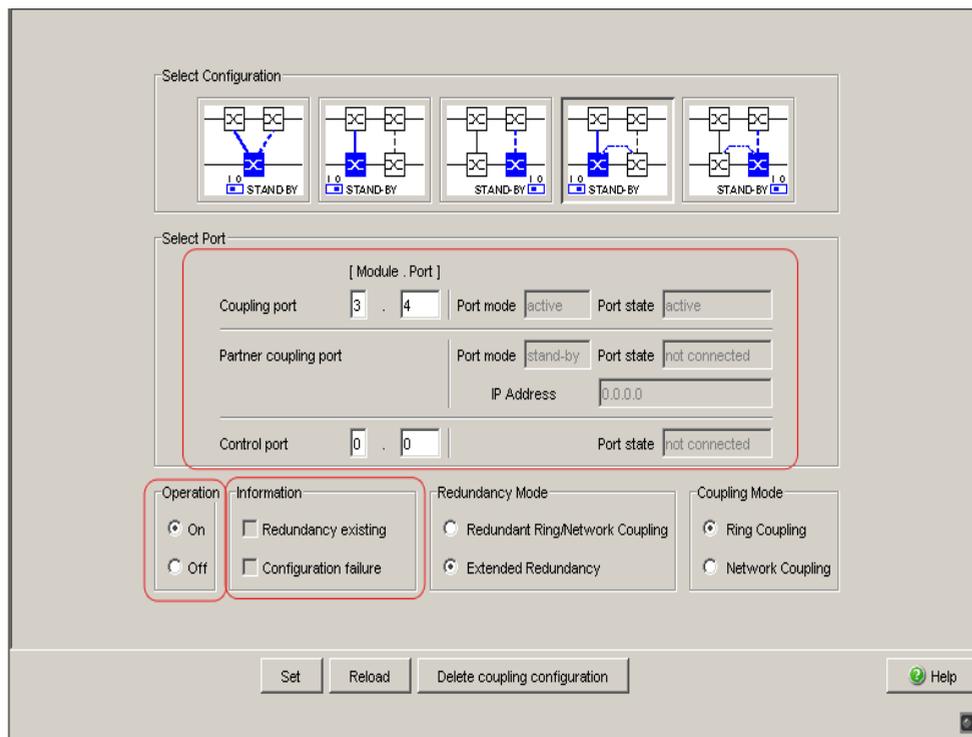


Figure 36: Two-Switch coupling with control line: Selecting the port and enabling/disabling operation

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.

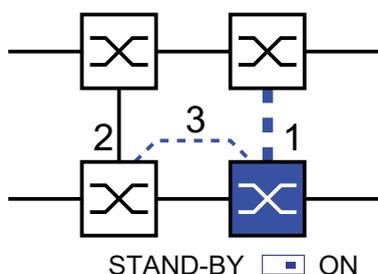
**Note:** The following settings are required for the coupling ports (you select the `Basic Settings:Port Configuration` dialog):

See [table 3 on page 33](#).

**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 37](#)).



*Figure 37: 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 36](#)).  
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 11](#).
- 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 36)  
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 36)
  - 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

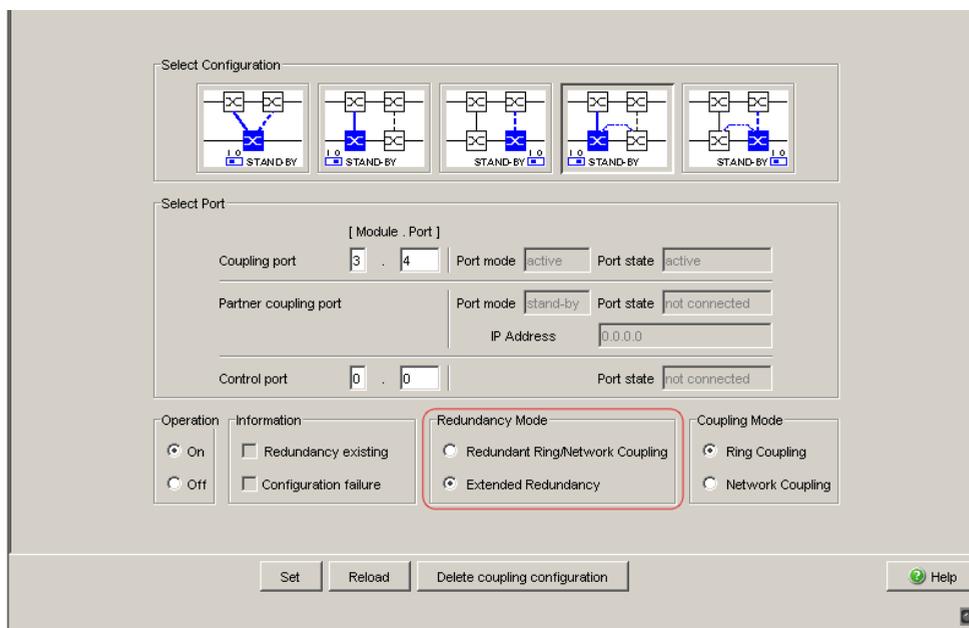
while the connections are in operation at these ports.

**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 38: 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 25). During the reconfiguration period, package duplications may occur. Therefore, only select this setting if your application detects package duplications.

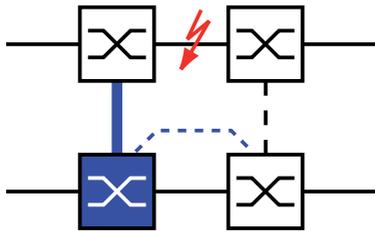


Figure 39: Extended redundancy

### Coupling mode

The coupling mode indicates the type of the connected network.

- In the “Coupling Mode” frame, select:
  - “Ring coupling”
  - or
  - “Network Coupling”

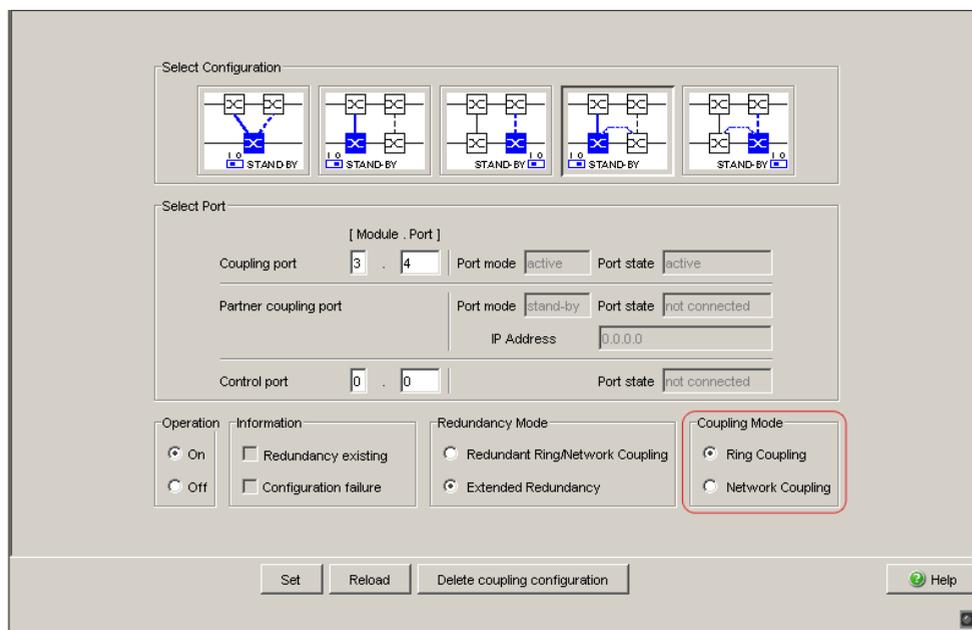


Figure 40: Two-Switch coupling with control line: Selecting the coupling mode

- 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.

## 6 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.

## 6.1 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.

### 6.1.1 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`, [\(see table 14\)](#))
- ▶ 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

## 6.1.2 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

## 6.1.3 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 41: Bridge Identifier, Example (values in hexadecimal notation)

### 6.1.4 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 12). 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.

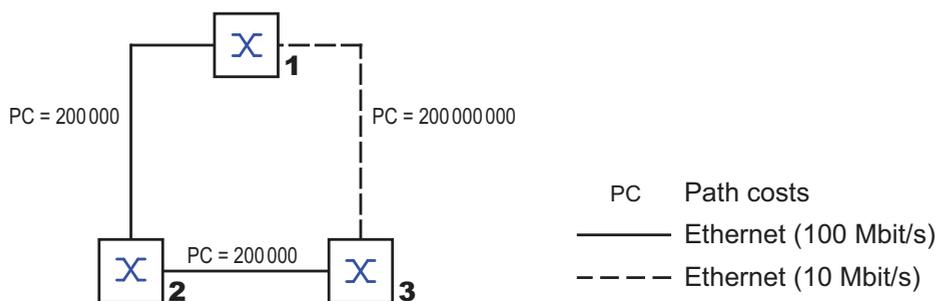


Figure 42: Path costs

| 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  |

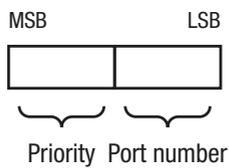
Table 12: Recommended path costs for RSTP based on the data rate.

- 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.

**Note:** If link aggregation ([see on page 19 “Link Aggregation”](#)) is used to combine the connection lines between devices into a trunk, then the automatically specified path costs are reduced by half.

### 6.1.5 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 43: Port Identifier*

---

## 6.2 Rules for Creating the Tree Structure

### 6.2.1 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).

### 6.2.2 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 43](#)). 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.

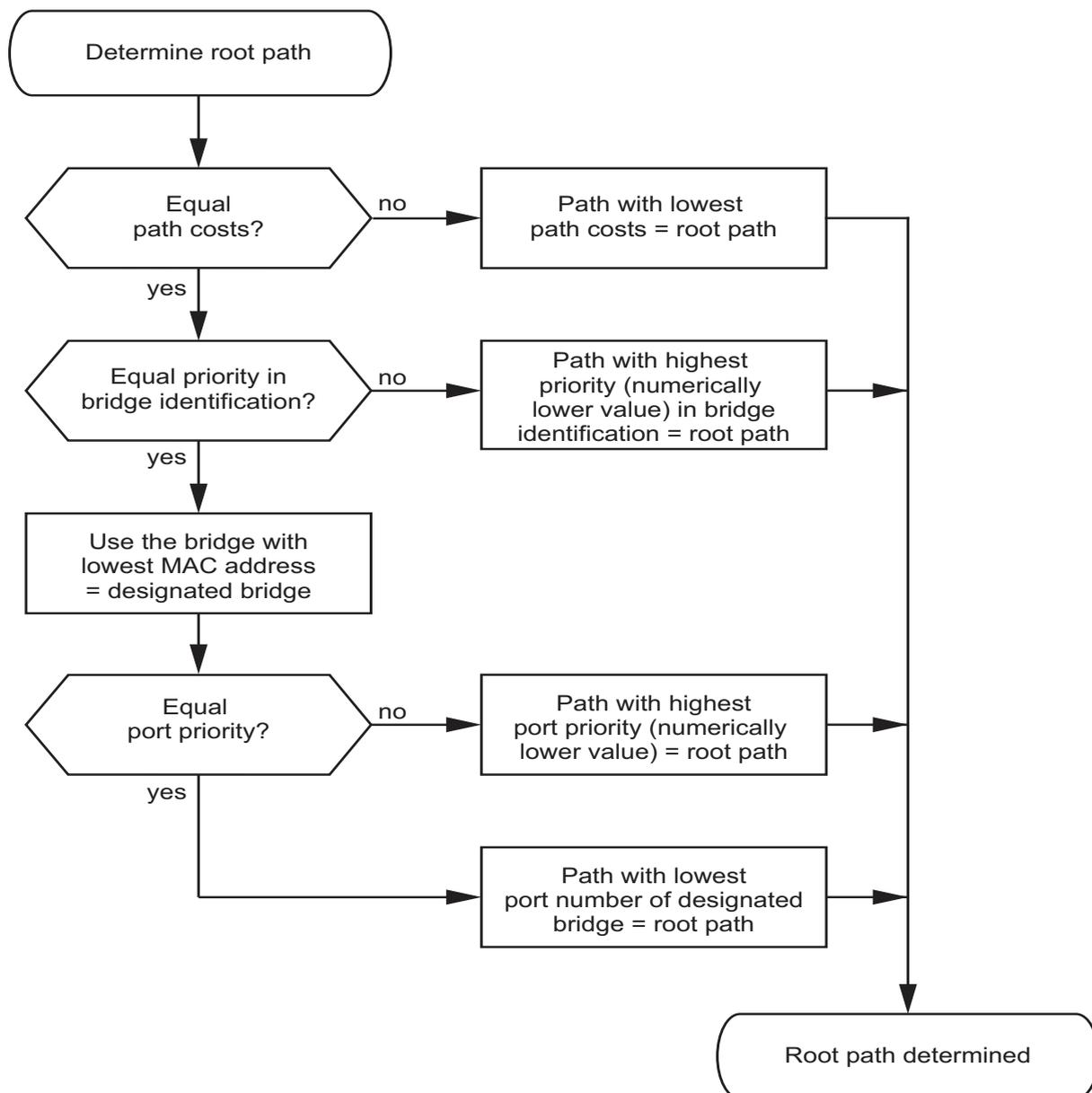


Figure 44: Flow diagram for specifying the root path

---

## 6.3 Example of determining the root path

You can use the network plan (see figure 45) to follow the flow chart (see figure 44) 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).

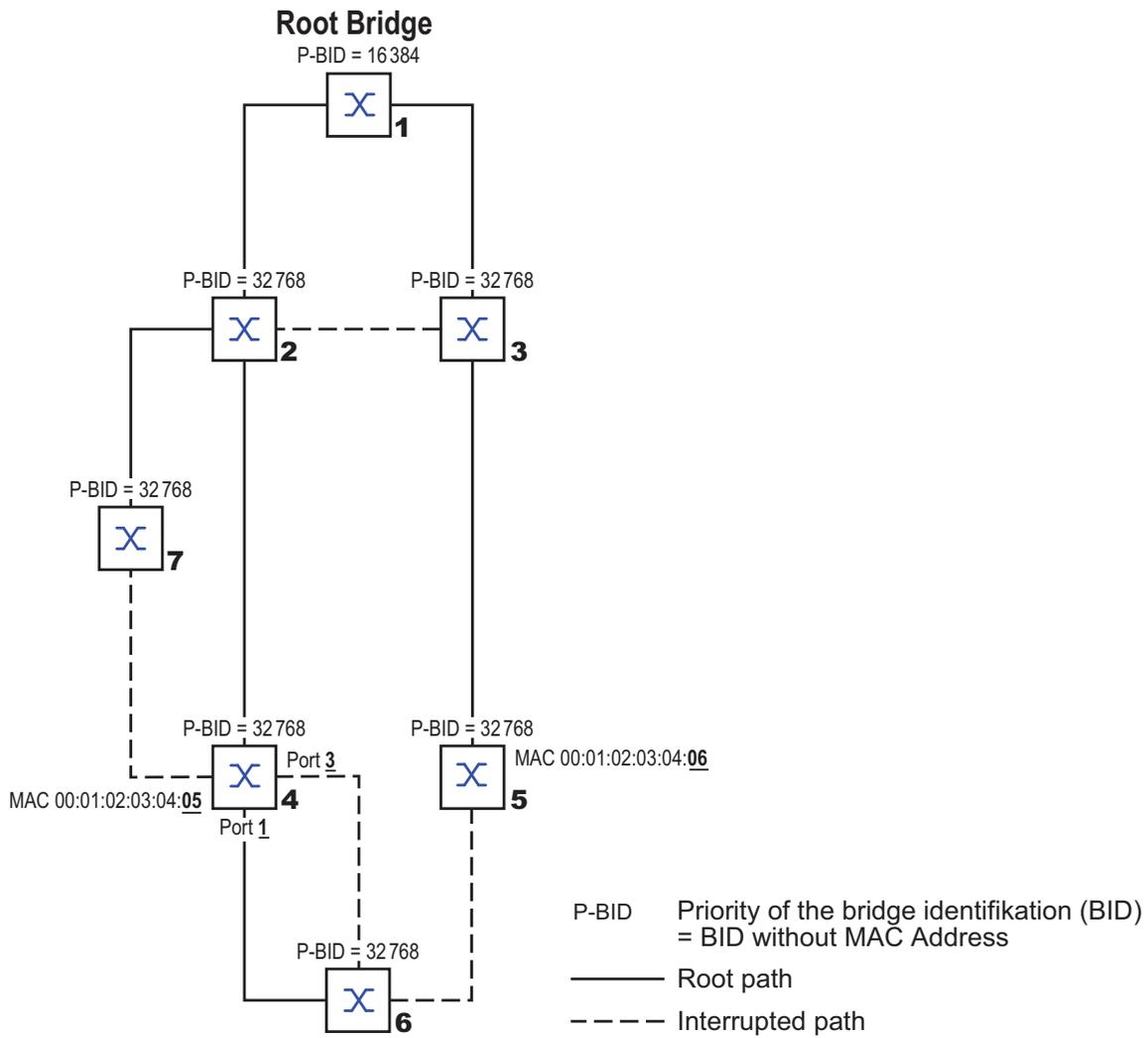


Figure 45: Example of determining the root path

## 6.4 Example of manipulating the root path

You can use the network plan (see figure 45) to follow the flow chart (see figure 44) 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.

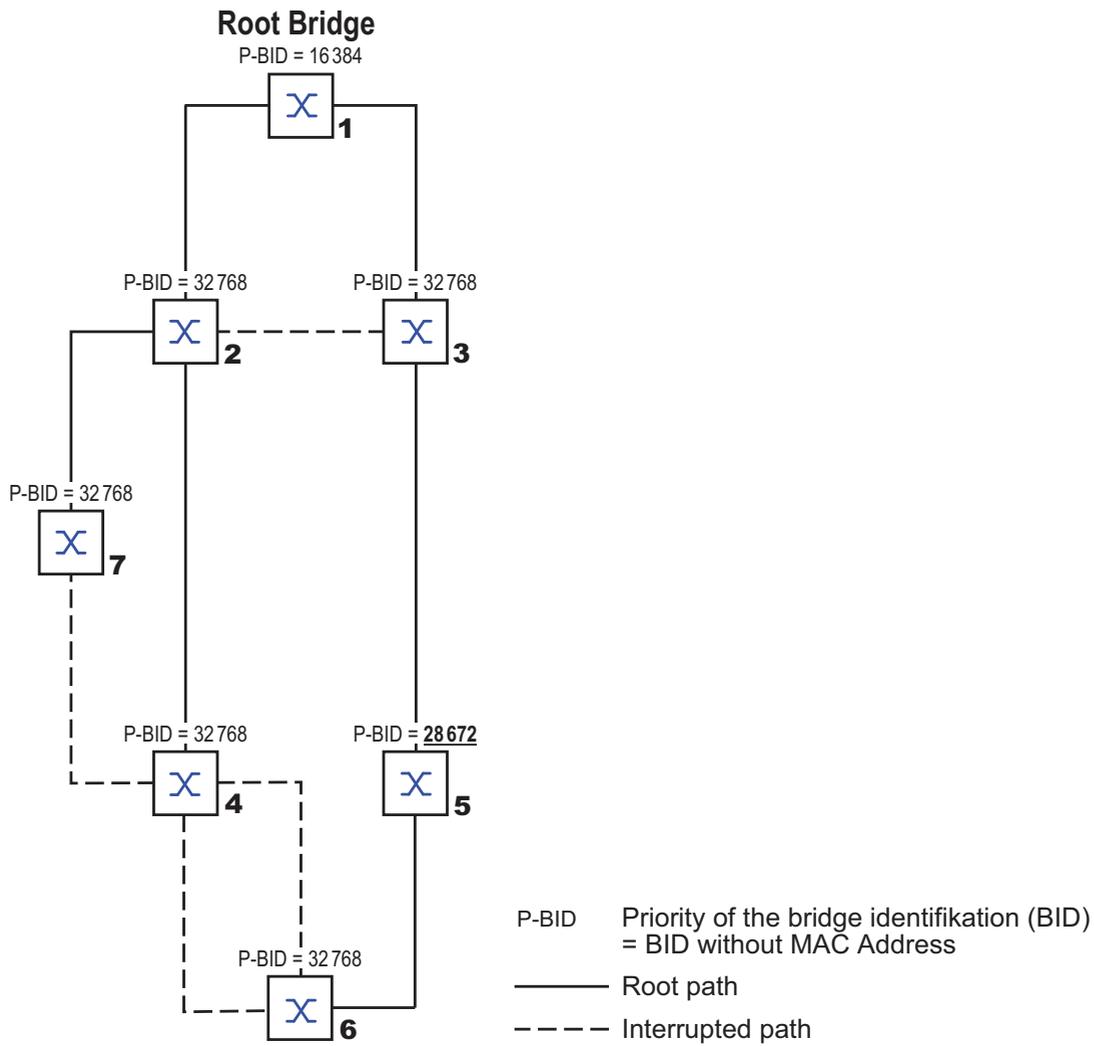


Figure 46: Example of manipulating the root path

## 6.5 Example of manipulating the tree structure

The Management Administrator soon discovers that this configuration with bridge 1 as the root bridge (see on page 93 “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 47). The path costs for most of the bridges to the root bridge have decreased.

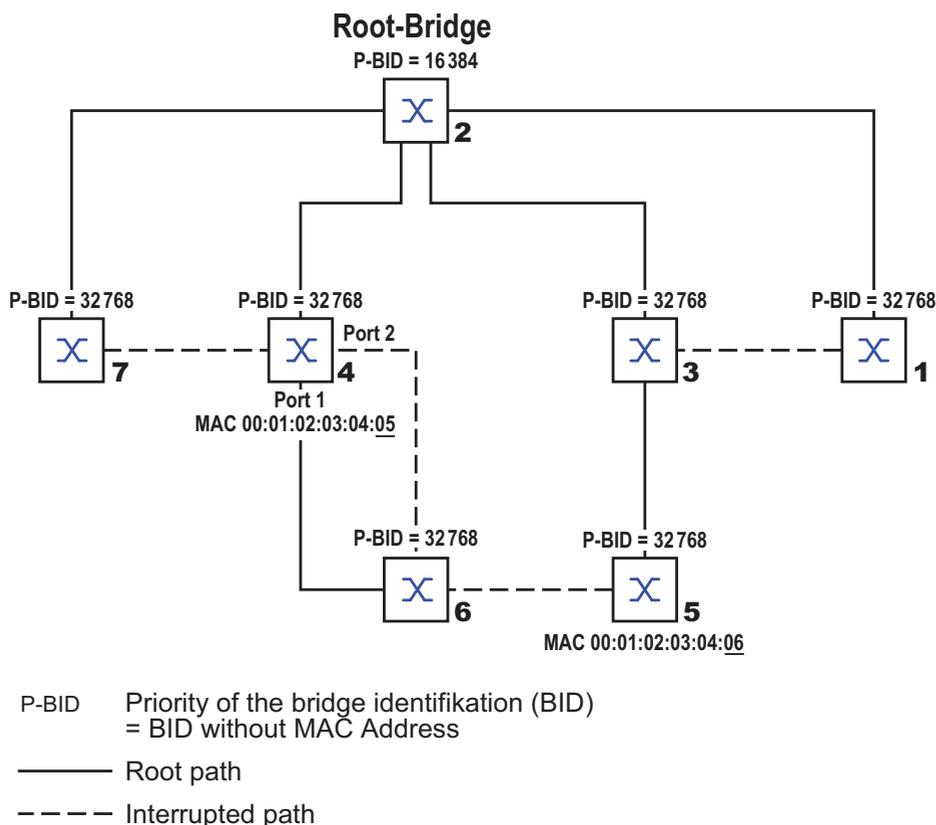


Figure 47: Example of manipulating the tree structure

## 6.6 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.

### 6.6.1 Port roles

RSTP assigns each bridge port one of the following roles ([see figure 48](#)):

► **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 44](#)).

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.

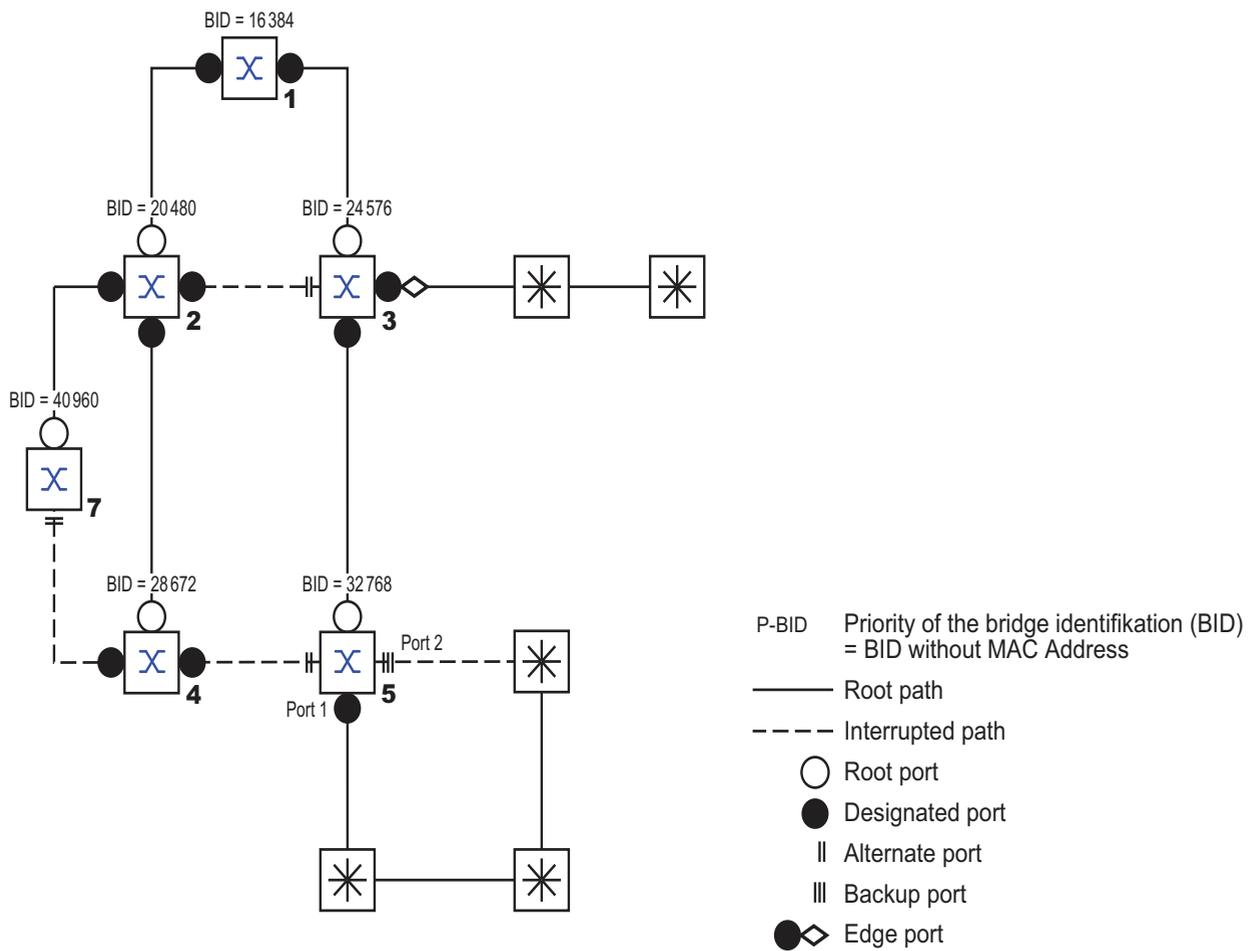


Figure 48: Port role assignment

## 6.6.2 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 13: 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)

### 6.6.3 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.

### 6.6.4 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 14) 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.

### 6.6.5 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

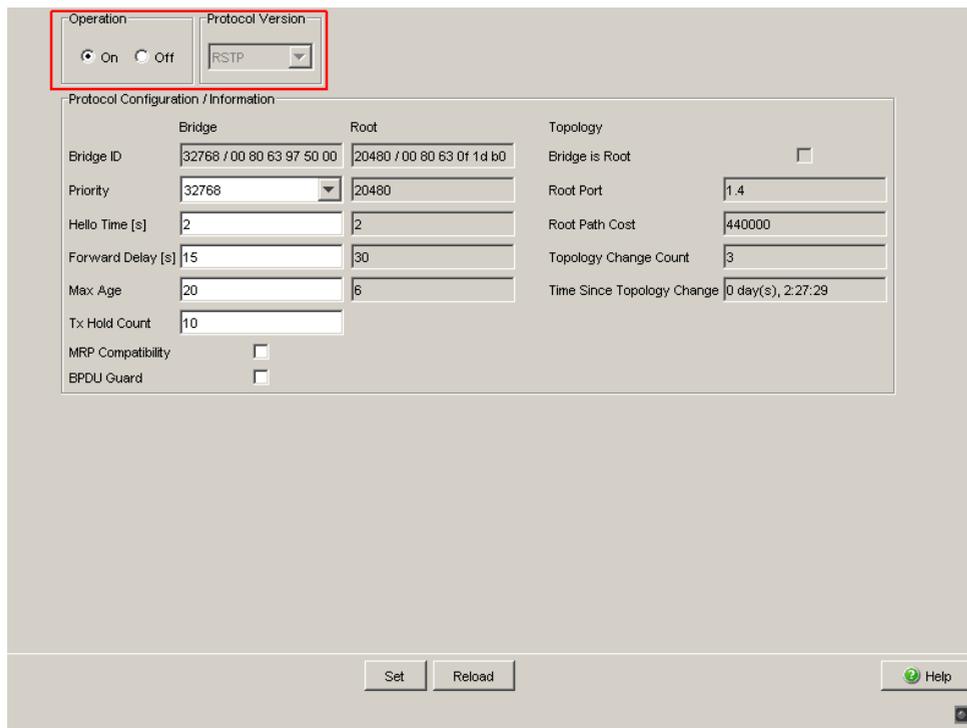


Figure 49: Operation on/off

- 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 14). 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 14](#).

| 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 50: 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 14: Global RSTP settings

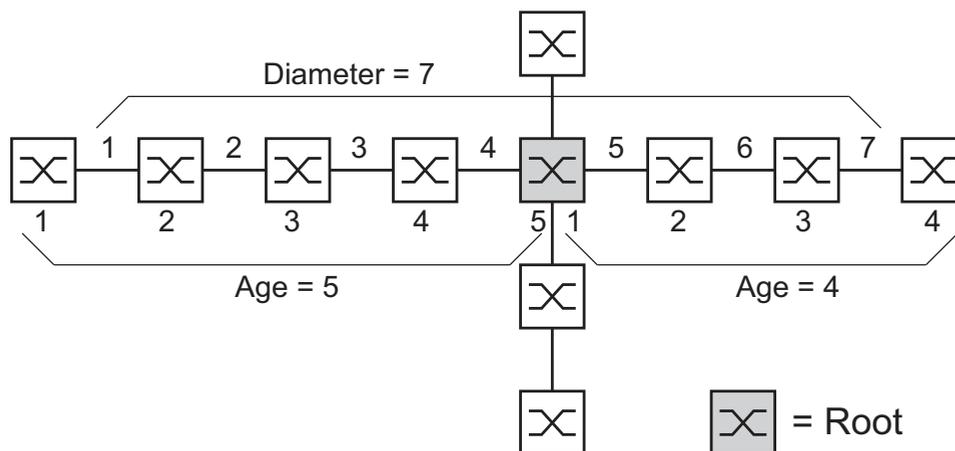


Figure 51: Definition of diameter and age

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                 |

Set Reload Help

Figure 52: 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 15: 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 15: 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 15: 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.

## 6.7 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 51) 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.

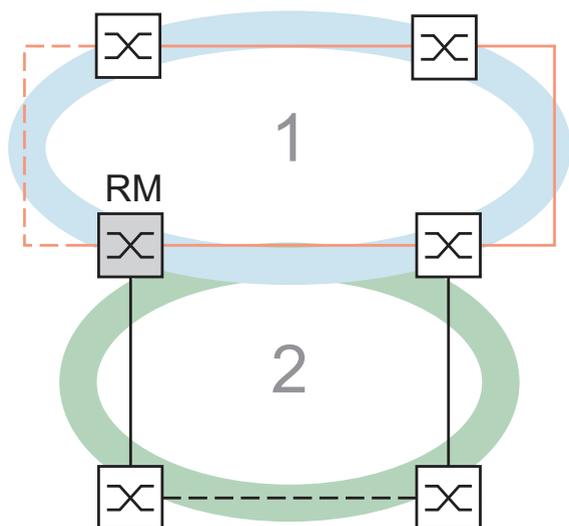


Figure 53: Combination of RSTP and MRP

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.

## 6.7.1 Application example for the combination of RSTP and MRP

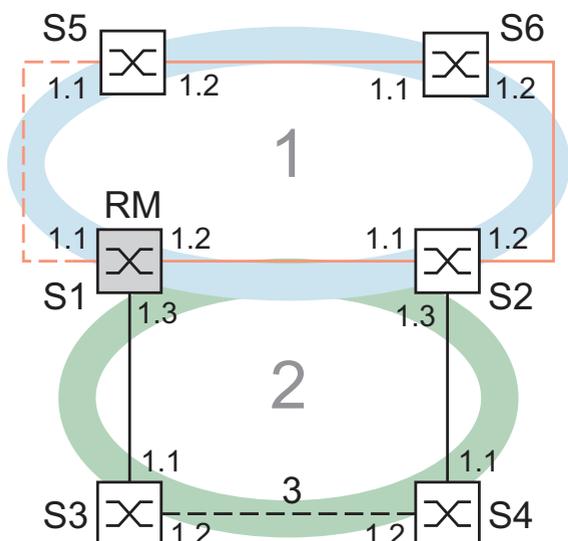
The figure (see figure 54) shows an example for the combination of RSTP and MRP.

| 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 16: 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 54: 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 16](#)).

```
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 16](#)).
- Connect the redundant RSTP connection.

## 7 VRRP/HiVRRP

The Virtual Router Redundancy Protocol (VRRP) is a procedure that enables the system to react to the failure of a router.

VRRP is used in networks with terminal devices that only support one entry for the default gateway. If the default gateway fails, VRRP ensures that the terminal devices find a redundant gateway.

The Hirschmann company has further developed the VRRP into the Hirschmann Virtual Router Redundancy Protocol (HiVRRP). With the appropriate configuration, HiVRRP provides switching times of less than 400 ms.

**Note:** You will find detailed information on VRRP and HiVRRP in the "Routing Configuration" user manual.

## 7.1 VRRP/HiVRRP Configuration

With this dialog you can enter general settings and settings for each port for the VRRP.

You can configure

- up to 8 virtual routers per port and
- up to 16 entries with HiVRRP per router.

### 7.1.1 General settings

- ▶ Operation: Switch the VRRP function on and off.
- ▶ Version: Display the VRRP version.
- ▶ Send VRRP Master Trap: As soon as the router takes over the VRRP master function, it sends a master trap.
- ▶ Send VRRP Authentication Error Trap: As soon as the router receives a VRRP message with an incorrect authentication, it sends a VRRP authentication error trap.

| Module | Port | VRID | Function | State      | Priority | Current Priority | VRRP IP Address | HiVRRP Advert Interval [ms] | Preempt mode                        | Pre De |
|--------|------|------|----------|------------|----------|------------------|-----------------|-----------------------------|-------------------------------------|--------|
| 2      | 1    | 1    | up       | initialize | 100      | 100              | 10.0.11.1       | 1000                        | <input checked="" type="checkbox"/> |        |
| 2      | 1    | 2    | up       | initialize | 100      | 100              | 10.0.14.1       | 1000                        | <input checked="" type="checkbox"/> |        |
| 2      | 1    | 5    | up       | initialize | 100      | 100              | 10.0.12.1       | 1000                        | <input checked="" type="checkbox"/> |        |
| 2      | 1    | 255  | up       | initialize | 100      | 100              | 10.0.13.1       | 1000                        | <input checked="" type="checkbox"/> |        |

Figure 55: VRRP/HiVRRP Configuration dialog

## 7.1.2 VRRP instance settings

- ▶ Module: Module of the device
- ▶ Port: Port to which this entry applies
- ▶ VRID: Virtual router ID (value 1-255)
- ▶ Operation: Switch the VRRP instances on and off
- ▶ Status: VRRP state
  - initialize: VRRP is in the initialization phase. No master has been named yet.
  - backup: the Switch sees the possibility of becoming master.
  - master: the Switch is master.
- ▶ Priority: VRRP priority set (range: 1 to 255; default: 100).  
The router with the highest value is the master. If the virtual router IP address is the same as the IP address of the router interface, then this router is the “owner”. If an owner exists, then VRRP assigns the owner the VRRP priority 255 and thus declares it the master.

- ▶ Current Priority: VRRP priority actually used (range: 1 to 255). This value is usually the same as the VRRP priority set but can be smaller if tracking objects monitored have the status “down”.
- ▶ VRRP IP address: Primary virtual router IP address.
- ▶ HiVRRP advertisement Interval: Interval for sending out messages (advertisements) as the master (range for VRRP: 1 to 255 s, range for HiVRRP: 100 to 255.000 ms, default setting: 1 s).
- ▶ Preempt mode: This setting specifies whether this router, as a backup router, will take over the master role from a master router with a lower VRRP priority. If the preempt mode is switched off, this router only takes on the master role if the IP Multicast message from the existing master does not appear.
- ▶ Preempt delay: The preempt mode, in collaboration with VRRPtracking, can enable a switch to a better router. However, dynamicrouting procedures take a certain amount of time to react to changedroutes and refill their routing table. To avoid the loss of packetsduring this time, delayed switching (preempt delay) from the masterrouter to the backup router enables the dynamic routing procedureto fill the routing tables (value: 0-65535 s, default setting 0 s).
- ▶ Domain ID: The domain ID is a number identifying the domain ([see on page 123 “HiVRRP Domains”](#)). Range: 0 to 8, default setting 0: no domain.
- ▶ Domain role:
  - none: not a member of a domain
  - member: copies the behavior of the supervisor
  - supervisor: determines the behavior of the domains
- ▶ Authentication: Type of authentication used:
  - `noAuthentication`: VRRP information is exchanged without authentication.
  - `simpleTextPassword`: VRRP information is exchanged with plain text password authentication.
- ▶ Key: Password for authentication. In order to communicate, the routers with the same virtual router IP address must have the same authentication setting.
- ▶ Master IP Address: Actual router interface IP address of the master.

### 7.1.3 Setting up the VRRP router instance

- In the `Redundancy:VRRP/HiVRRP:Configuration` dialog, click “Wizard” at the bottom right.
- In the table in the Wizard dialog, select a port row and enter the virtual router ID in the VRID row. You can configure up to 8 virtual routers per interface.
- Click “Continue”.
- Under “Edit entry” in the “Basic configuration” frame, enter:

- the IP address of the virtual router
- the VRRP priority
- the type of authentication
- the key for the authentication
- the preempt delay
- the advertisement interval.

If necessary, select the preempt mode

Switch on the operation of VRRP.

If you want

- switching times of less than 3 s,
- the routers to use Unicasts to communicate with each other,
- to set up domains or
- to send link-down notifications,

you activate the “HiVRRP” field.

In the “HiVRRP” frame, enter:

- the “Advertisement Interval”
- the “Destination Address”. The HiVRRP destination address is the IP address of the partner HiVRRP router.
- the IP address of the second router to which the link-down notifications are sent. This function can be used when the virtual router consists of two VRRP routers.
- the domain ID
- the domain role

- Click “Finish” to transfer the VRRP router interface to the VRRP router interface table

or

- Click “Next” to assign tracking objects to the virtual router under “Tracking”. If a tracking object’s status changes to “down”, the VRRP priority is decremented.

Select an existing tracking entry and click “Add”. You can add up to 8 tracking objects. Ascertain that the sum of the decrements of all the assigned tracking entries is less than the VRRP priority of this VRRP interface.

**Note:** As the IP address owner has the fixed VRRP priority 255 by definition, the VRRP tracking function requires the IP addresses of the VRRP router interfaces to differ from the virtual router IP address.

**Note:** Activate the preempt mode so that, the backup router can take over the master role after the decrementation of the master's VRRP priority via the tracking function.

- Click “Finish” to transfer the VRRP router interface to the VRRP router interface table  
or
- Click “Next” if you want to enter additional IP addresses under “Associated IP Addresses” (Multinetting).
- Click “Finish” to transfer the VRRP router interface to the VRRP router interface table.

### 7.1.4 Configuring the VRRP router instance

- In the `Redundancy:VRRP/HiVRRP:Configuration` dialog, double-click a cell of the table and edit the entry or right-click a cell and select a value.
- As an alternative to editing directly in the table, you can mark a row in the table and use the Wizard to edit it.

### 7.1.5 Deleting a VRRP router instance

- In the `Redundancy:VRRP/HiVRRP:Configuration` dialog, select a row and click “Remove”. You thus delete the row.

---

## 7.2 HiVRRP Domains

A HiVRRP instance is a router instance configured as HiVRRP with functions that HiVRRP contains. In a HiVRRP domain you combine multiple HiVRRP instances of a router into one administrative unit. You nominate one HiVRRP instance as the supervisor of the HiVRRP domain. This supervisor regulates the behavior of all HiVRRP instances in its domain. The router supports up to 8 domains.

### 7.2.1 Displaying HiVRRP domains

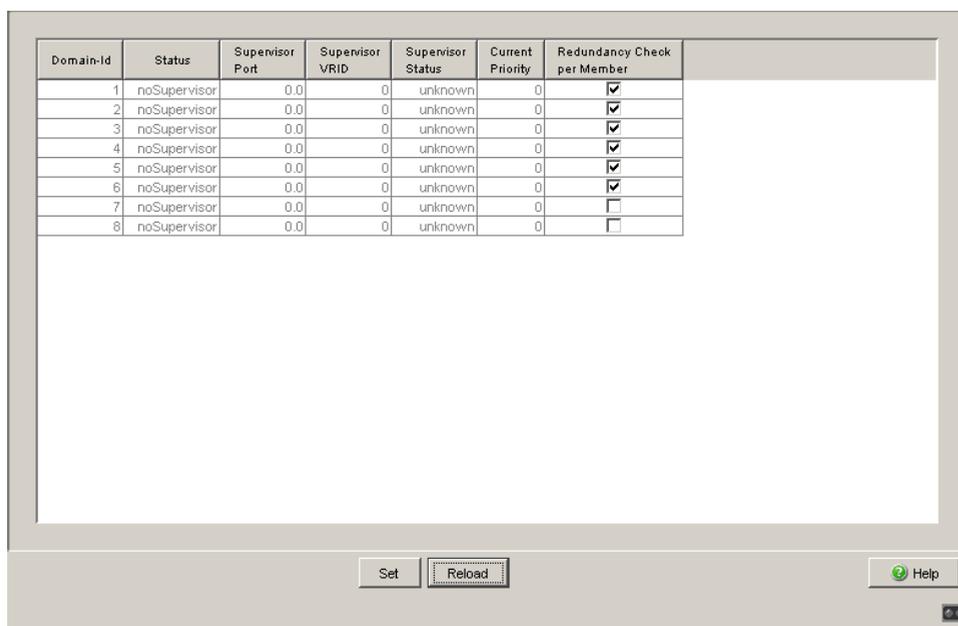
- ▶ Domain ID: identification of the domains
- ▶ Status: status of the supervisor of the domains
  - Supervisor: supervisor is active
  - SupervisorDown: supervisor is not active
  - noSupervisor: no supervisor defined
- ▶ Supervisor Port: HiVRRP instance (module and port, written as <Slot>.<Port>) that was defined as the supervisor
- ▶ Supervisor VRID: VRID of the supervisor
- ▶ Supervisor Status: status of the supervisor
  - initialize: VRRP is in the initialization phase. No master has been named yet.
  - backup: the Switch sees the possibility of becoming master.
  - master: the Switch is master
  - unknown: no supervisor
- ▶ Current Priority: the current VRRP priority

## 7.2.2 HiVRRP domain instances at different ports

If domain instances (members) are divided among different physical ports, the router monitors by default only the supervisor's connection for line interruptions (“Redundancy Check per Member” deactivated).

You have the option of activating the monitoring of the other connections for line interruptions within the domain. Monitoring means that the router sends HiVRRP messages when it detects a line interruption. If there is a low probability of a line interruption, you select a long HiVRRP message interval (see on page 119 “VRRP instance settings”) in order to minimize the network load.

- In the “Redundancy check per member” column, you can activate the function for a chosen domain as required.



| Domain-Id | Status       | Supervisor Port | Supervisor VRID | Supervisor Status | Current Priority | Redundancy Check per Member         |
|-----------|--------------|-----------------|-----------------|-------------------|------------------|-------------------------------------|
| 1         | noSupervisor | 0.0             | 0               | unknown           | 0                | <input checked="" type="checkbox"/> |
| 2         | noSupervisor | 0.0             | 0               | unknown           | 0                | <input checked="" type="checkbox"/> |
| 3         | noSupervisor | 0.0             | 0               | unknown           | 0                | <input checked="" type="checkbox"/> |
| 4         | noSupervisor | 0.0             | 0               | unknown           | 0                | <input checked="" type="checkbox"/> |
| 5         | noSupervisor | 0.0             | 0               | unknown           | 0                | <input checked="" type="checkbox"/> |
| 6         | noSupervisor | 0.0             | 0               | unknown           | 0                | <input checked="" type="checkbox"/> |
| 7         | noSupervisor | 0.0             | 0               | unknown           | 0                | <input type="checkbox"/>            |
| 8         | noSupervisor | 0.0             | 0               | unknown           | 0                | <input type="checkbox"/>            |

Figure 56: HiVRRP domain dialog

---

## 7.3 Statistics

The VRRP statistics window displays the numbers on counters that count events relevant to VRRP.

### 7.3.1 VRRP statistic for all ports

- ▶ Checksum errors: Number of VRRP advertisements received with the wrong checksum.
- ▶ Version errors: Number of VRRP advertisements received with an unknown or unsupported version number.
- ▶ VRID errors: Number of VRRP advertisements received with an invalid VRID for this virtual router.

### 7.3.2 VRRP statistics per port

- ▶ Module: Module of the device
- ▶ Port: Port to which this entry applies
- ▶ VRID: Virtual router ID.
- ▶ Become Master: Number of times the Switch has become the master.
- ▶ Advertise receives: Number of VRRP advertisements received.
- ▶ Advertise interval errors: Number of VRRP advertisements received by the router outside the advertisement interval.
- ▶ Authentication failures: Number of VRRP messages received with authentication errors.

- ▶ IP TTL errors: Number of VRRP advertisements received with an IP-TTL not equal to 255.
- ▶ Priority Zero packets received: Number of VRRP advertisements via a VRRP participant with a priority of 0.
- ▶ Priority Zero packets sent: Number of VRRP messages that the device has sent with a priority of 0.
- ▶ Received Bad Packets: Number of VRRP advertisements received with an invalid type.
- ▶ Address errors: Number of VRRP messages received for which the address list does not match the address list configured locally for the virtual router.
- ▶ Invalid authentication type: Number of VRRP advertisements received with an invalid authentication type.
- ▶ Authentication type mismatch: Number of VRRP messages received with an incorrect authentication type.
- ▶ Packet length errors: Number of VRRP messages received with an incorrect packet length.

|                 |  |   |  |
|-----------------|--|---|--|
| Checksum errors |  | 0 |  |
| Version errors  |  | 0 |  |
| VRID errors     |  | 0 |  |

| Module | Port | VRID | Become master | Advertise received | Advertise Interval errors | Authentication failures | IP TTL errors | Priority |
|--------|------|------|---------------|--------------------|---------------------------|-------------------------|---------------|----------|
| 2      | 1    | 1    | 0             | 0                  | 0                         | 0                       | 0             | 0        |
| 2      | 1    | 2    | 0             | 0                  | 0                         | 0                       | 0             | 0        |
| 2      | 1    | 5    | 0             | 0                  | 0                         | 0                       | 0             | 0        |
| 2      | 1    | 255  | 0             | 0                  | 0                         | 0                       | 0             | 0        |

Figure 57: VRRP statistics dialog

## 7.4 Tracking

The VRRP Tracking window displays the status of all the tracking objects assigned to VRRP objects.

- ▶ Port: Port to which this entry applies, in the form <Slot>.<Port>
- ▶ VRID: Virtual router ID of the assigned virtual router.
- ▶ TrackID: the tracking object's ID number.
- ▶ Decrement: Change value by which the current VRRP priority of the assigned VRRP priority is reduced when the tracking object gets the status "down".
- ▶ Status: Current status of the tracking object: "up" or "down".
- ▶ Active: Entry is displayed as "active" if the tracking object is completely set up and is activated.  
If the entry is active, you can find more information about it in the ["Tracking dialog"](#) (see on page [NOT DEFINED](#)).  
If the entry is not active, its status is always "up".

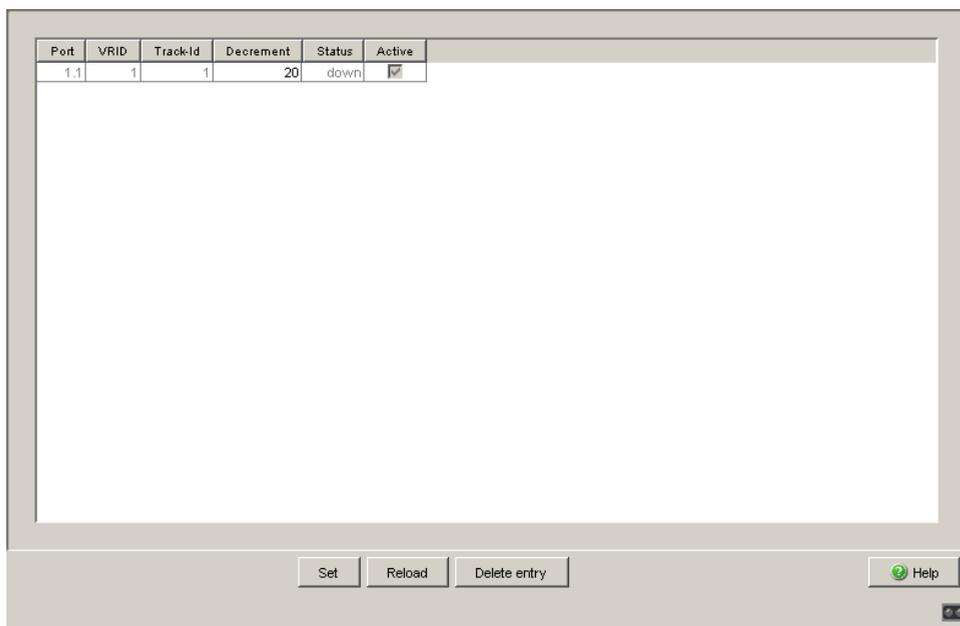


Figure 58: Tracking dialog

## 7.4.1 Deleting a tracking object

- In the `Redundancy:VRRP:Tracking` dialog, select a row and click “Remove”. You thus delete the row.

# 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>                               |                | <b>N</b>                           |            |
| Advanced Mode                          | 37             | Network load                       | 83, 85     |
| Age                                    | 107            | <b>P</b>                           |            |
| Alternate port                         | 99             | Path costs                         | 87, 90     |
| Authentication                         | 121            | Port Identifier                    | 86, 89     |
| <b>B</b>                               |                | Port number                        | 89         |
| Backup port                            | 99             | Port priority (Spanning Tree)      | 89         |
| BPDU                                   | 90             | Port roles (RSTP)                  | 98         |
| Bridge Identifier                      | 86             | Port-State                         | 101        |
| Bridge Protocol Data Unit              | 90             | PROFINET IO                        | 9          |
| <b>C</b>                               |                | <b>R</b>                           |            |
| Configuration error                    | 36, 40         | Rapid Spanning Tree                | 13, 98     |
| <b>D</b>                               |                | Reconfiguration                    | 85         |
| Designated bridge                      | 98             | Redundancy                         | 9, 83      |
| Designated port                        | 98             | Redundancy existing                | 36, 40     |
| DIP-switch                             | 32             | Redundancy functions               | 13         |
| Diameter                               | 107            | Redundancy Manager                 | 30         |
| Disabled port                          | 99             | Ring                               | 29         |
| <b>E</b>                               |                | Ring Manager                       | 30         |
| Edge port                              | 99             | Ring manager                       | 29         |
| <b>F</b>                               |                | Ring Redundancy                    | 14, 14, 14 |
| FAQ                                    | 133            | Ring structure                     | 30         |
| Forward Delay                          | 106            | Ring/Network coupling              | 13         |
| <b>H</b>                               |                | RM function                        | 29         |
| Hello Time                             | 106            | Root Bridge                        | 90         |
| HIPER-Ring                             | 13, 16, 26, 32 | Root Path Cost                     | 86         |
| HiVRRP                                 | 16, 117        | Root path                          | 93, 95     |
| HiVRRP domains                         | 123            | Root port                          | 98         |
| HiVRRP (configuration)                 | 118            | Router                             | 9          |
| <b>I</b>                               |                | RSTP                               | 13         |
| Industrial HiVision                    | 10             | RST BPDU                           | 99, 102    |
| Industry Protocols                     | 9              | <b>S</b>                           |            |
| <b>L</b>                               |                | STP-BPDU                           | 90         |
| LACP Link Aggregation Control Protocol | 19             | Sub-Ring                           | 13, 44     |
| Link Aggregation                       | 13, 16, 26     | Symbol                             | 11         |
| Loops                                  | 70, 72, 79, 80 | <b>T</b>                           |            |
| <b>M</b>                               |                | Technical Questions                | 133        |
| Max Age                                | 106            | Tracking (VRRP)                    | 127        |
| MRP-Ring                               | 13, 16, 25     | Training Courses                   | 133        |
| <b>N</b>                               |                | Tree structure (Spanning Tree)     | 90, 97     |
| <b>P</b>                               |                | Trunk                              | 19         |
| <b>R</b>                               |                | <b>V</b>                           |            |
| <b>S</b>                               |                | Virtual Router Redundancy Protocol | 117        |
| <b>T</b>                               |                | VLAN (HIPER-Ring)                  | 35         |
| <b>V</b>                               |                | <b>U</b>                           |            |
| <b>U</b>                               |                | UM RedundConfig L3P                |            |
| <b>U</b>                               |                | Release 9.0 02/2015                |            |

|                                |          |
|--------------------------------|----------|
| VRRP                           | 16, 117  |
| VRRP Authentication Error Trap | 118      |
| VRRP advertisement interval    | 121      |
| VRRP instance                  | 119      |
| VRRP Master Trap               | 118      |
| VRRP router instance           | 121      |
| VRRP statistics                | 125      |
| VRRP Tracking                  | 127, 127 |
| VRRP (configuration)           | 118      |
| VRRP/HiVRRP                    | 13       |

## 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



**HIRSCHMANN**

A **BELDEN** BRAND

# User Manual

**Routing Configuration**

**Industrial ETHERNET (Gigabit-)Switch**

**PowerMICE, MACH 104, MACH 1040, MACH 4000**

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>7</b>  |
|          | <b>About this Manual</b>                                          | <b>9</b>  |
|          | <b>Key</b>                                                        | <b>11</b> |
| <b>1</b> | <b>Configuration</b>                                              | <b>13</b> |
| <b>2</b> | <b>Routing - Basics</b>                                           | <b>15</b> |
| 2.1      | ARP                                                               | 18        |
| 2.2      | CIDR                                                              | 21        |
| 2.3      | Net-directed Broadcasts                                           | 23        |
| 2.4      | Multinetting                                                      | 24        |
| <b>3</b> | <b>Static Routing</b>                                             | <b>25</b> |
| 3.1      | Port-based Router Interface                                       | 26        |
|          | 3.1.1 Configuration of the router interfaces                      | 27        |
| 3.2      | VLAN-based Router-Interface                                       | 29        |
| 3.3      | Configuration of a Static Route                                   | 33        |
|          | 3.3.1 Configuration of a simple static route                      | 34        |
|          | 3.3.2 Configuration of a redundant static route                   | 35        |
|          | 3.3.3 Configuration of a redundant static route with load sharing | 37        |
| 3.4      | Static route tracking                                             | 38        |
|          | 3.4.1 Description of the static route tracking function           | 38        |
|          | 3.4.2 Application example for the static route tracking function  | 39        |
| 3.5      | Adaptation for non-IP-compliant devices                           | 42        |
| <b>4</b> | <b>Tracking</b>                                                   | <b>45</b> |
| 4.1      | Interface tracking                                                | 46        |
| 4.2      | Ping tracking                                                     | 48        |
| 4.3      | Logical tracking                                                  | 50        |

|          |                                            |           |
|----------|--------------------------------------------|-----------|
| 4.4      | Configuring the tracking                   | 51        |
| 4.4.1    | Configuring interface tracking             | 51        |
| 4.4.2    | Application example for ping tracking      | 53        |
| 4.4.3    | Application example for logical tracking   | 54        |
| <b>5</b> | <b>VRRP/HiVRRP</b>                         | <b>57</b> |
| 5.1      | VRRP                                       | 58        |
| 5.1.1    | Configuration of VRRP                      | 61        |
| 5.2      | HiVRRP                                     | 62        |
| 5.3      | HiVRRP Domains                             | 66        |
| 5.3.1    | Configuration of HiVRRP domains            | 67        |
| 5.3.2    | Example of configuration of HiVRRP domains | 68        |
| 5.4      | VRRP tracking                              | 72        |
| 5.5      | VRRP with load sharing                     | 78        |
| 5.6      | VRRP mit Multinetting                      | 79        |
| <b>6</b> | <b>RIP</b>                                 | <b>81</b> |
| 6.1      | Convergence                                | 83        |
| 6.2      | Maximum Network Size                       | 86        |
| 6.3      | General Properties of RIP                  | 87        |
| 6.4      | Configuring the RIP                        | 88        |
| <b>7</b> | <b>OSPF</b>                                | <b>91</b> |
| 7.1      | OSPF-Topology                              | 93        |
| 7.1.1    | Autonomous System                          | 93        |
| 7.1.2    | Router ID                                  | 94        |
| 7.1.3    | Areas                                      | 94        |
| 7.1.4    | Virtual Link                               | 97        |
| 7.1.5    | OSPF Router                                | 99        |
| 7.1.6    | Link State Advertisement                   | 99        |
| 7.2      | General Operation of OSPF                  | 101       |
| 7.3      | Setting up the Adjacency                   | 102       |
| 7.4      | Synchronization of the LSD                 | 105       |
| 7.5      | Route Calculation                          | 107       |
| 7.6      | Configuring OSPF                           | 108       |

|          |                                              |            |
|----------|----------------------------------------------|------------|
| <b>8</b> | <b>Protocol-based VLANs</b>                  | <b>113</b> |
| 8.1      | General Configuration                        | 115        |
| 8.2      | Configuration of the Example                 | 116        |
| <b>9</b> | <b>Multicast Routing</b>                     | <b>119</b> |
| 9.1      | Multicast Addresses                          | 121        |
| 9.1.1    | IP Multicast Addresses                       | 121        |
| 9.1.2    | MAC Multicast Addresses                      | 123        |
| 9.1.3    | Mapping IP MAC Multicast Addresses           | 124        |
| 9.2      | Multicast Group Registration                 | 125        |
| 9.3      | PIM-DM/PIM-SM/DVMRP                          | 127        |
| 9.3.1    | How PIM-DM and DVMRP function                | 129        |
| 9.3.2    | How PIM-SM functions                         | 132        |
| 9.4      | Scoping                                      | 141        |
| 9.5      | Multicast Configuration                      | 142        |
| 9.5.1    | Example with Layer 3 Redundancy              | 142        |
| 9.5.2    | Example with Layer 2 redundancy (HIPER-Ring) | 146        |
| 9.5.3    | Tips for the configuration                   | 147        |
| <b>A</b> | <b>Appendix</b>                              | <b>151</b> |
| A.1      | Abbreviations used                           | 152        |
| A.2      | Underlying IEEE Standards                    | 154        |
| A.3      | List of RFCs                                 | 155        |
| A.4      | Entering the IP Parameters                   | 158        |
| A.5      | Copyright of Integrated Software             | 163        |
| A.5.1    | Bouncy Castle Crypto APIs (Java)             | 163        |
| A.5.2    | Broadcom Corporation                         | 164        |
| <b>B</b> | <b>Readers' Comments</b>                     | <b>165</b> |
| <b>C</b> | <b>Index</b>                                 | <b>167</b> |
| <b>D</b> | <b>Further Support</b>                       | <b>171</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 “Routing Configuration User Manual” document contains the information you need to start operating the routing function. It takes you step-by-step from a small router application through to the router configuration of a complex network.

The manual enables you to configure your router by following the examples.

The “Routing Configuration” user manual requires you to be familiar with the content of the “Basic Configuration” user manual.

You can use this manual to configure simple networks without any special knowledge. The configuration of complex networks requires well-founded knowledge on the subject of routing and of the protocols IP, RIP, OSPF, IGMP and VRRP.

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 and PROFINET IO.

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:

- ▶ 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](http://www.hirschmann.com)).

# 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 Configuration

Because the configuration of a router is very dependent on the conditions in your network, you are first provided with a general list of the individual configuration steps. To optimally cover the large number of options, this list is followed by examples of networks that usually occur in the industry sector. The examples are selected so that the configurations for other applications can be easily derived from them.

The configuration of the routing function usually contains the following steps:

- Drawing a network plan  
Create a picture of your network so that you can clearly see the division into subnetworks and the related distribution of the IP addresses. This step is very important. Good planning of the subnetworks with the corresponding network masks makes the router configuration much easier.
- Router basic settings  
Along with the global switching on of the routing function, the router basic settings also contain the assignment of IP addresses and network masks to the router interfaces.

**Note:** Adhere to the sequence of the individual configuration steps so that the configuration computer has access to all the layer 3 Switches throughout the entire configuration phase.

**Note:** When you assign an IP address from the subnetwork of the management IP address to a router interface, the Switch deletes the management IP address. You access the Switch via the IP address of the router interface.

Activate the routing globally before you assign an IP address from the subnetwork of the management IP address to a router interface.

**Note:** When you assign the VLAN ID of the management VLAN to a router interface, the Switch deactivates the management IP address. You access the Switch via the IP address of the router interface. The management VLAN is the VLAN by means of which you access the management of all the Switches.

**Note:** Depending on your configuration steps, it may be necessary to change the IP parameters of your configuration computer to enable access to the layer 3 Switches.

- Selecting a routing procedure  
On the basis of the network plan and the communication requirements of the connected devices, you select the optimal routing procedure (static routes, RIP, OSPF) for your situation. In doing so, consider which routing procedures the routers can use along a route.
- Configuring a routing procedure  
Configure the selected routing procedure.

## 2 Routing - Basics

A router is a node for exchanging data on the layer 3 of the ISO/OSI layer model.

This ISO/OSI reference model had the following goals:

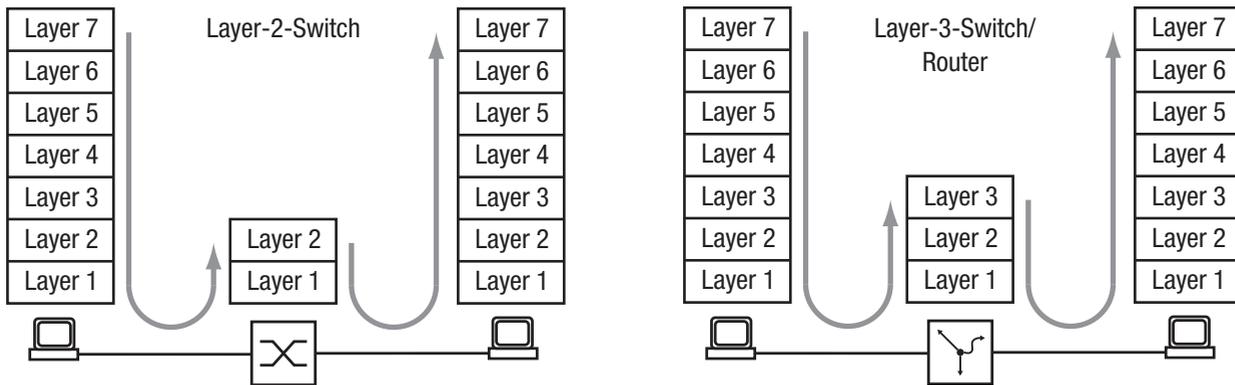
- ▶ To define a standard for information exchange between open systems;
- ▶ To provide a common basis for developing additional standards for open systems;
- ▶ To provide international teams of experts with functional framework as the basis for independent development of every layer of the model;
- ▶ To include in the model developing or already existing protocols for communications between heterogeneous systems;
- ▶ To leave sufficient room and flexibility for the inclusion of future developments.

The reference model consists of 7 layers, ranging from the application layer to the physical layer.

|   |              |                                                                                       |
|---|--------------|---------------------------------------------------------------------------------------|
| 7 | Application  | Access to communication services from an application program                          |
| 6 | Presentation | Definition of the syntax for data communication                                       |
| 5 | Session      | Set up and breakdown of connections by synchronization and organization of the dialog |
| 4 | Transport    | Specification of the terminal connection, with the necessary transport quality        |
| 3 | Network      | Transparent data exchange between two transport entities                              |
| 2 | Data-Link    | Access to physical media and detection of transmission errors                         |
| 1 | Physical     | Transmission of bit strings via physical media                                        |

*Table 1: OSI Reference Model*

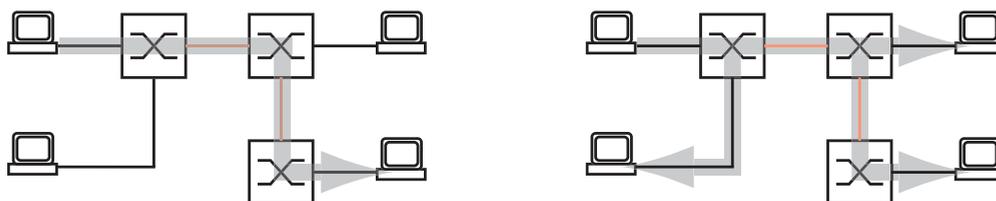
What does the data exchange on the layer 3 mean in comparison with the data exchange on the layer 2?



*Figure 1: Data Transport by a Switch and a Router in the OSI Reference Model's Layers*

On the layer 2, the MAC address signifies the destination of a data packet. The MAC address is an address tied to the hardware of a device. The layer 2 expects the receiver in the connected network. The data exchange to another network is the task of layer 3. Layer 2 data traffic is spread over the entire network. Every subscriber filters the data relevant for him from the data stream. Layer 2 switches are capable of steering the data traffic that is intended for a specific MAC address. It thus relieves some of the load on the network. Broadcast and multicast data packets are forwarded by the layer 2 switches at all ports.

IP is a protocol on the layer 3. IP provides the IP address for addressing data packets. The IP address is assigned by the network administrator. By systematically assigning IP addresses, he can thus structure his network, breaking it down into subnets ([see on page 21 "CIDR"](#)). The bigger a network gets, the greater the data volume. Because the available bandwidth has physical limitations, the size of a network is also limited. Dividing large networks into subnets limits the data volume on these subnets. Routers divide the subnets from each other and only transmit the data that is intended for another subnet.



*Figure 2: MAC Data Transmission: Unicast Data Packet (left) and Broadcast Data Packet (right)*

This illustration clearly shows that broadcast data packets can generate a considerable load on larger networks. You also make your network easier to understand by forming subnets, which you connect with each other using routers and, strange as it sounds, also separate securely from each other.

A Switch uses the MAC destination address to transmit, and thus uses layer 2.

A router uses the IP destination address to transmit, and thus uses layer 3. The subscribers associate the MAC and IP addresses using the Address Resolution Protocol (ARP).

## 2.1 ARP

The Address Resolution Protocol (ARP) determines the MAC address that belongs to an IP address. What is the benefit of this?

Let's suppose that you want to configure your Switch using the Web-based interface. You enter the IP address of your Switch in the address line of your browser. But which MAC address will your PC now use to display the information in the Switch in your browser window?

If the IP address of the Switch is in the same subnet as your PC, then your PC sends what is known as an ARP request. This is a MAC broadcast data packet that requests the owner of the IP address to send back his MAC address. The Switch replies with a unicast data packet containing his MAC address. This unicast data packet is called an ARP reply.

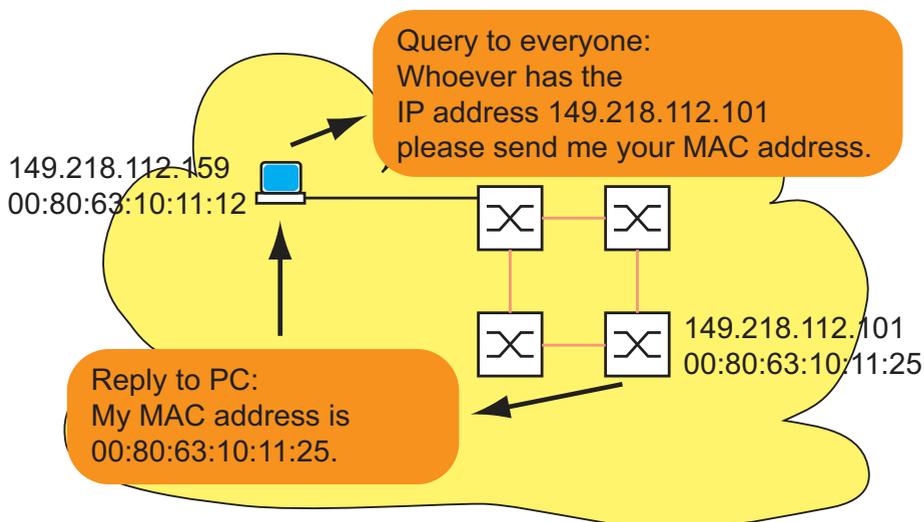


Figure 3: ARP request and reply

If the IP address of the Switch is in a different subnet, then the PC asks for the MAC address of the gateway entered in the PC. The gateway/router replies with its MAC address.

Now the PC packs the IP data packet with the IP address of the switch, the final destination, into a MAC frame with the MAC destination address of the gateway/router and sends the data.

The router receives the data and releases the IP data packet from the MAC frame, so that it can then forward it in accordance with its transmission rules.

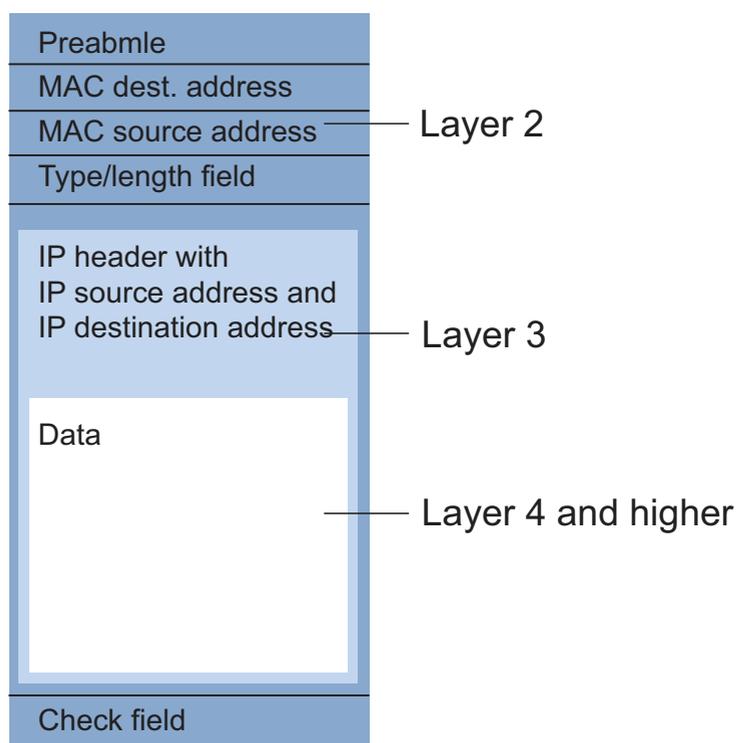


Figure 4: Structure of a data packet from the ISO/OSI layer model perspective

All terminal devices still working with IPs of the first generation, for example, are not yet familiar with the term 'subnet'. They also send an ARP request when they are looking for the MAC address for an IP address in a different subnet. They neither have a network mask with which they could recognize that the subnet is a different one, nor do they have a gateway entry. In the example below, the left PC is looking for the MAC address of the right PC, which is in a different subnet. In this example, it would normally not get a reply.

Because the router knows the route to the right PC, the proxy ARP function replies to this router interface on behalf of the right PC with its own MAC address. Thus the left PC can address its data to the MAC address of the router, which then forwards the data to the right PC.

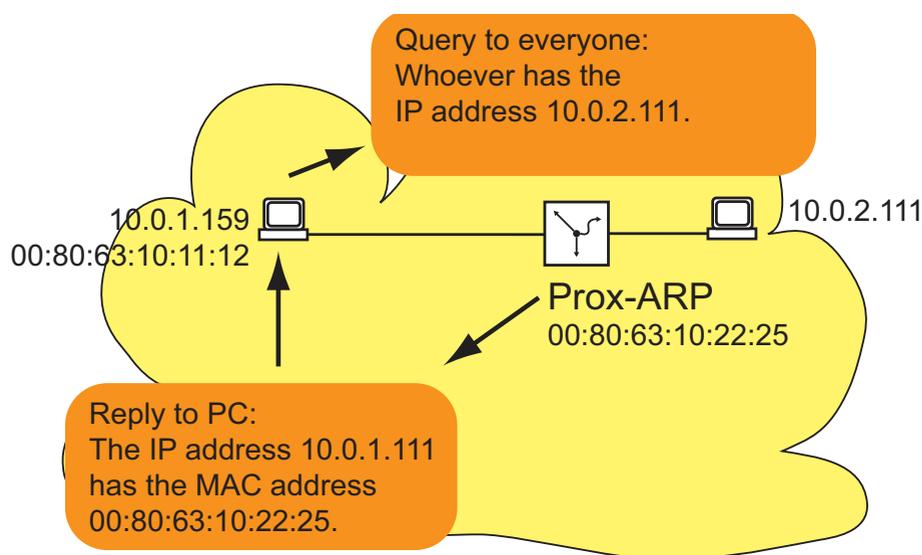


Figure 5: ARP proxy funktion

The proxy ARP function is available on the router interfaces on which you switch on the proxy ARP.

---

## 2.2 CIDR

The original class allocation of the IP addresses only planned for three address classes to be used by the users (see “Basics of IP Parameters” in the basic configuration of the user manual).

Since 1992, five classes of IP address have been defined in the RFC 1340.

| Class | Network part | Host part | Address range                |
|-------|--------------|-----------|------------------------------|
| A     | 1 byte       | 3 bytes   | 1.0.0.0 to 126.255.255.255   |
| 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*

Class C with a maximum of 254 addresses was too small, and class B with a maximum of 65534 addresses was too large for most users, as they would never require so many addresses. 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 this destination address.

The Classless Inter-Domain Routing (CIDR) provides a solution to these problems. The 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 network mask. The network mask indicates the number of bits that are identical for all IP addresses, the network part, 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 |
|                     |                       | ----- 25 mask bits -----            |

CIDR notation: 149.218.112.0/25

└----- Mask bits

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.

Using mask bits simplifies the routing table. The router determines in that direction in which most of the mask bits match (longest prefix match).

---

## 2.3 Net-directed Broadcasts

A net-directed Broadcast is an IP data packet that a device sends to the network Broadcast address<sup>1</sup> of a network to contact all the receivers of the network. A net-directed Broadcast is sent as a MAC Unicast frame in a transfer network. If the router locally responsible for this network supports net-directed Broadcasts, then it transmits this data packet as a MAC Broadcast frame into its local network. With VLAN-based router interfaces it transmits the frame to all the ports that are members in the VLAN of the Router interface.

Thus net-directed Broadcasts can relieve your transfer network of the multiple IP Unicasts that would be necessary to replace a net-directed Broadcast.

If the router does not support net-directed Broadcasts or if you switch off this function for a router interface, the router discards IP data packets received at the network Broadcast address of the router interface. With multinetting, this also applies to the secondary IP addresses of the router interface.

1. The network Broadcast address is the highest IP address of an IP network for which a router interface is responsible. The device determines the Broadcast address from its interface IP address and the related netmask. For example, if a router interface has the IP address 192.168.1.1 and the netmask 255.255.255.0, it is responsible for network 192.168.1.0/24. The network Broadcast address here is 192.168.1.255.

## 2.4 Multinetting

Multinetting allows you to connect a number of subnets to one router port. Multinetting provides a solution for when you want to connect existing subnets to a router within a physical medium. In this case you can use multinetting to assign a number of IP addresses for the different subnets to the routing port to which you are connecting the physical medium.

For a long-term solution, other network design strategies provide more advantages with regard to problem solving and bandwidth management.

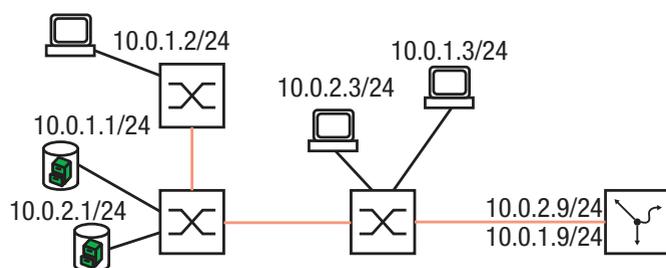


Figure 6: Example of multinetting

## 3 Static Routing

Static routes are user-defined routes which the Switch uses to transmit data from one subnet to another.

The user specifies to which router (next hop) the Switch forwards data for a particular subnet. Static routes are kept in a table which is permanently stored in the Switch.

Compared to dynamic routing, the advantage of this transparent route selection is offset by the increased workload involved in configuring the static routes. Static routing is therefore suited to very small networks or to selected areas of larger networks. Static routing makes the routes transparent for the administrator and can be easily configured in small networks.

If, for example, a line interruption causes the topology to change, the dynamic routing can react automatically to this, in contrast to the static routing. If you combine static and dynamic routing, you can configure the static routes in such a way that they have a higher priority than a route selected by a dynamic routing procedure.

The first step in configuring the router is to globally switch on the router function and configure the router interfaces.

The Switch allows you to define port-based and VLAN-based router interfaces (see figure 7).

Example: Connecting two production cells

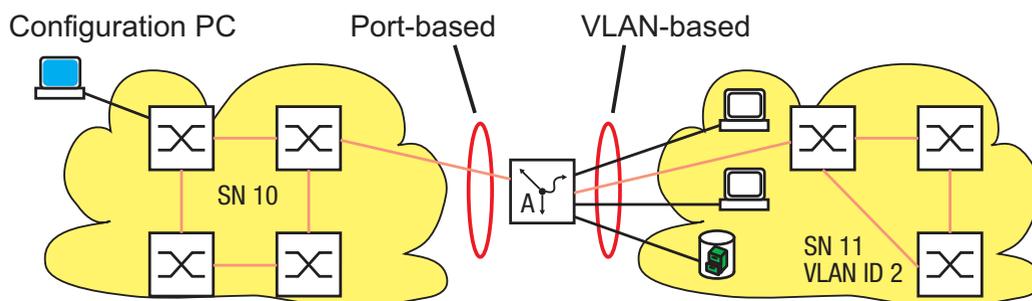


Figure 7: Static routes

## 3.1 Port-based Router Interface

A characteristic of the port-based router interface is that a subnet is connected to a port ([see figure 7](#)).

Special features of port-based router interfaces:

- ▶ If there is no active connection, then the entry from the routing table is omitted, because the router transmits exclusively to those ports for which the data transfer is likely to be successful.  
The entry in the interface configuration table remains.
- ▶ A port-based router interface does not recognize VLANs, which means that the router rejects tagged frames which it receives at a port-based router interface.
- ▶ A port-based router interface rejects all the non-routable packets.

Below ([see figure 8](#)) you will find an example of the simplest case of a routing application with port-based router interfaces.

### 3.1.1 Configuration of the router interfaces

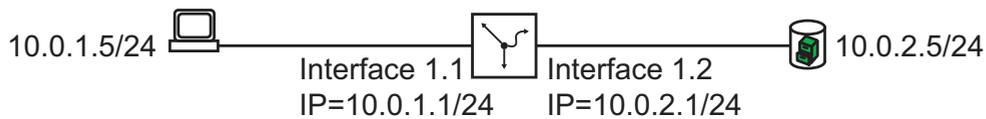


Figure 8: Simplest case of a route

```

enable
configure
ip routing

interface 2/1
ip address 10.0.1.1
 255.255.255.0
routing
exit

interface 2/2
ip address 10.0.2.1
 255.255.255.0
routing
ip netdirbcast

exit
exit

show ip interface brief

Interface IP Address IP Mask Netdir Multi
----- -
2/1 10.0.1.1 255.255.255.0 Disable Disable
2/2 10.0.2.1 255.255.255.0 Enable Disable

show ip interface 2/1

```

Change to the privileged EXEC mode.  
Change to the Configuration mode.  
Switch on the router function globally.

Select the first port for entering the router interface IP address.  
Assign the port its IP parameters.

Switch on the router function at this port.  
Change to the Configuration mode.

Select the second port for entering the router interface IP address.  
Assign the port its IP parameters.

Switch on the router function at this port.  
Einschalten der Vermittlung von Netdirected Broadcasts an diesem Port.

Change to the Configuration mode.  
Change to the privileged EXEC mode.

Check the entries.

Check the remaining settings for interface 2/1.

```

Primary IP Address..... 10.0.1.1/255.255.255.0
Routing Mode..... Enable
Administrative Mode..... Enable
Forward Net Directed Broadcasts..... Enable
Proxy ARP..... Disable
Active State..... Active
Link Speed Data Rate..... 100 Full
MAC Address..... 00:80:63:51:74:0C
Encapsulation Type..... Ethernet
IP MTU..... 1500

```

show ip route

Verify the routing table:

```

Total Number of Routes..... 2
 Network Subnet Next Hop Next Hop
 Address Mask Protocol Intf IP Address

10.0.1.0 255.255.255.0 Local 2/1 10.0.1.1
10.0.2.0 255.255.255.0 Local 2/2 10.0.2.1

```

show ip route bestroutes

Check which routes the router actually uses for the transmission.

```

 Network Subnet Next Hop Next Hop
 Address Mask Protocol Intf IP Address

10.0.1.0 255.255.255.0 Local 2/1 10.0.1.1
10.0.2.0 255.255.255.0 Local 2/2 10.0.2.1

Total Number of Routes..... 2

```

**Note:** To be able to see these entries in the routing table, you need an active connection at the ports.

## 3.2 VLAN-based Router-Interface

A characteristic of the VLAN-based router interface is that a number of devices in a VLAN are connected to different ports. The devices within a subnet belong to one VLAN (see figure 7).

Within a VLAN, the Switch exchanges data packets on layer 2. Terminal devices address data packets with a destination address in another subnet to the router as a gateway. The router then exchanges the data packets layer 3.

Below you will find an example of the simplest case of a routing application with VLAN-based router interfaces. For the VLAN 2, the router combines ports 3.1 and 3.2 into the VLAN router interface 9.1. A VLAN router interface remains in the routing table until at least one port of the VLAN has a connection.

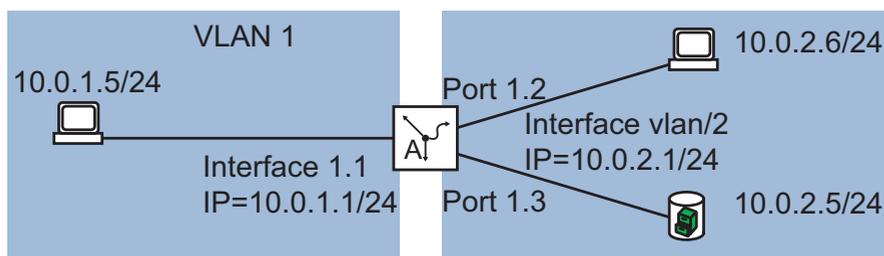


Figure 9: VLAN-based router interface

Configuring a VLAN router interface:

```
enable
vlan database
vlan 2

vlan name 2 Gerhard
vlan routing 2

exit
```

Switch to the privileged EXEC mode.

Switch to the VLAN mode.

Create a VLAN by entering the VLAN ID. The VLAN ID is between 1 and 4,042 (MACH 4000: 3,966).

Assign the name "Gerhard" to VLAN 2.

Create a virtual router interface and activate the router function at this interface.

Switch to the privileged EXEC mode.

show ip vlan Display the virtual router interface that the router has set up for the VLAN.

```
show ip vlan
 Logical
VLAN ID Interface IP Address Subnet Mask MAC Address

2 9/1 0.0.0.0 0.0.0.0 00:80:63:51:74:2C
```

show ip interface brief Check the entry for the virtual router interface.

```
Interface IP Address IP Mask Netdir Multi

9/1 0.0.0.0 0.0.0.0 Disable Disable
```

```
configure Switch to the Configuration mode.
interface 9/1 Change to the interface configuration mode of interface 9/1.

ip address 10.0.2.1 Assign the IP parameters to the router interface.
255.255.255.0

routing Activate the router function at this interface.
ip netdirbcast Enable the transmission of net-directed broadcasts for this interface.

exit Switch to the Configuration mode.

interface 3/1 Switch to the interface configuration mode of interface 3/1.

vlan participation include 2 Declare port 3.1 a member of VLAN 2.
vlan participation exclude 1 Remove port 3.1 from VLAN 1. In the state on delivery, every port is assigned to VLAN 1.

vlan pvid 2 Set the port VLAN-ID to 2, which means that data packets that are received without a tag at that port are assigned to VLAN 2 by the Switch.

exit Switch to the Configuration mode.

interface 3/2 Switch to the interface configuration mode of interface 3/2.

vlan participation include 2 Declare port 3.2 a member of VLAN 2.
vlan participation exclude 1 Remove port 3.2 from VLAN 1. In the state on delivery, every port is assigned to VLAN 1.

vlan pvid 2 Set the port VLAN-ID to 2, which means that data packets that are received without a tag at that port are assigned to VLAN 2 by the Switch.

exit Switch to the Configuration mode.
exit Switch to the privileged EXEC mode.
```

```
show vlan 2
```

Check your entries in the static VLAN table.

```
VLAN ID: 2
VLAN Name: Gerhard
VLAN Type: Static
```

| Interface | Current | Configured | Tagging  |
|-----------|---------|------------|----------|
| 1/1       | Exclude | Autodetect | Untagged |
| 1/2       | Exclude | Autodetect | Untagged |
| 1/3       | Exclude | Autodetect | Untagged |
| 1/4       | Exclude | Autodetect | Untagged |
| 2/1       | Exclude | Autodetect | Untagged |
| 2/2       | Exclude | Autodetect | Untagged |
| 2/3       | Exclude | Autodetect | Untagged |
| 2/4       | Exclude | Autodetect | Untagged |
| 3/1       | Include | Include    | Untagged |
| 3/2       | Include | Include    | Untagged |
| 3/3       | Exclude | Autodetect | Untagged |
| 3/4       | Exclude | Autodetect | Untagged |
| 4/1       | Exclude | Autodetect | Untagged |
| 4/2       | Exclude | Autodetect | Untagged |
| 4/3       | Exclude | Autodetect | Untagged |
| 4/4       | Exclude | Autodetect | Untagged |
| 8/1       | Exclude | Autodetect | Untagged |

```
show vlan port all
```

Check the VLAN-specific port settings.

| Interface | Port<br>VLAN ID | Acceptable<br>Frame Types | Ingress<br>Filtering | Default<br>Priority |
|-----------|-----------------|---------------------------|----------------------|---------------------|
| 1/1       | 1               | Admit All                 | Disable              | 0                   |
| 1/2       | 1               | Admit All                 | Disable              | 0                   |
| 1/3       | 1               | Admit All                 | Disable              | 0                   |
| 1/4       | 1               | Admit All                 | Disable              | 0                   |
| 2/1       | 1               | Admit All                 | Disable              | 0                   |
| 2/2       | 1               | Admit All                 | Disable              | 0                   |
| 2/3       | 1               | Admit All                 | Disable              | 0                   |
| 2/4       | 1               | Admit All                 | Disable              | 0                   |
| 3/1       | 2               | Admit All                 | Disable              | 0                   |
| 3/2       | 2               | Admit All                 | Disable              | 0                   |
| 3/3       | 1               | Admit All                 | Disable              | 0                   |
| 3/4       | 1               | Admit All                 | Disable              | 0                   |
| 4/1       | 1               | Admit All                 | Disable              | 0                   |
| 4/2       | 1               | Admit All                 | Disable              | 0                   |
| 4/3       | 1               | Admit All                 | Disable              | 0                   |
| 4/4       | 1               | Admit All                 | Disable              | 0                   |
| 8/1       | 1               | Admit All                 | Disable              | 0                   |

- Select the dialog `Routing:Interfaces:Configuration`.
- Click on “Assistant” at the bottom right to configure the VLAN router interface.
  
- Enter a number between 1 and 4,042 (MACH 4000: 3,966) as the VLAN-ID, in this example: 2.
- Click on “Next” at the bottom.
  
- In the “VLAN Name” line above, enter a name with which you want to identify the VLAN.
- In the “Member” column of the table, you select the ports which will belong to this VLAN.
- Click on “Next” at the bottom.
  
- In the “IP Address” line of the “Primary Address” frame, you enter the IP address for the VLAN.
- Enter the related network mask in the “Network mask” line.
- Click on “Close” to end the configuration of the VLAN-based router interface.

In the router interface table, the router interface 9.1 appears. In the static VLAN table, the VLAN appears.

- Tick the box in the column „net-directed broadcasts“ for the router interface 9.1.

With “Delete“, you have the opportunity to delete a selected virtual router interface from the table or to reset a physical router interface’s entry.

**Note:** When you delete a VLAN router interface, the entry for the VLAN will remain in the VLAN table.

Deleting a VLAN deletes the VLAN router interface’s entry in the router interface table.

## 3.3 Configuration of a Static Route

In the example below, router A requires the information that it can reach the subnet 10.0.3.0/24 via the router B (next hop). It can obtain this information via a dynamic routing protocol or via a static routing entry. With this information, router A can transmit data from subnet 10.0.1.0/24 via router B into subnet 10.0.3.0/24.

Vice versa to be able to forward data of subnet 10.0.1.0/24 router B also needs an equivalent route.

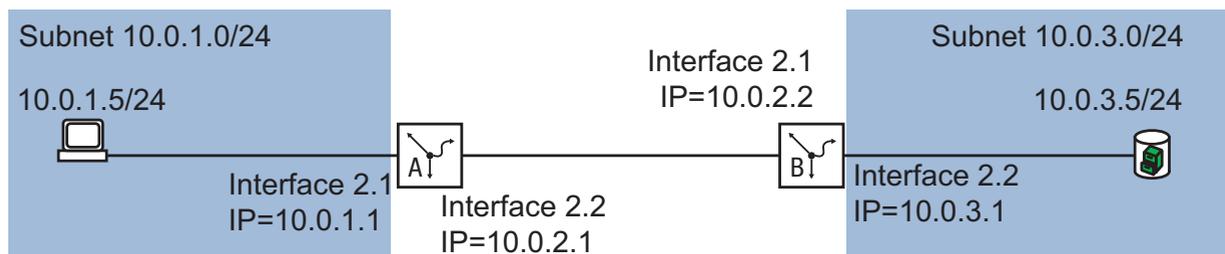


Figure 10: Static Routing

You can enter static routing for port-based and VLAN-based router interfaces.

### 3.3.1 Configuration of a simple static route

Enter a static route for router A based on the configuration of the router interface in the previous example (see figure 8):

```

enable Switch to the privileged EXEC mode.
configure Switch to the Configuration mode.
ip routing Switch on the router function globally.
ip route 10.0.3.0 Create the static routing entry
 255.255.255.0 10.0.2.2
exit Switch to the privileged EXEC mode.

show ip route Verify the routing table:

Total Number of Routes..... 3

 Network Subnet Next Hop Next Hop
 Address Mask Protocol Intf IP Address

10.0.1.0 255.255.255.0 Local 2/1 10.0.1.1
10.0.2.0 255.255.255.0 Local 2/2 10.0.2.1
10.0.3.0 255.255.255.0 Static 2/2 10.0.2.2

```

Configure router B in the same way.

### 3.3.2 Configuration of a redundant static route

To ensure a reliable connection between the two routers, you can connect the two routers with two or more lines.

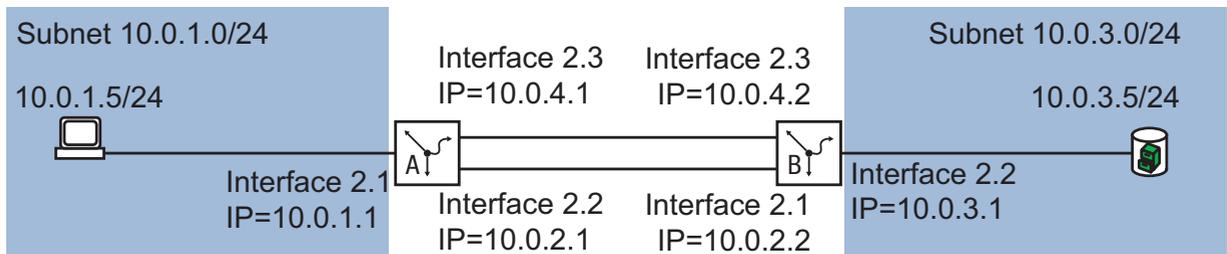


Figure 11: Redundant static route

You have the option of assigning importance (distance) to a route. If there are a number of routes to a destination, then the router chooses the route with the highest importance. If you do not assign a value for the importance during the configuration, the router takes the default value “1” for the importance. This is the highest importance.

□ Configure router A.

```
enable
configure
interface 2/3

ip address 10.0.4.1
 255.255.255.0

routing
exit

ip route 10.0.3.0
 255.255.255.0 10.0.4.2 2
```

Switch to the privileged EXEC mode.

Switch to the Configuration mode.

Select the port at which you want to connect the redundant route.

Assign the port its IP parameters.

Switch on the router function at this port.

Switch to the Configuration mode.

Create the static routing entry for the redundant route. The “2” at the end of the command is the importance value.

When both routes are available, the router uses the route via subnetwork 10.0.2.0/24, because this route has the higher importance (default value = 1) ([see on page 34 “Configuration of a simple static route”](#)).

show ip route

Verify the routing table:

Total Number of Routes..... 5

| Network Address | Subnet Mask   | Protocol | Next Hop Intf | Next Hop IP Address |
|-----------------|---------------|----------|---------------|---------------------|
| 10.0.1.0        | 255.255.255.0 | Local    | 2/1           | 10.0.1.1            |
| 10.0.2.0        | 255.255.255.0 | Local    | 2/2           | 10.0.2.1            |
| 10.0.3.0        | 255.255.255.0 | Static   | 2/2           | 10.0.2.2            |
| 10.0.3.0        | 255.255.255.0 | Static   | 2/3           | 10.0.4.2            |
| 10.0.4.0        | 255.255.255.0 | Local    | 2/3           | 10.0.4.1            |

show ip route bestroutes

Check which routes the router actually uses for the transmission.

| Network Address | Subnet Mask   | Protocol | Next Hop Intf | Next Hop IP Address |
|-----------------|---------------|----------|---------------|---------------------|
| 10.0.1.0        | 255.255.255.0 | Local    | 2/1           | 10.0.1.1            |
| 10.0.2.0        | 255.255.255.0 | Local    | 2/2           | 10.0.2.1            |
| 10.0.3.0        | 255.255.255.0 | Static   | 2/2           | 10.0.2.2            |
| 10.0.4.0        | 255.255.255.0 | Local    | 2/3           | 10.0.4.1            |

Total Number of Routes..... 4

Configure router B in the same way.

### 3.3.3 Configuration of a redundant static route with load sharing

The router shares the load between the two routes (load sharing), when the routes have the same importance (distance).

```
ip route 10.0.3.0
255.255.255.0 10.0.2.2 2
```

assign the importance "2" to the existing static routing entry (see on page 34 "Configuration of a simple static route").

When both routes are available, the router uses both routes for the data transmission.

```
show ip route
```

Verify the routing table:

```
Total Number of Routes..... 4
```

| Network Address | Subnet Mask   | Protocol | Next Hop Intf | Next Hop IP Address |
|-----------------|---------------|----------|---------------|---------------------|
| 10.0.1.0        | 255.255.255.0 | Local    | 2/1           | 10.0.1.1            |
| 10.0.2.0        | 255.255.255.0 | Local    | 2/2           | 10.0.2.1            |
| 10.0.3.0        | 255.255.255.0 | Static   | 2/2           | 10.0.2.2            |
| 10.0.4.0        | 255.255.255.0 | Local    | 2/3           | 10.0.4.2            |
| 10.0.4.0        | 255.255.255.0 | Local    | 2/3           | 10.0.4.1            |

```
show ip route bestroutes
```

Check which routes the router actually uses for the transmission.

| Network Address | Subnet Mask   | Protocol | Next Hop Intf | Next Hop IP Address |
|-----------------|---------------|----------|---------------|---------------------|
| 10.0.1.0        | 255.255.255.0 | Local    | 2/1           | 10.0.1.1            |
| 10.0.2.0        | 255.255.255.0 | Local    | 2/2           | 10.0.2.1            |
| 10.0.3.0        | 255.255.255.0 | Static   | 2/2           | 10.0.2.2            |
| 10.0.4.0        | 255.255.255.0 | Local    | 2/3           | 10.0.4.2            |
| 10.0.4.0        | 255.255.255.0 | Local    | 2/3           | 10.0.4.1            |

```
Total Number of Routes..... 4
```

## 3.4 Static route tracking

### 3.4.1 Description of the static route tracking function

With static routing, if there are a number of routes to a destination, the router chooses the route with the highest importance. The router detects an existing route by the state of the router interface. While connection L 1 (see table 3) on the router interface may be fine, the connection to remote router B at location L 2 may be interrupted. In this case, the router continues transmitting via the interrupted route.

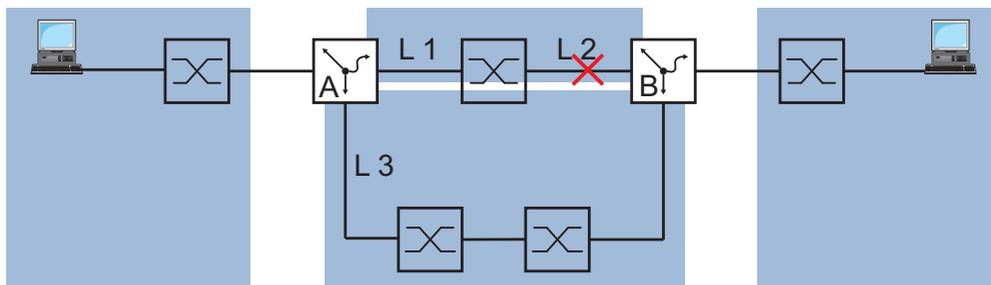


Figure 12: Example of static route tracking

With the static route tracking function, the router uses a tracking object such as a ping tracking object (see on page 48 “Ping tracking”) to detect the connection interruption. The active static route tracking function then deletes the interrupted route from the current routing table. If the tracking object returns to the “up” state, the router enters the static route in the current routing table again.

### 3.4.2 Application example for the static route tracking function

The figure (see figure 13) shows an example of the static route tracking function:

Router A monitors the best route via L 1 with ping tracking. If there is a connection interruption, router A transmits via redundant connection L 3. The following is known:

| Parameter                     | Router A      | Router B      |
|-------------------------------|---------------|---------------|
| IP address interface (IF) 1.1 | 10.0.4.1      |               |
| IP address interface (IF) 1.2 | 10.0.2.1      | 10.0.4.2      |
| IP address interface (IF) 1.3 |               | 10.0.2.53     |
| IP address interface (IF) 1.4 | 10.0.1.112    |               |
| IP address interface (IF) 2.2 |               | 10.0.5.1      |
| Netmask                       | 255.255.255.0 | 255.255.255.0 |

Prerequisites for further configuration:

- ▶ The IP parameters of the router interface are configured. (see on page 27 “Configuration of the router interfaces”)
- ▶ The router function is activated globally and at the ports/router interface.
- ▶ Ping tracking at interface 1.2 of router A is configured (see on page 53 “Application example for ping tracking”).

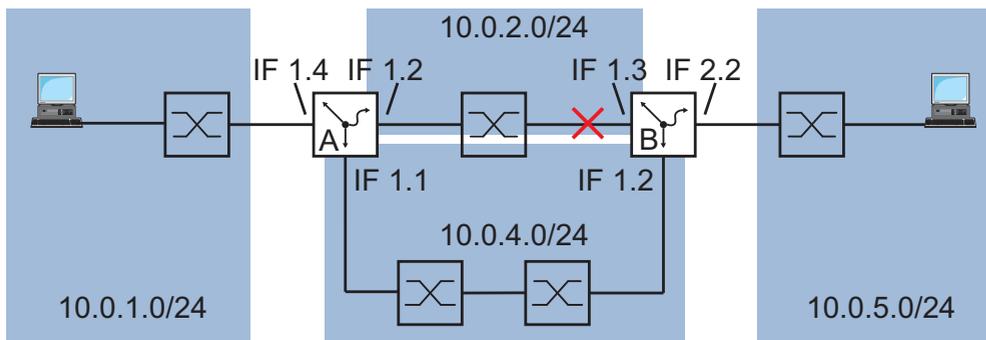


Figure 13: Configuring static route tracking

- Enter the two routes to destination network 10.0.5.0/24 in the static routing table of router A.

- Select the dialog  
Routing:Routing Table:Static.
- Click on “Create Entry”.  
You thus open the input window for a new entry.
- Enter the data for the first static route:
 

|                       |               |
|-----------------------|---------------|
| “Destination Network” | 10.0.5.0      |
| “Destination Netmask” | 255.255.255.0 |
| “Next Hop”            | 10.0.2.53     |
| “Track ID”            | 21            |
- Click "OK".
- Click on “Create Entry”.  
You thus open the input window for a new entry.

- Enter the data for the first static route:
  - “Destination Network”                    10.0.5.0
  - “Destination Netmask”                    255.255.255.0
  - “Next Hop”                                10.0.4.2
  - “Track ID”                                 0
- Click "OK".

```

enable
configure
ip route 10.0.5.0
 255.255.255.0 10.0.2.53 1
 track 21
ip route 10.0.5.0
 255.255.255.0 10.0.4.2 2
exit

show ip route

Total Number of Routes..... 3

 Network Subnet Next Hop Next Hop
 Address Mask Protocol Intf IP Address

10.0.1.0 255.255.255.0 Local 1/4 10.0.1.112
10.0.2.0 255.255.255.0 Local 1/2 10.0.2.1
10.0.5.0 255.255.255.0 Static 1/2 10.0.2.53

```

- On router B, create a ping tracking object with the track ID, for example 22, for IP address 10.0.2.1.
- Enter the two routes to destination network 10.0.1.0/24 in the static routing table of router B.

| Destination Network | Destination Netmask | Next Hop | Preference | Track ID |
|---------------------|---------------------|----------|------------|----------|
| 10.0.1.0            | 255.255.255.0       | 10.0.2.1 | 1          | 22       |
| 10.0.1.0            | 255.255.255.0       | 10.0.4.1 | 2          |          |

Table 3: Static routing entries for router B

## 3.5 Adaptation for non-IP-compliant devices

Some devices use a simplified IP stack that does not correspond to the IP standard. Without an ARP request, these devices send their responses to the MAC address contained as the source address in the requesting packet (see figure below, no MAC/IP address resolution). These devices exhibit this behavior with ping requests in particular (ICMP echo request). Some of these devices also exhibit this behavior with other data packets.

As long as the router interface of the router to which such a device is connected is itself connected to the MAC address of the physical port, the router can receive and transmit the packet.

However, if the physical port belongs to a VLAN, the VLAN router interface then has its own MAC address. Thus the router rejects packets that are being sent to the port's MAC address.

A terminal device that performs the MAC/IP address resolution according to the IP standard starts an ARP request to determine the correct MAC address before sending the reply to the determined VLAN MAC address (see figure below: MAC/IP standard address resolution using ARP).

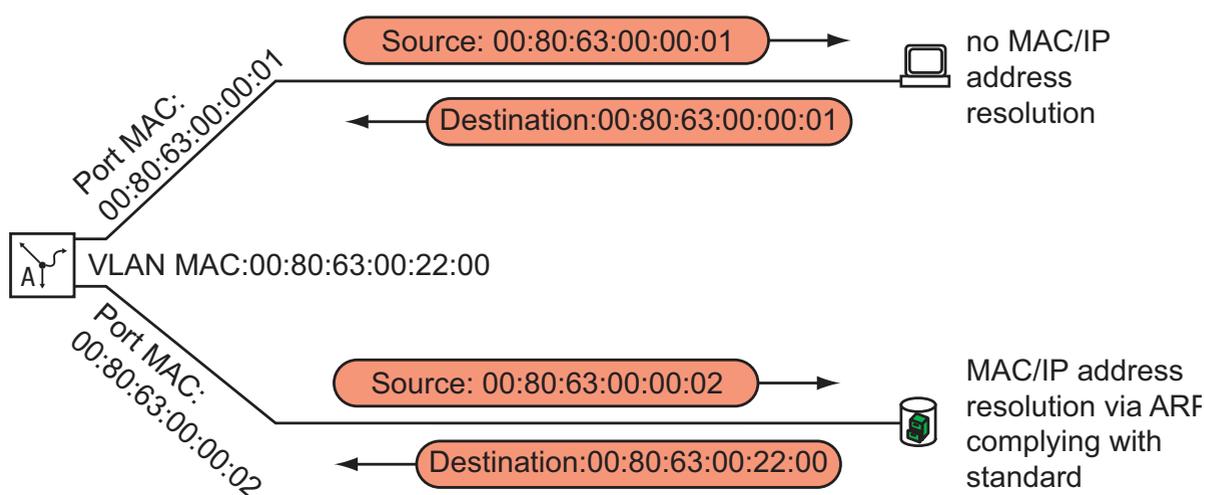


Figure 14: Addressing with simplified IP stack and compliant with the standard

For you also to be able to connect devices with a simplified IP stack to a VLAN-based router interface, the router provides you with the VLAN single MAC mode.

In the VLAN single MAC mode, all VLAN interfaces and all physical ports use the same MAC address, with the exception of the port-based router interface.

Activating the VLAN single MAC mode:

```
enable
configure
ip vlan-single-mac
exit
```

Switch to the privileged EXEC mode.  
Switch to the Configuration mode.  
Activating the VLAN single MAC mode.  
Switch to the privileged EXEC mode.

```
show ip vlan
```

Display the VLAN IP parameters

| VLAN ID | Logical Interface | IP Address    | Subnet Mask   | MAC Address       |
|---------|-------------------|---------------|---------------|-------------------|
| 100     | 9/1               | 192.168.100.1 | 255.255.255.0 | 00:80:63:51:74:2B |
| 200     | 9/2               | 192.168.200.1 | 255.255.255.0 | 00:80:63:51:74:2B |



## 4 Tracking

The tracking function gives you the option of monitoring certain objects, such as the availability of an interface.

A special feature of this function is that it forwards an object status change to an application, e.g. VRRP, which previously registered as an interested party for this information.

Tracking can monitor the following objects:

- ▶ Link status of an interface (interface tracking)
- ▶ Accessibility of a device (ping tracking)
- ▶ Result of logical connections of tracking entries (logic tracking)

An object can have the following statuses:

- ▶ up (OK)
- ▶ down (not OK)

The definition of "up" and "down" depends on the type of the tracking object (e.g. interface tracking).

Tracking can forward the state changes of an object to the following applications:

- ▶ VRRP ([see on page 72 "VRRP tracking"](#))
- ▶ Static routing ([see on page 38 "Static route tracking"](#))

## 4.1 Interface tracking

With interface tracking the Switch monitors the link status of:

- ▶ physical ports
- ▶ link aggregation interfaces (interfaces 8.x)
- ▶ VLAN router interfaces (interfaces 9.x)

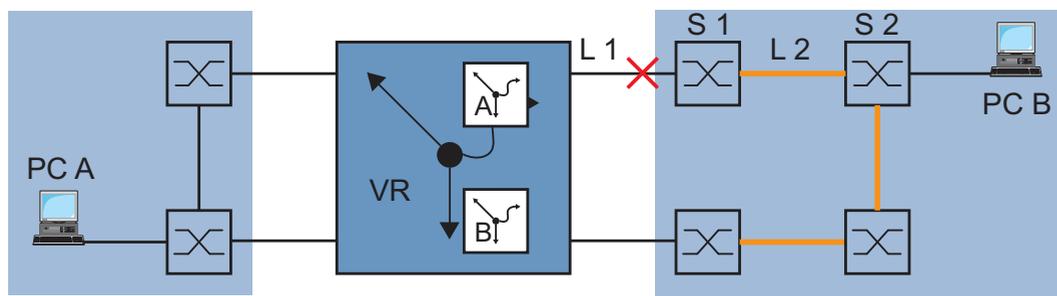


Figure 15: Monitoring a line with interface tracking

Ports/interfaces can have the following link statuses:

- ▶ interrupted physical link (link down) and
- ▶ existing physical link (link up).

A link aggregation interface has link status “down” if the link to all the participating ports is interrupted.

A VLAN router interface has link status “down” if the link is interrupted from all the physical ports/link aggregation interfaces that are members of the corresponding VLAN.

Setting a delay time enables you to insert a delay before informing the application about an object status change.

An interface tracking object is given the “down” status if the physical link interruption remains for longer than the “link down delay” delay time.

An interface tracking object is given the “up” status if the physical link holds for longer than the “link up delay” delay time.

State on delivery: delay times = 0 seconds.

This means that if a status changes, the registered application is informed immediately.

You can set the “link down delay” and “link up delay” delay times independently of each other in the range from 0 to 255 seconds.

You can define an interface tracking object for each interface.

## 4.2 Ping tracking

With ping tracking, the device uses ping requests to monitor the link status to other devices.

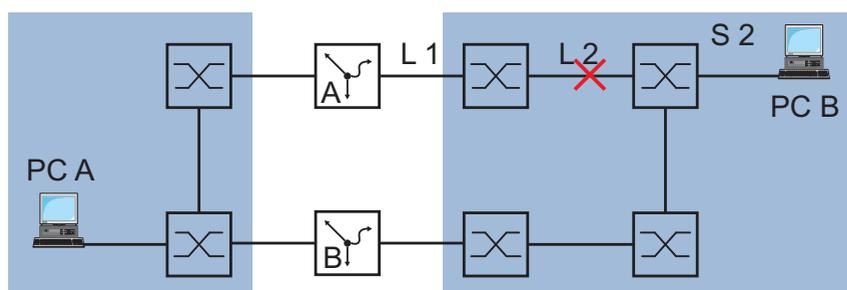


Figure 16: Monitoring a line with ping tracking

The device sends ping requests to the device with the IP address that you entered in the “IP Address” column.

The “Ping Interval” column allows you to define the frequency for sending ping requests, and thus the additional network load.

If the response comes back within the time entered in the “Ping Timeout” column, this response is a valid “Ping response received”.

If the response comes back after the time entered in the “Ping Timeout” column, or not at all, this response is evaluated as “No ping response”.

Ping tracking objects can have the following statuses:

- ▶ the number of “No ping responses” is greater than the number entered (down) and
- ▶ the number of “Ping responses received” is greater than the number entered (up).

Entering a number for unreceived or received ping responses enables you to set the sensitivity of the ping behavior of the device. The device informs the application about an object status change.

Ping tracking enables you to monitor the accessibility of defined devices. As soon as a monitored device can no longer be accessed, the device can choose to use an alternative path.

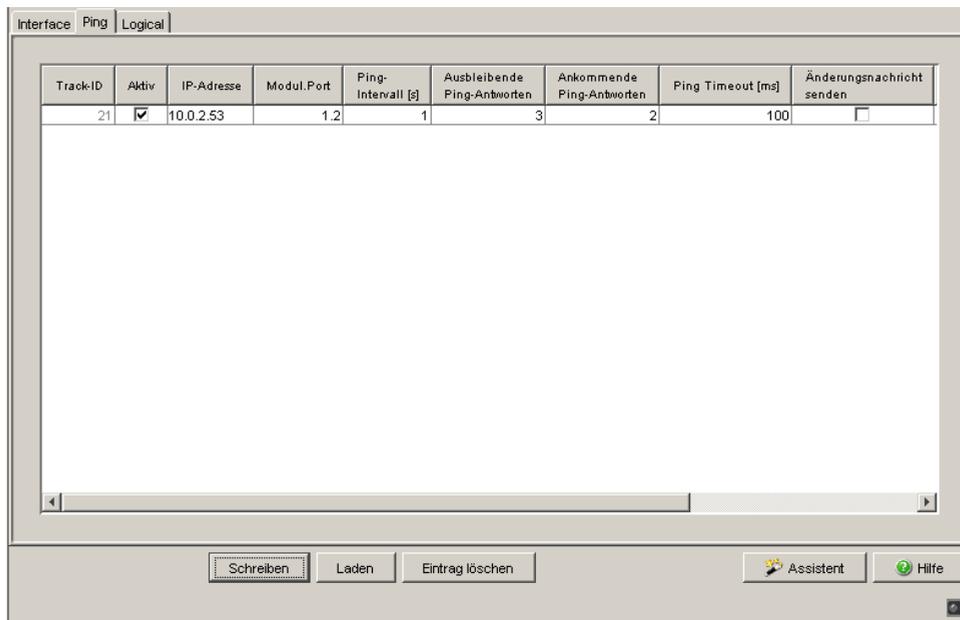


Figure 17: Ping Tracking dialog

## 4.3 Logical tracking

Logical tracking enables you to logically link multiple tracking objects with each other and thus perform relatively complex monitoring tasks.

You can use logical tracking, for example, to monitor the link status for a network node to which redundant paths lead ([see on page 54 “Application example for logical tracking”](#)).

The device provides the following options for a logical link:

- ▶ AND
- ▶ OR

For a logical link, you can combine up to 8 operands with one operator.

Logical tracking objects can have the following statuses:

- ▶ The result of the logical link is incorrect (down).
- ▶ The result of the logical link is correct (up).

When a logical link delivers the result “incorrect”, the device can choose to use an alternative path.

## 4.4 Configuring the tracking

You configure the tracking by setting up tracking objects. The following steps are required to set up a tracking object:

- ▶ Enter the tracking object ID number (track ID).
- ▶ Select a tracking type, e.g. interface.
- ▶ Depending on the track type, enter additional options such as “port” or “link up delay” in the interface tracking.

**Note:** The registration of applications (e.g. VRRP) to which the tracking function reports status changes is performed in the application itself ([see on page 72 “VRRP tracking”](#)).

### 4.4.1 Configuring interface tracking

- Set up interface tracking at port 1.1 with a link down delay of 0 seconds and a link up delay of 3 seconds.

- In the `Routing:Tracking:Configuration` dialog, click on “Wizard” at the bottom right.

Select type:

- Enter the values you desire:

Track ID:

1

Type:

interface

- Click on “Continue”.

**Properties:**

- 
- Enter the values you desire:

Module.Port: 1.1

Link up delay: 3

Link down delay: 0

- 
- Click on “Finish” to leave the Wizard and save the entry temporarily in the configuration.

```

enable Change to the privileged EXEC mode.
configure Change to the Configuration mode.
track 1 interface 1/1 Enter the tracking parameters and activate this
 link-down-delay 0 tracking object.
 link-up-delay 3
Tracking ID 1 created
 Tracking type set to Interface
 Target interface set to 1/1
 Link Down Delay for target interface set to 0 sec
 Link Up Delay for target interface set to 3 sec
Tracking ID 1 activated
exit Change to the privileged EXEC mode.
show track Display the configured tracks

```

| ID | Type | Intf | Link Down | Link Up | Status | Mode   | No. of Changes | Time since last change |
|----|------|------|-----------|---------|--------|--------|----------------|------------------------|
| 1  | Intf | 1/1  | 0s        | 3s      | DOWN   | Enable | 0              | 0 day(s), 00:00:29     |

Unconfigured Track-IDs with registered applications:  
-----

## 4.4.2 Application example for ping tracking

While the interface tracking monitors the directly connected link (see figure 15), the ping tracking monitors the entire link to Switch S2 (see figure 16).

- Set up ping tracking at port 1.2 for IP address 10.0.2.53 with the preset parameters.

- In the `Routing:Tracking:Configuration` dialog, click on “Wizard” at the bottom right.

Select type:

- Enter the values you desire:

Track ID: 21  
Type: ping

- Click on “Continue”.

Properties:

- Enter the values you desire:

IP address: 10.0.2.53  
Module.Port: 1.2  
Ping interval [s]: 1  
No ping response: 3  
Ping responses received: 2  
Ping timeout [ms]: 100

- Click on “Finish” to leave the Wizard and save the entry temporarily in the configuration.

```
enable
configure
track 21 ping 10.0.2.53
interface 1/2 interval 1 miss
3 success 2 timeout 100
```

Change to the privileged EXEC mode.

Change to the Configuration mode.

Enter the tracking parameters and activate this tracking object.

```

Tracking ID 21 created
 Tracking type set to Ping
 Target IP address set to 10.0.2.53
 Interface used for sending pings to target set to 1/2
 Ping Interval for target set to 1 sec
 Max. no. of missed ping replies from target set to 3
 Min. no. of received ping replies from target set to 2
 Timeout for ping replies from target set to 100 ms
Tracking ID 21 activated
exit
show track
Ping Tracking

```

Change to the privileged EXEC mode.

Display the configured tracks

| ID | Type | IP Address | Intvl | Status | Mode   | No. of Changes | Time since last change |
|----|------|------------|-------|--------|--------|----------------|------------------------|
| 21 | Ping | 10.0.2.53  | 1s    | DOWN   | Enable | 1              | 0 day(s), 00:13:39     |

### 4.4.3 Application example for logical tracking

The figure (see figure 15) shows an example of monitoring the connection to a redundant ring.

By monitoring lines L 2 and L 4, you can detect a line interruption from router A to the redundant ring.

With a ping tracking object at port 1.1 of router A, you monitor the connection to Switch S2.

With an additional ping tracking object at port 1.1 of router A, you monitor the connection to Switch S4.

Only the OR link of both ping tracking objects delivers the precise result that router A has no connection to the ring.

One ping tracking object for Switch S3 could indicate an interrupted connection to the redundant ring, but in this case there could be another reason for the lack of a ping response from Switch S3. For example, there could be a power failure at Switch S3.

The following is known:

| Parameter                | Value |
|--------------------------|-------|
| Operand No. 1 (track ID) | 21    |
| Operand No. 2 (track ID) | 22    |

Prerequisites for further configuration:

- ▶ The ping tracking objects for operands 1 and 2 are configured (see on page 53 “Application example for ping tracking”).

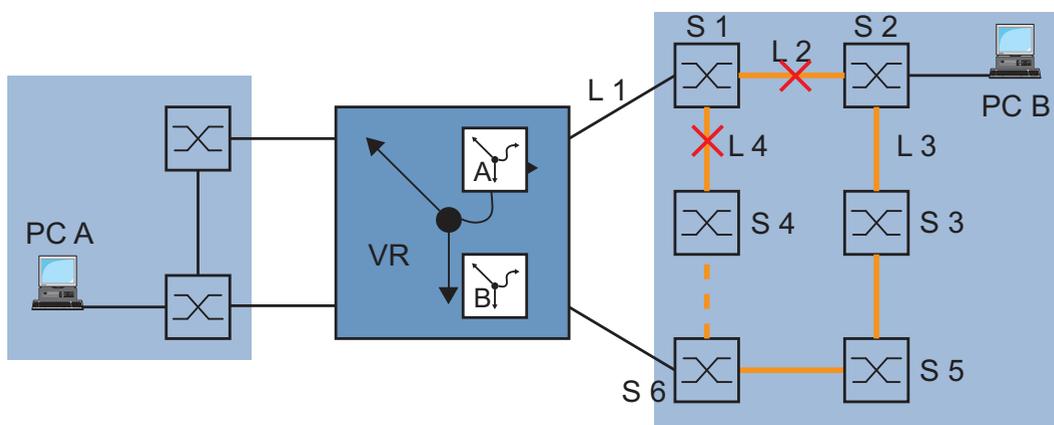


Figure 18: Monitoring the accessibility of a device in a redundant ring

Set up a logical tracking object as an OR link.

- In the `Routing:Tracking:Configuration` dialog, click on “Wizard” at the bottom right.

Select type:

- Enter the values you desire:

Track ID:

31

Type:

Logical

- Click on “Continue”.

**Properties:**

- Enter the values you desire:

Operator: or

Operand 1 (track ID): 21

Operand 2 (track ID): 22

- Click on "Finish" to leave the Wizard and save the entry temporarily in the configuration.

```

enable Change to the privileged EXEC mode.
configure Change to the Configuration mode.
track 31 logical or 21 22 Enter the tracking parameters and activate this
 tracking object.

Tracking ID 31 created
 Tracking type set to Logical
 Logical Operator set to or
 Logical Instance 21 included
 Logical Instance 1 included
Tracking ID 31 activated
exit Change to the privileged EXEC mode.
show track Display the configured tracks
Ping Tracking

 ID Type IP Address Intvl Status Mode No. of Time since

 21 Ping 10.0.2.53 1s DOWN Enable 1 0 day(s), 00:13:39

Ping Tracking

 ID Type IP Address Intvl Status Mode No. of Time since

 22 Ping 10.0.2.54 1s DOWN Enable 1 0 day(s), 00:14:39

Logical Tracking

 ID Type Instances Status Mode No. of Time since last change

 31 OR 21,22 DOWN Enable 0 0 day(s), 00:04:58

```

## 5 VRRP/HiVRRP

Terminal devices usually give you the option of entering a default gateway for transmitting data packets in external subnetworks. Here the term “Gateway” applies to a router by means of which the terminal device can communicate in other subnetworks.

If this router fails, the terminal device cannot send any more data to external subnetworks.

In this case, the Virtual Router Redundancy Protocol (VRRP) provides assistance.

VRRP is a type of “gateway redundancy”. VRRP describes a process that groups multiple routers into one virtual router. Terminal devices always address the virtual router, and VRRP ensures that a physical router belonging to the virtual router takes over the data transmission.

Even if a physical router fails, VRRP ensures that another physical router takes over the distribution tasks as part of the virtual router.

VRRP has typical switching times of 3 to 4 seconds when a physical router fails.

In many cases, such as Voice over IP, Video over IP, industrial controllers, etc., these long switching times are not acceptable.

The Hirschmann company has further developed the VRRP into the Hirschmann Virtual Router Redundancy Protocol (HiVRRP).

With the appropriate configuration, HiVRRP guarantees maximum switching times of 400 milliseconds.

Thanks to this guaranteed switching time, HiVRRP enables the use of “gateway redundancy” in time-critical applications. Even in tunnel controllers that require switching times of less than one second, the user can improve the network availability with this form of “gateway redundancy”.

## 5.1 VRRP

All the routers within a network on which VRRP is active specify among themselves which router is to be the master. This router contains the IP and MAC address of the virtual router. All the devices in the network that have entered this virtual IP address as the default gateway use the master as the default gateway.

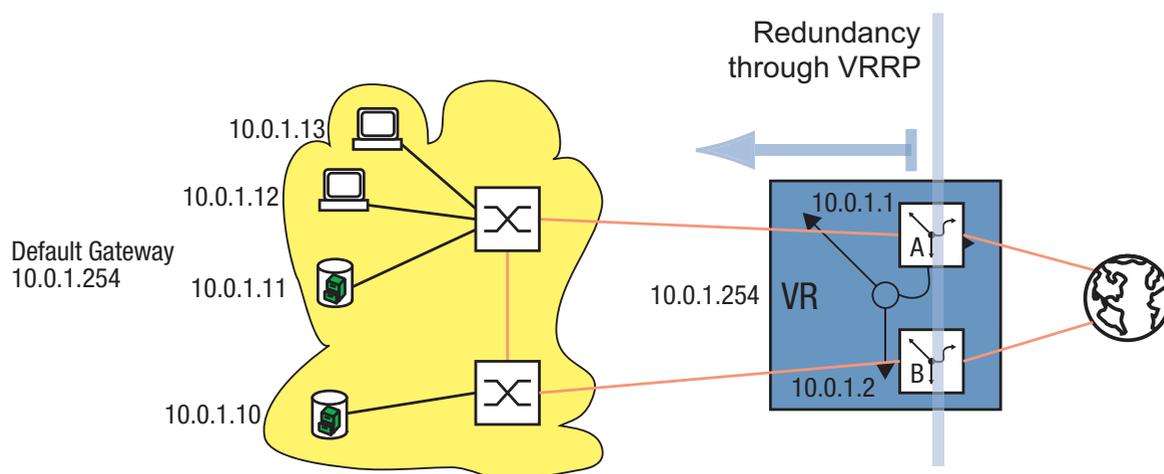


Figure 19: Illustration of the virtual router

If the master fails, then the remaining routers use the VRRP to specify a new master. This router then takes over the IP and MAC address of the virtual router. Thus the devices find their route via their default gateway, as before. The devices always only see the master with the virtual MAC and IP addresses, regardless of which router is actually behind this virtual address. The virtual router IP address is assigned by the administrator.

The VRRP specifies the virtual MAC address with:

00:00:5e:00:01:<VRID>.

The first 5 octets form the fixed part in accordance with RFC 2338.

The last octet is the virtual router ID (VRID). It is a number between 1 and 255. On the basis of this, the administrator can define 255 virtual routers within a network.



Figure 20: Virtual MAC address

The VRRP router sends IP Multicast messages to the IP Multicast address 224.0.0.18 in order to determine the master. The router with the highest VRRP priority becomes the master. The VRRP priority is specified by the administrator. If the VRRP priorities are the same, then the highest IP interface address of the VRRP routers is decisive. If the virtual IP address is the same as the IP address of a router interface, then this router is the IP address owner. VRRP sets the VRRP priority of an IP address owner to the value 255 and thus declares it the master. If there is no IP address owner, then VRRP declares the router with the highest VRRP priority the master.

The master regularly sends IP Multicast messages (default: 1 s) to the other VRRP routers in order to signal that it is ready for operation. If this message does not appear three times in a row, then the VRRP router with the highest remaining VRRP priority declares itself the new master.

- |                                                                                  |
|----------------------------------------------------------------------------------|
| 1. The IP address owner as it has the highest VRRP priority (255) by definition. |
| 2. The VRRP router with the highest VRRP priority.                               |
| 3. If the priorities are the same, the VRRP router with the highest IP address.  |

Table 4: Who shall be the master?

### VRRP terms:

- ▶ Virtual router  
A virtual router is a router or group of routers that act as the default gateway in a network and use the Virtual Router Redundancy Protocol.
- ▶ VRRP router  
A VRRP router is a router that uses VRRP. It can be part of one or more virtual routers.

- ▶ **Master router**  
The master router is the router within the virtual router that is currently responsible for forwarding data packets and responding to ARP queries. The master router periodically sends messages (advertisements) to the other VRRP routers (backup routers) to inform them about its existence.
- ▶ **Ip address owner**  
The IP address owner is the VRRP router whose IP address is identical to the IP address of the virtual router. By definition, it has the highest VRRP priority (255) and is thus automatically the master router.
- ▶ **Backup router**  
The backup router is a VRRP router that is not the master router. The backup router is ready to take over the master role, should the master fail.
- ▶ **VRRP priority**  
The VRRP priority is a number between 1 and 255. It is used to determine the master router. The value 255 is reserved for the IP address owner.
- ▶ **VRID**  
The VRID (virtual router ID) uniquely identifies a virtual router.
- ▶ **Virtual router MAC address**  
The virtual router MAC address is the MAC address of the virtual router (see figure 4).
- ▶ **Virtual router IP address**  
The virtual router IP address is the IP address of the virtual router.
- ▶ **Advertisement interval**  
The advertisement interval describes the frequency with which the master router sends its existence message (advertisement) to all the VRRP routers of its virtual router. The values for the advertisement interval are between 1 and 255 seconds. The default value is 1 second.
- ▶ **Skew time**  
The skew time is the time, dependent on the VRRP priority, that specifies the time when the backup router names itself the master router.  
$$\text{Skew time} = ((256 - \text{VRRP priority}) / 256) \cdot 1 \text{ second}$$
- ▶ **Master down interval**  
The master down interval specifies the time when the backup router names itself the master router.  
$$\text{Master down interval} = 3 \cdot \text{advertisement interval} + \text{skew time}$$

## 5.1.1 Configuration of VRRP

The configuration of VRRP requires the following steps:

- ▶ Switch on routing globally (if this has not already been done).
- ▶ Switch on VRRP globally.
- ▶ Configure port - assign IP address and network mask.
- ▶ Switch on VRRP at the port.
- ▶ Create virtual router ID (VRID), because you have the option of activating a multiple virtual routers for each port.
- ▶ Assign virtual router IP address.
- ▶ Switch on virtual router.
- ▶ Assign VRRP priority.

```
enable
configure
ip routing
ip vrrp

interface 2/3
ip address 10.0.1.1
 255.255.255.0
routing
ip vrrp 1

ip vrrp 1 mode
ip vrrp 1 ip 10.0.1.100
ip vrrp 1 priority 200
```

Switch to the privileged EXEC mode.  
Switch to the Configuration mode.  
Switch on the router function globally.  
Switch on VRRP globally.

Select the port for setting up VRRP.  
Assign the port its IP parameters.

Activate the router function at this interface.  
Create the VRID for the first virtual router at this port.

Switch on the first virtual router at this port.  
Assign virtual router 1 its IP address.  
Assign virtual router 1 the router priority 200.

- You configure every port at which VRRP will be active in the same way.
- You also perform the same configuration on the redundant router.

## 5.2 HiVRRP

HiVRRP provides a number of mechanisms for shortening the switching times or reducing the number of Multicasts:

- ▶ shorter advertisement intervals
- ▶ link-down notification
- ▶ preempt delay
- ▶ Unicast advertisement
- ▶ domains

In compliance with RFC 2338, the master sends IP Multicast messages (advertisements) at intervals of one second to the other VRRP routers. Only if this message does not appear three times do the remaining routers select a new master.

VRRP has typical switching times of 3 to 4 seconds.

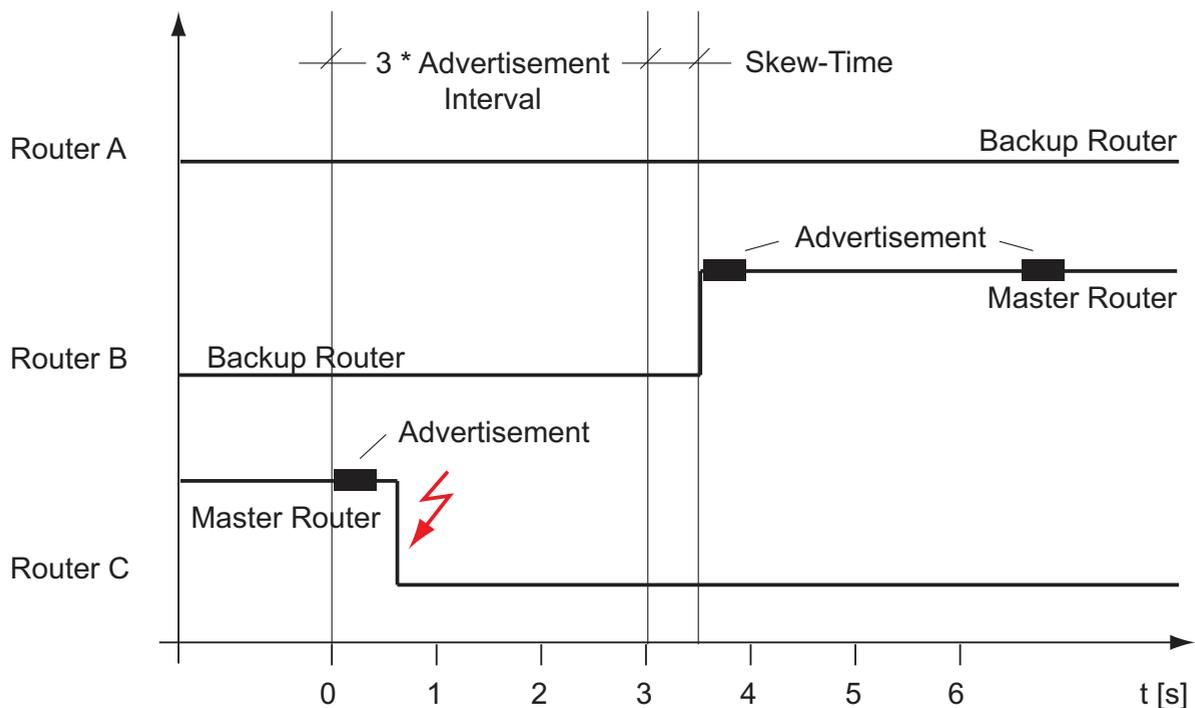


Figure 21: Master router <-> backup router switching times according to RFC 2338

VRRP priority router A = 64

VRRP priority router B = 128

VRRP priority router C = 254

To be able to achieve faster switching times, Hirschmann provides HiVRRP so that the cycle for sending the IP Multicast message can be shortened to as little as 0.1 seconds. You can thus achieve switching times that are up to 10 times as fast.

The router supports up to 16 VRRP router interfaces with this shortened sending cycle.

► HiVRRP skew time

The HiVRRP skew time is the time, dependent on the VRRP priority, that specifies the time when the HiVRRP backup router names itself the HiVRRP master router.

HiVRRP skew time =

$$(256 - \text{VRRP priority}) / 256 \cdot \text{advertisement interval}$$

Times shown in milliseconds

► HiVRRP master down interval

The HiVRRP master down interval specifies the time when the HiVRRP backup router names itself the HiVRRP master router.

HiVRRP master down interval =

$$3 \cdot \text{advertisement interval} + \text{HiVRRP skew time}$$

Times shown in milliseconds

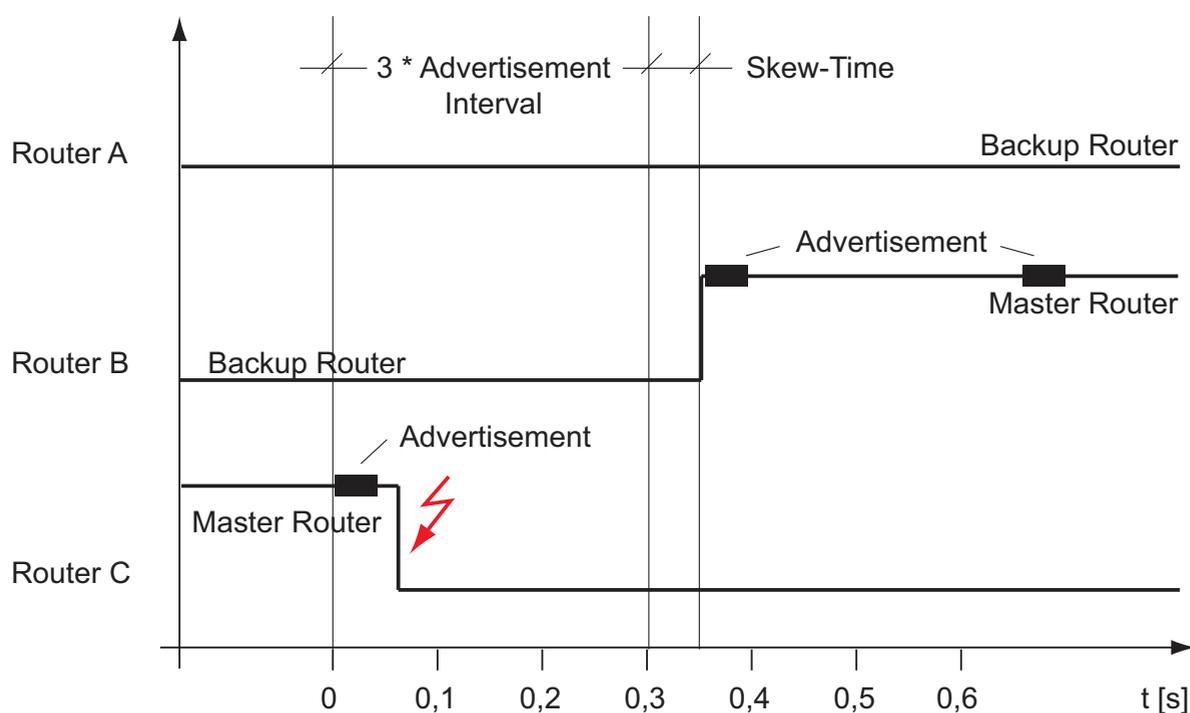


Figure 22: Master router <-> backup router switching times according to HiVRRP

VRRP priority router A = 64

VRRP priority router B = 128

VRRP priority router C = 254

Another option provided by HiVRRP for shortening the switching times dramatically is the link-down notification. You can use this function when the virtual router consists of two VRRP routers. As two VRRP routers are participating, it is sufficient to send the link-down notification in the form of a Unicast message. In contrast to the Multicast message, the Unicast message travels beyond the boundaries of the subnetwork. This means that if the link is down to your own subnetwork, the link-down notification can also travel via another subnetwork to reach the second router of the virtual router. As soon as HiVRRP detects that the link is down, it sends the link-down notification to the second router via a different route. The second router takes over the master function immediately after receiving the link-down notification.

In the preempt mode, the backup router can take over the master function from the master router as soon as the backup router receives an advertisement from the master router for which the VRRP priority is lower than its own.

Thus the preempt mode, in collaboration with VRRP tracking ([see on page 72 “VRRP tracking”](#)), can enable a switch to a better router. However, dynamic routing procedures take a certain amount of time to react to changed routes and refill their routing table.

To avoid the loss of packets during this time, delayed switching (preempt delay) from the master router to the backup router enables the dynamic routing procedure to fill the routing tables.

HiVRRP provides an additional advantage for networks with devices that have problems with higher volumes of Multicasts. Instead of sending advertisements in the form of Multicasts, HiVRRP can send the advertisements in the form of Unicast data packets (VRRP destination address) when using up to two HiVRRP routers.

**Note:** If you want to avail of the advantages of HiVRRP, then only use VRRP routers equipped with the HiVRRP function from Hirschmann as the virtual router.

---

## 5.3 HiVRRP Domains

In large, flat network structures, HiVRRP domains enable you to

- ▶ switch over all HiVRRP routers very quickly in the case of redundancy
- ▶ use the available bandwidth more effectively
- ▶ configure more than 16 VRRP router interfaces for each router using HiVRRP
- ▶ operate Multicast-sensitive terminal devices in large HiVRRP networks

A HiVRRP instance is a router interface configured as HiVRRP with functions that HiVRRP contains. In a HiVRRP domain you combine multiple HiVRRP instances of a router into one administrative unit. You nominate one HiVRRP instance as the supervisor of the HiVRRP domain. This supervisor regulates the behavior of all HiVRRP instances in its domain.

- ▶ The supervisor sends its advertisements on behalf of all HiVRRP instances in its domain.
- ▶ The supervisor puts itself and the other HiVRRP instances together into the master role or the backup role.

See [figure 23](#) for an example of a flat network structure. All cross-VLAN data streams pass through the ring.

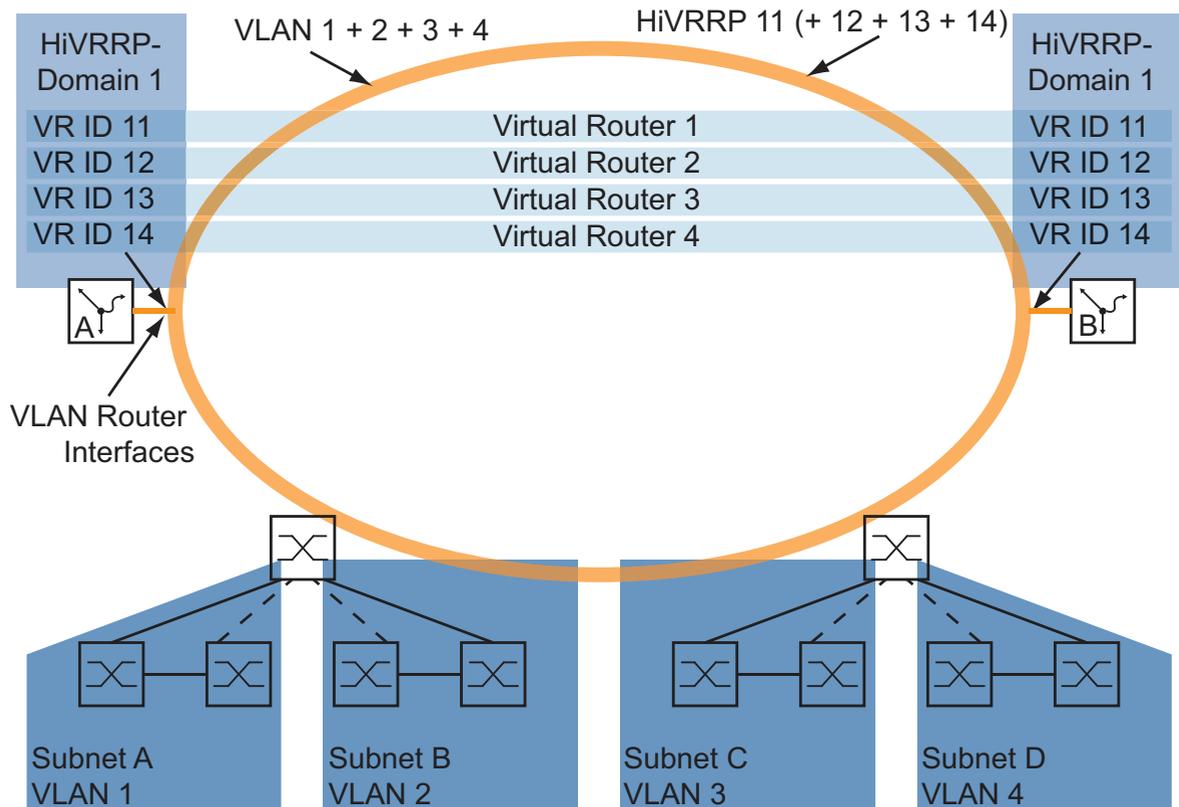


Figure 23: Example of how a HiVRRP domain is used

### 5.3.1 Configuration of HiVRRP domains

The configuration of HiVRRP domains consists of the following steps:

- ▶ Create VLANs
- ▶ Configure VLAN router interfaces
- ▶ Assign the IP addresses to the router interfaces
- ▶ Configure HiVRRP instances
  - Activate VRRP instance (all instances)
  - Assign IP address (all instances)
 

Within a router, you either configure all instances as IP address owners, or no instance as an IP address owner.
  - Assign priority (supervisor)
 

Assign the supervisors different priorities so that the VRRP routers can agree on a master router.

- Switch on HiVRRP (all instances)
  - Assign to the domain (all instances)
  - Specify sending interval (supervisor)
- ▶ Configure HIPER-Ring (in applications as in the above example)
  - ▶ Define the (Ring) ports as members of the VLANs
  - ▶ Switch on routing and VRRP globally

### 5.3.2 Example of configuration of HiVRRP domains

Example of possible settings for the application in [figure 23](#):

| Subnetwork | IP address range | VLAN | VLAN ID |
|------------|------------------|------|---------|
| A          | 10.0.11.0/24     | 1    | 11      |
| B          | 10.0.12.0/24     | 2    | 12      |
| C          | 10.0.13.0/24     | 3    | 13      |
| D          | 10.0.14.0/24     | 4    | 14      |

Table 5: Configuration of the Switches in the subnetwork

| Virtual router | VR ID | IP address of the virtual router | Router interface of router A: IP address | Router interface of router B: IP address | VLAN ID |
|----------------|-------|----------------------------------|------------------------------------------|------------------------------------------|---------|
| 1              | 11    | 10.0.11.1/24                     | 10.0.11.2/24                             | 10.0.11.3/24                             | 11      |
| 2              | 12    | 10.0.12.1/24                     | 10.0.12.2/24                             | 10.0.12.3/24                             | 12      |
| 3              | 13    | 10.0.13.1/24                     | 10.0.13.2/24                             | 10.0.13.3/24                             | 13      |
| 4              | 14    | 10.0.14.1/24                     | 10.0.14.2/24                             | 10.0.14.3/24                             | 14      |

Table 6: Configuration of the two routers

Configure VLAN router interface and assign IP address:

```

enable
vlan database
vlan 11
vlan name 11 VLAN1
vlan routing 11

exit

show ip vlan

show ip vlan
VLAN ID Interface Logical
----- -
11 9/1 0.0.0.0 0.0.0.0 00:80:63:51:74:2C

show ip interface brief

Interface IP Address IP Mask Netdir Multi
----- -
9/1 0.0.0.0 0.0.0.0 Disable Disable

configure
interface 9/1

ip address 10.0.11.2
255.255.255.0
routing

```

Switch to the privileged EXEC mode.

Switch to the VLAN mode.

Create a VLAN by entering the VLAN ID.

Assign the name "VLAN1" to VLAN 11.

Create a virtual router interface and activate the router function at this interface.

Switch to the privileged EXEC mode.

Display the virtual router interface that the router has set up for the VLAN.

Check the entry for the virtual router interface.

Switch to the Configuration mode.

Change to the interface configuration mode of interface 9/1.

Assign the interface its IP parameters.

Activate the router function at this interface.

Set up virtual router and configure port

```

ip vrrp 1

ip vrrp 1 priority 200
ip vrrp 1 mode
ip vrrp 1 ip 10.0.11.1
ip vrrp 1 domain 1 supervisor

```

Create the VRID for the first virtual router at this port.

Assign virtual router 1 the router priority 200.

Switch on the first virtual router at this port.

Assign virtual router 1 its IP address.

Assign the HiVRRP domain and the domain role to the interface.

```
ip vrrp 1 timers advertise milliseconds 100
exit
exit
```

Assign the HiVRRP notification interval to the interface.

Switch to the Configuration mode.

Switch to the privileged EXEC mode.

```
show ip vrrp interface 9/1 1
```

Display the configuration of VLAN 11

```
Primary IP Address..... 10.0.11.1
VMAC Address..... 00:00:5e:00:01:01
Authentication Type..... None
Base Priority..... 200
Advertisement Interval (milliseconds)..... 100
Pre-empt Mode..... Enable
Administrative Mode..... Enable
State..... Initialized
Current Priority..... 200
Preemption Delay (seconds)..... 0
Link Down Notification..... Disabled
VRRP Domain..... 1
VRRP Domain Role..... Supervisor
VRRP Domain State..... Supervisor is down
Advertisement Address..... 224.0.0.18
```

#### Define the (Ring) port as a member of the VLAN

```
interface 2/1
vlan participation include 11
exit
exit
show vlan 11
```

Switch to the Interface Configuration mode of interface 2/1.

Assign the interface to the VLAN.

Change to the Configuration mode.

Change to the privileged EXEC mode.

Display the configuration of VLAN 11

```

VLAN ID : 11
VLAN Name : VLAN1
VLAN Type : Static
VLAN Creation Time: 0 days, 00:00:06 (System Uptime)

```

| Interface | Current | Configured | Tagging  |
|-----------|---------|------------|----------|
| 1/1       | Exclude | Autodetect | Untagged |
| 1/2       | Exclude | Autodetect | Untagged |
| 1/3       | Exclude | Autodetect | Untagged |
| 1/4       | Exclude | Autodetect | Untagged |
| 2/1       | Include | Include    | Untagged |
| 2/2       | Exclude | Autodetect | Untagged |
| 2/3       | Exclude | Autodetect | Untagged |
| 2/4       | Exclude | Autodetect | Untagged |
| 3/1       | Exclude | Autodetect | Untagged |
| 3/2       | Exclude | Autodetect | Untagged |
| 9/1       | Exclude | Autodetect | Untagged |

### Switch on routing and VRRP globally

```

enable
configure
ip routing
ip vrrp

```

Switch to the privileged EXEC mode.  
Switch to the Configuration mode.  
Switch on the router function globally.  
Switch on VRRP globally.

## 5.4 VRRP tracking

By monitoring certain router statuses (e.g. line interruption), VRRP tracking makes it possible to switch to a better router when a link goes down.

If there is a line interruption between Switch S1 and router A (see figure 25), router B takes over the master function for virtual router 10.0.1.254.

Router A remains the master for virtual router 10.0.2.254. However, router A no longer has a link to subnetwork 10.0.1.0.

The virtual router interfaces are independent of each other.

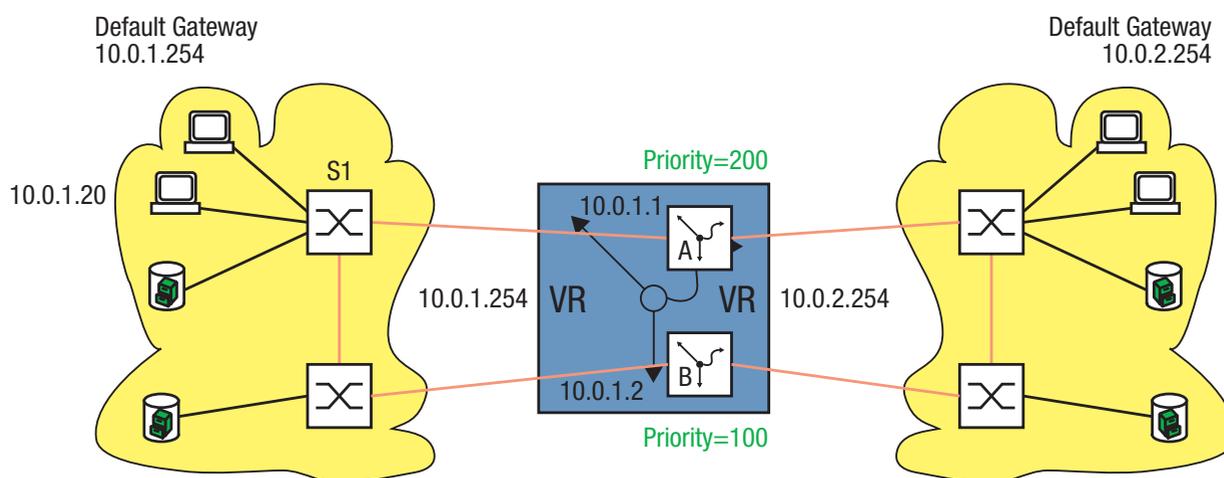


Figure 24: Typical VRRP application

As soon as the VRRP master router with the VRRP tracking function active detects the interruption of one of its links, it lowers its VRRP priority and informs the other VRRP routers of this.

Then another VRRP router, which now has the highest priority due to this change in the situation, can take over the master function within the skew time.

Solution without tracking:

Configure router A with a static route to router B or with a dynamic routing procedure, so that router A finds a route into subnetwork 10.0.1.0.

A direct link with preference 0 is the best route.  
The static route with preference 1 is the second-best route. Then comes the dynamic route.

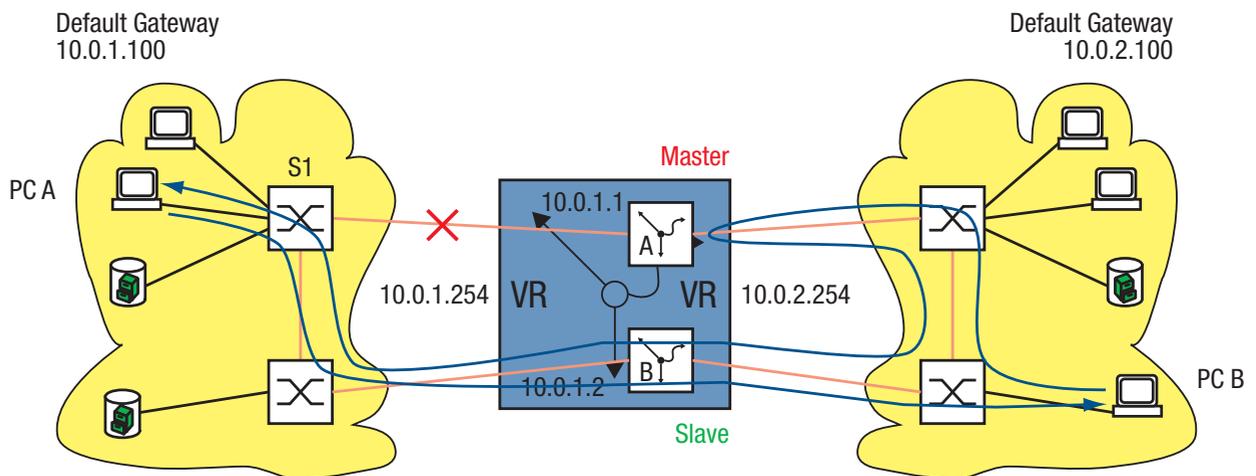


Figure 25: Transmission path from PC B to PC A in the case of a line interruption without tracking

The data from PC B is then transferred to PC A via router A and router B.

Solution with tracking:

For an optimal route, you can now use the tracking function to also make router B the master for virtual router 10.0.2.254.

By "tracking" the interrupted link and registering the virtual routers for this tracking object (see on page 45 "Tracking"), router A decrements its VRRP priority. Thus when router B receives the next advertisement from router A, router B detects that its own VRRP priority is higher than that of router A and takes over the master function (see figure 26).

**Note:** As the IP address owner has the fixed VRRP priority 255 by definition, the VRRP tracking function requires the IP addresses of the VRRP router interfaces to differ from the virtual router IP address.

**Note:** For the backup router to be able to take over the master function from the master router with the lower priority, the VRRP tracking function requires that the preempt mode is activated.

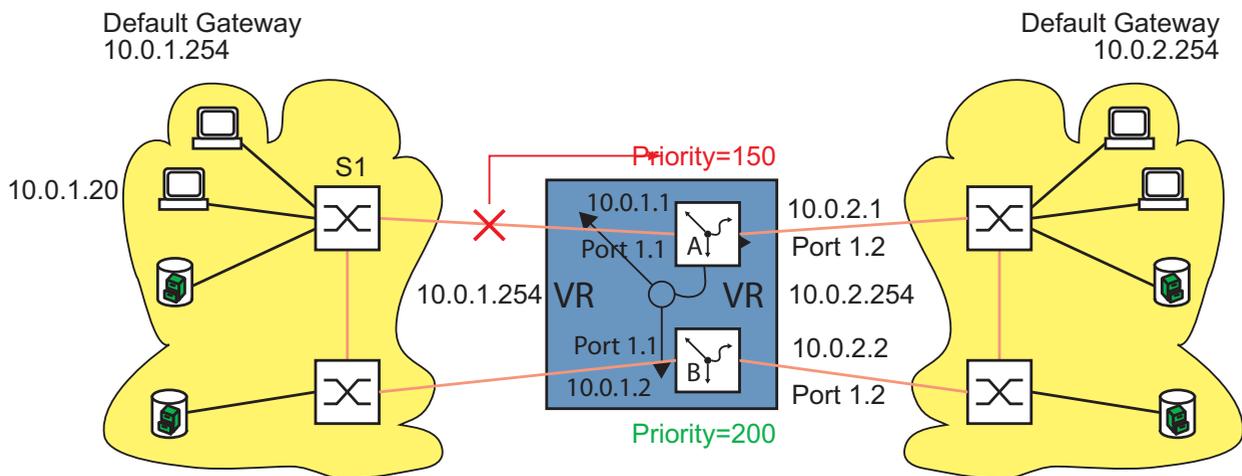


Figure 26: VRRP tracking after a line interruption

|                 | Router A    | Router A    | Router B    | Router B    |
|-----------------|-------------|-------------|-------------|-------------|
| Interface       | 1.1         | 1.2         | 1.2         | 1.1         |
| IP address      | 10.0.1.1/24 | 10.0.2.1/24 | 10.0.2.2/24 | 10.0.1.2/24 |
| VRID            | 1           | 2           | 2           | 1           |
| VRRP IP address | 10.0.1.254  | 10.0.2.254  | 10.0.2.254  | 10.0.1.254  |
| VRRP priority   | 250         | 250         | 200         | 200         |
| VRRP preemption | Enabled     | Enabled     | Enabled     | Enabled     |
| Track ID        | 2           | 1           | -           | -           |
| Track decrement | 100         | 100         | -           | -           |

Table 7: VRRP tracking configuration for the example above

|           | Router A  | Router A  | Router B | Router B |
|-----------|-----------|-----------|----------|----------|
| Track ID  | 1         | 2         | -        | -        |
| Type      | Interface | Interface | -        | -        |
| Interface | 1.1       | 1.2       | -        | -        |

Table 8: Tracking configuration for the example above

The configuration of VRRP tracking requires the following steps:

- ▶ Configure the tracking object  
(see on page 51 “Configuring the tracking”).
  - ▶ Configure the VRRP.
  - ▶ Add the track ID to the VRRP entry (= register the VRRP entry for the tracking object).
- Set up interface tracking at port 1.1 with a link down delay of 0 seconds and a link up delay of 3 seconds.

- In the `Routing:Tracking:Configuration` dialog, click on “Wizard” at the bottom right.

Select type:

- Enter the values you desire:

Track ID: 1  
Type: interface

- Click on “Continue”.

Properties:

- Enter the values you desire:

Module.Port: 1.1  
Link up delay: 3  
Link down delay: 0

- Click on “Finish” to leave the Wizard and save the entry temporarily in the configuration.

```
enable
configure
track 1 interface 1/1
 link-down-delay 0
 link-up-delay 3
```

Switch to the privileged EXEC mode.

Switch to the Configuration mode.

Enter the tracking parameters and activate this tracking object.

Switch on routing and VRRP globally.

- Select the `Routing:Global` dialog.
- Select "Routing".
- Click "Set" to save the changes temporarily.
- Select the dialog  
`Redundancy:VRRP/HiVRRP:Configuration`.
- Select "Operation".
- Click "Set" to save the changes temporarily.

`ip routing`  
`ip vrrp`

Switch on the router function globally.  
Switch on VRRP globally.

Configure the IP address and VRRP at port 1.2.

- In the `Redundancy:VRRP/HiVRRP:Configuration` dialog, click "Wizard" at the bottom right.

Create entry:

- Enter the values you desire:
 

|           |   |
|-----------|---|
| "Module": | 1 |
| "Port":   | 2 |
| "VRID":   | 2 |

- Click on "Continue".

Edit entry:

- Enter the values you desire:
 

|                    |            |
|--------------------|------------|
| "VRRP IP address": | 10.0.2.254 |
| "Priority":        | 250        |
| "Preempt mode":    | 1          |

- Click on "Continue".

```

interface 1/2
ip address 10.0.2.1
255.255.255.0
routing
ip vrrp 2

ip vrrp 2 mode
ip vrrp 2 ip 10.0.2.254
ip vrrp 2 priority 250

```

Select the port for setting up VRRP.  
Assign the port its IP parameters.

Switch on the router function at this port.  
Create the VRID for the first virtual router at this port.

Switch on the first virtual router at this port.

Assign virtual router 1 its IP address.

Assign virtual router 1 the router priority 250.

- Register VRRP for the tracking object.

### Tracking

- Enter the values you desire:

“Track ID”: 1  
“Decrement”: 100

- Click on “Add”.
- Click on “Continue”.
- Click on “Finish” to leave the Wizard and save the entry temporarily in the configuration.

```

ip vrrp 2 track 1 decrement
100
exit
exit

```

Register the first VRRP entry for the tracking object.

Switch to the Configuration mode.

Switch to the privileged EXEC mode.

```
show track applications
```

Display the registered applications.

| TrackId | Application      | Changes | Time since last change |
|---------|------------------|---------|------------------------|
| 1       | VRRP 1/2 VRID: 2 | 0       | 0 day(s), 00:38:24     |

- You also perform the same configuration on the redundant router.

## 5.5 VRRP with load sharing

With the simple configuration, a router performs the gateway function for all terminal devices. The capacity of the redundant router lies idle. VRRP allows you to also use the capacity of the redundant router. By setting up a number of virtual routers, you can enter different default gateways on the connected terminal devices and thus steer the data flow.

When both routers are active, the data flows via the router on which the IP address of the default gateway has the higher VRRP priority. If a router fails, then all the data flows via the remaining routers.

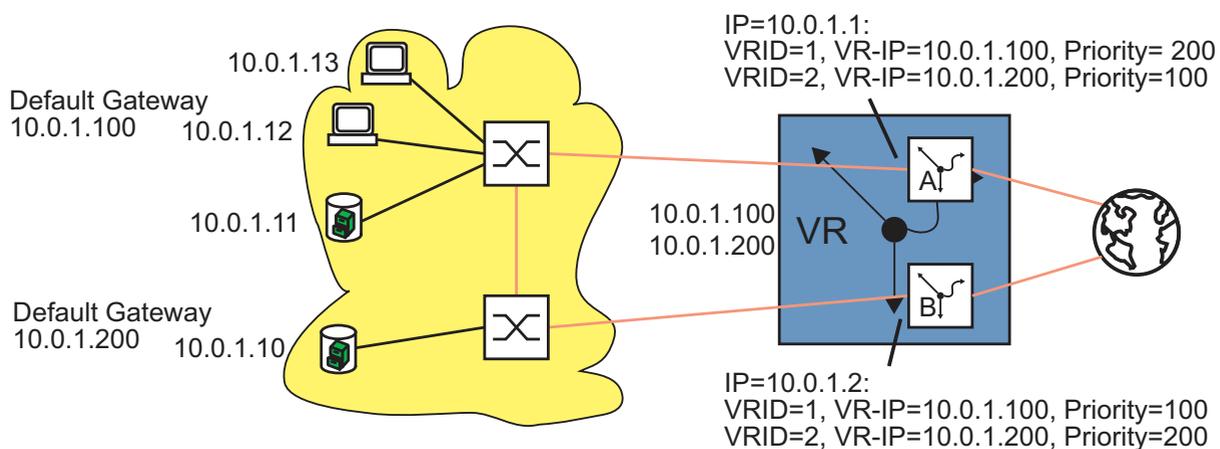


Figure 27: Virtual router with load sharing

To use load sharing, you perform the following configuration steps:

- Define a second VRID for the same router interface.
- Assign the router interface its own IP address for the second VRID.
- Assign the second virtual router a lower priority than the first virtual router.
- When configuring the redundant router, make sure that you assign the second virtual router a higher priority than the first.
- Give the terminal devices one of the virtual router IP addresses as a default gateway.

## 5.6 VRRP mit Multinetting

The router allows you to combine VRRP with Multinetting.

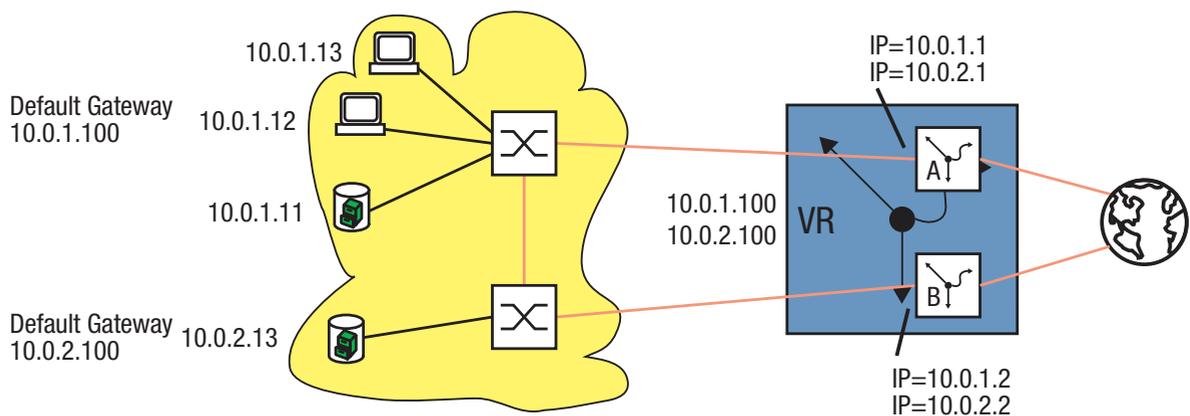


Figure 28: Virtual router with multinetting

To use VRRP with multinetting, you perform the following configuration steps on the basis of an existing VRRP configuration (see figure 19):

- Assign a second (secondary) IP address to the port.
- Assign a second (secondary) IP address to the virtual router.

```
interface 2/3
ip address 10.0.2.1
255.255.255.0 secondary
ip vrrp 1 ip 10.0.2.100
secondary
```

Select the port at which you want to configure multinetting.

Assign the second IP address to the port.

Assign the second IP address to the virtual router with the VR-ID 1.

- Perform the same configuration on the redundant router also.



## 6 RIP

The Routing Information Protocol (RIP) is a routing protocol based on the distance vector algorithm. It is used for the dynamic creation of the routing table for routers.

When you start a router, the router only knows the networks directly connected to it, and it sends this routing table to the neighboring routers. At the same time, it requests the routing tables of its neighboring routers. The router adds this information to its routing table and thus learns which networks can be accessed via which routers, and how much effort is involved in this. In order to detect changes in the network (when a router fails or starts), the routers regularly repeat the exchange of all the routing tables, usually every 30 seconds. This involves a considerable bandwidth requirement in large networks.

The costs, also known as the metric, refer to the work involved in reaching a particular network. RIP uses the hop count for this, which describes the number of routers that are traversed along the path to the destination network. The name 'distance vector' is derived from the fact that the distance (metric) is the criterion for determining the route, and the direction is specified by the next hop (vector). The next hop refers to the neighboring router along the path to the destination address.

An entry in the routing table consists of the address of the next hop, the destination address and the metric. The RIP routing table always contains the most efficient route to the destination. This is the route with the smallest metric and the longest suitable network mask prefix.

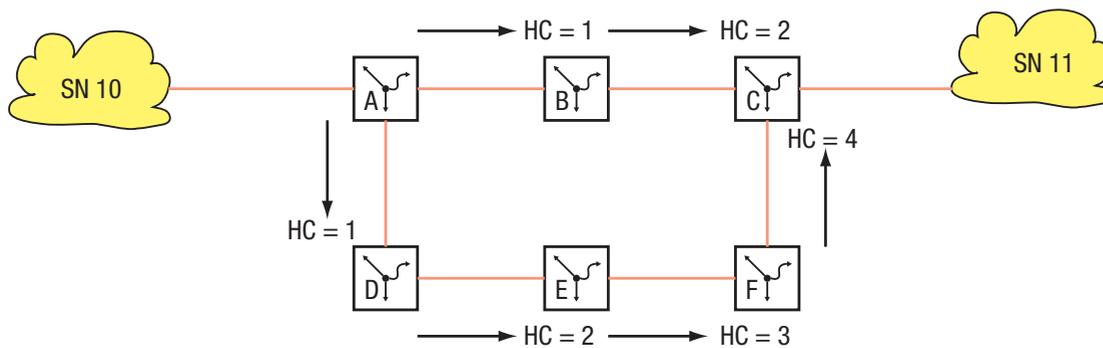


Figure 29: Counting Hops

| Router A     |          |        | Router B     |          |        | Router D     |          |        |
|--------------|----------|--------|--------------|----------|--------|--------------|----------|--------|
| Destinati on | Next Hop | Metric | Destinati on | Next Hop | Metric | Destinati on | Next Hop | Metric |
| SN 10        | lokal    | 0      | SN 10        | Router A | 1      | SN 10        | Router A | 1      |
| SN 11        | Router B | 2      | SN 11        | Router C | 1      | SN 11        | Router E | 3      |

Table 9: Routing table to the figure above

In contrast to OSPF, a RIP router regularly exchanges the content of its entire routing table with its direct neighbor. Every router knows only its own routes and the routes of its direct neighbor. Thus it only has a local perspective.

When changes are made in the network, it takes a while until all the routers have the same uniform view of the network. The process of achieving this condition is known as convergence.

## 6.1 Convergence

How does RIP react to changes in the topography?

In the following example of a line interruption between router B and router C, you can see the resulting changes in the address table:

Assumptions:

- ▶ The interruption occurs 5 seconds after B sent its routing table.
- ▶ The routers send their routing table every 30 seconds (= factory setting).
- ▶ There is an interval of 15 seconds between when router A sends its routing table and when router B sends its routing table.

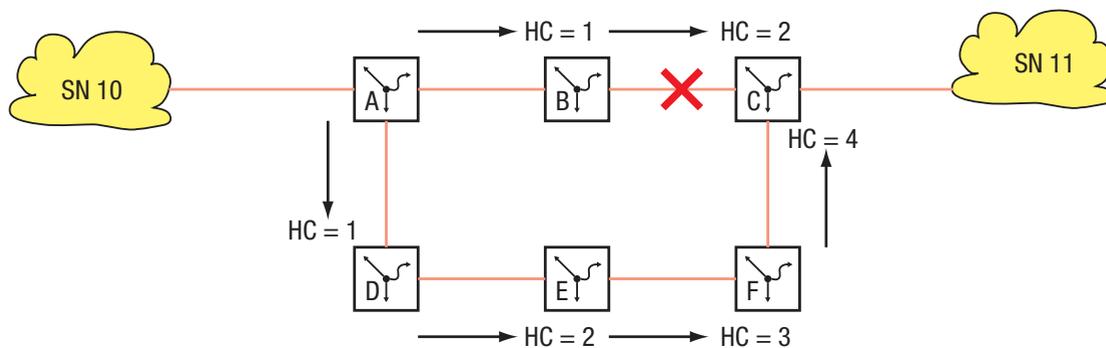


Figure 30: Hop Count

Time elapsing before convergence:

0 seconds:  
Interruption

10 seconds  
Router A sends its routing table:

| Router A    |          |        |
|-------------|----------|--------|
| Destination | Next hop | Metric |
| SN 10       | local    | 0      |
| SN 11       | Router B | 2      |

Using the routing table from router A, router B sees that router A knows a connection to destination SN 11 with a metric of 2. Because it does not have its own connection to router C as the next hop to SN 11, router B changes its entry to destination SN 11. It enters router A as the next hop and increases the metric from router A by 1 to 3 (distance = learned distance + 1).

25 seconds Router B sends its routing table:

| Router B    |          |        |
|-------------|----------|--------|
| Destination | Nex- Hop | Metrik |
| SN 10       | Router A | 1      |
| SN 11       | Router A | 3      |

Using the routing table from router B, router A sees that router B knows a connection to SN 11 with a metric of 3. So router A increases its metric for SN 11 by 1 to 4.

40 seconds Router A sends its routing table:

| Router A    |          |        |
|-------------|----------|--------|
| Destination | Next hop | Metric |
| SN 10       | local    | 1      |
| SN 11       | Router B | 4      |

Using the routing table from router A, router B sees that router A knows a connection to destination SN 11 with a metric of 4. So router B increases its metric for SN 11 by 1 to 5.

55 seconds Router B sends its routing table

| Router B    |          |        |
|-------------|----------|--------|
| Destination | Next hop | Metric |
| SN 10       | Router A | 1      |
| SN 11       | Router A | 5      |

Using the routing table from router B, router A sees that router B knows a connection to SN 11 with a metric of 5. So router A increases its metric for SN 11 by 1 to 6. Because router A can see in the routing table from router D that router D has a connection to SN 11 with the smaller metric of 3, router A changes its entry for SN 11.

70 seconds Router A sends its routing table:

| Router A    |          |        |
|-------------|----------|--------|
| Destination | Next hop | Metric |

| Router A |            |
|----------|------------|
| SN 10    | Router A 1 |
| SN 11    | Router D 4 |

After 70 seconds, convergence has been achieved again.

## 6.2 Maximum Network Size

The biggest problem with RIP is that routers only know their neighbors directly. This results in long convergence times and the count-to-infinity problem. Infinity refers to the inaccessibility of a destination, and it is designated by hop count 16 in RIP. If the above example did not contain the parallel path via routers D, E and F, then routers A and B would keep sending their routing tables until the metric reached a value of 16. Then the routers recognize that the destination is inaccessible.

Using the “split horizon” approach eliminates this looping problem between two neighboring routers. Split horizon has two operating modes.

---

|                                          |                                                                                                                                          |
|------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------|
| Simple split horizon                     | Omits the entries known by a neighbor when sending the routing table to this neighbor.                                                   |
| Simple split horizon with poison reverse | Sends the routing table to a neighbor with the entries known by this neighbor, but denotes these entries with the infinity metric (=16). |

---

Thus the hop count 16 specifies the maximum size of a network with RIP as the routing procedure. The longest paths may use up to 15 routers.

## 6.3 General Properties of RIP

The RFC 1058 from June 1988 specifies RIP version 1. Version 1 has the following restrictions:

- ▶ Use of broadcasts for protocol messages.
- ▶ Does not support subnetworks/CIDR.
- ▶ No authentication.

The standardization of RIP version 2 in the RFC 2453 in 1998 eliminates the above restrictions.

RIP V2 sends its protocol messages as a multicast with the destination address 224.0.0.9, and supports subnetwork masks and authentication. However, the restrictions relating to the size of the network remain.

| Advantages           | Disadvantages                                                                                                                                                                                            |
|----------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Easy to implement    | Routing tables in large networks very comprehensive                                                                                                                                                      |
| Easy to administrate | Routing information is distributed slowly, because there are fixed sending intervals. This applies in particular to connections that have elapsed, since the routing table only contains existing paths. |
|                      | Count-to-infinity                                                                                                                                                                                        |

*Table 10: Advantages and disadvantages of Vector Distance Routing*

## 6.4 Configuring the RIP

The advantage of RIP is the simple configuration. After the router interface is defined and the RIP is switched on, RIP automatically enters the required routes in the routing table.

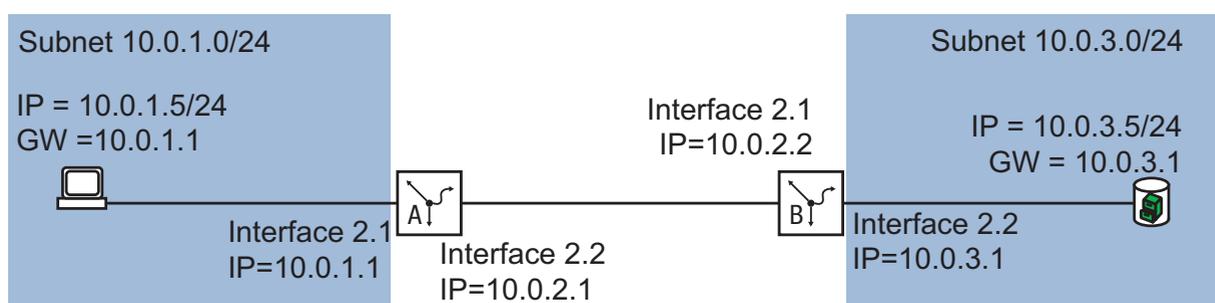


Figure 31: Example of the configuration of RIP

The configuration of RIP requires the following steps:

- ▶ Configure router interfaces - assign IP address and network mask.
- ▶ Switch on RIP on port.
- ▶ Switch on RIP globally.
- ▶ Switch on routing globally (if this has not already been done).

### ■ Configuration for router B

```
enable
configure
```

Change to the privileged EXEC mode.  
Change to the Configuration mode.

```
interface 2/2
```

Change to the interface configuration mode of interface 2/2.

```
ip address 10.0.3.1
255.255.255.0
```

Assign the IP parameters to the port.

```
routing
exit
```

Switch on the router function at this port.  
Change to the Configuration mode.

```

interface 2/1
ip address 10.0.2.2
255.255.255.0
routing
ip rip
exit

```

Switch to the Interface Configuration mode of interface 2/1.  
Assign the IP parameters to the port.  
Switch on the router function at this port.  
Switch on RIP at this port.  
Change to the Configuration mode.

```
show ip rip interface brief
```

Verify the settings for the RIP configuration.

| Interface | IP Address | Send Version | Receive Version | RIP Mode | Link State |
|-----------|------------|--------------|-----------------|----------|------------|
| 2/1       | 0.0.0.0    | RIP-2        | Both            | Enable   | Down       |

The IP address entries remain at 0.0.0.0 as long as the routing function is switched off globally.

```

router rip
redistribute connected

enable
exit
ip routing

```

Switch to the router configuration mode  
Tell RIP to send the routes of the locally connected interfaces along with the learned routes in the RIP information  
Switch on RIP globally.  
Change to the Configuration mode.  
Switch on the router function globally.

```
show ip rip interface brief
```

Verify the settings for the RIP configuration.

| Interface | IP Address | Send Version | Receive Version | RIP Mode | Link State |
|-----------|------------|--------------|-----------------|----------|------------|
| 2/1       | 10.0.2.2   | RIP-2        | Both            | Enable   | Up         |

```
show ip route
```

Verify the routing table:

Total Number of Routes..... 3

| Network Address | Subnet Mask   | Protocol | Next Hop Intf | Next Hop IP Address |
|-----------------|---------------|----------|---------------|---------------------|
| 10.0.1.0        | 255.255.255.0 | RIP      | 2/1           | 10.0.2.1            |
| 10.0.2.0        | 255.255.255.0 | Local    | 2/1           | 10.0.2.2            |
| 10.0.3.0        | 255.255.255.0 | Local    | 2/2           | 10.0.3.1            |

Also perform the corresponding configuration on the other RIP routers.



## 7 OSPF

Open Shortest Path First (OSPF) is a dynamic routing protocol based on the Link State Algorithm. This algorithm is based on the link states between the routers involved.

The significant metric in OSPF is the “OSPF costs”, which is calculated from the available bit rate of a link.

OSPF was developed by IETF. OSPF is currently specified as OSPFv2 in RFC 2328. Along with many other advantages of OSPF, the fact that it is an open standard has contributed to the wide usage of this protocol. OSPF has replaced the Routing Information Protocol (RIP) as the standard Interior Gateway Protocol (IGP) in large networks.

OSPF has a number of significant advantages to offer:

- ▶ **Cost-based routing metrics:** In contrast to RIP, OSPF provides clear metrics based on the bandwidth of each individual network connection. OSPF provides major flexibility in designing a network, because the user can simply change these costs.
- ▶ **Routing via multiple paths (equal cost multiple path/ECMP):** OSPF is able to support a number of equal paths to a given destination. OSPF thus provides efficient utilization of the network resources (load distribution) and improves the availability (redundancy).
- ▶ **Hierarchical routing:** By logically dividing the network into areas, OSPF shortens the time required to distribute routing information. The messages about changes in a subnetwork remain within the subnetwork, without putting any load on the rest of the network.
- ▶ **Support of Classless Inter-Domain Routing (CIDR) and Variable Length Subnet Mask (VLSM):** This allows the network administrator to assign the IP address resources efficiently.
- ▶ **Fast tuning time:** OSPF supports the fast distribution of messages about route changes. This speeds up the tuning time for updating the network topology.

- ▶ Saving network resources / bandwidth optimization: Because OSPF, in contrast to RIP, does not exchange the routing tables at regular, short intervals, no bandwidth is unnecessarily “wasted” between the routers.
- ▶ Support of authentication: OSPF supports the authentication of all nodes that send routing information.

| Advantages                                                                                                                                                                          | Disadvantages                                              |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------|
| Every router calculates its routes independently of the other routers.                                                                                                              | Complicated to implement                                   |
| All the routers have the same basic information.                                                                                                                                    | Complex administration due to the large number of options. |
| Rapid detection of link interruptions and rapid calculation of alternative routes.                                                                                                  |                                                            |
| The data volume for router information is relatively small, because information is only sent when it is required, and only the information that applies to the immediate neighbors. |                                                            |
| Optimal path selection through evaluation of the link quality.                                                                                                                      |                                                            |

*Table 11: Advantages and disadvantages of Link State Routing*

OSPF is a routing protocol based on the states of the links between the routers.

Using the link states collected from all the routers and the Shortest Path First algorithm, an OSPF router dynamically creates its routing table.

## 7.1 OSPF-Topology

OSPF is hierarchically structured in order to limit the scope of the OSPF information to be exchanged in large networks. You divide up your network using what are known as areas.

### 7.1.1 Autonomous System

An Autonomous System (AS) is a number of routers that are managed by a single administration and use the same Interior Gateway Protocol (IGP). Exterior Gateway Protocols (EGP), on the other hand, are used to connect a number of autonomous systems. OSPF is an Interior Gateway Protocol.

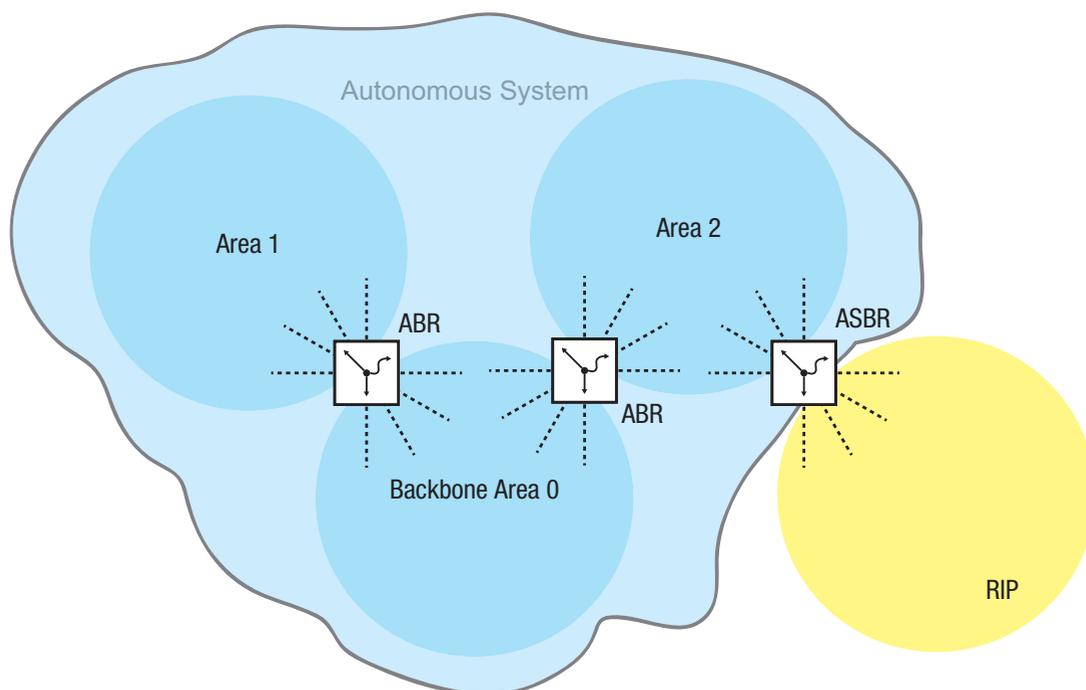


Figure 32: Autonomous System

An AS uses an “Autonomous System Boundary Router” (ASBR) to connect with the outside world. An ASBR understands multiple protocols and serves as a gateway to routers outside the areas. An ASBR is able to transfer routes from different protocols into the OSPF. This process is known as redistribution.

## 7.1.2 Router ID

The router ID in the form of an IP address is used to uniquely identify every router within an autonomous system. To improve the transparency, it is necessary to manually configure the router ID of every OSPF router. Thus there is no automatic function that selects the router ID from the IP interfaces of the router.

```
enable
configure
router ospf
router-id 192.168.1.0
enable
```

Switch to the privileged EXEC mode.  
Switch to the Configuration mode.  
Change to the Router Configuration mode.  
Assign router ID (e.g. 192.168.1.0).  
Switch on OSPF globally.

## 7.1.3 Areas

Each area first forms its own database using the link states within the area. The data exchange required for this remains within the area. Each area uses an Area Border Router (ABR) to link to other areas. The routing information is summarized as much as possible between the areas (route summarization).

Every OSPF router must be a member of at least one area.

An individual router interface can only be assigned to one area. In the state on delivery, every router interface is assigned to the backbone area.

OSPF distinguishes between the following particular area types:

▶ **Backbone-Area:**

This is by definition the area 0 or 0.0.0.0. An OSPF network consists of at least the backbone area. It is the central area, which is linked to all the other areas directly. The backbone area receives all the routing information and is responsible for forwarding this information.

▶ **Stub Area:**

You define an area as a stub area if external LSAs are not to be flooded into the area. External means outside the autonomous system. These external LSAs are the yellow and orange links in the illustration ([see figure 33](#)). Thus the routers within a stub area only learn internal routes (blue links – e.g. no routes that are exported into OSPF from another log / redistributing). All the destinations outside the autonomous system are assigned to a default route. Stub areas are thus generally used if only one route in the area has a link to outside the area.

The use of stub areas keeps the routing table small within the stub area.

**Totally Stubby Area:**

You define a totally stubby area if, along with the external (orange and yellow) LSAs, the LSAs of the internal (blue) routes are also not to be sent into the area. Internal means between the areas of the autonomous system. A router within a totally stubby area thus only knows the routes within its own area and the default route out of the area.

Configuration notes:

- ▶ For a stub area, all the routers within the stub area must be defined as stub routers.
  - ▶ A stub area does not allow passage for a virtual link.
  - ▶ The backbone area cannot be defined as a stub area.
- ▶ **Not So Stubby Area (NSSA):**
- You define an area as NSSA if the external (yellow) routes of a system directly connected to the NSSA that is outside your own autonomous system are to be led into the area (redistributed). These external (yellow) LSAs then also lead from the NSSA to other areas in your own autonomous system. External (orange) LSAs within your own autonomous system do not, on the other hand, lead into an NSSA. By using NSSAs, you can integrate ASBRs into the area without foregoing the advantage of stub areas, namely that external routes from the

backbone are not flooded into the corresponding area.

Thus NSSAs have the advantage that external routes coming from the backbone are not all entered in the routing tables of the internal routers. At the same time, however, a limited number of external networks (which can be reached across the boundaries of the NSSA) can be propagated into the backbone area.

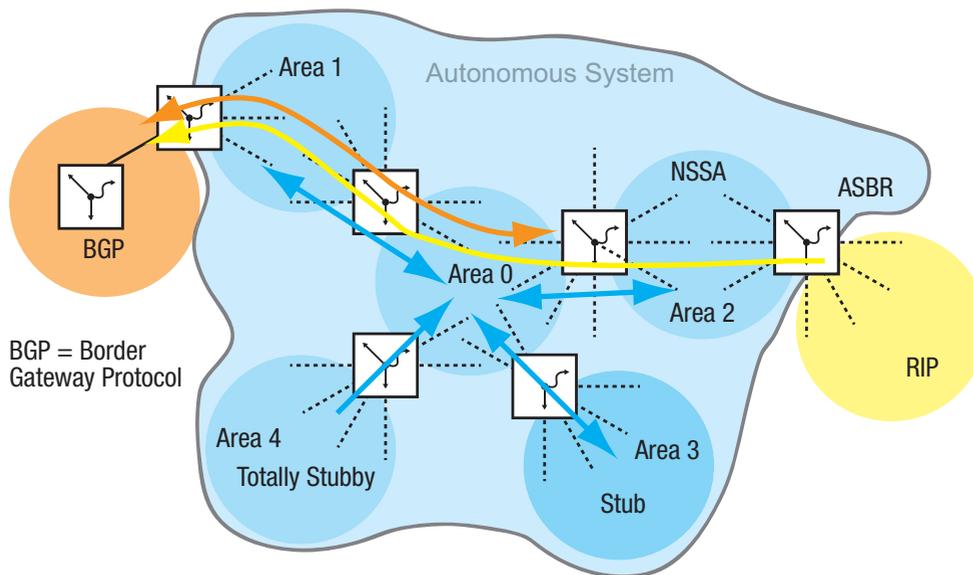


Figure 33: LSA distribution into the area types

```
enable
configure
router ospf
```

Switch to the privileged EXEC mode.  
Switch to the Configuration mode.  
Change to the Router Configuration mode.

```
area [area-id]
area 2 nssa
area 3 stub
area 3 default-cost 10
no area 3 stub summerylsa
```

Assign the area ID to the area.  
Define area 2 as the NSSA  
Define area 3 as the stub area  
Instruct the ABR to inject the default route with the metric 10 into the stub area.  
Make stub area 3 the totally stubby area

### 7.1.4 Virtual Link

OSPF requires that the backbone area can be passed through. However, if this is not actually possible, then OSPF provides a virtual link (VL) to connect parts of the backbone area with each other (see figure 35). A VL even allows you to connect an area that is connected with the backbone area via another area.

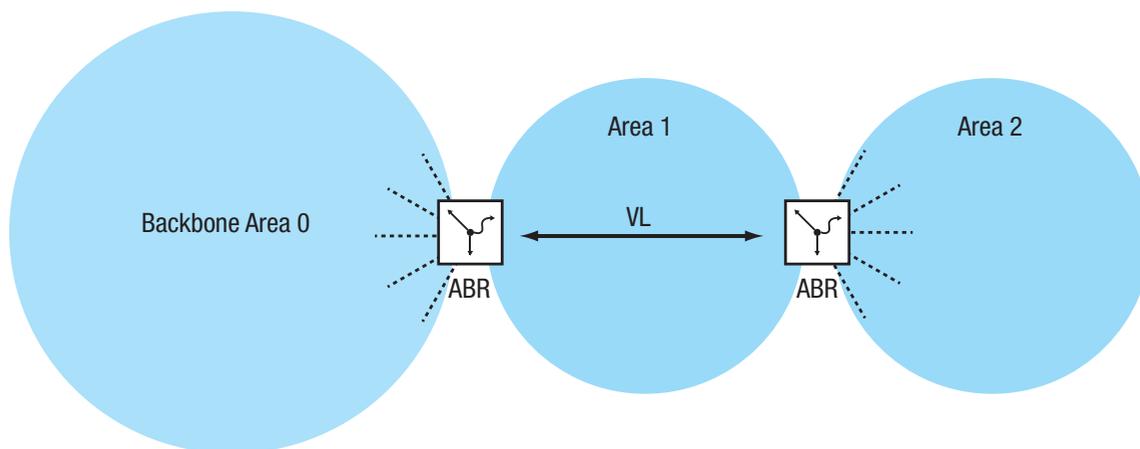


Figure 34: Linking a remote area to the backbone area via a virtual link (VL)

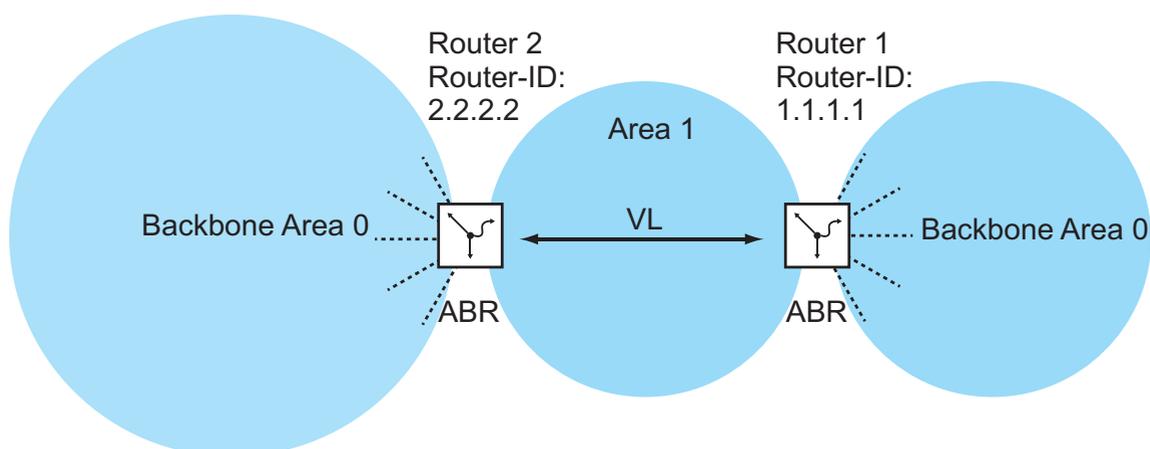


Figure 35: Expanding the backbone area via a virtual link (VL)

Configuration for expanding the backbone area (see figure 35):

### Router 1:

```
enable
configure
router ospf
```

Switch to the privileged EXEC mode.  
Switch to the Configuration mode.  
Change to the Router Configuration mode.

```
area 1 virtual-link 2.2.2.2
```

Enter the neighboring router ID for a virtual link in area 1.

### Router 2:

```
enable
configure
router ospf
```

Switch to the privileged EXEC mode.  
Switch to the Configuration mode.  
Change to the Router Configuration mode.

```
area 1 virtual-link 1.1.1.1
```

Enter the neighboring router ID for a virtual link in area 1.

### 7.1.5 OSPF Router

OSPF distinguishes between the following router types:

- ▶ **Internal Router:**  
All OSPF interfaces of an internal router are within the same area.
- ▶ **Area Border Router (ABR):**  
ABRs have OSPF interfaces in a number of areas, including the backbone area. ABRs thus participate in multiple areas. Where possible, you summarize a number of routes and send “Summary LSAs” to the backbone area.
- ▶ **Autonomous System Area Border Router (ASBR):**  
An ASBR is located on the boundary of an autonomous system and links OSPF to other autonomous systems / routing protocols. These external routes are transferred into OSPF using what is known as redistributing and are then summarized as “AS-external LSAs” and flooded into the area.  
Switch on the redistributing explicitly.  
If you want to use subnetting, then you enter this explicitly. In OSPF, the following “routing protocols” can be exported:
  - ▶ connected (local subnetworks on which OSPF is not switched on),
  - ▶ static (static routes),
  - ▶ RIP.

### 7.1.6 Link State Advertisement

As a basis for building up a database via the link states, OSPF uses Link State Advertisements (LSA).

An LSA contains information about

- ▶ the router,
- ▶ the connected subnets,
- ▶ the routes that can be reached,
- ▶ the network masks and
- ▶ the metrics.

OSPF unterscheidet folgende LSA-Typen:

- ▶ Router LSAs (type 1 LSAs):  
Every router sends a router LSA to all its connected areas. They describe the state and the costs of the router links (router interfaces) that the router has in the corresponding area. Router LSAs are only flooded within the area.
- ▶ Network LSAs (Type 2 LSAs):  
These LSAs are generated by the designated router, DR ([see on page 102 “Setting up the Adjacency”](#)) and are sent for every connected network/subnet within an area.
- ▶ Summary LSAs (type 3 /type 4 LSAs):  
Summary LSAs are generated by ABRs and describe inter-area destinations, meaning destinations in different areas of the same autonomous system.  
Type 3 LSAs describe targets for IP networks (individual routes or summarized routes).  
Type 4 LSAs describe routes to ASBRs.
- ▶ AS-external LSAs (type 5 LSAs):  
These LSAs are generated by ASBRs and describe routes outside the autonomous system. These LSAs are flooded everywhere apart from to stub areas and NSSAs.
- ▶ NSSA external LSAs (type 7 LSAs):  
A stub area does not flood any external routes (represented by type 5 LSAs) and therefore does not support any Autonomous System Border Routers (ASBRs) at its boundaries. Thus an ASBR cannot carry any routes from other protocols into a stub area.  
RFC 1587 specifies the functioning of NSSAs. According to RFC 1587, ASBRs send type 7 LSAs instead of type 5 LSAs for the external routes within an NSSA. These type 7 LSAs are then converted into type 5 LSAs by an ABR and flooded into the backbone area. This “translator role” is negotiated among the ABRs in an NSSA (the router with the highest router ID), but it can also be configured manually.

## 7.2 General Operation of OSPF

OSPF was specially tailored to the needs of larger networks and provides a fast convergence and minimum usage of protocol messages.

The concept of OSPF is based on the creation, maintenance and distribution of what is called the link state database. This data basis describes

- ▶ all the routers within a routing domain (area) and
- ▶ their active interfaces and routes,
- ▶ how they are linked to each other and
- ▶ the costs of these links.

All the routers within an area have an identical data basis, which means that they all know the exact topology within this area.

Every router plays its part in setting up the respective data basis by propagating its local viewpoint as Link State Advertisements (LSAs). These LSAs are then flooded to all the other routers within an area.

OSPF supports a range of different network types such as point-to-point networks (for example, packet over SONET/SDH), broadcast networks (Ethernet) or non-broadcast networks.

Broadcast networks are distinguished by the fact that a number of systems (terminal devices, switches, routers) are connected to the same segment and thus can all be addressed simultaneously via broadcasts/multicasts.

OSPF generally performs the following three steps in carrying out its tasks in the network:

- ▶ Setting up the neighbor relationships (hello protocol)
- ▶ Synchronizing the link state database
- ▶ Route calculation

## 7.3 Setting up the Adjacency

When a router is started, it uses what are called hello packets to contact its neighboring routers. With these hello packets, an OSPF router finds out which OSPF routers are near it and whether they are suitable for setting up a neighbor relationship (adjacency).

In broadcast networks such as Ethernet, the number of neighbors increases with the number of routers connected, as does the information exchange for clarifying and maintaining the neighbor relationships. To reduce these volumes within an area, OSPF uses the “hello” protocol to determine a designated router (DR) within the corresponding segment. Thus every router in an area only sets up the neighbor relationship with its designated router, instead of with every neighbor. The designated router is responsible for the distribution of all the link state information to its neighbor routers.

For security reasons, OSPF provides for the selection of a backup designated router (BDR), which takes over the tasks of the DR if the DR fails. The OSPF router with the highest router priority is the DR. The router priority is specified by the administrator. If two routers have the same priority, the router with the higher router ID is selected. The router ID is the smallest IP address of a router interface. You configure this router ID manually when starting up the OSPF router ([see on page 94 “Router ID”](#)).

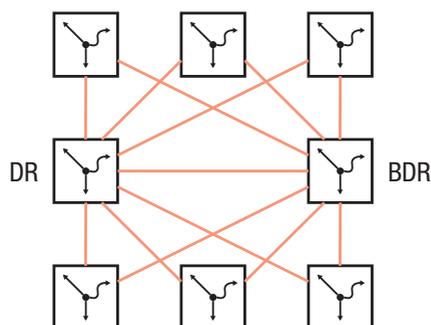


Figure 36: LSA distribution with designated router and backup designated router

To exchange information, OSPF uses reserved multicast addresses.

| Destination        | Multicast IP address | Mapped Multicast MAC address |
|--------------------|----------------------|------------------------------|
| All OSPF routers   | 224.0.0.5            | 01:00:5E:00:00:05            |
| Designated routers | 224.0.0.6: OSPF      | 01:00:5E:00:00:06            |

Table 12: OSPF - Multicast addresses

Hello packets are also used to check the configuration within an area (area ID, timer values, priorities) and to monitor the neighbor relationships. Hello packets are sent cyclically (hello interval). If hello packets are not received for a specific period (dead interval), the neighbor relationship is terminated and all the corresponding routes are deleted.

The hello interval (default: 10 seconds) and the dead interval (default: 30 seconds) can be configured for each router interface, but they must be uniform within an area.

```

enable
configure
interface 1/1

ip ospf hello-intervall 20
ip ospf dead-intervall 60
exit
exit

show ip ospf neighbor brief
all

```

Change to the privileged EXEC mode.  
Change to the Configuration mode.  
Change to the Interface Configuration mode of port 1/1.

Sets hello interval to 20 seconds.  
Sets dead interval to 60 seconds.  
Change to the Configuration mode.  
Change to the privileged EXEC mode.

Displays the neighbor relationships of the router.

| Router ID   | IP Address | Neighbor Interface | State |
|-------------|------------|--------------------|-------|
| 192.168.1.1 | 10.0.1.1   | 1/1                | Full  |
| 192.168.1.2 | 11.0.1.1   | 1/2                | Full  |
| 192.168.1.3 | 12.0.1.1   | 1/3                | Full  |
| 192.168.1.4 | 13.0.1.1   | 1/4                | Full  |

The neighbor relationships can have the following states:

|          |                                                                           |
|----------|---------------------------------------------------------------------------|
| Down     | No hello packets received yet                                             |
| Init     | Receiving hello packets                                                   |
| 2-way    | Bidirectional communication, determination of the DR and the BDR          |
| Exstart  | Determination of master/slave for LSA exchange                            |
| Exchange | LSAs are exchanged or flooded                                             |
| Loading  | Completion of the LSA exchange                                            |
| Full     | Data basis complete and uniform in the area. Routes can now be calculated |

## 7.4 Synchronization of the LSD

The central part of the OSPF is the link state database (LSD). This database contains a description of the network and the states of all the routers. It is the source for calculating the routing table. It reflects the topology of the network. It is set up after the designated router or the backup designated router has been determined within an area (Broadcast networks).

To set up the LSD and update any topology changes, the OSPF router sends link status advertisements (LSA) to all the directly accessible OSPF routers. These link status advertisements consist of the interfaces and the neighbors of the sending OSPF router that can be reached via these interfaces. OSPF routers put this information into their databases and flood the information to all the ports.

If no topology changes occur, every router repeats its own LSAs every 30 minutes.

You can view the content of the Link State Database with the CLI command “show ip ospf database”, whereby the entries are output in accordance with the areas.

```
enable
```

Switch to the privileged EXEC mode.

```
show ip ospf database
```

Displays the neighbor relationships of the router.

## Router Link States (Area 0.0.0.0)

| Link Id     | Adv Router  | Age | Sequence Chksm  | Options | Rtr Opt |
|-------------|-------------|-----|-----------------|---------|---------|
| 192.168.1.1 | 192.168.1.1 | 122 | 80000007 0x5380 | -E----  | ---E-   |
| 192.169.1.1 | 192.169.1.1 | 120 | 80000007 0xbf0e | -E----  | ---E-   |

## Network Link States (Area 0.0.0.0)

| Link Id  | Adv Router  | Age | Sequence Chksm  | Options | Rtr Opt |
|----------|-------------|-----|-----------------|---------|---------|
| 10.0.1.2 | 192.169.1.1 | 129 | 80000002 0xad5a | -E----  |         |
| 11.0.1.2 | 192.169.1.1 | 135 | 80000002 0xa066 | -E----  |         |
| 12.0.1.2 | 192.169.1.1 | 137 | 80000002 0x9372 | -E----  |         |
| 13.0.1.2 | 192.169.1.1 | 132 | 80000002 0x867e | -E----  |         |

## AS External States

| Link Id     | Adv Router  | Age | Sequence Chksm  | Options | Rtr Opt |
|-------------|-------------|-----|-----------------|---------|---------|
| 192.169.0.0 | 192.169.1.1 | 178 | 80000002 0xca1c |         |         |

The interpretation of the link ID presented depends on the corresponding LSA type:

|                        |                                                                      |
|------------------------|----------------------------------------------------------------------|
| Router Link States     | Link ID corresponds to router ID of source                           |
| Network Link States    | Link ID corresponds to interface IP address of the designated router |
| Network Summary States | Link ID corresponds to the corresponding network                     |
| Summary ASBR States    | Link ID corresponds to router ID of described ASBR                   |
| AS External States     | Link ID corresponds to the external network                          |

## 7.5 Route Calculation

After the LSDs are learned and the neighbor relationships go to the full state, every router calculates a path to every destination using the Shortest Path First (SPF) algorithm. After the optimal path to every destination has been determined, these routes are entered in the routing table. The route calculation is generally based on the accessibility of a hop and the metric (costs). The costs are added up over all the hops to the destination.

The costs of an individual router interface are based on the available bandwidth of this link. The calculation for the standard setting is based on the following formula:

$$\text{Metric} = 10\,000\,000 / \text{bandwidth (bits/sec)} .$$

For Ethernet, this leads to the following costs:

|           |                         |
|-----------|-------------------------|
| 10 Mbit   | 10                      |
| 100 Mbit  | 1                       |
| 1000 Mbit | 1 (0.1 rounded up to 1) |

The table shows that this form of calculation in the standard configuration does not permit any distinction between Fast Ethernet and Gigabit Ethernet. You can change the standard configuration by assigning a different value for the costs to each OSPF interface. This enables you to differentiate between Fast Ethernet and Gigabit Ethernet.

```
enable
configure
interface 1/1

ip ospf cost 2
```

Switch to the privileged EXEC mode.  
 Switch to the Configuration mode.  
 Switch to the Interface Configuration mode of interface 1/1.  
 Assigns the value 2 to port 1.1 for the OSPF costs.

## 7.6 Configuring OSPF

In the state on delivery, the default values are selected so that you can configure simple OSPF functions in just a few steps.

After the router interface is defined and OSPF is switched on, OSPF automatically enters the required routes in the routing table.

The example (see figure 37) shows a simple OSPF configuration. Area 0 is already defined in the state on delivery. The terminal devices do not have an OSPF function, so you do not have to activate OSPF on the corresponding router interface. By activating the redistribute function, you can inject the routes to the terminal devices into the OSPF.

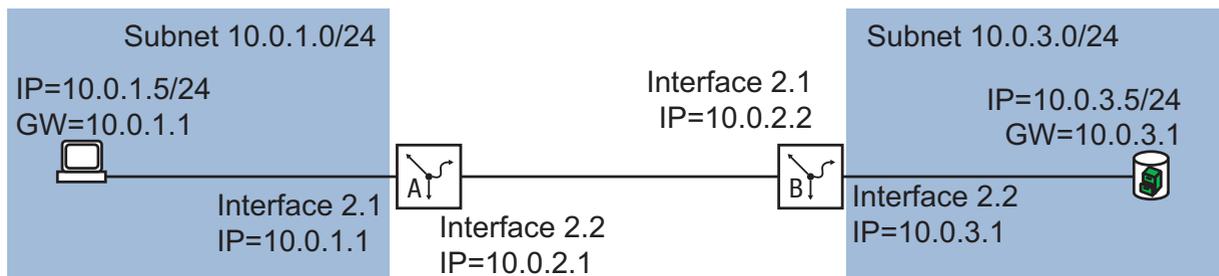


Figure 37: Example of the configuration of OSPF

The configuration of OSPF requires the following steps:

- ▶ Configure router interfaces – assign IP address and network mask.
- ▶ Switch on OSPF at port.
- ▶ Switch on OSPF globally.
- ▶ Switch on routing globally (if this has not already been done).

## ■ Configuration for router B

```
enable
configure
interface 2/2

ip address 10.0.3.1
255.255.255.0
routing
exit

interface 2/1

ip address 10.0.2.2
255.255.255.0
routing
ip ospf
exit

router ospf
enable
router-id 10.0.2.2
redistribute connected
subnets

exit
exit

show ip ospf
```

Switch to the privileged EXEC mode.

Switch to the Configuration mode.

Change to the interface configuration mode of interface 2/2.

Assign the IP parameters to the port.

Switch on the router function at this port.

Switch to the Configuration mode.

Switch to the interface configuration mode of interface 2.1 to set up OSPF.

Assign the IP parameters to the port.

Switch on the router function at this port.

Switch on OSPF at this port.

Switch to the Configuration mode.

Change to the Router Configuration mode.

Switch on OSPF globally.

Assign router ID 10.0.2.2 to router B.

Instruct OSPF to

- send the routes of the locally connected interfaces along with the learned routes in the RIP information and

- include subnetworks without OSPF in OSPF (CIDR).

Switch to the Configuration mode.

Switch to the privileged EXEC mode.

Check the settings for the global OSPF configuration.

```

Router ID..... 10.0.2.2
OSPF Admin Mode..... Enable
ASBR Mode..... Enable
RFC 1583 Compatibility..... Enable
ABR Status..... Disable
Exit Overflow Interval..... 0
External LSA Count..... 0
External LSA Checksum..... 0
New LSAs Originated..... 0
LSAs Received..... 0
External LSDB Limit..... No Limit
Default Metric..... Not configured

Default Route Advertise..... Disabled
Always..... FALSE
Metric.....
Metric Type..... External Type 2
Maximum Paths..... 4

Redistributing.....
Source..... Connected
Metric..... Not Configured
--More-- or (q)uit
Metric Type..... 2
Tag..... 0
Subnets..... Yes
Distribute List..... Not configured

```

show ip ospf interface brief **Check the settings for the OSPF interface configuration.**

| Interface | AdminMode | Area ID | Router ID | Hello Priority | Dead Intval | Retrax Intval | Retrax Intval | LSAAck Delay |
|-----------|-----------|---------|-----------|----------------|-------------|---------------|---------------|--------------|
| 2/1       | Enable    | 0.0.0.0 | 1         | 10             | 40          | 5             | 1             | 1            |
| 2/2       | Disable   | 0.0.0.0 | 1         | 10             | 40          | 5             | 1             | 1            |

```

configure Switch to the Configuration mode.
ip routing Switch on the router function globally.
exit Switch to the privileged EXEC mode.

```

- Also perform the corresponding configuration on the other OSPF routers.

show ip ospf neighbor brief **Check the OSPF neighborhood relationships.**

| Router ID | IP Address | Neighbor Interface | State |
|-----------|------------|--------------------|-------|
| 10.0.2.1  | 10.0.2.1   | 2/1                | Full  |

show ip route

Verify the routing table:

Total Number of Routes..... 3

| Network Address | Subnet Mask   | Protocol    | Next Hop Intf | Next Hop IP Address |
|-----------------|---------------|-------------|---------------|---------------------|
| 10.0.1.0        | 255.255.255.0 | OSPF Ext T2 | 2/1           | 10.0.2.1            |
| 10.0.2.0        | 255.255.255.0 | Local       | 2/1           | 10.0.2.2            |
| 10.0.3.0        | 255.255.255.0 | Local       | 2/2           | 10.0.3.1            |



## 8 Protocol-based VLANs

Along with port-based VLANs based on IEEE 802.1Q, the Switch also supports protocol-based VLANs based on IEEE 802.1v.

With port-based VLANs, the Switch uses the port VLAN ID of the receiving port to determine which VLAN a data packet belongs to if it is received without a VLAN tag.

With protocol-based VLANs, the Switch uses the protocol of the received data packet to determine which VLAN a data packet belongs to if it is received without a VLAN tag. The Switch supports the protocols

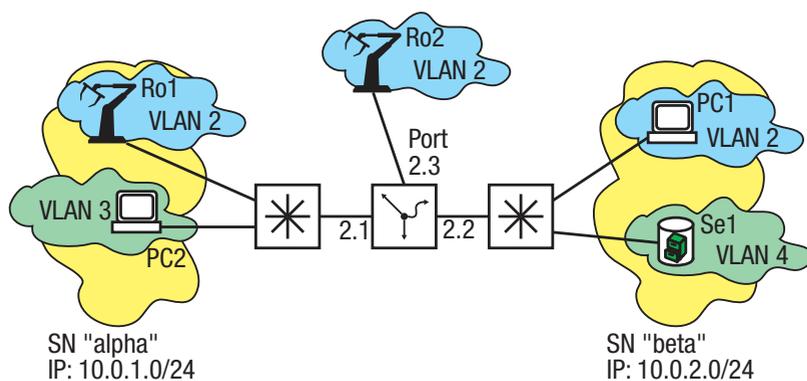
- ▶ IP,
- ▶ ARP,
- ▶ IPX.

Data packets from other protocols received without a VLAN tag are assigned to a VLAN by the Switch in accordance with the port VLAN ID.

For the VLAN assignment, the Switch takes into account

- ▶ firstly, the VLAN tag,
- ▶ then the protocol the data packet belongs to,
- ▶ and finally, the port VLAN ID.

Protocol-based VLANs enable you to transfer data packets not relevant to routing across IP subnetwork boundaries. Data packets relevant to routing are IP and ARP data packets.



*Figure 38: Example of a protocol-based VLAN*

In the example (see [figure 38](#)), PC2 and Se1 communicate via IP. These data packets are routed.

The devices Ro1, Ro2 and PC1 communicate via other Ethernet-based protocols. These data packets are switched in VLAN 2.

Thus all IP data packets remain in their subnetworks, apart from the IP data packets that are meant for a different subnetwork.

## 8.1 General Configuration

- Create a VLAN protocol group for each subnetwork.
- Assign the protocols to the VLAN protocol group for each subnetwork.
- Create the VLANs.
- Switch on the VLAN routing in the VLANs affected and thus create the virtual router interfaces.
- Assign the VLAN protocol groups to the VLANs.
- Configure the port interfaces:
  - ▶ VLAN membership
  - ▶ Port VLAN ID for non-ARP/IP data packets
  - ▶ Port of a VLAN protocol group and thus assign to a VLAN
- Configure virtual router interfaces:
  - ▶ Assign IP address
  - ▶ Switch on routing
- Switch on routing globally.

## 8.2 Configuration of the Example

```

enable
configure
vlan protocol group alpha
vlan protocol group beta
exit

show protocol all

```

| Group Name | Group ID | Protocol(s) | VLAN | Interface(s) |
|------------|----------|-------------|------|--------------|
| alpha      | 1        |             | 0    |              |
| beta       | 2        |             | 0    |              |

```

configure
vlan protocol group add
 protocol 1 ip
vlan protocol group add
 protocol 1 arp
vlan protocol group add
 protocol 2 ip
vlan protocol group add
 protocol 2 arp
exit

show protocol all

```

| Group Name | Group ID | Protocol(s) | VLAN | Interface(s) |
|------------|----------|-------------|------|--------------|
| alpha      | 1        | IP, ARP     | 0    |              |
| beta       | 2        | IP, ARP     | 0    |              |

```

vlan database
vlan 2
vlan 3
vlan 4
vlan routing 3

```

Change to the privileged EXEC mode.

Change to the Configuration mode.

Create VLAN protocol group 1 for alpha subnetwork.

Create VLAN protocol group 2 for beta subnetwork.

Change to the privileged EXEC mode.

Display the VLAN protocol groups created.

Change to the Configuration mode.

Add IP of VLAN protocol group 1.

Add ARP of VLAN protocol group 1.

Add IP of VLAN protocol group 2.

Add ARP of VLAN protocol group 2.

Change to the privileged EXEC mode.

Display the protocols assigned to the protocol groups.

Change to the VLAN mode.

Create VLAN 2.

Create VLAN 3.

Create VLAN 4.

Create a virtual router interface and activate the routing function for this interface.

```

vlan routing 4
protocol group 1 3
protocol group 2 4
exit

show protocol all

Group Name Group ID Protocol(s) VLAN Interface(s)

alpha 1 IP,ARP 3
beta 2 IP,ARP 4

show ip vlan

VLAN ID Logical Interface IP Address Subnet Mask MAC Address

3 9/1 0.0.0.0 0.0.0.0 00:80:63:51:74:2C
4 9/2 0.0.0.0 0.0.0.0 00:80:63:51:74:2D

configure
interface 2/1

vlan participation exclude 1
vlan participation include 2
vlan participation include 3
vlan pvid 2

protocol vlan group 1

exit

interface 2/2

vlan participation exclude 1
vlan participation include 2
vlan participation include 4
vlan pvid 2

```

Create a virtual router interface and activate the routing function for this interface.

Assign VLAN protocol group 1 to VLAN 3.  
Assign VLAN protocol group 2 to VLAN 4.  
Change to the privileged EXEC mode.

Display the protocols and VLANs assigned to the VLAN protocol groups.

Display the assignment of the virtual router interfaces to the VLANs.

Change to the Configuration mode.  
Switch to the Interface Configuration mode of interface 2/1.

Remove port 2.1 from VLAN 1.  
Declare port 2.1 a member of VLAN 2.  
Declare port 2.1 a member of VLAN 3.  
Set the port VLAN ID to 2, which means that the Switch assigns non-IP/ARP data packets to VLAN 2.

Assign VLAN protocol group 1 to interface 2.1, which means that the Switch assigns IP/ARP data packets to VLAN 3.  
Change to the Configuration mode.

Change to the interface configuration mode of interface 2/2.

Remove port 2.2 from VLAN 2.  
Declare port 2.2 a member of VLAN 2.  
Declare port 2.2 a member of VLAN 4.  
Set the port VLAN ID to 2, which means that the Switch assigns non-IP/ARP data packets to VLAN 2.

```

protocol vlan group 2
exit

interface 2/3
vlan participation exclude 1
vlan participation include 2
vlan pvid 2
exit

interface 9/1
ip address 10.0.1.1
255.255.255.0
routing
exit

interface 9/2
ip address 10.0.2.1
255.255.255.0
routing
exit
exit

show ip interface brief

Interface IP Address IP Mask Netdir Multi
----- -
9/1 10.0.1.1 255.255.255.0 Disable Disable
9/2 10.0.2.1 255.255.255.0 Disable Disable

configure
ip routing

```

Assign VLAN protocol group 2 to interface 2.2, which means that the Switch assigns IP/ARP data packets to VLAN 4.

Change to the Configuration mode.

Switch to the Interface Configuration mode of interface 2.3.

Remove port 2.3 from VLAN 1.

Declare port 2.3 a member of VLAN 2.

Set the port VLAN-ID to 2, which means that data packets that are received without a tag at that port are assigned to VLAN 2 by the Switch.

Change to the Configuration mode.

Switch to the interface configuration mode of interface 9/1.

Assign the IP parameters to the router interface.

Activate the router function at this interface.

Change to the Configuration mode.

Switch to the interface configuration mode of interface 9/2.

Assign the IP parameters to the router interface.

Activate the router function at this interface.

Change to the Configuration mode.

Change to the privileged EXEC mode.

Display the entries of the virtual router interface.

Change to the Configuration mode.

Switch on the router function globally.

## 9 Multicast Routing

Multicast data streams are data packets that a sender sends to multiple recipients. To reduce the network load, the sender uses a Multicast address. He thus sends each packet only once to the Multicast address instead of sending it to each recipient individually. The recipients recognize a Multicast data stream intended for them by the Multicast address.

A common reason for introducing subnetworks is the restriction of Broadcast data streams. Switches flood Broadcast/Multicast data streams to all ports, while routers block Broadcast/Multicast data streams. Multicast routing enables you to accurately transmit Multicast data streams beyond the boundaries of subnetworks. Accurate transmission means sending data streams with defined Multicast addresses exclusively to those devices that want to receive the Multicast data stream.

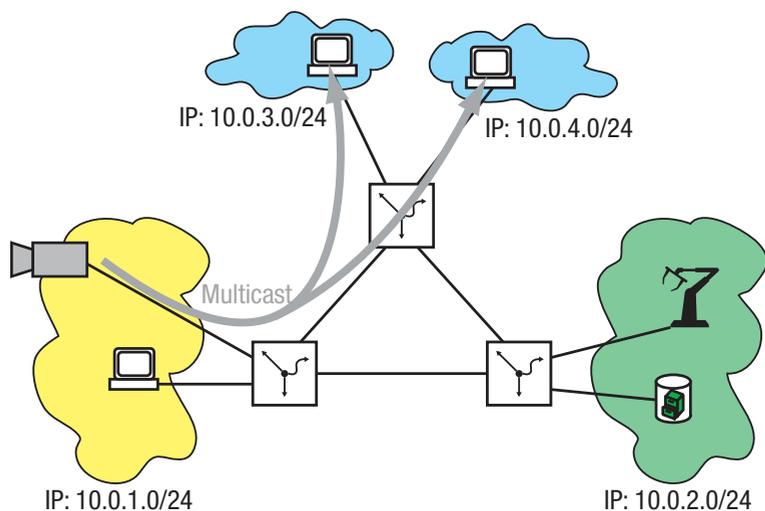


Figure 39: Example of a Multicast application

To the use of Multicast routing pertains:

- ▶ Defined Multicast addresses
- ▶ A protocol for Multicast group registration that organizes the exchange of information by means of Multicast data streams (e.g. IGMP). This information relates to the reporting that network participants wish to receive Multicast data streams and querying this wish by means of intermediate devices.
- ▶ A protocol that guides the Multicast data streams in accordance with the information on Multicast data streams (e.g. PIM-DM, DVMRP).

# 9.1 Multicast Addresses

## 9.1.1 IP Multicast Addresses

The IANA (Internet Assigned Numbers Authority) defines the IP addresses of the class D IP address space as Multicast addresses. IP Multicast addresses are in the range from 224.0.0.0 to 239.255.255.255.

| IP address range            | Assignment                                                                                                                                                                                                                                                                                                                                                                                                          |
|-----------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 224.0.0.0                   | Base address, reserved                                                                                                                                                                                                                                                                                                                                                                                              |
| 224.0.0.1 - 224.0.0.255     | Local Network Control Block, reserved for routing protocols, IGMP, etc. For example:<br>224.0.0.1 - all hosts of a subnetwork<br>224.0.0.2 - all routers of a subnetwork<br>224.0.0.4 - all DVMRP routers<br>224.0.0.5 - all OSPF routers<br>224.0.0.6 - all OSPF DR routers<br>224.0.0.9 - all RIP v2 routers<br>224.0.0.13 - all PIM routers<br>224.0.0.18 - all VRRP routers<br>224.0.0.22 - all IGMP v3 reports |
| 224.0.1.0 - 224.0.1.255     | Internetwork Control Block                                                                                                                                                                                                                                                                                                                                                                                          |
| 224.0.2.0 - 224.0.255.255   | AD HOC Block                                                                                                                                                                                                                                                                                                                                                                                                        |
| 224.1.0.0 - 238.255.255.255 | Various organizations, protocols, applications, reservations. For example:<br>232.0.0.0-232.255.255.255 - Source-specific Multicasts                                                                                                                                                                                                                                                                                |
| 239.0.0.0 - 239.255.255.255 | Administratively scoped IP v4 Multicast space<br>These Multicast addresses are not transferred by any router beyond the local boundaries and into the Internet. Therefore the administrator can assign these addresses any way he wants within these local boundaries.                                                                                                                                              |

*Table 13: Assignment of the IP Multicast address range*

---

The administratively scoped IP v4 Multicast area is subdivided further by the IANA:

| IP address range                  | Assignment                                   |
|-----------------------------------|----------------------------------------------|
| 239.000.000.000 - 239.191.255.255 | Reserved [IANA]                              |
| 239.192.000.000 - 239.251.255.255 | Organization-local scope [Meyer, RFC2365]    |
| 239.252.000.000 - 239.254.255.255 | Site-local scope (reserved) [Meyer, RFC2365] |
| 239.255.000.000 - 239.255.255.255 | Site-local scope [Meyer, RFC2365]            |

*Table 14: Assignment of the administratively scoped IP v4 Multicast area*

In the end, the following multicast IP address ranges are left over for disposal by an organisation's administrator:

- ▶ 239.192.000.000 - 239.251.255.255  
for an organisation's local areas.
- ▶ 239.255.000.000 - 239.255.255.255  
for an organisation's entire area.

**Note:** When selecting the Multicast IP addresses, ensure that they can be uniquely mapped onto MAC Multicast addresses ([see on page 124 “Mapping IP MAC Multicast Addresses”](#)).

## 9.1.2 MAC Multicast Addresses

The IEEE calls the 48-bit MAC address an “Extended Unique Identifier”. It is the unique identifier of a device. The first 24 bits of the MAC address (Organizationally Unique Identifier, OUI) is assigned by the IEEE to the manufacturer. The manufacturer uses the last 24 bits to uniquely identify their device interfaces.

A number of MAC addresses are reserved for specific applications:

| MAC-Address       | Type  | Use                              |
|-------------------|-------|----------------------------------|
| 01-00-5E-00-00-00 | 0800  | Internet Multicast [RFC1112]     |
| 01-80-C2-00-00-00 | -802- | Spanning tree (for bridges)      |
| FF-FF-FF-FF-FF-FF | 0806  | ARP (for IP and CHAOS) as needed |
| FF-FF-FF-FF-FF-FF | 8035  | Reverse ARP                      |

*Table 15: Examples of reserved MAC addresses*

### 9.1.3 Mapping IP MAC Multicast Addresses

When IP data packets are sent via Ethernet, the IP address is assigned to a MAC address, and therefore IP Multicast addresses are also mapped onto MAC Multicast addresses.

The 23 lower-value bits of the 32-bit IP Multicast address make up the 23 lower-value bits of the 48-bit MAC Multicast address.

Of the remaining 9 bits of the IP Multicast address, 4 bits are used as the class D identification for the Multicast address.

The remaining 5 bits ensure that 32 IP Multicast addresses can be mapped onto one and the same MAC Multicast address.

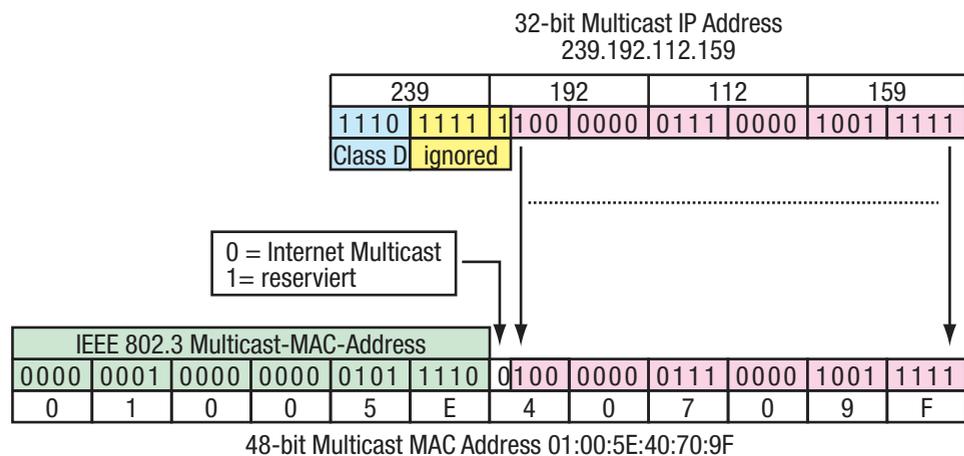


Figure 40: Conversion of the IP address to the MAC address

---

## 9.2 Multicast Group Registration

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, or to find out who is interested in becoming a group member.

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 target address field only in accordance with the routing table.

Devices which no longer want to be members of a Multicast group can cancel their membership by means of a Leave message (from IGMP version 2), and they do not transmit any more Report messages. The router removes the routing table entry if it does not receive any Report messages within a specified period of time (aging time).

If there are multiple routers with an active IGMP function in the subnetwork, then

- ▶ for IGMP version 1, all routers in this subnetwork periodically send queries
- ▶ for IGMP versions 2 and 3, the routers decide which router takes over the query function (Querier Election).

| Protocol | Standard |
|----------|----------|
| IGMP v1  | RFC 1112 |
| IGMP v2  | RFC 2236 |
| IGMP v3  | RFC 3376 |

*Table 16: Standards which describe the Multicast Group Membership Discovery*

An advantage that IGMP version 2 has over IGMP version 1 is that a Multicast recipient can cancel his membership in a Multicast group, thus freeing up his bandwidth more quickly. Another advantage is the introduction of the Querier Election.

IGMP version 3 provides more security with the Source Filtering option. Multicast recipients can define the sources from which they want to receive Multicast data streams. The router blocks Multicast data streams with other source addresses.

The different versions of IGMP are compatible downwards. This means that an IGMP version 3 router can also process version 1 and version 2. If there are different IGMP versions in a subnetwork, the participating routers agree on the smallest version.

## 9.3 PIM-DM/PIM-SM/DVMRP

The DVMRP (Distance Vector Multicast Routing Protocol) is a routing protocol that uses its own distance vector algorithm to create its own Multicast routing table. DVMRP works similarly to RIP and is limited to 32 hops.

In the past, DVMRP was very widely-used, and it is used today because of its compatibility with existing applications.

PIM-DM (Protocol Independent Multicast - Dense Mode) is a routing protocol that uses the available Unicast routing table of other protocols to steer Multicast data streams.

This ability, and the fast convergence it enables, is the reason why PIM-DM is now very widely-used.

DVRP and PIM-DM use what is known as the Implicit Join method, which means that a participant who has left the Multicast data stream is not included in the data flow. To enable a participant who has left to receive Multicast data streams again, the routers transmit to all participants again after the hold time has elapsed. For DVMRP, the hold time is fixed at 2 hours. For PIM-DM, the variable hold time is set at 210 seconds. PIM-DM requires that you set the hold time to the same value for all the participating routers.

| DVMRP                                                          | PIM-DM                                                     |
|----------------------------------------------------------------|------------------------------------------------------------|
| Knows the topology better because DVMRP uses its own protocol. | Fast convergence<br>Optimization through changeable timers |

*Table 17: Advantages of the protocols*

PIM-SM (Protocol Independent Multicast - Sparse Mode) is an extended variant of PIM-DM.

This version of PIM is mainly suitable for networks with a restricted bandwidth (e.g. WANs) and for networks with few participants from Multicast groups.

PIM-SM differs from PIM-DM and DVMRP in the following ways, as regards subscribing and unsubscribing participants:

- ▶ PIM-DM and DVMRP assume that very many participants are interested in the Multicast groups. Therefore, at the start of the communication, PIM-DM and DVMRP flood the information about available Multicast groups into the entire network. Participants who are not interested in a Multicast group unsubscribe from this group explicitly.
- ▶ In contrast, PIM-SM assumes that very few participants in the network are interested in the Multicast groups. PIM-SM waits for the participants to actively subscribe without itself sending information about available Multicast groups to the network. All participants who are interested in a Multicast group subscribe to a group explicitly. With this procedure, PIM-SM reduces the data traffic in the network.

### 9.3.1 How PIM-DM and DVMRP function

In the first step for setting up the Multicast routes, a PIM-DM/DVMRP router floods Multicast data streams to all ports, with the exception of the receiving port (= flooding).

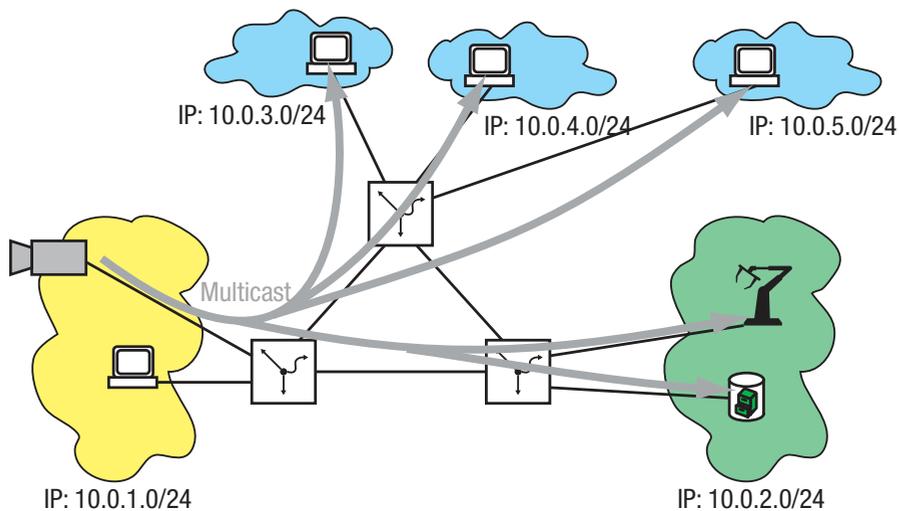


Figure 41: Multicast Flooding

Routers that are not interested in the Multicast data stream send what are known as prune messages so that they will not be sent any Multicast data streams from this source in the future.

The routers send the prune messages back in the direction from which they received the Multicast data streams (upstream).

A router transmits a Multicast data stream until the hold time has elapsed,

- ▶ when it is using IGMP to determine a Multicast recipient which is connected to a port directly or via a switch or
- ▶ when a router that is connected to a Multicast recipient is connected directly to a port.

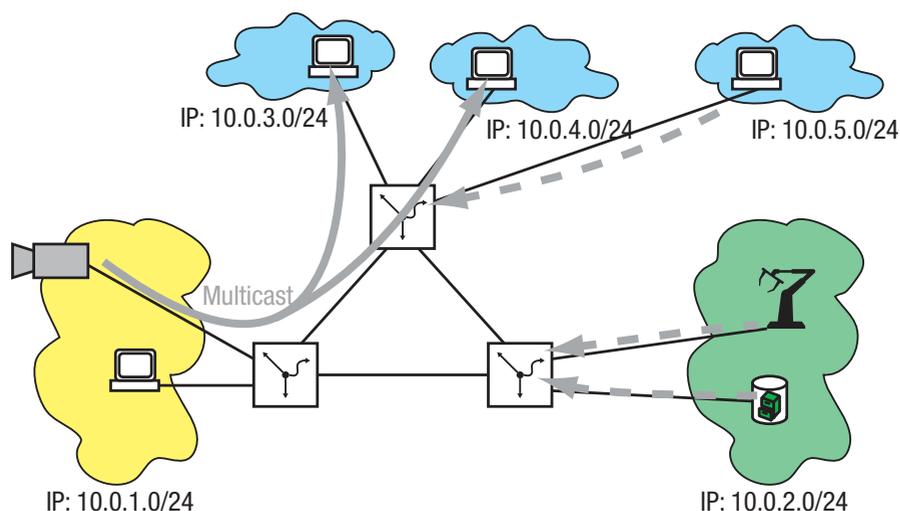


Figure 42: Multicast Pruning

In the second step, PIM-DM/DVMRP calculates the shortest paths (STP - Shortest Path Tree) between the Multicast source and the Multicast recipients. The result is the source-routed Multicast distribution tree. Source-routed means that the calculation method is tracing back from the recipient to the source (RPF - Reverse Path Forwarding). To avoid loops, RPF rejects all Multicast data streams received at a port that belongs to a longer path than the shortest path.

The method of the shortest paths is very efficient with regard to the data paths. However, it does have the disadvantage that, depending on the topology, the routers require a lot of memory space to store the many Multicast trees.

A participant who has unsubscribed from the Multicast data stream can subscribe to the Multicast data stream again. This procedure is known as grafting. Grafting enables the participant to receive Multicast data streams again before the hold time has elapsed.

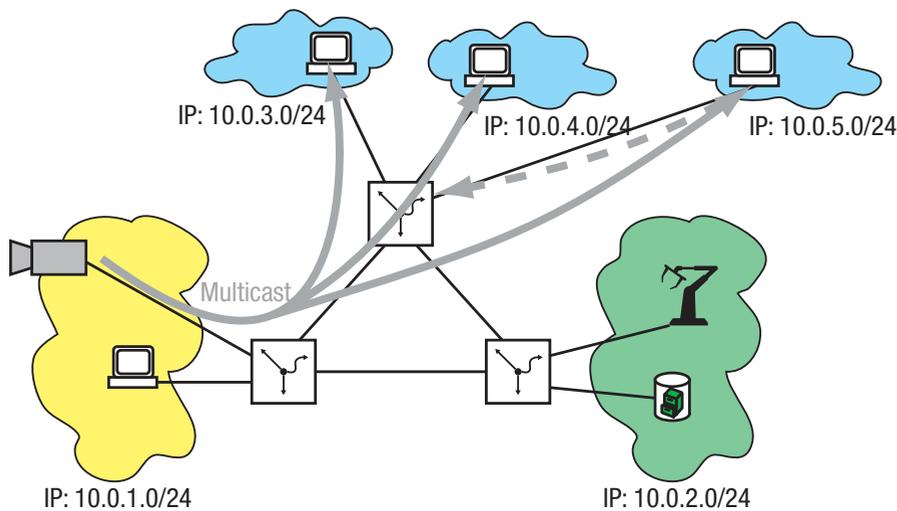


Figure 43: Multicast Grafting

### 9.3.2 How PIM-SM functions

PIM-SM differs from PIM-DM and DVMRP with regard to the topology of the Multicast distribution:

- ▶ PIM-DM and DVMRP always use the direct paths (SPT - Shortest Path Tree) between the Multicast source and the Multicast recipients.
- ▶ With the standard setting, PIM-SM uses the path via a central transmission point (Rendezvous Point – RP). This path is known as the Rendezvous Point Tree (RPT). At the rendezvous point, the Multicast recipients report their interest in a Multicast group. The Multicast sources register at a rendezvous point and send the data exclusively to this rendezvous point, which forwards the data to the Multicast recipients. There is exactly one rendezvous point for each group. A PIM-SM router serves as the rendezvous point for one or more Multicast groups. The rendezvous point tree extends between the rendezvous point of the Multicast group and the Multicast recipients. The recipients of a Multicast group share this RPT as a shared tree. With this procedure, PIM-SM reduces the amount of stored tree information in the routes and thus reduces the processor load for the devices.

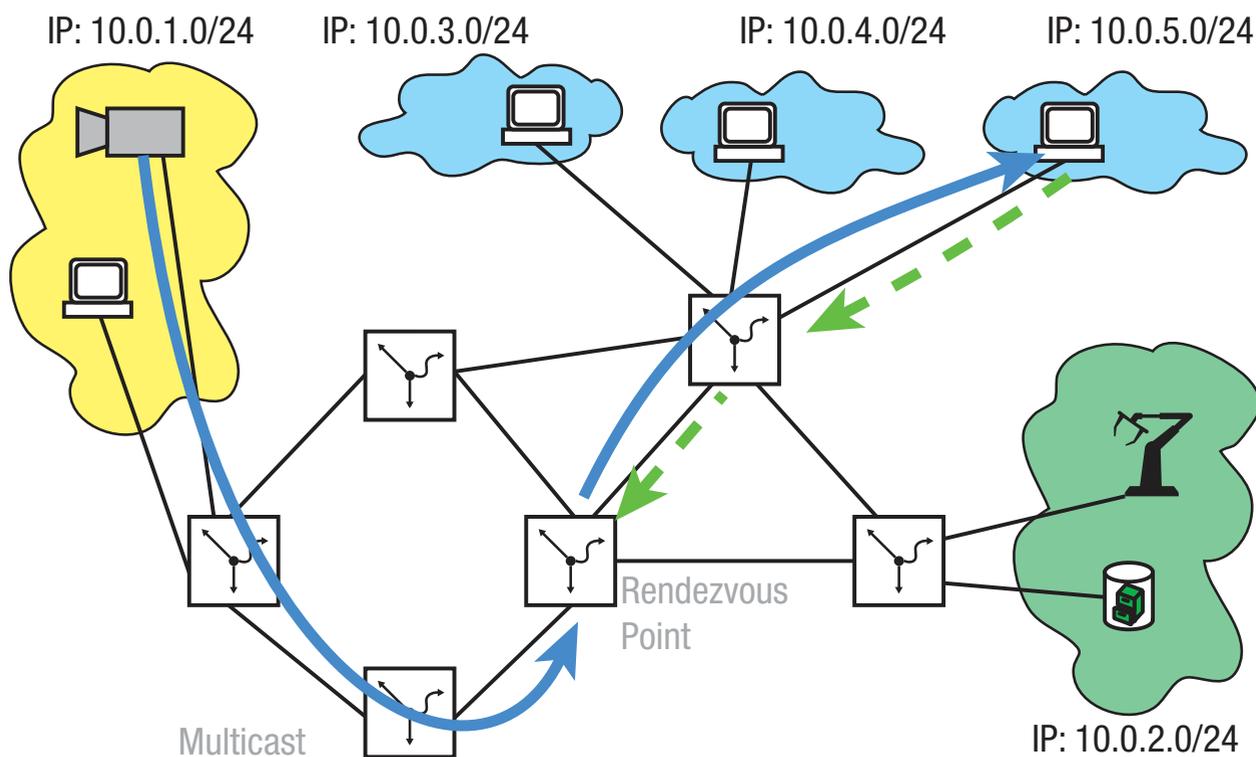


Figure 44: Rendezvous Point in the PIM-SM protocol

Depending on the application, there are shorter paths between the Multicast recipients and the Multicast source than the rendezvous point tree. In these cases, PIM-SM enables a switch to the direct path SPT. If the data rate for the Multicast transmission via the RPT exceeds a configurable threshold value, the router of the Multicast recipient unsubscribes from the rendezvous point. Instead, the router of the Multicast recipient creates a direct link to the last router before the Multicast source.

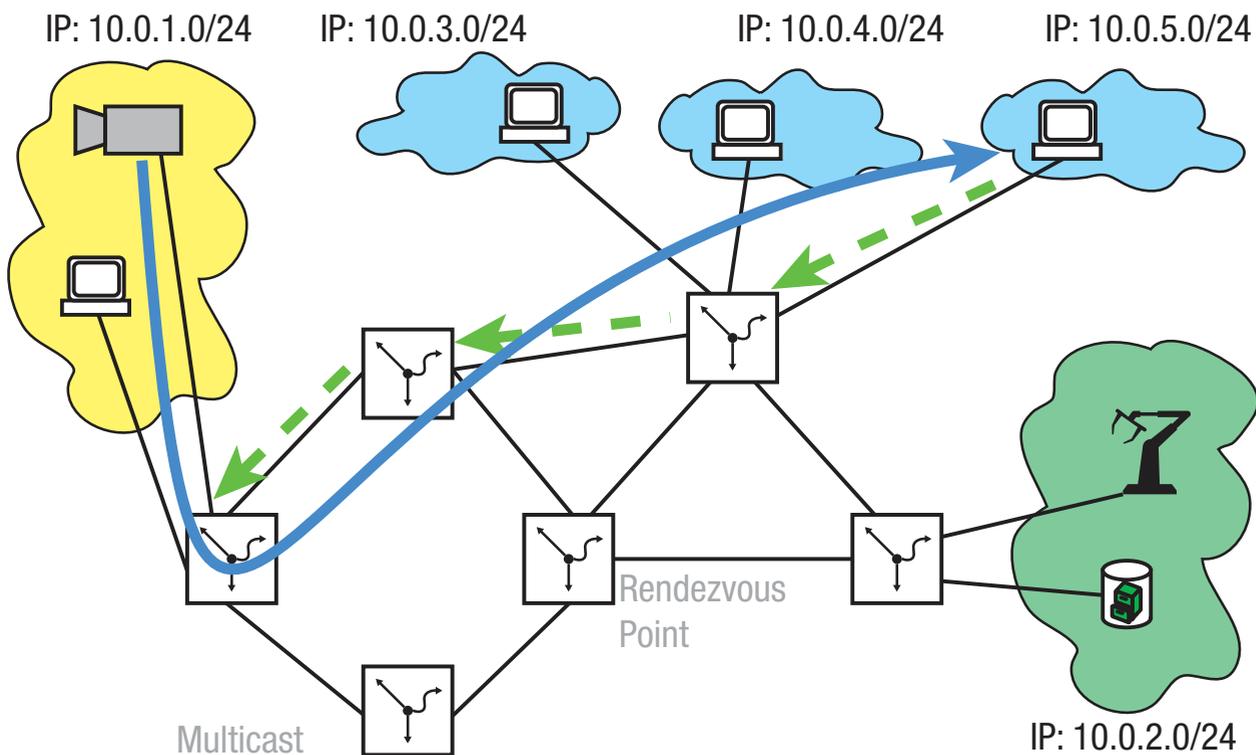


Figure 45: Topology change from the RPT to the direct path (STP)

### ■ Designated Router

A participant who is interested in a Multicast group sends a corresponding IGMP message to the next reachable router. This router then sends a join message in the direction of the rendezvous point. If there are additional routers between the sending router and the rendezvous point, these forward the join message. This transmission ends either at the rendezvous point itself or at an already existing branch of the RPT. After the participant subscribes, PIM-SM creates or extends the path between the rendezvous point and the participant. When a participant unsubscribes from a Multicast group, the next router reachable from the participant sends a prune message to the rendezvous point. The prune message thus removes the related branch from the RPT.

In a network with multiple PIM-SM routers, exactly one router takes over the transmission of the join and prune messages between the Multicast recipients and the rendezvous point. In the following figure, this procedure is represented by green arrows. On the side of the Multicast sources, one of the PIM-SM routers also registers the available Multicast groups at the rendezvous point. The figure uses blue arrows to show this procedure.

These routers are called designated routers (DR). In the standard setting,

the routers select the designated router using the IP address. The PIM-SM router with the highest IP address in a network segment takes over the task of the designated router. The DR selection can be controlled by setting a special priority for the designated routers. In this case, the router with the highest priority takes over the tasks of the designated router. The IP address is only used in the selection process if the priorities are the same.

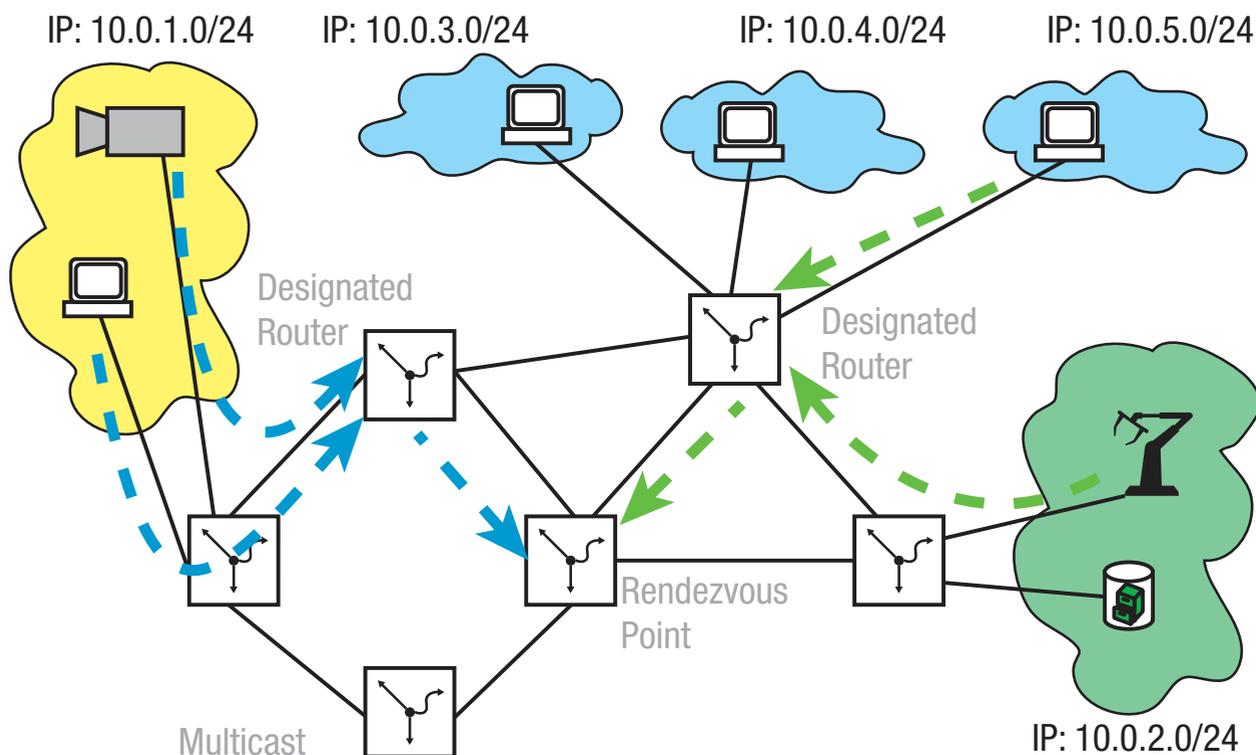


Figure 46: Designated routers forward messages from Multicast sources and Multicast participants to the rendezvous point

**■ Bootstrap router**

PIM-SM provides two procedures for selecting the rendezvous point for a Multicast group:

**▶ Static RP configuration**

In this procedure, one of the routers in the network is fixed as the rendezvous point for a Multicast group. The other routers contain the IP address of this router and the address of the related Multicast group in their configuration.

**▶ Dynamic RP configuration based on the Bootstrap Router procedure (BSR)**

In this procedure, the routers in the network determine the rendezvous point dynamically. A router has the option to offer itself as a candidate for the task of rendezvous point. The dynamic procedure uses bootstrap routers to select the rendezvous point for a Multicast group. The bootstrap messages also inform the other routers in the PIM-SM domain about the router selected as the rendezvous point. The PIM-SM routers forward the Bootstrap messages within the PIM-SM domain. The PIM-SM domain consists of all the reachable routers with an activated PIM-SM protocol. An active PIM-SM router has the option of limiting the domain as a BSR border. A router configured in this way drops the received BSR messages.

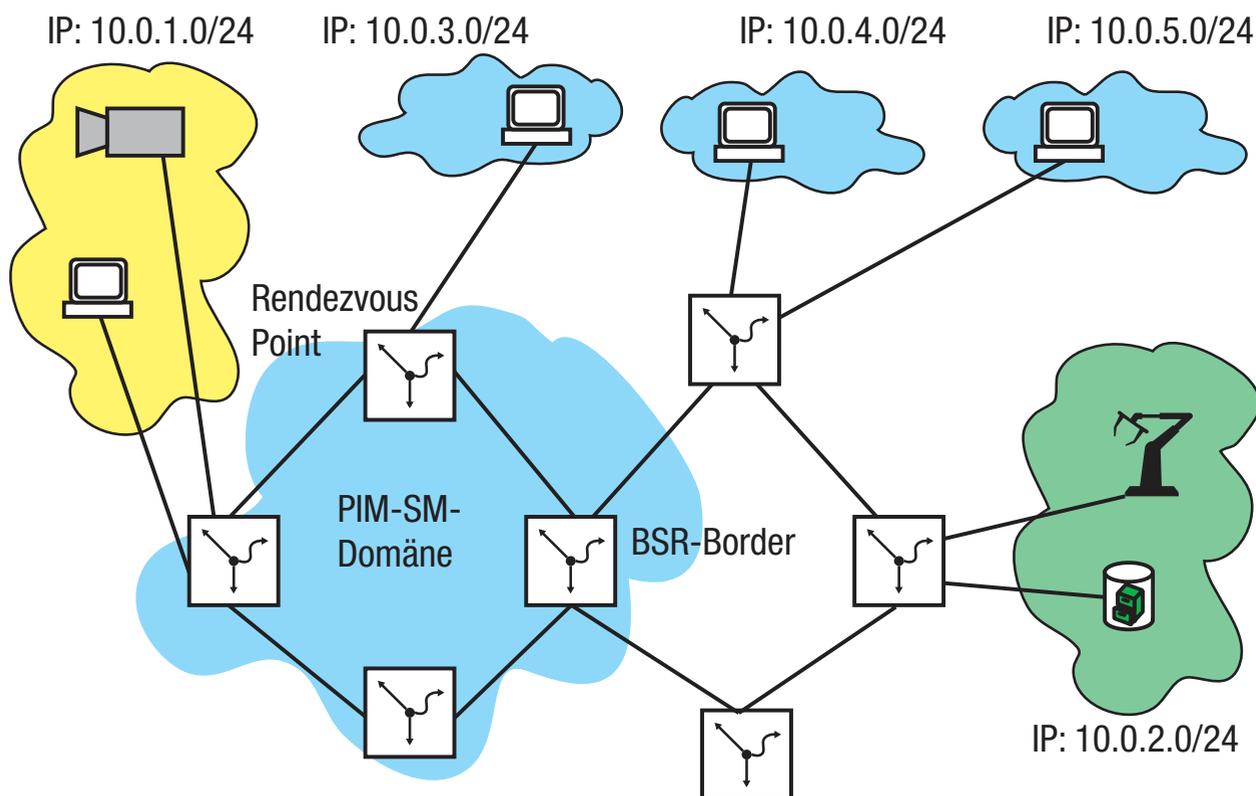


Figure 47: Routers in the configuration as BSR borders drop bootstrap messages and limit the PIM-SM domain

### ■ Application example for PIM-SM

The following example shows you how you can configure PIM-SM using the Command Line Interface.

Task assignment:

- ▶ Set up a PIM-SM example configuration (see following figure).
- ▶ Configure IGMP, OSPF and PIM-SM.
- ▶ Configure RP statically.
- ▶ Use Multicast address range 239.1.0.0/16.

**Note:** The Unicast (UC) protocol used in the example is OSPF. You can also use RIP instead of OSPF.

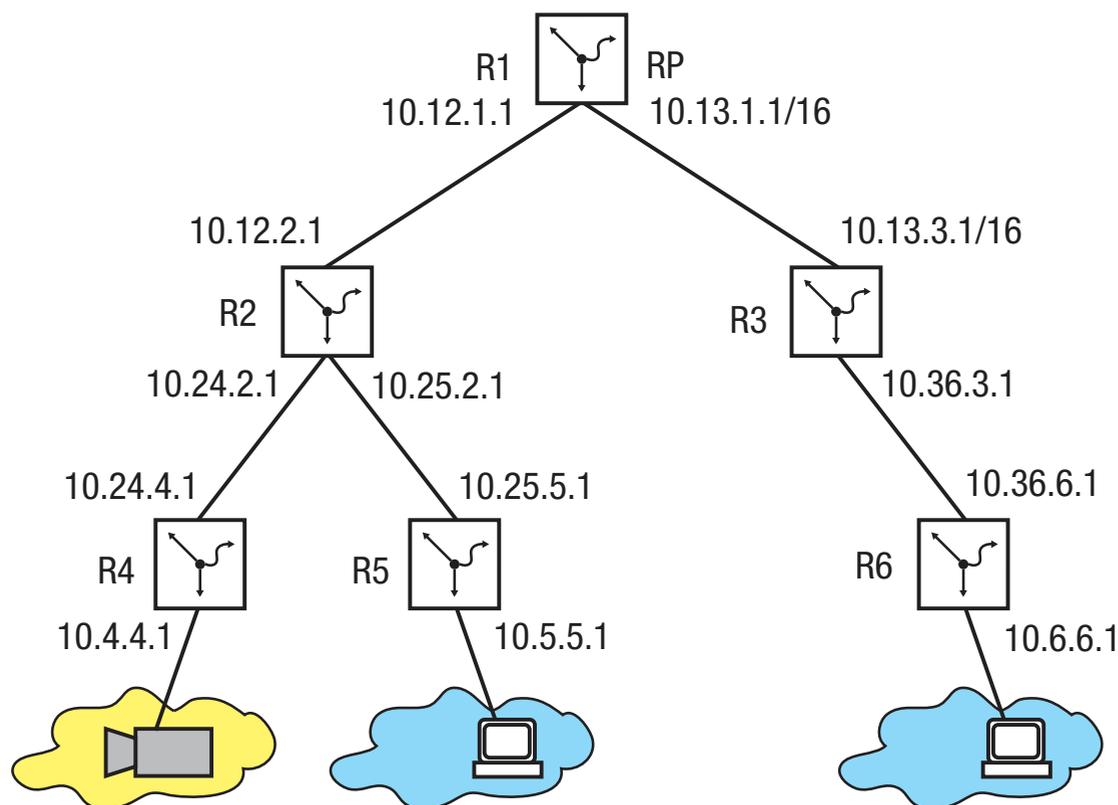


Figure 48: Example configuration for PIM-SM

- You use the following CLI command sequence to configure PIM-SM.

|                                                                |                                                                              |
|----------------------------------------------------------------|------------------------------------------------------------------------------|
| <code>enable</code>                                            | Switch to the privileged EXEC mode.                                          |
| <code># set prompt Rx</code>                                   | Set input prompt for better orientation (replace x by router number)         |
| <code># configure</code>                                       | Switch to the configuration mode.                                            |
| <code>(Config)# ip routing</code>                              | Enable routing                                                               |
| <code>(Config)# show ip brief</code>                           | Display overview of IP information.                                          |
| <code>(Config)# router ospf</code>                             | Configure UC routing protocol globally.                                      |
| <code>(Config-router)# router-id x.1.1.1</code>                | Switch to the router configuration mode for OSPF (Open Shortest Path First). |
| <code>(Config-router)# enable</code>                           |                                                                              |
| <code>(Config-router)# redistribute connected [subnets]</code> |                                                                              |
| <code>(Config-router)# exit</code>                             | Switch back to the configuration mode.                                       |
| <code>(Config)# ip igmp</code>                                 | Enable IGMP globally (automatically enables MC routing and IGMP snooping).   |
| <code>(Config)# ip multicast</code>                            | Enable Multicast forwarding (routing).                                       |
| <code>(Config)# ip pimsm</code>                                | Enable PIM-SM globally.                                                      |

|                                                      |                                                             |
|------------------------------------------------------|-------------------------------------------------------------|
| (Config)# ip pimsm rp-address <ip-@><br><MC @>...    | Set the static Rendezvous Point for a Multicast range.      |
| (Config)# interface <s/p>                            | Configure routing interfaces (slot/port).                   |
| (Interface s/p)# ip address <ip-@><br><mask>         | Configure IP address and subnetwork mask for the interface. |
| (Interface s/p)# routing                             | Enable routing at the interface.                            |
| (Interface s/p)# ip ospf area-id 0.0.0.0             | Configure UC routing protocol for each interface.           |
| (Interface s/p)# ip ospf                             | Activate OSPF on the interface.                             |
| (Interface s/p)# ip igmp                             | Enable IGMP for each interface.                             |
| (Interface s/p)# ip igmp version<br><1 2 3>          | Optional: Change version (default: 2).                      |
| (Interface s/p)# ip pimsm mode                       | Enable PIM-SM at the corresponding interfaces.              |
| (Interface s/p)# exit                                | Switch to the configuration mode.                           |
| (Config)# exit                                       | Switch to the privileged EXEC mode.                         |
| # show ip pimsm                                      | Display PIM-SM status of the router.                        |
| # copy system:running-config<br>nvram:startup-config | Save current configuration to NVRAM.                        |
| # logout                                             | End CLI session.                                            |

**Note:** Configure the rendezvous point (RP) on all routers on which you have enabled PIM-SM, also on the RP itself. Alternatively, define at least one bootstrap router (BSR) and at least one RP candidate. If you want to use the advantages of the redundancy function, configure 2 RP candidates and 2 BSR candidates.

- The following CLI show commands show the PIM-SM, Multicast and IGMP parameters for your current configuration.

|                        |                                              |
|------------------------|----------------------------------------------|
| (Interface s/p) # show | Display the possible show commands.          |
| # show ip pimsm        | Display the current PIM-SM configuration.    |
| # show ip mcast        | Display the current Multicast configuration. |
| # show ip igmp         | Display the current IGMP configuration.      |

- You can optionally perform the following configurations afterwards:

|                                                                |                                                      |
|----------------------------------------------------------------|------------------------------------------------------|
| (Interface s/p) # ip pimsm dr-<br>priority <0...2.147.483.647> | Configure DR priority.                               |
| (Interface s/p) # ip pimsm hello-interval<br><0...18000>       | Configure Hello Interval in seconds (default: 30 s). |

- Optional: Instead of defining the RPs statically, you can configure BSR and RP candidates, from which BSR and RP are selected.

```
(Config)# ip pimsm bsr- Configure BSR candidate.
candidate interface
<slot/port>

(Config)# ip pimsm rp- Configure RP candidate.
candidate interface
<slot/port>
```

## 9.4 Scoping

In the Multicast transmission, the protocol provides two options for limiting the expansion of the Multicast data stream:

► **Multicast Address Scoping / Boundary**

In the Multicast Address Scoping, the administrator assigns a Multicast IP address range to a router interface (see table 14). The router interface blocks the Multicast data streams with addresses within this address range.

Example:

```
ip mcast boundary 239.193.122.0 255.255.255.0
```

In this example, the router interface blocks Multicast data streams with a Multicast IP address in the range 239.193.122.0-239.193.122.255.

► **TTL Scoping**

Every Multicast data packet contains a TTL (Time To Live) The TTL is a counter which each router de-increments when it transmits a Multicast data packet.

In TTL Scoping, the administrator assigns a TTL threshold to an interface. The router interface blocks every Multicast data packet for which the TTL is below the TTL threshold.

Example:

```
ip multicast ttl-threshold 64
```

In this example, the router interface blocks Multicast data streams with a TTL whose value is less than 64.

| TTL   | Range                                                           |
|-------|-----------------------------------------------------------------|
| 0     | Restricted to the same host                                     |
| 1     | Restricted to the same subnetwork                               |
| < 32  | Restricted to a particular location, organization or department |
| < 64  | Restricted to the same region                                   |
| < 128 | Restricted to the same continent                                |
| < 255 | Unrestricted, global                                            |

Table 18: Usual scope for TTLs

---

## 9.5 Multicast Configuration

Select the Multicast protocol that suits your application best.

As the Multicast routing protocols use different methods for the Multicast transmission, the router prevents you from using more than one Multicast routing protocol at the same time.

When one Multicast routing protocol is activated, the router deactivates any other active Multicast routing protocol.

### 9.5.1 Example with Layer 3 Redundancy

The Multicast configuration consists of the following steps:

- ▶ Configure the routing function on the participating routers - for example, with OSPF ([see on page 108 “Configuring OSPF”](#)).
- ▶ Specify Multicast addresses, if applicable.
- ▶ Configure router interfaces. This also includes
  - ▶ specifying the Multicast boundaries
  - ▶ activating IGMP and
  - ▶ activating the selected Multicast routing protocol.
- ▶ Globally activate IGMP and therefore also IGMP Snooping.
- ▶ Globally activate the Multicast routing protocol.
- ▶ Activate Multicast transmission (forwarding).

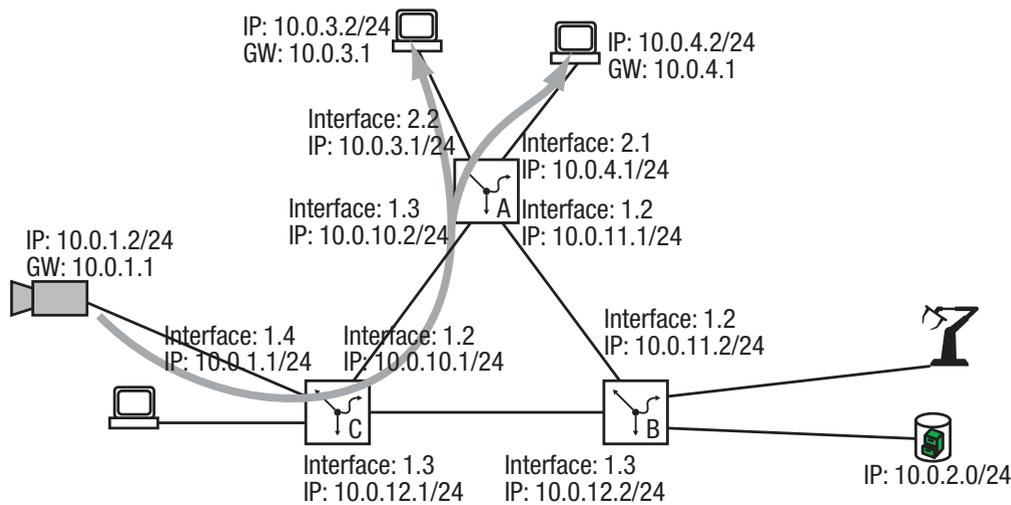


Figure 49: Multicast example configuration

□ Configure router interfaces using the example of router A (see figure 49):

|                              |                                                                    |
|------------------------------|--------------------------------------------------------------------|
| enable                       | Change to the privileged EXEC mode.                                |
| configure                    | Change to the Configuration mode.                                  |
| interface 2/1                | Switch to the Interface Configuration mode of interface 2/1.       |
| ip multicast ttl-threshold 3 | Set threshold for Multicast expansion (see on page 141 “Scoping”). |
| ip igmp                      | Activate IGMP at port.                                             |
| ip pimdm mode                | Activate PIM-DM as multicast protocol.                             |
| exit                         | Change to the Configuration mode.                                  |
| interface 2/2                | Change to the interface configuration mode of interface 2/2.       |
| ip multicast ttl-threshold 3 | Set threshold for Multicast expansion (see on page 141 “Scoping”). |
| ip igmp                      | Activate IGMP at port.                                             |
| ip pimdm mode                | Activate PIM-DM as multicast protocol.                             |
| exit                         | Change to the Configuration mode.                                  |

```

interface 1/3 Change to the Interface Configuration mode of
 interface 1/3.
ip multicast ttl-threshold 3 Set threshold for Multicast expansion (see on
 page 141 "Scoping").
ip igmp Activate IGMP at port.
ip pimdm mode Activate PIM-DM as multicast protocol.
exit Change to the Configuration mode.

```

- Globally activate IGMP using the example of router A (see figure 49):

```
ip igmp Activate IGMP at port.
```

- Globally activate Multicast using the example of router A (see figure 49):

```

ip pimdm Select the Multicast routing protocol in the
 configuration mode.
ip multicast Globally activate Multicast transmission.
exit Switch to the privileged EXEC mode.

```

- Check the Multicast routing settings

```

#show ip pimdm

Admin Mode..... Enable

 PIM-DM INTERFACE STATUS
Interface Interface Mode Protocol State

1/3 Enable Operational
2/1 Enable Operational
2/2 Enable Operational
#show ip mcast

Admin Mode..... Enable
Protocol State..... Operational
Table Max Size 256
Number Of Packets For Which Source Not Found .. 0
Number Of Packets For Which Group Not Found ... 0
Protocol..... PIMDM
Entry Count 0
Highest Entry Count 0
#show ip mcast mroute summary

 Multicast Route Table Summary
Source IP Group IP Protocol Incoming Outgoing
----- ----- -
10.0.1.159 239.192.1.1 PIMDM 1/3 2/1
10.0.1.159 239.192.1.1 PIMDM 1/3 2/2

```

```

#show ip igmp

IGMP Admin Mode..... Enable

 IGMP INTERFACE STATUS
Interface Interface Mode Protocol State

1/2 Enable Operational
1/3 Enable Operational
2/1 Enable Operational
2/2 Enable Operational

#show ip igmp interface 2/1

Slot/Port..... 2/1
IGMP Admin Mode..... Enable
Interface Mode..... Enable
IGMP Version..... 2
Query Interval (secs)..... 125
Query Max Response Time (1/10 of a second)..... 100
Robustness..... 2
Startup Query Interval (secs) 1
Startup Query Count..... 2
Last Member Query Interval (1/10 of a second).. 10
Last Member Query Count..... 2

```

- Configure router B and router C in the same way as router A.

## 9.5.2 Example with Layer 2 redundancy (HIPER-Ring)

VLAN 1 is assigned to the HIPER-Ring.

- Assign other VLAN IDs to the connected VLANs and leave the HIPER-Ring exclusively in VLAN 1. You thus enable the transmission of the Multicast data streams on Layer 3.

If you assign multiple VLANs to the HIPER-Ring as transfer networks, then the Switch transmits the Multicast data streams to every transfer network during the flood and prune phase. This means that the Switch transmits the Multicast data streams to every VLAN and the network load is thus multiplied in the HIPER-Ring.

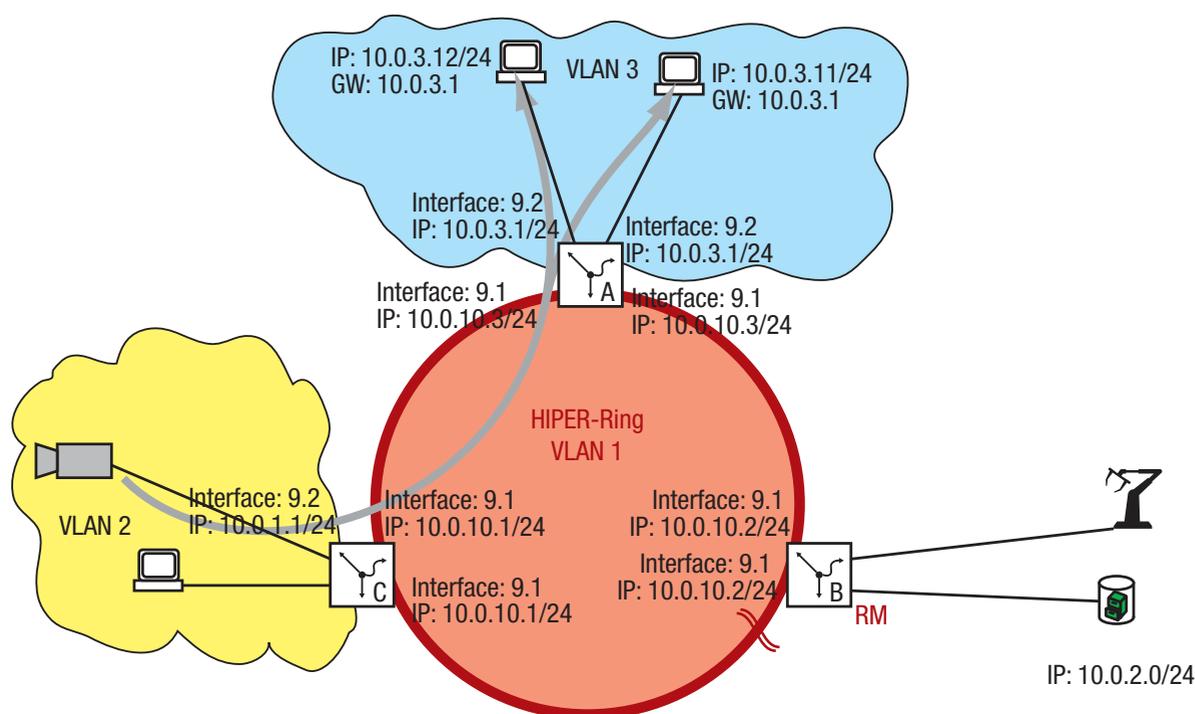


Figure 50: Multicast example configuration with HIPER-Ring

### 9.5.3 Tips for the configuration

#### ■ Selection of the PIM-DM Multicast routing protocol

You select PIM-DM if your application requires fast switching times and is able to tolerate any packet duplications during the switching time. You set fast switching times by reducing the “Hello Time”.

Packet duplications occur when multiple routers are connected to a subnetwork. In this case, the “Assert process” clarifies which router is permitted to send into the subnetwork. Until this is clarified, all routers send into this subnetwork.

#### ■ Selection of the DVMRP Multicast routing protocol

You select DVMRP if your application does not tolerate packet duplications and is content with higher switching times.

DVMRP provides a big advantage when you are using divided subnetworks/VLANs in a HIPER-Ring. With the Unicast table, DVMRP already knows the topology and thus prevents packet duplications.

#### ■ Selection of the PIM-SM Multicast routing protocol

You select PIM-SM if your application has few participants and you can tolerate longer paths for your application.

In this case, PIM-SM has the advantage that the data volume created in the routers remains small.

#### ■ Configuration as Rendezvous Point for PIM-SM

When using PIM-SM, you have the option of defining a router as a rendezvous point candidate for a Multicast group. To do this, you specify the Multicast group for which the router can be used as the rendezvous point.

 enable  
configure

Switch to the Privileged EXEC mode.  
Switch to the configuration mode.

|                                                                           |                                                                               |
|---------------------------------------------------------------------------|-------------------------------------------------------------------------------|
| <pre>ip pimsm rp-candidate interface 1/1 225.1.1.1 255.255.255.0</pre>    | Activate the router as the potential rendezvous point for group 225.1.1.1/24. |
| <pre>no ip pimsm rp-candidate interface 1/1 225.1.1.1 255.255.255.0</pre> | Deactivate the router as a potential rendezvous point.                        |

### ■ Configuration of the limit for the switch to SPT

When using PIM-SM, you have the option of defining the limit for the switch to SPT on the last routers for the Multicast recipients. To do this, you specify the limit for the data throughput in Kbit/s, and when this limit is reached the router switches to the shortest path SPT.

|                                        |                                                              |
|----------------------------------------|--------------------------------------------------------------|
| <pre>enable</pre>                      | Switch to the Privileged EXEC mode.                          |
| <pre>configure</pre>                   | Switch to the configuration mode.                            |
| <pre>ip pimsm spt-threshold 1000</pre> | Activate the limit of 1000 Kbit/s for the switch to the SPT. |
| <pre>no ip pimsm spt-threshold</pre>   | Deactivate the limit for the switch to the SPT.              |

### ■ Configuration as Designated Router for PIM-SM

When using PIM-SM, you have the option of defining a router as the designated router candidate. To do this, you specify the priority with which the router offers itself as the designated router.

|                                                   |                                                                                |
|---------------------------------------------------|--------------------------------------------------------------------------------|
| <pre>enable</pre>                                 | Switch to the Privileged EXEC mode.                                            |
| <pre>configure</pre>                              | Switch to the configuration mode.                                              |
| <pre>ip pimsm dr-priority 2/1 priority 2000</pre> | Activate the router as the potential designated router with the priority 2000. |
| <pre>no ip pimsm dr-priority 2/1</pre>            | Deactivate the router as a potential designated router.                        |

### ■ Configuration as Bootstrap Router for PIM-SM

When using PIM-SM, you have the option of defining a router as the bootstrap router candidate. To do this, you specify the priority with which the router offers itself as the bootstrap router.

|                      |                                     |
|----------------------|-------------------------------------|
| <pre>enable</pre>    | Switch to the Privileged EXEC mode. |
| <pre>configure</pre> | Switch to the configuration mode.   |

|                                                   |                                                                             |
|---------------------------------------------------|-----------------------------------------------------------------------------|
| <pre>ip pimsm bsr-candidate 2/1 priority 20</pre> | Activate the router as the potential bootstrap router with the priority 20. |
| <pre>no ip pimsm bsr-candidate 2/1</pre>          | Deactivate the router as a potential bootstrap router.                      |

### ■ Limiting the PIM-SM domain

When you define an interface of the device as a BSR border, the router does not forward any BSR messages via this interface. In this way, the router limits the PIM-SM domain.

|                                   |                                                              |
|-----------------------------------|--------------------------------------------------------------|
| <pre>enable</pre>                 | Switch to the privileged EXEC mode.                          |
| <pre>configure</pre>              | Switch to the Configuration mode.                            |
| <pre>interface 2/1</pre>          | Switch to the interface configuration mode of interface 2.1. |
| <pre>ip pimsm bsr-border</pre>    | Deactivate the forwarding of BSR messages via interface 2.1. |
| <pre>no ip pimsm bsr-border</pre> | Allow the forwarding of BSR messages via interface 2.1.      |

### ■ Reducing the switching times

With both DVMRP and PIM-DM you can reduce the switching times by reducing the IGMP querier interval on the router interface. This reduction becomes effective when an inactive router to which Multicast recipients are connected becomes active again.

|                                                 |                                                                                                                             |
|-------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------|
| <pre>enable</pre>                               | Switch to the privileged EXEC mode.                                                                                         |
| <pre>configure</pre>                            | Change to the Configuration mode.                                                                                           |
| <pre>interface 2/1</pre>                        | Switch to the Interface Configuration mode of interface 2/1.                                                                |
| <pre>ip igmp   query-max-response-time 10</pre> | Set the Query Max Response Time smaller than the Query Interval<br>In this example: 1 second<br>Default setting: 10 seconds |
| <pre>ip igmp query-interval 5</pre>             | Set Query Interval<br>In this example: 5 seconds<br>Default setting: 125 seconds.                                           |

With PIM-DM, if you reduce the Hello Time, a router can detect more quickly when a downstream router becomes inactive or active again.

```
ip pimdm query-interval 1
```

Set the PIM-DM Query Interval (Hello Time)  
In this example: 1 second  
Default setting: 30 seconds

With PIM-DM, using a default route that has been entered can reduce the switching time. While the router is gathering information about the path to the source (RPF), the router can use a default route that has been entered.

```
ip route 10.0.3.0
 255.255.255.0 10.0.2.2
exit
```

Create the static default route.  
Change to the Configuration mode.

### ■ Special feature of VLAN routing

The router floods a Multicast data stream to all ports of a VLAN routing interface if

- the Multicast data stream comes from another subnetwork and
- at least one recipient on this VLAN interface has registered via IGMP for this Multicast data stream.

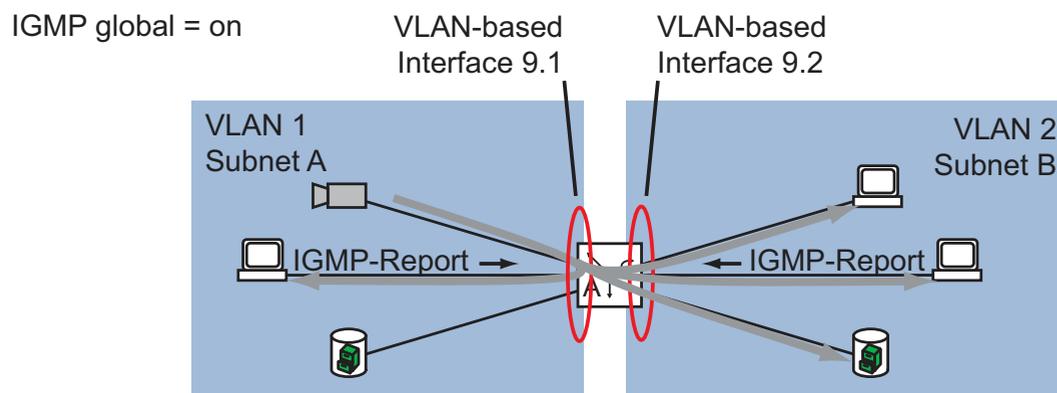


Figure 51: Registered Multicast data stream on the VLAN routing interface

# **A Appendix**

---

## A.1 Abbreviations used

|        |                                               |
|--------|-----------------------------------------------|
| ABR    | Area Border Router                            |
| ACA    | AutoConfiguration Adapter                     |
| AS     | Autonomous System                             |
| ASBR   | Autonomous System Border Router               |
| BC     | Broadcast                                     |
| BDR    | Backup designated Router                      |
| BGP    | Border Gateway Protocol                       |
| BOOTP  | Bootstrap Protocol                            |
| CIDR   | Classless Inter Domain Routing                |
| CLI    | Command Line Interface                        |
| DHCP   | Dynamic Host Configuration Protocol)          |
| DR     | Designated Router                             |
| DVMRP  | Distance Vector Multicast Routing Protocol    |
| EUI    | Extended Unique Identifier                    |
| FDB    | Forwarding Database                           |
| GARP   | General Attribute Registration Protocol       |
| GMRP   | GARP Multicast Registration Protocol          |
| http   | Hypertext Transfer Protocol                   |
| HiVRRP | Hirschmann Virtual Router Redundancy Protocol |
| IANA   | Internet Assigned Numbers Authority           |
| ICMP   | Internet Control Message Protocol             |
| IGMP   | Internet Group Management Protocol            |
| IGP    | Interior Gateway Protocol                     |
| IP     | Internet Protocoll                            |
| LED    | Light Emitting Diode                          |
| LLDP   | Link Layer Discovery Protocol                 |
| LSA    | Link Status Advertisement                     |
| LSD    | Link State Database                           |
| F/O    | Optical Fiber                                 |
| MAC    | Media Access Control                          |
| MC     | Multicast                                     |
| MICE   | Modular Industrial Communication Equipment    |
| NSSA   | Not So Stubby Area                            |
| NTP    | Network Time Protocol                         |
| OSPF   | Open Shortest Path First                      |
| OUI    | Organizationally Unique Identifier            |
| PC     | Personal Computer                             |
| PIM-DM | Protocol Independent Multicast-Dense Mode     |

|        |                                            |
|--------|--------------------------------------------|
| PIM-SM | Protocol Independent Multicast-Sparse Mode |
| PTP    | Precision Time Protocol                    |
| RFC    | Request For Comment                        |
| RM     | Redundancy Manager                         |
| RS     | Rail Switch                                |
| RSTP   | Rapid Spanning Tree Protocol               |
| RIP    | Routing Information Protocol               |
| RPF    | Reverse Path Forwarding                    |
| SFP    | Small Form-factor Pluggable                |
| SNMP   | Simple Network Management Protocol         |
| SNTP   | Simple Network Time Protocol               |
| SPT    | Shortest Path Tree                         |
| TCP    | Transfer Control Protocol                  |
| tftp   | Trivial File Transfer Protocol             |
| TP     | Twisted Pair                               |
| TTL    | Time-to-live                               |
| UDP    | User Datagram Protocol                     |
| URL    | Uniform Resource Locator                   |
| UTC    | Coordinated Universal Time                 |
| VL     | Virtual Link                               |
| VLAN   | Virtual Local Area Network                 |
| VLSM   | Variable Length Subnet Mask                |
| VRID   | Virtual Router Identification              |
| VRRP   | Virtual Router Redundancy Protocol         |

## A.2 Underlying IEEE Standards

- ▶ IEEE 802.1AB  
Topology Discovery (LLDP)
- ▶ IEEE 802.1D  
Switching, GARP, GMRP, Spanning Tree (Supported via 802.1S implementation)
- ▶ IEEE 802.1D-1998  
Media Access Control (MAC) Bridges (includes IEEE 802.1p Priority and Dynamic Multicast Filtering, GARP, GMRP)
- ▶ IEEE 802.1Q-1998  
Virtual Bridged Local Area Networks (VLAN Tagging, Port Based VLANs, GVRP)
- ▶ IEEE 802.1S  
Multiple Spanning Tree
- ▶ IEEE 802.1v  
Protocol Based VLANs
- ▶ IEEE 802.1 w.2001  
Rapid Reconfiguration, Supported via 802.1S implementation
- ▶ IEEE 802.1 X  
Port Authentication
- ▶ IEEE 802.3 - 2002  
Ethernet
- ▶ IEEE 802.3 ac  
VLAN Tagging
- ▶ IEEE 802.3 ad  
Link Aggregation with Static LAG and LACP support
- ▶ IEEE 802.3 x  
Flow Control

---

## A.3 List of RFCs

- ▶ RFC 768 (UDP)
- ▶ RFC 783 (TFTP)
- ▶ RFC 791 (IP)
- ▶ RFC 792 (ICMP)
- ▶ RFC 793 (TCP)
- ▶ RFC 826 (ARP)
- ▶ RFC 854 (Telnet)
- ▶ RFC 855 (Telnet Option)
- ▶ RFC 951 (BOOTP)
- ▶ RFC 1112 (Host Extensions for IP Multicasting)
- ▶ RFC 1155 (SMIPv1)
- ▶ RFC 1157 (SNMPv1)
- ▶ RFC 1212 (Concise MIB Definitions)
- ▶ RFC 1213 (MIB2)
- ▶ RFC 1493 (Dot1d)
- ▶ RFC 1542 (BOOTP-Extensions)
- ▶ RFC 1643 (Ethernet-like -MIB)
- ▶ RFC 1757 (RMON)
- ▶ RFC 1867 (HTML/2.0 Forms w/ file upload extensions)
- ▶ RFC 1901 (Community based SNMP v2)
- ▶ RFC 1905 (Protocol Operations for SNMP v2)
- ▶ RFC 1906 (Transport Mappings for SNMP v2)
- ▶ RFC 1907 (Management Information Base for SNMP v2)
- ▶ RFC 1908 (Coexistence between SNMP v1 and SNMP v2)
- ▶ RFC 1945 (HTTP/1.0)
- ▶ RFC 2068 (HTTP/1.1 protocol as updated by draft-ietf-http-v11-spec-rev-03)
- ▶ RFC 2131 (DHCP)
- ▶ RFC 2132 (DHCP-Options)
- ▶ RFC 2233 The Interfaces Group MIB using SMI v2
- ▶ RFC 2236 (IGMPv2)
- ▶ RFC 2246 (The TLS Protocol, Version 1.0)
- ▶ RFC 2271 (SNMP Framework MIB)
- ▶ RFC 2346 (AES Ciphersuites for Transport Layer Security)
- ▶ RFC 2362 (PIM-SM)
- ▶ RFC 2365 (Administratively Scoped Boundaries)
- ▶ RFC 2570 (Introduction to SNMP v3)
- ▶ RFC 2571 (Architecture for Describing SNMP Management Frameworks)

- ▶ RFC 2572 (Message Processing and Dispatching for SNMP)
- ▶ RFC 2573 (SNMP v3 Applications)
- ▶ RFC 2574 (User Based Security Model for SNMP v3)
- ▶ RFC 2575 (View Based Access Control Model for SNMP)
- ▶ RFC 2576 (Coexistence between SNMP v1,v2 & v3)
- ▶ RFC 2578 (SMI v2)
- ▶ RFC 2579 (Textual Conventions for SMI v2)
- ▶ RFC 2580 (Conformance statements for SMI v2)
- ▶ RFC 2613 (SMON)
- ▶ RFC 2618 (RADIUS Authentication Client MIB)
- ▶ RFC 2620 (RADIUS Accounting MIB)
- ▶ RFC 2674 (Dot1p/Q)
- ▶ RFC 2818 (HTTP over TLS)
- ▶ RFC 2851 (Internet Addresses MIB)
- ▶ RFC 2865 (RADIUS Client)
- ▶ RFC 2866 (RADIUS Accounting)
- ▶ RFC 2868 (RADIUS Attributes for Tunnel Protocol Support)
- ▶ RFC 2869 (RADIUS Extensions)
- ▶ RFC 2869bis (RADIUS support for EAP)
- ▶ RFC 2933 (IGMP MIB)
- ▶ RFC 3164 (The BSD Syslog Protocol)
- ▶ RFC 3376 (IGMPv3)
- ▶ RFC 3580 (802.1X RADIUS Usage Guidelines)
- ▶ RFC 4330 (SNTP, obsoletes RFCs 1769 and 2330)

## ■ Routing

- ▶ RFC 826 Ethernet ARP
- ▶ RFC 894 Transmission of IP Datagrams over Ethernet Networks
- ▶ RFC 896 Congestion Control in IP/TCP Networks
- ▶ RFC 919 IP Broadcast
- ▶ RFC 922 IP Broadcast in the presence of subnets
- ▶ RFC 950 IP Subnetting
- ▶ RFC 1027 Using ARP to implement Transparent Subnet Gateways (Proxy ARP)
- ▶ RFC 1256 ICMP Router Discovery Messages
- ▶ RFC 1321 Message Digest Algorithm
- ▶ RFC 1519 CIDR
- ▶ RFC 1724 RIP v2 MIB Extension
- ▶ RFC 1765 OSPF Database Overflow
- ▶ RFC 1812 Requirements for IP Version 4 Routers

- 
- ▶ RFC 1850 OSPF MIB Draft-ietf-ipv6-rfc2096-update-07.txt  
IP Forwarding Table MIB
  - ▶ RFC 2082 RIP-2 MD5 Authentication
  - ▶ RFC 2131 DHCP Relay
  - ▶ RFC 2328 OSPF Version 2
  - ▶ RFC 2453 RIP v2
  - ▶ RFC 2787 VRRP MIB
  - ▶ RFC 2863 The Interfaces Group MIB
  - ▶ RFC 2932 IPv4 Multicast Routing MIB
  - ▶ RFC 2934 PIM MIB for IPv4
  - ▶ RFC 3046 DHCP/BootP Relay
  - ▶ RFC 3101 The OSPF "Not So Stubby Area" (NSSA) Option
  - ▶ RFC 3376 IGMPV3
  - ▶ RFC 3768 VRRP, Virtual Router Redundancy Protocol
  - ▶ Draft-holbrook-idmr-igmpv3-ssm-08.txt – IGMPv3 / MLDv2 for SSM
  - ▶ Draft-ietf-idmr-dvmrp-mib-11.txt – DVMRP MIB
  - ▶ Draft-ietf-idmr-dvmrp-v3-10 – DVMRP
  - ▶ Draft-ietf-magma-igmpv3-and-routing-05.txt – IGMPv3 an Multicast Routing Protocol Interaction
  - ▶ Draft-ietf-magma-mgmd-mib-03.txt – Multicast Group Membership Discovery MIB
  - ▶ Draft-ietf-pim-v2-dm-03 – PIM-DM
  - ▶ Draft-ietf-smm-arch-06.txt – Source -Specific Multicast for IP

## A.4 Entering the IP Parameters

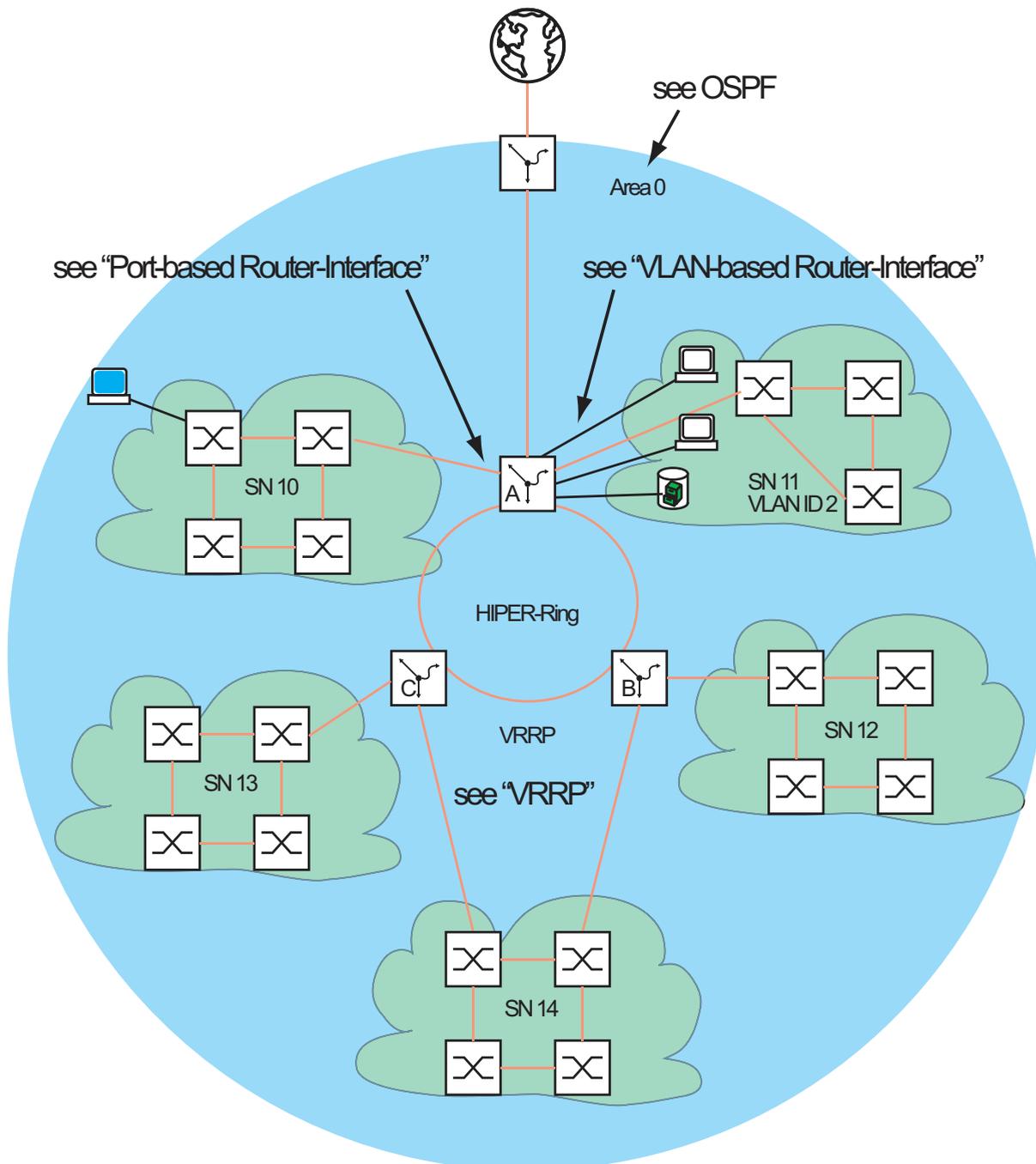


Figure 52: Network plan

To configure the layer 3 function, you require access to the management of the Switch, as described in the “Basic Configuration” user manual. Depending on your own application, you will find many options for assigning IP addresses to the devices. The following example describes one option that often arises in practice. Even if you have other prerequisites, this example shows the general method for entering the IP parameters and points out important things that you should note.

The prerequisites for the following example are:

- ▶ All layer 2 and layer 3 switches have the IP address 0.0.0.0 (= state on delivery)
- ▶ The IP addresses of the switches and router interfaces and the gateway IP addresses are defined in the network plan.
- ▶ The devices and their connections are installed.
- ▶ Redundant connections are open (see VRRP and HIPER-Ring). To avoid loops in the configuration phase, close the redundant connections only after the configuration phase.

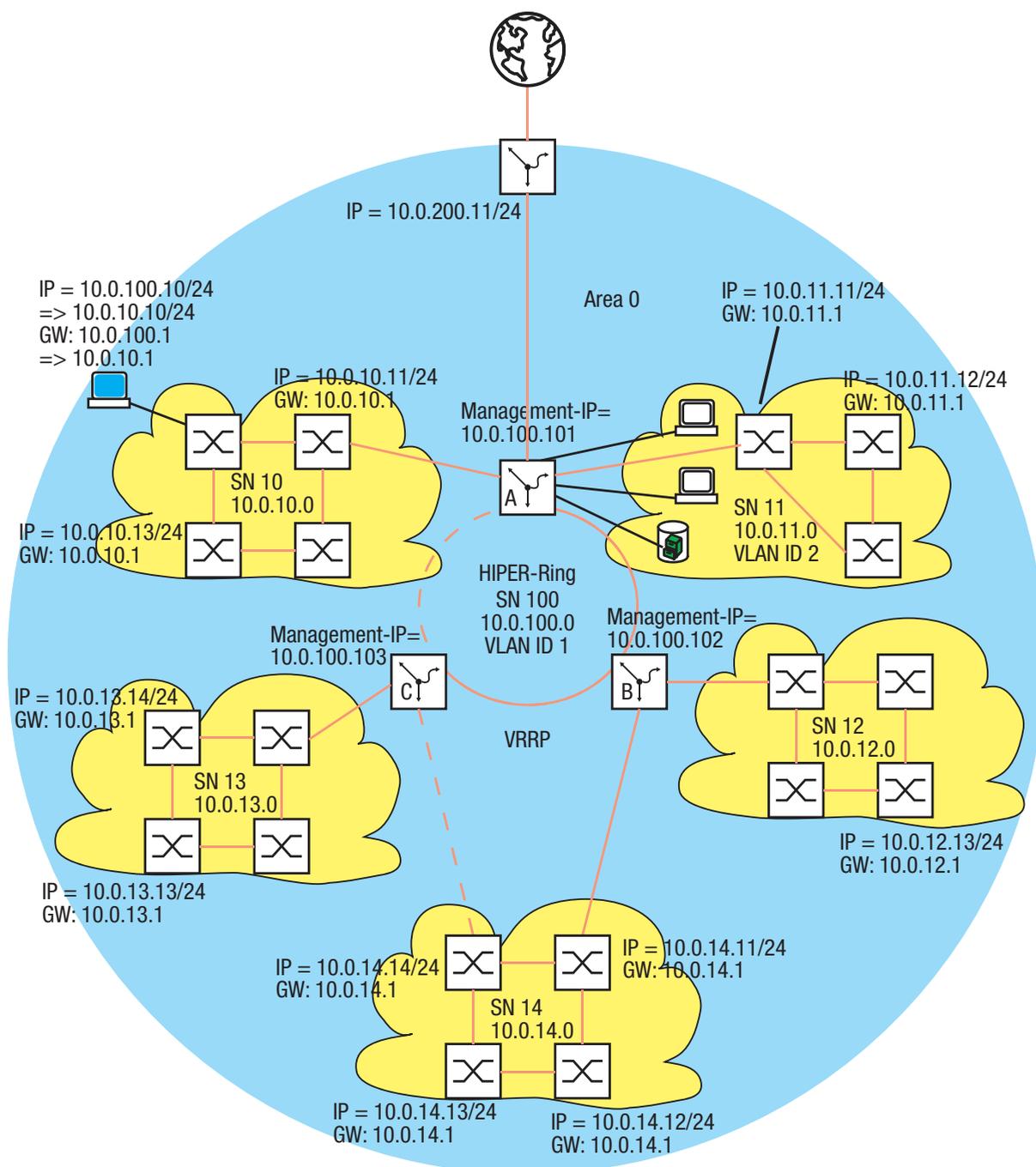


Figure 53: Network plan with management IP addresses

- Assign the IP parameters to your configuration computer. During the configuration phase, the configuration computer is located in subnet 100. This is necessary, so that the configuration computer has access to the layer 3 switches throughout the entire configuration phase.
- Start HiDiscovery on your configuration computer.

- Give all the layer 2 and layer 3 switches their IP parameters in accordance with the network plan.

You can access the devices in subnets 10 to 14 again when you have completed the following router configuration.

- Configure the router function for the layer 3 switches.

Note the sequence:

1. Layer 3 switch C
2. Layer 3 switch B

The sequence is important; you thus retain access to the devices.

As soon as you assign an IP address from the subnet of the management IP address (= SN 100) to a router interface, the Switch deletes the management IP address. You access the Switch via the IP address of the router interface.

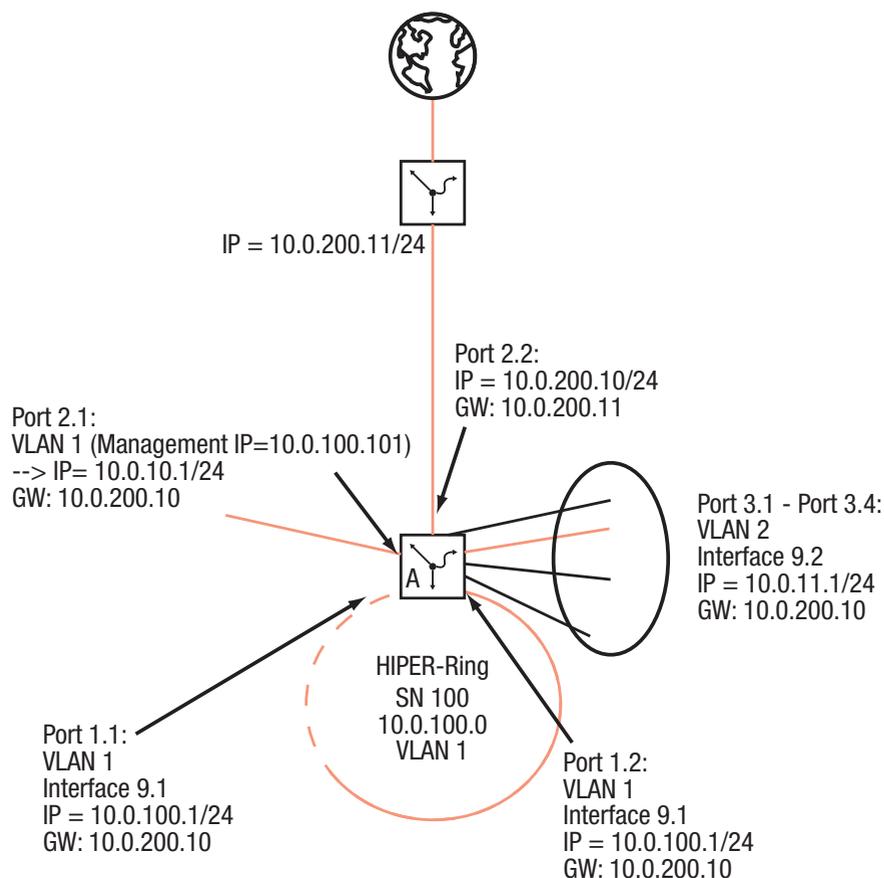


Figure 54: IP parameters for layer 3 switch A

- Configure the router function for layer 3 switch A.  
You first configure the router interface at a port to which the configuration computer is connected. The result of this is that in future you will access the layer 3 switch via subnet 10.
- Change the IP parameters of your configuration computer to the values for subnet 10. You thus access layer 3 switch A again, namely via the IP address of the router interface set up beforehand.
- Finish the router configuration for layer 3 switch A (see figure 54).

After the configuration of the router function on all layer 3 switches, you have access to all the devices.

## **A.5 Copyright of Integrated Software**

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

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

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

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

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

## **A.5.2 Broadcom Corporation**

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

## B 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>H</b>                           |                        |
| ABR                                        | 94, 99     | Hello packets                      | 102                    |
| Address Resolution Protocol                | 18         | HIPER-Ring                         | 147                    |
| Adjacency                                  | 102        | HiRRRP                             | 62                     |
| Advertisement                              | 60         | Hop count                          | 81, 86                 |
| Advertisement interval                     | 60         |                                    |                        |
| Aging time                                 | 125        | <b>I</b>                           |                        |
| ARP                                        | 18, 20, 42 | IANA                               | 122                    |
| ARP data packet                            | 113        | IGMP                               | 125                    |
| Area Border Router                         | 94, 99     | IGMP Querier Interval              | 149                    |
| ASBR                                       | 94, 99     | Implicit Join                      | 127                    |
| Assert process                             | 147        | Importance                         | 35, 37, 38             |
| Autonomous System Area Border Router       | 99         | Industrial HiVision                | 10                     |
| Autonomous System Boundary Router          | 94         | Industry Protocols                 | 9                      |
|                                            |            | Infinity                           | 86                     |
| <b>B</b>                                   |            | Interface tracking                 | 45, 46, 51, 53, 53, 75 |
| Backup Designated Router                   | 102        | Interface tracking object          | 46                     |
| Backup designated router                   | 105        | Interner Router                    | 99                     |
| Backup router                              | 60, 60     | Internet Group Management Protocol | 125                    |
| BDR                                        | 102        | IP                                 | 16                     |
| Boundary                                   | 141        | IP address                         | 58                     |
| Broadcast                                  | 16         | IP address owner                   | 59, 60, 60             |
|                                            |            | IP data packet                     | 113                    |
| <b>C</b>                                   |            | IP stack                           | 42                     |
| CIDR                                       | 21, 91     | ISO/OSI layer model                | 15                     |
| Classless Inter-Domain Routing             | 21, 91     |                                    |                        |
| Convergence                                | 82         | <b>L</b>                           |                        |
| Count-to-infinity                          | 86         | Leave message                      | 125                    |
|                                            |            | Link aggregation interface         | 46                     |
| <b>D</b>                                   |            | Link down delay                    | 47                     |
| Default gateway                            | 58, 59     | Link State Advertisement           | 99                     |
| Designated Router                          | 102        | Link State Database                | 105                    |
| Designated router                          | 105        | Link up delay                      | 47                     |
| Distance                                   | 35, 37     | Link-down notification             | 65, 65                 |
| Distance Vector Multicast Routing Protocol | 127        | Load sharing                       | 37                     |
|                                            |            | Logical tracking                   | 50, 54                 |
| Distance vector algorithm                  | 81         | Logic tracking                     | 45                     |
| DR                                         | 102        | LSA                                | 99, 105                |
| DVMRP                                      | 127        | LSD                                | 105                    |
|                                            |            |                                    |                        |
| <b>E</b>                                   |            | <b>M</b>                           |                        |
| Extended Unique Identifier                 | 123        | MAC address                        | 16, 58                 |
|                                            |            | MAC/IP address resolution          | 42                     |
| <b>F</b>                                   |            | Master router                      | 60, 60, 60             |
| FAQ                                        | 171        | Metric                             | 81                     |
| Flooding                                   | 129        | Multicast                          | 16                     |
|                                            |            | Multicast address                  | 102, 120               |
| <b>G</b>                                   |            | Multinetting                       | 24                     |
| Grafting                                   | 131        |                                    |                        |

|                                       |            |                              |                |
|---------------------------------------|------------|------------------------------|----------------|
| <b>N</b>                              |            |                              |                |
| Neighbor relationship                 | 102        | Router priority              | 102            |
| Netdirected Broadcasts                | 23         | Route Summarization          | 94             |
| Netdirected Broadcasts (Port-basiert) | 27         | Route tracking               | 38             |
| Netdirected Broadcasts (VLAN-basiert) | 30         | Routingabelle                | 127            |
| Network plan                          | 13         | Routing Information Protocol | 81             |
| Next hop                              | 81         | Routing table                | 28, 29, 38, 81 |
| Not So Stubby Area                    | 95         | Routing tables               | 65             |
| NSSA                                  | 95         | RPF                          | 130            |
| <b>O</b>                              |            | <b>S</b>                     |                |
| Open Shortest Path First              | 91         | Scoping                      | 141            |
| Operand                               | 55         | Shortest Path First          | 107            |
| Operators                             | 50         | Shortest Path Tree           | 130            |
| Organizationally Unique Identifier    | 123        | Skew time                    | 60             |
| OSI layer model                       | 15         | Source filtering             | 126, 126       |
| OSI reference model                   | 15         | Source-routed                | 130            |
| OSPF                                  | 14, 82, 91 | SPF                          | 107            |
| OUI                                   | 123        | SPT                          | 130            |
| <b>P</b>                              |            | Split horizon                | 86             |
| Packet duplications                   | 147        | Static routes                | 14             |
| PIM-DM                                | 127        | Static route tracking        | 38             |
| PIM-SM                                | 127        | Static routing               | 45             |
| Ping interval                         | 48         | Stub Area                    | 95             |
| Ping request                          | 48         | Switching times              | 147            |
| Ping response                         | 48         | Symbol                       | 11             |
| Ping timeout                          | 48         | <b>T</b>                     |                |
| Ping tracking                         | 38, 45, 48 | Technical Questions          | 171            |
| Port-based router Interface           | 26         | Time to Live.                | 141            |
| PROFINET IO                           | 9          | Totally Stubby Area          | 95             |
| Preempt delay                         | 65         | Tracking                     | 38, 45         |
| Preempt mode                          | 65         | Tracking (VRRP)              | 45             |
| Preference                            | 73         | Training Courses             | 171            |
| Protocol-based VLAN                   | 113        | TTL                          | 141            |
| Proxy ARP                             | 20         | <b>U</b>                     |                |
| Prune messages                        | 130        | Upstream                     | 130            |
| port-based router interface           | 43         | <b>V</b>                     |                |
| <b>Q</b>                              |            | Variable Length Subnet Mask  | 91             |
| Querier Election                      | 125        | Virtual MAC address          | 58             |
| <b>R</b>                              |            | Virtual router               | 59             |
| Redistribute                          | 95         | Virtual router ID            | 58             |
| Redistributing                        | 95         | Virtual router IP address    | 60             |
| Redistribution                        | 94         | Virtual router interface     | 115            |
| Redundancy                            | 9          | Virtual router MAC address   | 60             |
| Redundant static route                | 35         | VL                           | 97             |
| Report message                        | 125        | VLAN protocol group          | 115            |
| Reverse Path Forwarding               | 130        | VLAN router interface        | 46             |
| RFC                                   | 155        | VLAN routing                 | 115            |
| RIP                                   | 14, 81     | VLAN-based router interface  | 43             |
| Router                                | 9          | VLSM                         | 91             |
| Router ID                             | 102        | VRID                         | 58, 60         |
|                                       |            | VRRP                         | 45             |

## Index

---

|               |            |
|---------------|------------|
| VRRP priority | 59, 60, 60 |
| VRRP router   | 59         |
| VRRP Tracking | 45         |
| virtual link  | 97         |



## 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