HIRSCHMANN

A BELDEN BRAND

Reference Manual

GUI Graphical User Interface
Industrial ETHERNET (Gigabit-)Switch
RS20/RS30/RS40, MS20/MS30, OCTOPUS, PowerMICE, RSR20/RSR30, MACH 100, MACH 1000, MACH 4000

RM GUI L2P
Release 8.0 05/2013

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

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

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

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

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

Rel. 8.0 - 05/2013 – 30.04.2013

Contents

About this Manual

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

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

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

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

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

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

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

- 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.

Maintenance

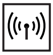
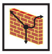
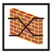
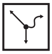
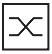
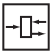
Hirschmann is continually working to improve and develop our software. You should regularly check whether there is a new version of the software that provides you with additional benefits. You will find software information and downloads on the product pages of the Hirschmann website.

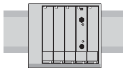
Key

The designations used in this manual have the following meanings:

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

Symbols used:

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

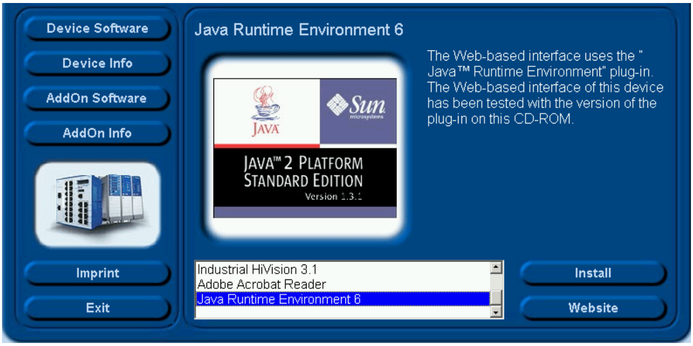
	Hub
	A random computer
	Configuration Computer
	Server
	PLC - Programmable logic controller
	I/O - Robot

Opening the Graphical User Interface

To open the graphical user interface, you need a Web browser, for example Mozilla Firefox version 3.5 or later, or Microsoft Internet Explorer version 6 or later.

Note: The graphical user interface uses Java 6 or Java 7.

Install the software from the enclosed CD-ROM. To do this, you go to “Additional Software”, select `Java Runtime Environment` and click on “Installation”.

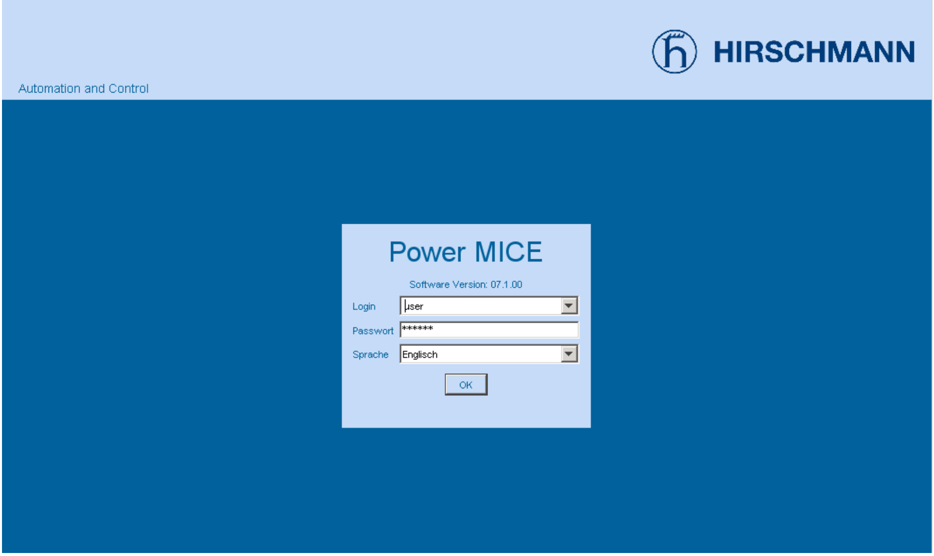


The Web-based interface uses the " Java™ Runtime Environment" plug-in. The Web-based interface of this device has been tested with the version of the plug-in on this CD-ROM.

Figure 1: Installing Java

□ Start your Web browser.
□ Activate Java in the security settings of your Web browser.
□ Establish the connection by entering the IP address of the device which you want to administer via the Web-based management in the address field of the Web browser. Enter the address in the following form:
`http://xxx.xxx.xxx.xxx`

The login window appears on the screen.



Power MICE

Software Version: 07.1.00

Login: user

Passwort: ******

Sprache: Englisch

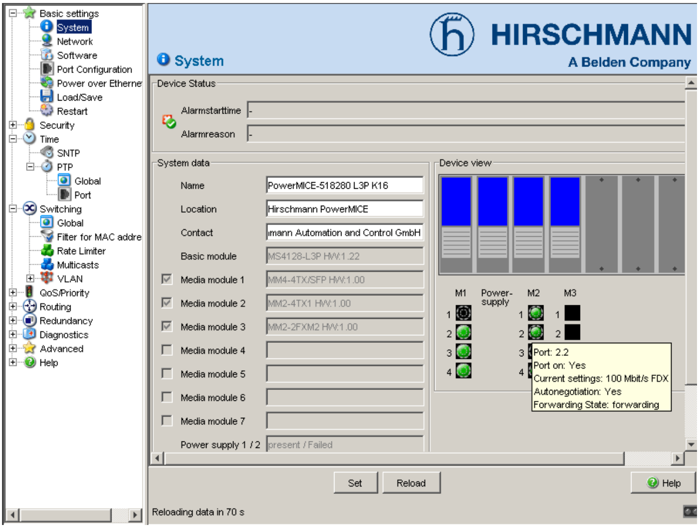
Figure 2: Login window

□ Click on OK.

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

Note: The changes you make in the dialogs will be copied to the volatile memory of the device (RAM) when you click “Set”. Click “Reload” to update the display.
To save any changes made so that they will be retained after a power cycle or reboot of the device use the save option on the "Load/Save" dialog (see on page 48 “Load/Save”).

Note: If you enter an incorrect configuration, you may block access to your device.
Activating the function “Cancel configuration change” in the “Load/Save” dialog enables you to return automatically to the last configuration after a set time period has elapsed. This gives you back your access to the device.



Alarmstarttime -

Alarmreason -

Name PowerMICE-518280 L3P K16

Location Hirschmann PowerMICE

Contact ımann Automation and Control GmbH

Basic module MS4128-L3P HW:1.22

☑ Media module 1 MM4-4TX/SFP HW:1.00

☑ Media module 2 MM2-4TX1 HW:1.00

☑ Media module 3 MM2-2FXM2 HW:1.00

□ Media module 4

□ Media module 5

□ Media module 6

□ Media module 7

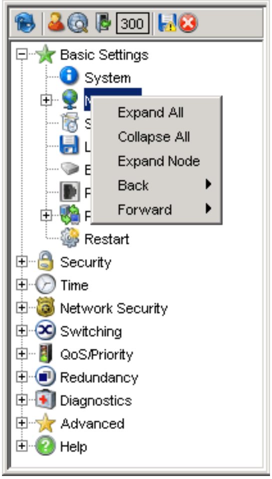
Power supply 1 / 2 present / Failed

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

Reloading data in 70 s

Figure 3: User interface (Web-based Interface) of the device with speech-bubble help

The menu section displays the menu items. By placing the mouse pointer in the menu section and clicking the alternate mouse button you can use “Back” to return to a menu item you have already selected, or “Forward” to jump to a menu item you have already selected.



1 Basic Settings

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

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

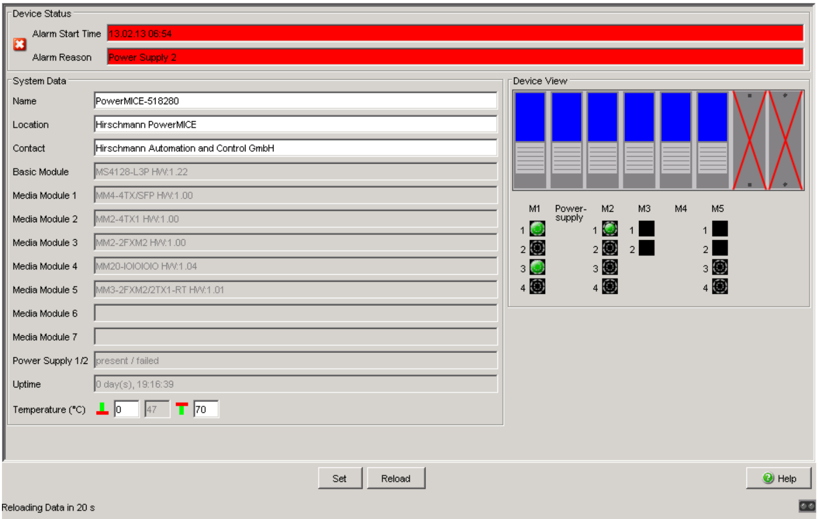
Note: The graphical user interface uses Java 6 or Java 7.

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



Device Status

Alarm Start Time: 13.02.13 06:54

Alarm Reason: Power Supply 2

System Data

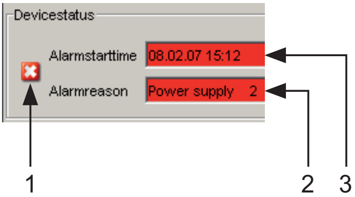
Name	PowerMICE-518280
Location	Hirschmann PowerMICE
Contact	Hirschmann Automation and Control GmbH
Basic Module	MS4128-L3P HW:1.22
Media Module 1	MM4-4TX/SFP HW:1.00
Media Module 2	MM2-4TX1 HW:1.00
Media Module 3	MM2-2FXM2 HW:1.00
Media Module 4	MM20-IOIOIOIO HW:1.04
Media Module 5	MM3-2FXM2/2TX1-RT HW:1.01
Media Module 6	
Media Module 7	
Power Supply 1/2	present / failed
Uptime	0 day(s), 19:16:39
Temperature (°C)	0 47 70

Reloading Data in 20 s

Figure 4: "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.



Devicestatus

Alarmstarttime 08.02.07 15:12

Alarmreason Power supply 2

Figure 5: 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
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
Fan	Status of fans

Table 1: System Data

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

Table 1: System Data

Device View

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

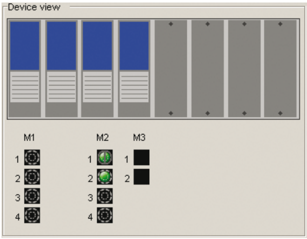


Figure 6: Device View

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.

Reloading data in 70 s

Figure 7: 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 `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 2: 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.

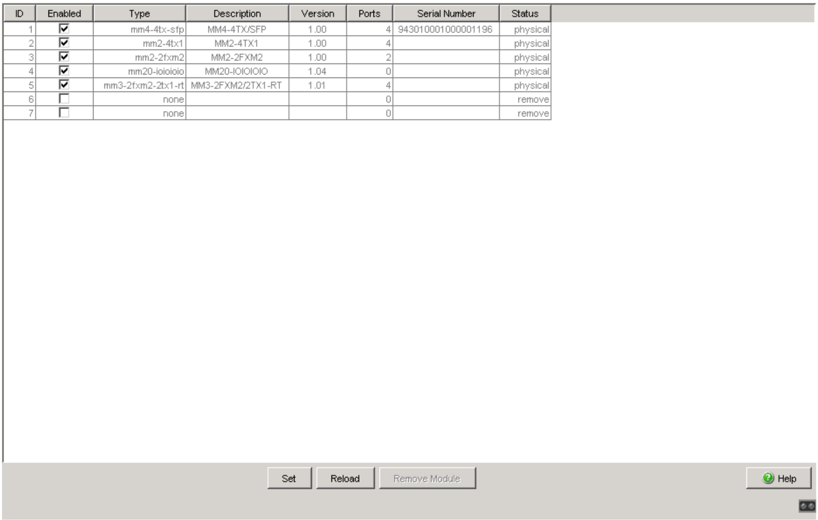
Use the following work steps when deinstalling a module helps deny network access using an empty slot.

☐ 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.

Note: The following modular devices support this function: MS (soho), PowerMICE (ms4128), MACH102 (soho) and MACH4000 (ex and dx) family.



ID	Enabled	Type	Description	Version	Ports	Serial Number	Status
1	☑	mm4-4tx-sfp	MM4-4TX/SFP	1.00	4	943010001000001196	physical
2	☑	mm2-4tx1	MM2-4TX1	1.00	4		physical
3	☑	mm2-2fxm2	MM2-2FXM2	1.00	2		physical
4	☑	mm20-ioioioio	MM20-IOIOIOIO	1.04	0		physical
5	☑	mm3-2fxm2-2tx1-rt	MM3-2FXM2/2TX1-RT	1.01	4		physical
6	□	none			0		remove
7	□	none			0		remove

Figure 8: "Modules" Dialog

This configuration table allows you to enable or disable the slots and also displays the module parameters.

- The "ID" column identifies the slot to which the entry refers.
- The "Enabled" column activates network access to modules installed in this slot. When disabled, the device places a red „X“ over the slot in the "Device View" frame of the `Basic Settings:System` dialog. When disabled, the device recognizes the module installed in this slot and the module is configurable.
- The "Type" column lists the type of module installed in the slot. A value of `none` indicates that the slot is empty.
- The "Description" column gives a short description of the installed module.
- The "Version" column lists the module version.
- The "Ports" column lists how many ports are available on the module.

- 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.

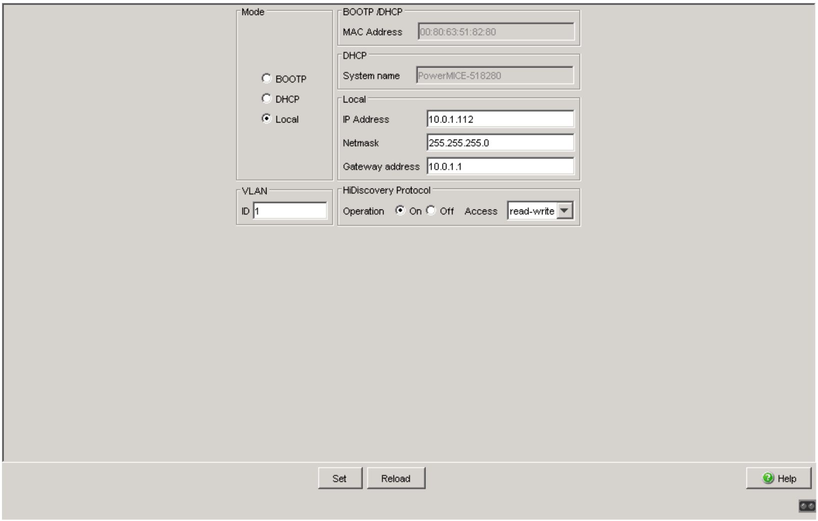
Buttons

Button	Meaning
Set	Transfers the changes to the volatile memory (`RAM`) of the device. To permanently save the changes, open the `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.
Remove Module	Removes the module configuration from the device when the slot is empty.
Help	Opens the online help.

Table 3: 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.



Mode
○ BOOTP
○ DHCP
● Local

BOOTP /DHCP
MAC Address: 00:80:63:51:82:80

DHCP
System name: PowerMICE-518280

Local
IP Address: 10.0.1.112
Netmask: 255.255.255.0
Gateway address: 10.0.1.1

VLAN
ID: 1

HiDiscovery Protocol
Operation: ● On ○ Off Access: read-write

Figure 9: Network parameters dialog

□ Under “Mode”, you enter where the device gets its IP parameters:

- ▶ In the BOOTP mode, the configuration is via a BOOTP or DHCP server on the basis of the MAC address of the device (see on page 48 “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 48 “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 on the basis of its MAC address. Activate the HiDiscovery protocol if you want to allocate an IP address to the device from your PC with the enclosed HiDiscovery software (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

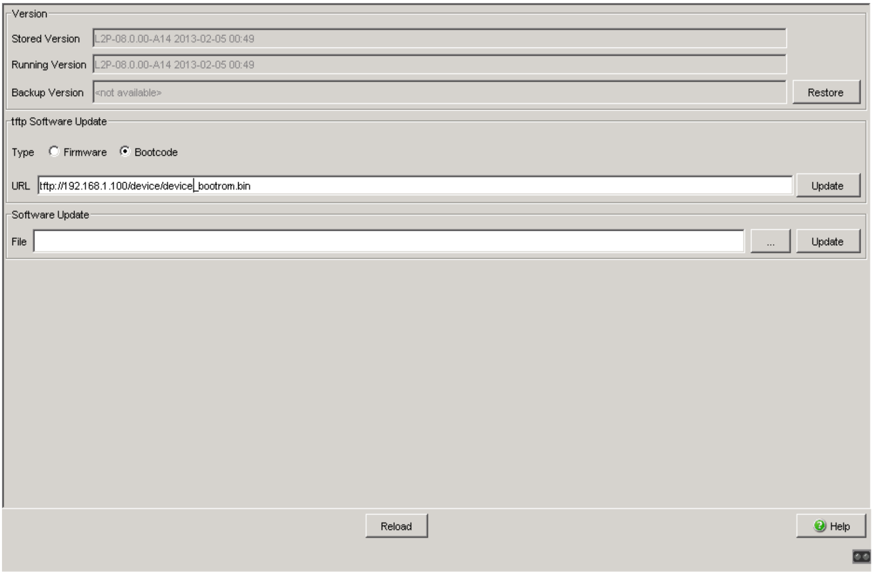
Button	Meaning
Set	Transfers the changes to the volatile memory (`RAM`) of the device. To permanently save the changes, open the `Basic Settings:Load/Save` dialog, select the location to save the configuration, and click "Save".
Reload	Updates the fields with the values that are saved in the volatile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

Table 4: 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.



Version

Stored Version: L2P-08.0.00-A14 2013-02-05 00:49

Running Version: L2P-08.0.00-A14 2013-02-05 00:49

Backup Version: <not available>

tftp Software Update

Type ○ Firmware ● Bootcode

URL: tftp://192.168.1.100/device/device_bootrom.bin

Software Update

File:

Figure 10: 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 63.

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 63.

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 5: 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 148 “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 210 “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 6: 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 `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 7: 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.

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

Nominal power for MS20/30, MACH 1000 and PowerMICE:
The device provides the nominal power for the sum of all PoE ports plus a surplus. Because the PoE media module gets its PoE voltage externally, the device does not know the possible nominal power.
The device therefore assumes a “nominal power” of 60 Watt per PoE media module for now.

Nominal power for OCTOPUS 8M-PoE and OCTOPUS 24M-8PoE:
The device provides the nominal power for the sum of all PoE ports plus a surplus. Because the device gets its PoE voltage externally, the device does not know the possible nominal power.
The device therefore assumes a “nominal power” of 15 Watt per PoE port for now.

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.

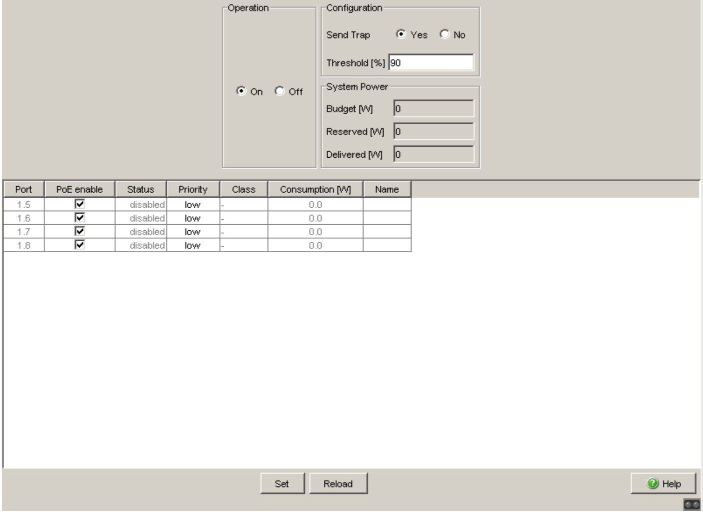
Port Table:

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
● On ○ Off

Configuration
Send Trap ● Yes ○ No
Threshold [%] 90

System Power
Budget [W] 0
Reserved [W] 0
Delivered [W] 0

Port	PoE enable	Status	Priority	Class	Consumption [W]	Name
1.5	☑	disabled	low	-	0.0	
1.6	☑	disabled	low	-	0.0	
1.7	☑	disabled	low	-	0.0	
1.8	☑	disabled	low	-	0.0	

Figure 11: 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 `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 8: 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 9: PoE+ Global - Operation

Frame "Configuration":

Parameter	Meaning	Value Range	Default Setting
Send Trap	Causes the device to send a trap in the following cases: ▶ If a value exceeds/falls below the performance threshold. ▶ If the PoE+ supply voltage is switched on/off at at least one port.	`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 10: 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`	-

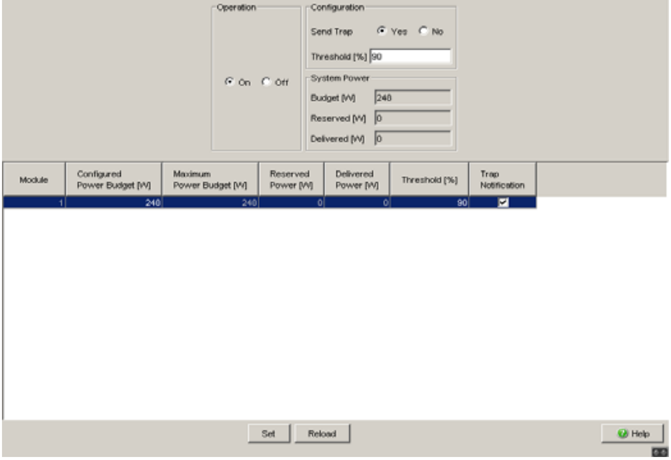
Table 11: PoE+ Global - System Power

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	▶ 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%`l
Trap notification	Causes 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.	`On, Off`	`On`

Table 12: Power over Ethernet Plus - Global



Operation

● On ○ Off

Configuration

Send Trap ● Yes ○ No

Threshold [%] 90

System Power

Budget [W] 240

Reserved [W] 0

Delivered [W] 0

Module	Configured Power Budget [W]	Maximum Power Budget [W]	Reserved Power [W]	Delivered Power [W]	Threshold [%]	Trap Notification
1	240	240	0	0	90	☑

Figure 12: 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

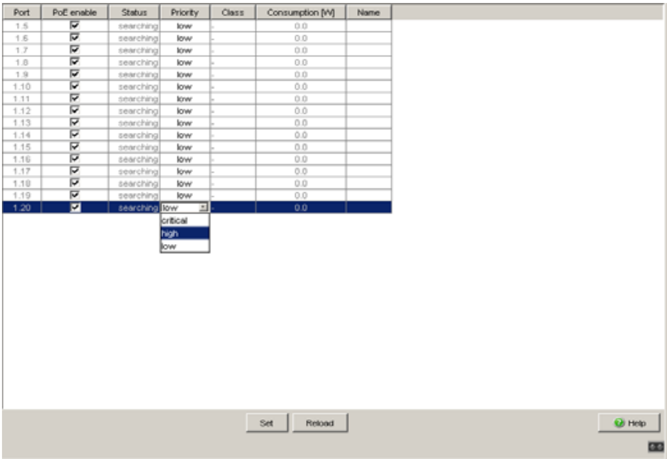
The table only shows ports that support PoE+.

Parameter	Meaning	Value Range	Default Setting
Port	Module and port numbers of the PoE+ ports to which this entry applies. For the MACH104-16TX-PoEP device the ports support 1.5 to 1.20 PoE+.	`1.5 - 1.20`	-
PoE enable	Switching Power over Ethernet Plus operation on/off for this port.	`On, Off`	`On`

Table 13: Power over Ethernet Plus - Port

Parameter	Meaning	Value Range	Default Setting
Status	Displays the port's PoE+ status.	`searching, ...`	`searching, ...`
Priority	Specify the port's PoE+ priority.	`low, high, critical`	`low`
Class	Displays the class of the device connected: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`	-
Name	Displays the name of the port, see `Basic settings:Port configuration`	-	-

Table 13: Power over Ethernet Plus - Port



Port	PoE enable	Status	Priority	Class	Consumption [W]	Name
1.5	☑	searching	low	-	0.0	
1.6	☑	searching	low	-	0.0	
1.7	☑	searching	low	-	0.0	
1.8	☑	searching	low	-	0.0	
1.9	☑	searching	low	-	0.0	
1.10	☑	searching	low	-	0.0	
1.11	☑	searching	low	-	0.0	
1.12	☑	searching	low	-	0.0	
1.13	☑	searching	low	-	0.0	
1.14	☑	searching	low	-	0.0	
1.15	☑	searching	low	-	0.0	
1.16	☑	searching	low	-	0.0	
1.17	☑	searching	low	-	0.0	
1.18	☑	searching	low	-	0.0	
1.19	☑	searching	low	-	0.0	
1.20	☑	searching	low	-	0.0	

Figure 13: Power over Ethernet Plus Dialog:Port

Buttons

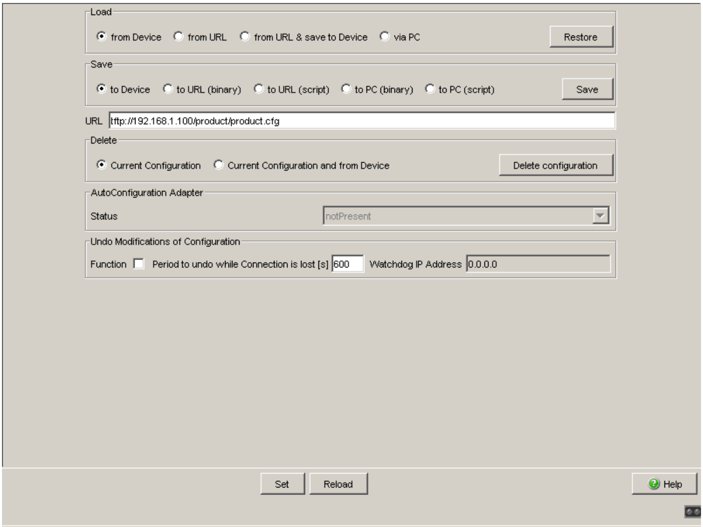
Button	Meaning
Set	Transfers the changes to the volatile memory (`RAM`) of the device. To permanently save the changes, open the `Basic Settings:Load/Save` dialog, select the location to save the configuration, and click "Save".
Reload	Updates the fields with the values that are saved in the volatile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

Table 14: 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.



Load

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

Save

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

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

Delete

● Current Configuration ○ Current Configuration and from Device

AutoConfiguration Adapter

Status notPresent

Undo Modifications of Configuration

Function □ Period to undo while Connection is lost [s] 600 Watchdog IP Address 0.0.0.0

Figure 14: 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

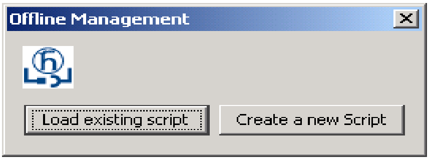


Figure 15: Offline Management selection

▶ 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.

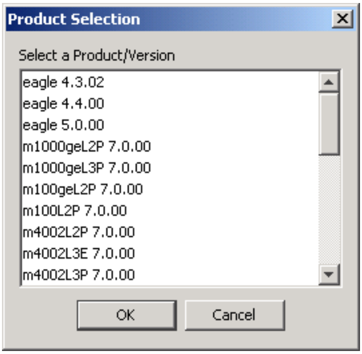


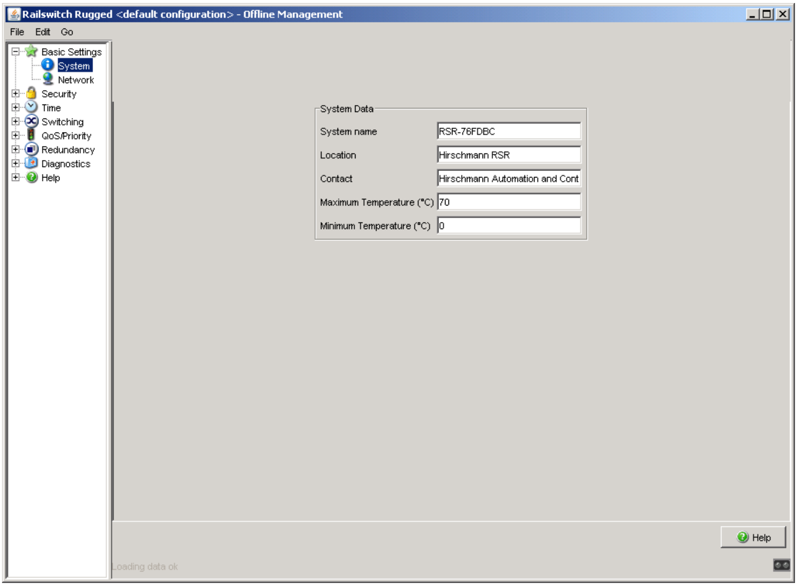
Figure 16: Creating New Script Dialog - Product Selection

□ 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

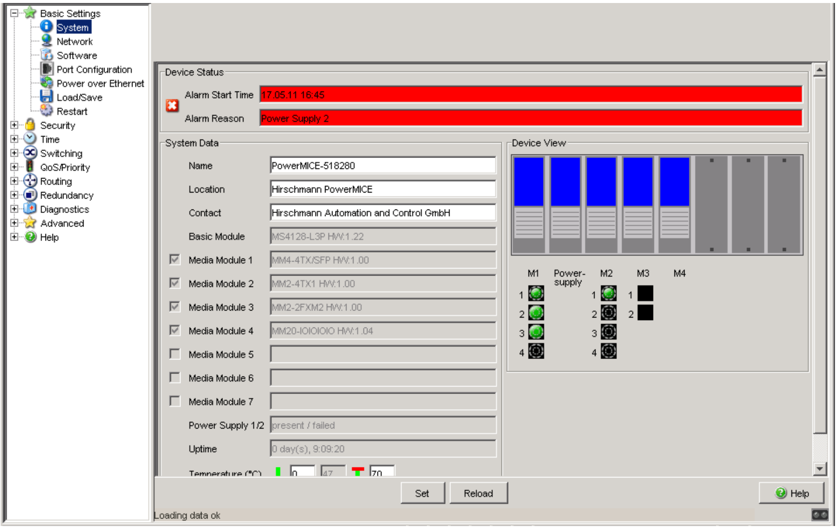


System Data

System name	RSR-76FDBC
Location	Hirschmann RSR
Contact	Hirschmann Automation and Cont
Maximum Temperature (°C)	70
Minimum Temperature (°C)	0

Help

Figure 17: Basic Settings Dialog:System in the Offline Configurator



Device Status

Alarm Start Time: 17.05.11 16:45

Alarm Reason: Power Supply 2

System Data

Name: PowerMICE-518280

Location: Hirschmann PowerMICE

Contact: Hirschmann Automation and Control GmbH

Basic Module: MS4128-L3P HW:1.22

☑ Media Module 1: MM4-4TX/SFP HW:1.00

☑ Media Module 2: MM2-4TX1 HW:1.00

☑ Media Module 3: MM2-2FXM2 HW:1.00

☑ Media Module 4: MM20-IOIOIOIO HW:1.04

□ Media Module 5:

□ Media Module 6:

□ Media Module 7:

Power Supply 1/2: present / failed

Uptime: 0 day(s), 9:09:20

Temperature (°C): 0 47 70

Loading data ok

Figure 18: Basic Settings Dialog:System in the Graphical User Interface

The following applies to the above example: You can find a description of the parameters that can be set in the offline configurator `Basic Settings:System` dialog.
See “System” on page 20.

□ Once you have set the desired parameters appropriate to your requirements in the offline configurator interface, save the configuration:
▶ `File - Save as` or
▶ `File - Save`

□ Quit the offline configurator with File - Quit.

Loading an XML configuration file onto the device

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

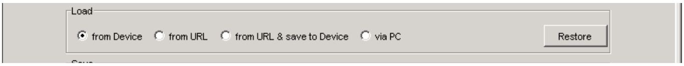
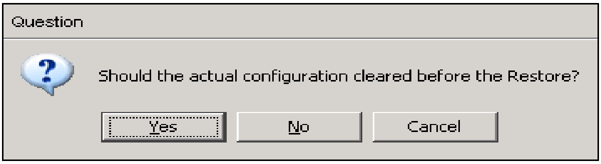


Figure 19: Loading the Configuration Dialog - Via PC

□ 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.


Question

Should the actual configuration cleared before the Restore?

Figure 20: Query - Resetting Configuration

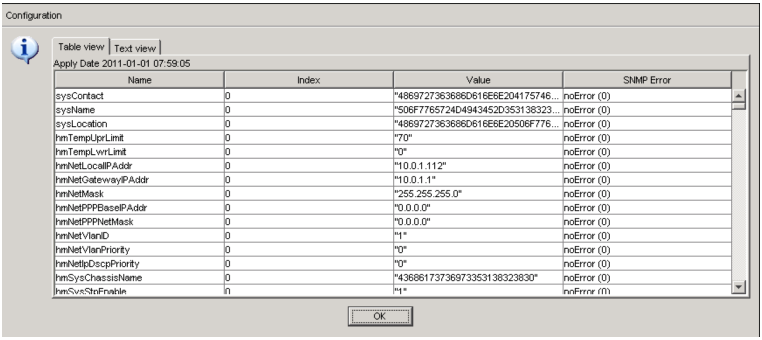
□ To reset the current configuration on your device before loading the offline configuration file, click on "Yes".

□ 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



Apply Date 2011-01-01 07:59:05

Name	Index	Value	SNMP Error
sysContact	0	"4869727363686D616E6E204175746...	noError (0)
sysName	0	"506F7765724D4943452D353138323...	noError (0)
sysLocation	0	"4869727363686D616E6E20506F776...	noError (0)
hmTempUprLimit	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)
hmNetPPPBaseIPAddr	0	"0.0.0.0"	noError (0)
hmNetPPPNetMask	0	"0.0.0.0"	noError (0)
hmNetVlanID	0	"1"	noError (0)
hmNetVlanPriority	0	"0"	noError (0)
hmNetIpDscpPriority	0	"0"	noError (0)
hmSysChassisName	0	"436861737369733531383230"	noError (0)
hmSysStpEnable	0	"1"	noError (0)

Figure 21: Information - Configuration - Tables View

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

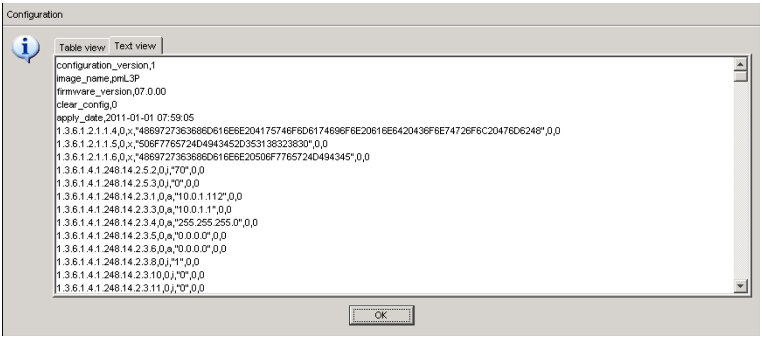
Parameters	Meaning	Possible values
Application date	Point in time (date and time of day) when you loaded the offline configuration file onto the device. Notation: `yyyy-mm-dd hh-mm-ss`	`yyyy` = valid year `mm` = 1 to 12 `dd` = 1 to 31 `hh` = 0 to 23 `mm` = 0 to 59 `ss` = 0 to 59
Name	Name of the configuration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

Table 15: 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	▶ (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 15: Information - Configuration - Tables View

Text View



```
configuration_version,1
image_name,pmL3P
firmware_version,07.0.00
clear_config,0
apply_date,2011-01-01 07:59:05
1.3.6.1.2.1.1.4,0,x,"4869727363686D616E6E204175746F6D6174696F6E20616E6420436F6E74726F6C20476D6248",0,0
1.3.6.1.2.1.1.5,0,x,"506F7765724D4943452D353138323830",0,0
1.3.6.1.2.1.1.6,0,x,"4869727363686D616E6E20506F7765724D494345",0,0
1.3.6.1.4.1.248.14.2.5.2,0,i,"70",0,0
1.3.6.1.4.1.248.14.2.5.3,0,i,"0",0,0
1.3.6.1.4.1.248.14.2.3.1,0,a,"10.0.1.112",0,0
1.3.6.1.4.1.248.14.2.3.3,0,a,"10.0.1.1",0,0
1.3.6.1.4.1.248.14.2.3.4,0,a,"255.255.255.0",0,0
1.3.6.1.4.1.248.14.2.3.5,0,a,"0.0.0.0",0,0
1.3.6.1.4.1.248.14.2.3.6,0,a,"0.0.0.0",0,0
1.3.6.1.4.1.248.14.2.3.8,0,i,"1",0,0
1.3.6.1.4.1.248.14.2.3.10,0,i,"0",0,0
1.3.6.1.4.1.248.14.2.3.11,0,i,"0",0,0
```

Figure 22: 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 15, "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 59 “Deleting a configuration”). The configuration in the non-volatile memory is kept, along with the IP address. Thus the device remains reachable.

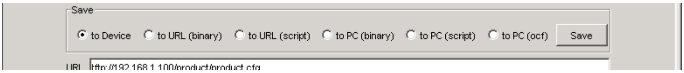
Note: The loading process started by DHCP/BOOTP (see on page 27 “Network”) shows the selection of “from URL & save local” in the “Load” frame. If you get an error message when saving a configuration, this could be due to an active loading process. DHCP/BOOTP only finishes a loading process when a valid configuration has been loaded. If DHCP/BOOTP does not find a valid configuration, finish the loading process by loading the local configuration from the device in the “Load” frame.

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

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

Saving configuration for the offline configurator

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



● to Device ○ to URL (binary) ○ to URL (script) ○ to PC (binary) ○ to PC (script) ○ to PC (ocf)

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

Figure 23: 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 75 “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 16: 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 16: ACAstatus

[a] In these cases, the ACA status is identical to the status “not in sync”, which sends “Not OK” to the signal contacts and the device status.,

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

1.8.6 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 `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 17: Buttons

1.9 Restart

This dialog provides you with the following functions:

- initiate a cold start or delayed cold start of the device. Here 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. Here 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.

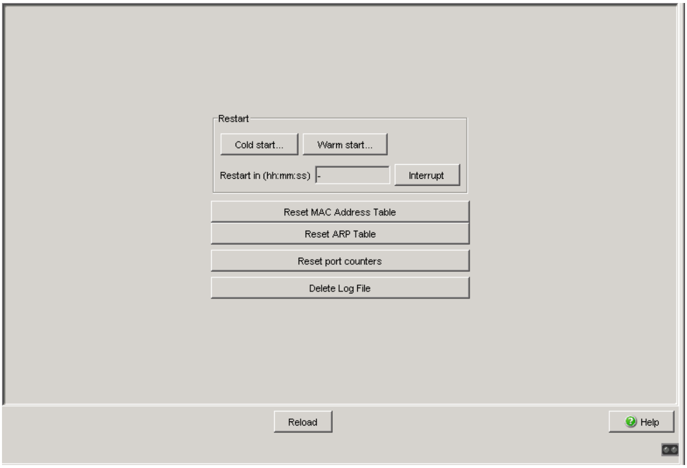


Figure 24: Restart Dialog

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".

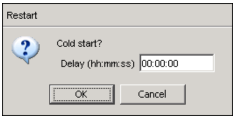


Figure 25: Delayed Restart Dialog

■ 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 18: 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

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.

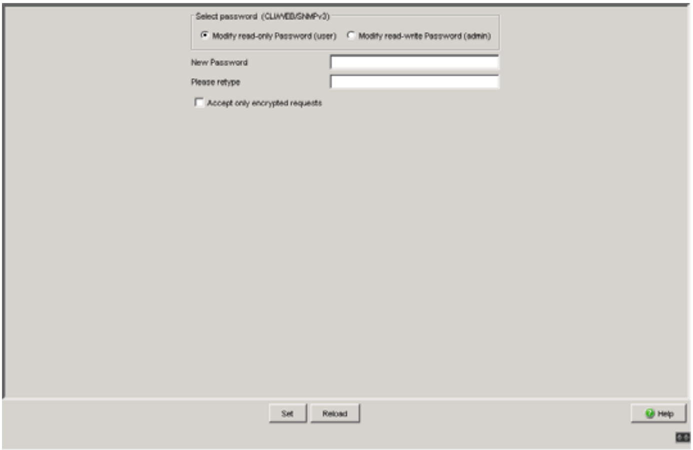
☐ Select “Modify read-write password (admin)” to enter the read/write password.
☐ Enter the read/write password and repeat your entry.

☐ 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.

Note: When you change the SNMPv3 password for the read/write access, the device automatically synchronizes the readWrite community for the SNMPv1/v2 access to the same value. Similarly, when the read access password is changed, the device synchronizes the readOnly community for SNMPv1/v2 .
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.



Select password (CLI/WEB/SNMPv3)

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

New Password

Please retype

☐ Accept only encrypted requests

Figure 26: 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 75.

Access at IP address level is restricted in a separate dialog.
See “SNMPv1/v2 Access Settings” on page 72.

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 19: 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 for the access restriction.
- In the “Password” column, you enter the password with which a management station may access the device via SNMPv1/v2 from the specified address range.

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

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

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

- In the "Access Mode" column, you specify whether this computer can access the device with the read password (access mode `readOnly`) or with the read/write password (access mode `readWrite`).
  See “Password / SNMPv3 access” on page 68.

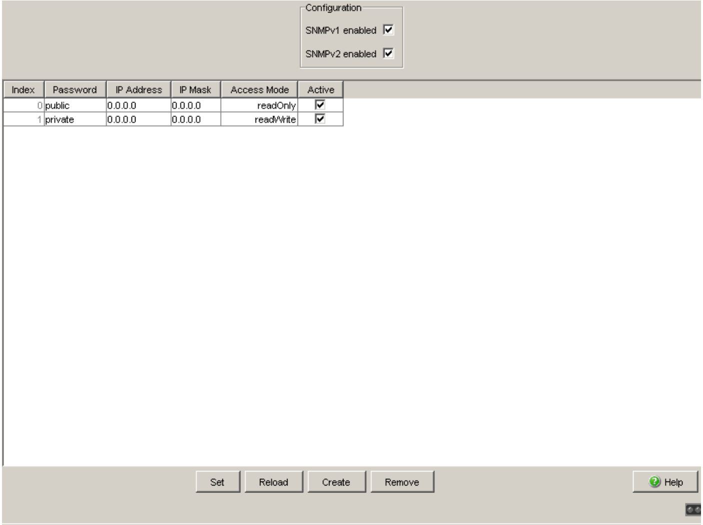
  Note: The password for the `readOnly` access mode is the same as the SNMPv3 password for read access.
  The password for the `readWrite` access mode is the same as the SNMPv3 password for read/write access.
  If you are changing one of the passwords, manually set the corresponding password for SNMPv3 to the same value. This way you ensure that you can also access with the same password via SNMPv3.

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

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

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

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



Configuration

SNMPv1 enabled ☑

SNMPv2 enabled ☑

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

Figure 27: SNMPv1/v2 Access Dialog

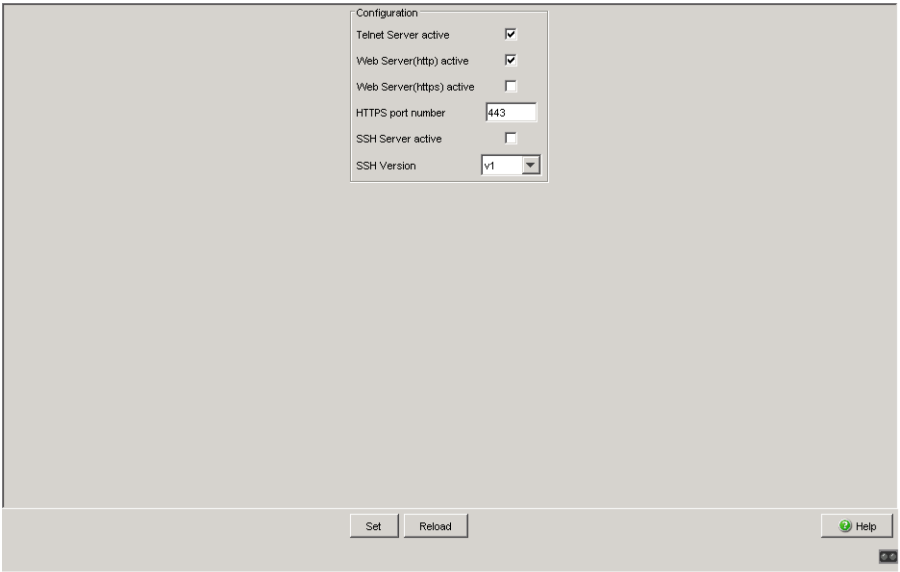
■ Buttons

Button	Meaning
Set	Transfers the changes to the volatile memory (`RAM`) of the device. To permanently save the changes, open the `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.
Create	Adds a new table entry.
Remove	Removes the selected table entry.
Help	Opens the online help.

Table 20: 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.



Configuration

Telnet Server active ☑

Web Server(http) active ☑

Web Server(https) active □

HTTPS port number 443

SSH Server active □

SSH Version v1

Figure 28: 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 21: 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 21: 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 `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 22: 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
- 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 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.

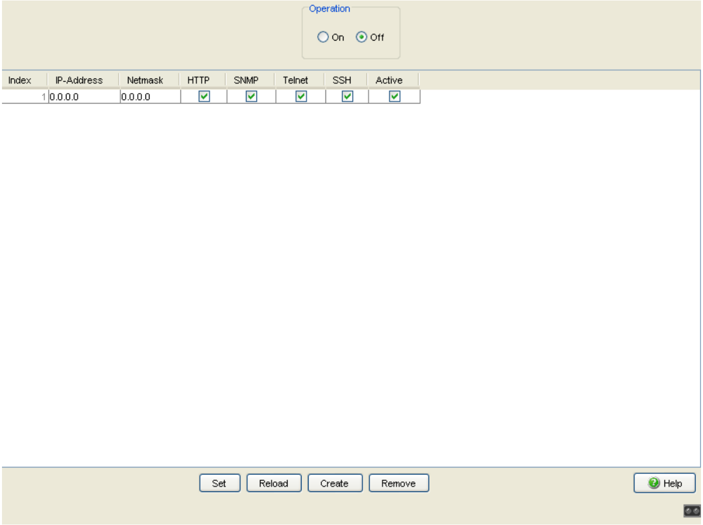
Parameters	Meaning	Possible values	Default setting
Operation	Switches the function on and off for the device.	On Off	Off
Index	Sequential number of the entry. When you delete an entry, this leaves a gap in the numbering. When you create a new entry with the Web-based interface, the device fills the first 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)
SNMP	Activates or deactivates the SNMP service (SNMP access) for this entry.	On Off	On (for all newly created entries)

Table 23: Restricted management access

Parameters	Meaning	Possible values	Default setting
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 23: 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	SNMP	Telnet	SSH	Active
1	0.0.0.0	0.0.0.0	☑	☑	☑	☑	☑

Figure 29: 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 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.
Create	Adds a new table entry.
Remove	Removes the selected table entry.
Help	Opens the online help.

Table 24: 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.

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 25: Configuration of port security globally for all ports

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

Name	Meaning
Module.Port	Port identification using module and port numbers of the device, e.g. 2.1 for port one of module two.
Port Status	`enabled`: Port is switched on and transmitting. `disabled`: Port is switched off and not transmitting. The port is switched on if - an authorized address accesses the port or - an unauthorized address attempts to access the port and `trapOnly` or `none` is selected under “Action”. The port is switched off if - an unauthorized address attempts to access the port and `portDisable` is selected under “Action”.

Table 26: Configuration of port security for a single port

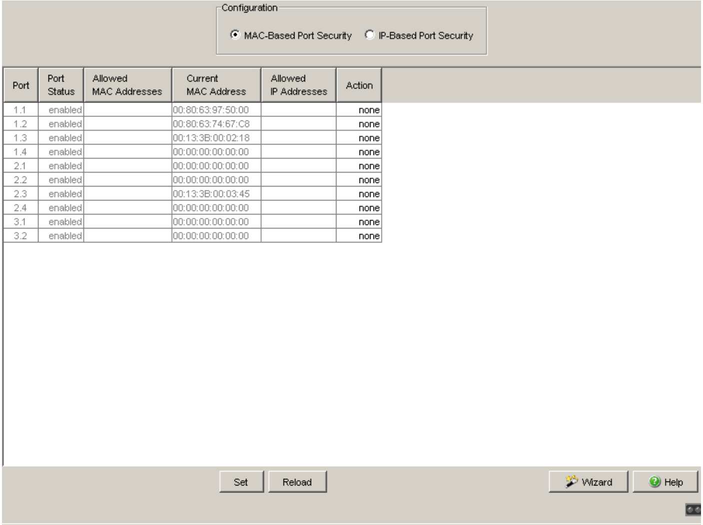
Name	Meaning
Allowed MAC Addresses	MAC addresses of the devices with which you allow data exchange on this port. The graphical user interface allows you to enter up to 50 MAC addresses, each separated by a space. After each MAC address you can enter a slash followed by a number identifying an address area. This number, between 2 and 47, indicates the number of relevant bits. Example: 00:80:63:01:02:00/40 stands for 00:80:63:01:02:00 to 00:80:63:01:02:FF or 00:80:63:00:00:00/24 stands for 00:80:63:00:00:00 to 00:80:63:FF:FF:FF If there is no entry, any number of devices can communicate via this port.
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	IP addresses of the devices with which you allow data exchange on this port. The graphical user interface allows you to enter up to 10 IP addresses, each separated by a space. If there is no entry, any number of devices can communicate via this port.
Action	Action performed by the device after an unauthorized access: – `none`: no action – `trapOnly`: send alarm – `portDisable`: disable the port with the corresponding entry in the port configuration table and send an alarm.

Table 26: Configuration of port security for a single port

Note: This entry in the port configuration table is part of the configuration and is saved together with the configuration.
See “Load/Save” on page 48.

Note: Prerequisites for the device to be able to send an alarm (trap):
See “Alarms (Traps)” on page 317.

- 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".



Configuration

● MAC-Based Port Security ○ IP-Based Port Security

Port	Port Status	Allowed MAC Addresses	Current MAC Address	Allowed IP Addresses	Action
1.1	enabled		00:80:63:97:50:00		none
1.2	enabled		00:80:63:74:67:C8		none
1.3	enabled		00:13:3B:00:02:18		none
1.4	enabled		00:00:00:00:00:00		none
2.1	enabled		00:00:00:00:00:00		none
2.2	enabled		00:00:00:00:00:00		none
2.3	enabled		00:13:3B:00:03:45		none
2.4	enabled		00:00:00:00:00:00		none
3.1	enabled		00:00:00:00:00:00		none
3.2	enabled		00:00:00:00:00:00		none

Figure 30: 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 `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.
Wizard	Opens the "Wizard". With the "Wizard" you assign the permitted MAC addresses to a port.
Help	Opens the online help.

Table 27: 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 28: 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	Lists the MAC Addresses allowed access to the port. Possible values: ▶ `Valid Unicast MAC addresses` Click "Add" to transfer the MAC address to the "Allowed MAC Addresses" field.
MAC Address	Defines the MAC address allowed access to the port. Possible values: ▶ Valid Unicast MAC address Enter the value in one of the following formats: – 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` Click "Add" to transfer the MAC address to the "Allowed MAC Addresses" field.
Mask	Defines number of significant digits in the MAC address range. Possible values: ▶ 1..48 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.
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 29: 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	Action performed by the device after an unauthorized access: Possible values: ▶ `none` The port continues to forward traffic without notification of the intrusion. ▶ `trapOnly` The device sends a trap to the active management terminal. ▶ `portDisable` The device disables the port with the corresponding entry in the port configuration table and sends a trap to the active management terminal.

Table 30: Wizard in the `Security:Port Security` *dialog, "Action" page*

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

Note: Prerequisites for the device to be able to send an alarm (trap): See “Alarms (Traps)” on page 317.
- 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".

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 31: 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	Activates or deactivates the assigning of a VLAN ID via the RADIUS server to a port. 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. Note the following information about VLAN assignment.	`On`, `Off`	`Off`

Table 32: 802.1X Port Security Dialog, Part 1

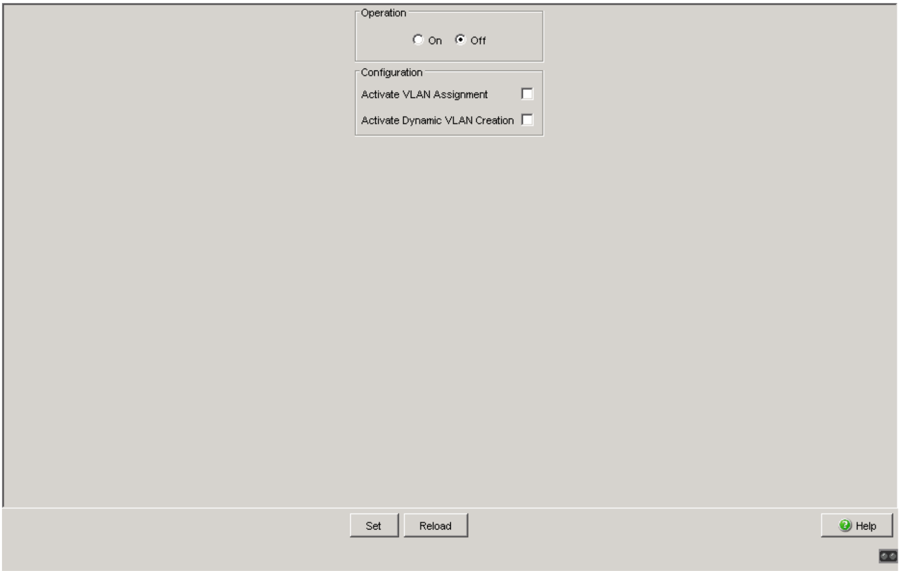
Note:

- **For devices MACH 104 and MACH 1040:**
  The Switch can assign incoming untagged frames to a VLAN based on the MAC sender address. If you have connected several terminal devices to one port, the Switch can also assign these devices' untagged frames to different VLANs.
- **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	**For the device families other than MACH 104 and MACH 1040:** 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. ▶ `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 33: 802.1X Port Security Dialog, Part 2



Operation

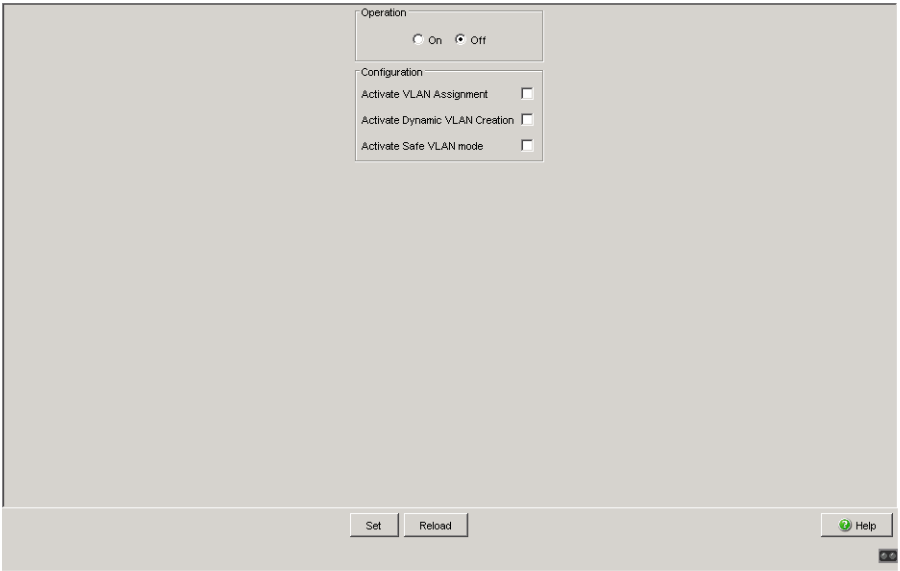
○ On ● Off

Configuration

Activate VLAN Assignment □

Activate Dynamic VLAN Creation □

Figure 31: 802.1X Global Dialog for the MACH 104 and MACH 1040 device families



Operation

○ On ● Off

Configuration

Activate VLAN Assignment □

Activate Dynamic VLAN Creation □

Activate Safe VLAN mode □

Figure 32: 802.1X Global Dialog

Preparing the device for the 802.1X port authentication:

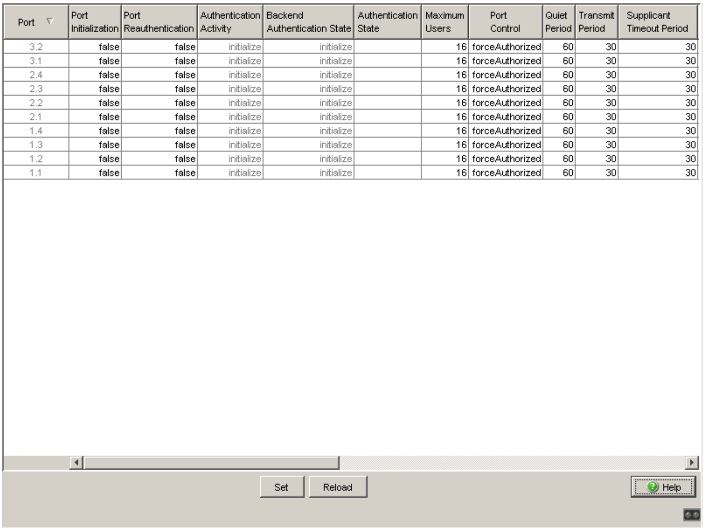
□ Configure the device's IP parameters.
□ Activate the 802.1X port authentication function globally.
□ Set the 802.1X "Port Control" to `auto`. The default setting is `forceAuthorized`.
□ Configure a RADIUS server for authorization and authentication.

■ Buttons

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

Table 34: 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 33: 802.1X Port Configuration Table

Parameters	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 35: 802.1X Setting Options per Port, entries in the configuration table

Parameters	Meaning	Possible values	Default setting
Port Control	Setting for the port access control. **Note:** ▶ In the ForceAuthorized, ForceUnauthorized and auto 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 macBased 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.	▶ ForceAuthorized: Access is also available for all clients without authentication. ▶ ForceUnauthorized: Access is blocked for all clients, even for clients with authentication. ▶ auto: Access to the port depends on the result of the authentication. ▶ macBased: Behavior like for auto. Access is also available for clients with a MAC address which the client uses in the course of authentication.	ForceAuthorized
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 35: 802.1X Setting Options per Port, entries in the configuration table

Parameters	Meaning	Possible values	Default setting
Assigned VLAN ID	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. Prerequisite: The port control is set to `auto`. **Note:** If you are using the multi-client setting by setting “Port Control” to `macBased`, take into account: ▶ the device-dependent resolution of possible VLAN assignment conflicts for untagged received frames; (see on page 90 “802.1X Global Configuration”) ▶ the VLANs assigned, you can find the current values in the “Port Clients” table . (see on page 102 “802.1X Port Clients”)	`0 - 4094`	0

Assignment Reason	Reason for assigning the VLANs to the port.
	Prerequisite: The port control is set to `auto`.
	Note: If you are using the multi-client setting by setting “Port Control” to `macBased`, take into account:
	▶ the device-dependent resolution of possible VLAN assignment conflicts for untagged received frames; (see on page 90 “802.1X Global Configuration”)
	▶ the VLANs assigned, you can find the current values in the “Port Clients” table . (see on page 102 “802.1X Port Clients”)
		`notAssigned`
		`radius`
		`unauthenticatedVLAN`
			`notAssigned`

Table 35: 802.1X Setting Options per Port, entries in the configuration table

Parameters	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	ID of a VLAN that the Switch assigns to the port, if: ▶ the 802.1X protocol is active on the port and the port control is set to `auto` or `macBased`, ▶ 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. The Switch: ▶ switches the port to the authenticated state, ▶ allows data traffic, ▶ but only to the guest VLAN. Specify a guest VLAN ID if you want to allow devices without 802.1X support access to a guest VLAN. **Note:** ▶ 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 With a VLAN ID of 0, the Switch blocks the data traffic because it denies a VLAN setup with this ID.	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 35: 802.1X Setting Options per Port, entries in the configuration table

Parameters	Meaning	Possible values	Default setting
Unauthenticated VLAN ID	ID of a VLAN that the Switch assigns to the port, if: ▶ 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. The Switch: ▶ switches the port to the authenticated state, ▶ allows data traffic, ▶ but only to the unauthenticated VLAN. Specify a VLAN ID for unauthenticated devices, if: ▶ 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. **Note:** ▶ Use only as an unauthenticated VLAN a VLAN that you have set up statically in the Switch.	0 - 4094 With a VLAN ID of 0, the Switch blocks the data traffic because it denies a VLAN setup with this ID.	0

Table 35: 802.1X Setting Options per Port, entries in the configuration table

Parameters	Meaning	Possible values	Default setting
MAC Authorized Bypass Enable	The Switch makes authenticated access available via MAB, if: ▶ You have set the “Port Control” to `macBased`, ▶ 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. The Switch: ▶ 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. Activate this function, if: ▶ you want to allow particular devices normal access, ▶ however these devices do not support 802.1X. **Note:** ▶ 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.	`On` `Off`	`Off`

Table 35: 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 `Basic Settings:Load/Save` dialog and click "Save".
Reload	Updates the fields with the values that are saved in the volatile memory (`RAM`) of the device.
Help	Opens the online help.

Table 36: 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.

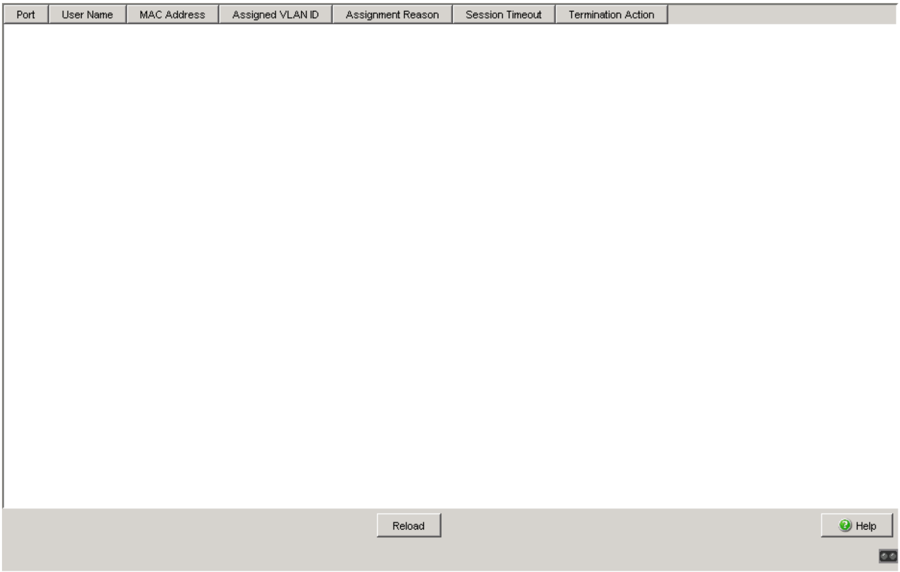


Figure 34: 802.1X Port Client Table

Parameters	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 37: 802.1X Setting Options per Port, entries in the port client table

Parameters	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 **Note:** If you are using the multi-client setting by setting “Port Control” to `macBased`, take into account: ▶ the device-dependent resolution of possible VLAN assignment conflicts for untagged received frames; (see on page 90 “802.1X Global Configuration”) ▶ the VLANs assigned, you can find the current values in the “Port Clients” table . (see on page 102 “802.1X Port Clients”)	`0 - 4094`	-
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`	?

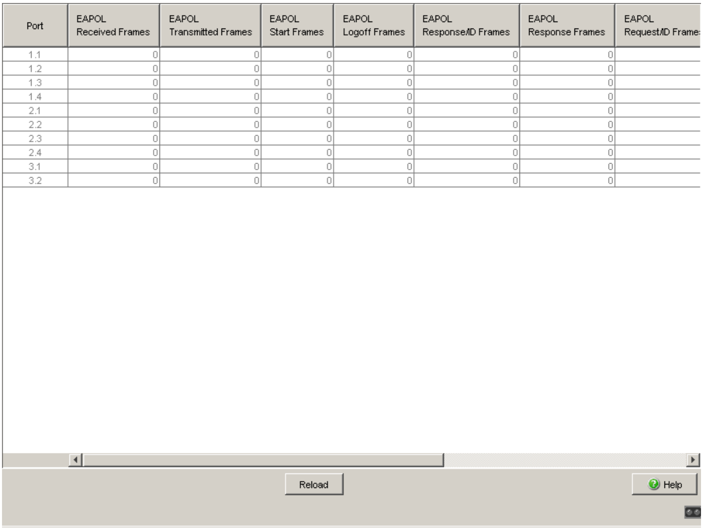
Table 37: 802.1X Setting Options per Port, entries in the port client table

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 38: 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 Frame
1.1	0	0	0	0	0	0	
1.2	0	0	0	0	0	0	
1.3	0	0	0	0	0	0	
1.4	0	0	0	0	0	0	
2.1	0	0	0	0	0	0	
2.2	0	0	0	0	0	0	
2.3	0	0	0	0	0	0	
2.4	0	0	0	0	0	0	
3.1	0	0	0	0	0	0	
3.2	0	0	0	0	0	0	

Figure 35: 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 39: 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 39: 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 40: 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 terminal device to the RADIUS client at the access point.

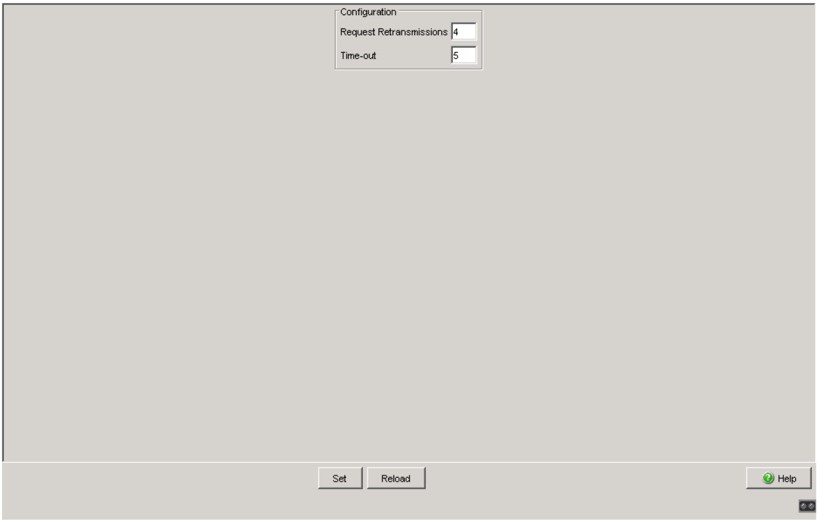
The device forwards the users’ login data to the primary authentication server. The authentication server decides whether the login data is valid and transfers the user’s authorizations to the device.

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.



Configuration

Request Retransmissions 4

Time-out 5

Figure 36: `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 41: Security:RADIUS:RADIUS Global dialog

Buttons

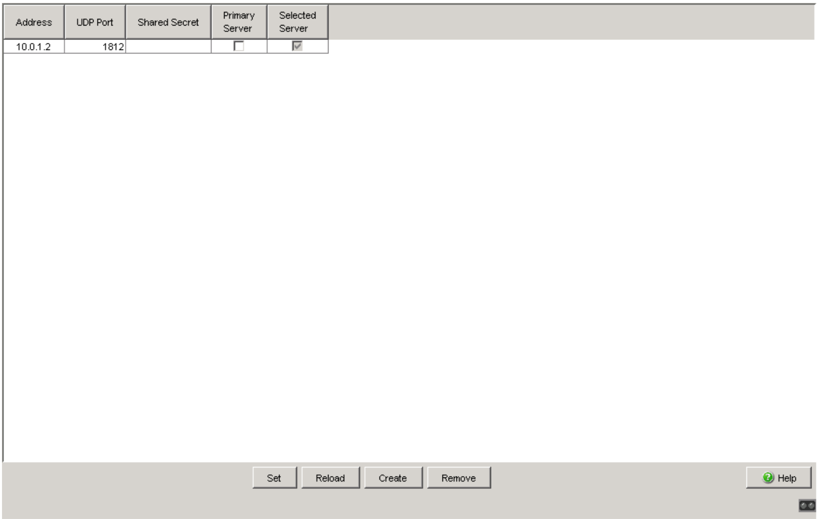
Button	Meaning
Set	Transfers the changes to the volatile memory (`RAM`) of the device. To permanently save the changes afterwards, you open the `Basic Settings:Load/Save` dialog and click "Save".
Reload	Updates the fields with the values that are saved in the volatile memory (`RAM`) of the device.
Help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

Table 42: Buttons

2.7.2 RADIUS Server

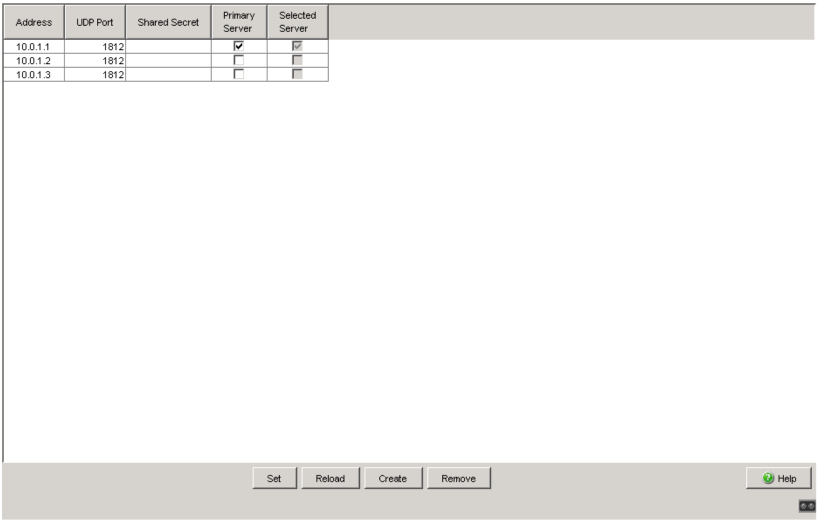
This dialog allows you to define up to 3 RADIUS servers. A RADIUS server authenticates and authorizes the users when the device forwards the login data to the server.

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		☐	☑

Figure 37: `Security:RADIUS:RADIUS Server` *dialog for the Power MICE*



Address	UDP Port	Shared Secret	Primary Server	Selected Server
10.0.1.1	1812		☑	☑
10.0.1.2	1812		☐	☐
10.0.1.3	1812		☐	☐

Figure 38: `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 43: Table in the `Security:RADIUS:RADIUS Server` *dialog*

Parameters	Meaning
Primary Server	Specifies the authentication server as primary or secondary. Possible values: ▶ `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	Shows the connection to an active server. Possible values: ▶ `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 43: 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 `Basic Settings:Load/Save` dialog and click "Save".
Reload	Updates the fields with the values that are saved in the volatile memory (`RAM`) of the device.
Create	Adds a new table entry.
Remove	Removes the selected table entry.
Help	Opens the online help.

Table 44: Buttons

■ RADIUS Server Settings

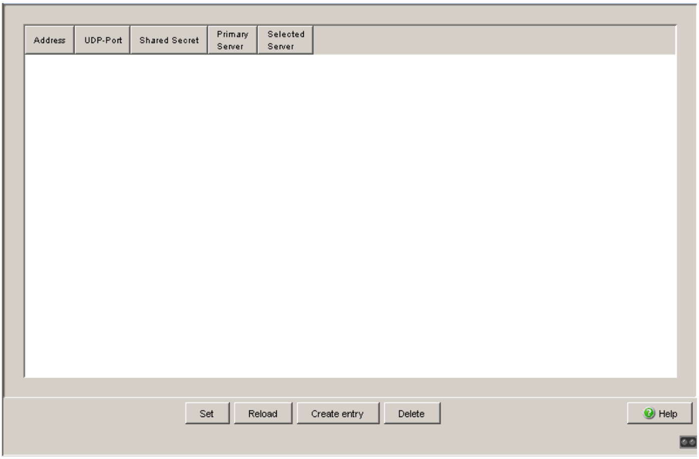


Figure 39: RADIUS Server Dialog

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 Banner

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

Banner Text

Parameters	Meaning
Banner Text	Specifies the greeting or information text that the device displays in the login dialog of the graphical user interface (GUI) and of the Command Line Interface (CLI). Possible values: ▶ Maximum 255 alphanumeric characters ▶ including spaces, tabs, line breaks and the following special characters: !#$&'()*+,-./:;<=>?@[\\]^_`{}~
Remaining Characters	Shows how many characters are still available in the "Banner Text" field. Possible values: ▶ `255..0`

Table 45: Rahmen "Banner Text" frame in the `Security:Login Banner` dialog

Buttons

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

Table 46: Buttons

3 Time

3.1 Basic Settings

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

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

- The "System Time" uses "System Time (UTC)", allowing for the local time difference from "System Time (UTC)".
  "System Time" = "System Time (UTC)" + "Local Offset".

- "Time Source" displays the source of the following time data. The device automatically selects the source with the greatest accuracy.
  Possible sources are: `local`, `ptp` and `sntp`. The source is initially `local`.
  If PTP is activated and the device receives a valid PTP frame, it sets its time source to `ptp`. If SNTP is activated and if the device receives a valid SNTP packet, the device sets its time source to `sntp`. The device gives the PTP time source priority over SNTP.

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

- The "Local Offset" is for displaying/entering the time difference between the local time and the "System Time (UTC)".

□ With "Set Offset from PC", the device determines the time zone on your PC and uses it to calculate the local time difference.

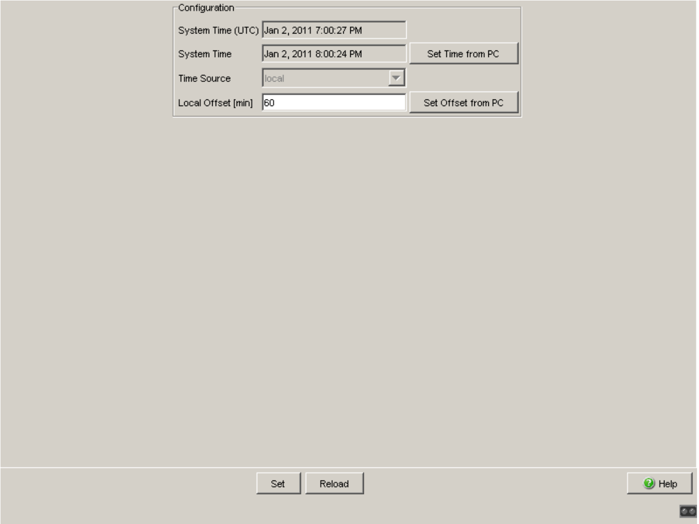
The device is equipped with a buffered hardware clock. This keeps the current time

- 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.



Configuration

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

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

Time Source: local

Local Offset [min]: 60

Figure 40: 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 `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 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.

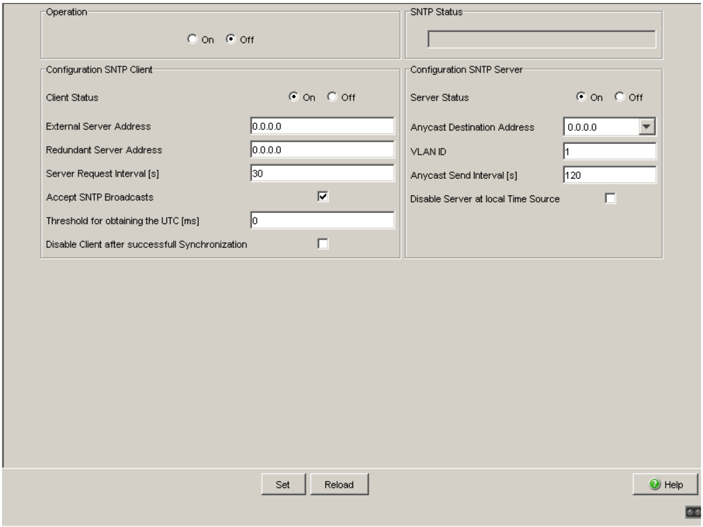
Note: If you are receiving the system time from an external/redundant server address, switch off the reception of SNTP Broadcasts (see “Accept SNTP Broadcasts”). You thus ensure that the device only takes the time from a defined SNTP server.

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 `local` (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



Operation

○ On ● Off

SNTP Status

Configuration SNTP Client

Client Status ● On ○ Off

External Server Address 0.0.0.0

Redundant Server Address 0.0.0.0

Server Request Interval [s] 30

Accept SNTP Broadcasts ☑

Threshold for obtaining the UTC [ms] 0

Disable Client after successfull Synchronization □

Configuration SNTP Server

Server Status ● On ○ Off

Anycast Destination Address 0.0.0.0

VLAN ID 1

Anycast Send Interval [s] 120

Disable Server at local Time Source □

Figure 41: SNTP 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 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

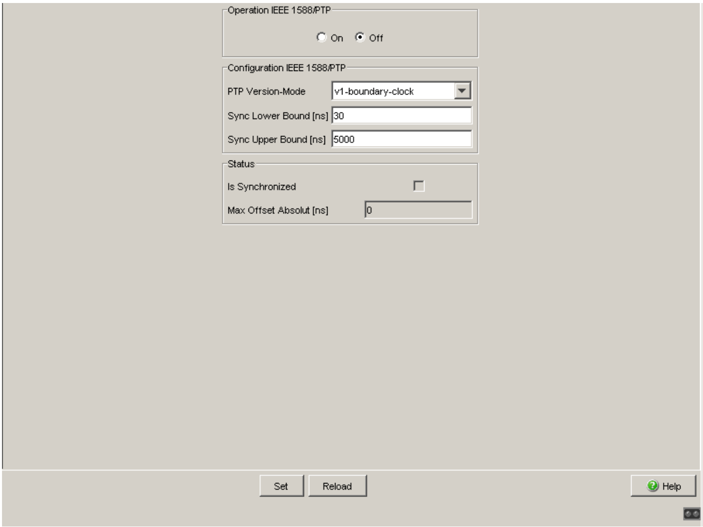
  support the modes
  - `v1-boundary-clock`
  - `v1-simple-mode`
  - `v2-boundary-clock-twostep`, only with the network protocol `UDP/IPv4` and the runtime measurement `E2E`

- 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.



Operation IEEE 1588/PTP

○ On ● Off

Configuration IEEE 1588/PTP

PTP Version-Mode: v1-boundary-clock

Sync Lower Bound [ns]: 30

Sync Upper Bound [ns]: 5000

Status

Is Synchronized □

Max Offset Absolut [ns]: 0

Figure 42: 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` **Note:** For the MS20, MS30 and PowerMICE devices with MM23 or MM33 modules, see sections “Devices without PTP hardware support” on page 125 and “Devices with PTP hardware support” on page 126.	Version 2	Yes	Process
	`v2-boundary-clock-twostep`	Version 2	Yes	Process
	`v2-transparent-clock`	Version 2	Yes	Forward

Table 54: Selecting the PTP version and the PTP mode

The PTP modes
- v1-boundary-clock
- v2-boundary-clock-onestep[1]
- 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 125 and “Devices with PTP hardware support” on page 126.

Value for PTP version and PTP mode	Meaning
`v1-boundary-clock`	Boundary Clock function based on IEEE1588-2002 (PTPv1). 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 125 and “Devices with PTP hardware support” on page 126.
`v1-simple-mode`	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. Select this mode if the device only has ports absent a timestamp unit.
`v2-boundary-clock-onestep`	Boundary Clock function based on IEEE 1588-2008 (PTPv2). The one-step mode determines the precise PTP time with 1 message. For the MS20, MS30 and PowerMICE devices with MM23 or MM33 modules, see sections “Devices without PTP hardware support” on page 125 and “Devices with PTP hardware support” on page 126.
`v2-boundary-clock-twostep`	Boundary Clock function based on IEEE 1588-2008 (PTPv2). The two-step mode determines the precise PTP time with 2 messages.
`v2-transparent-clock`	Transparent Clock function based on IEEE 1588-2008 (PTPv2). Here, the MS20, MS30 and PowerMICE devices with MM23 or MM33 modules use only the one-step mode. Here, the MACH 104 and MACH 1040 devices use only the two-step mode. They support a receive rate of 8 frames/s max.
`v2-simple-mode`	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. Select this mode if the device only has ports absent a timestamp unit.

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 `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.
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 `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 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 identifty	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.	-2147483648 to 2147483647	35
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 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 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	
	Port is in PTP slave mode.	slave	
Sync Interval [s]	Interval in seconds for the synchronization messages	0,5; 1; 2	1
Runtime Measuring Mechanism	Mechanism for measuring the message runtime. Enter the same mechanism for the PTP device connected to this port.		
	A PTP slave port measures the runtime of the entire transmission path to the master. The device displays the measured value in the PTP:Version 2(BC):Global dialog (see on page 135 “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. The MS20, MS30 and PowerMICE devices with MM23 or MM33 modules, as well as the MACH 104 and MACH 1040 devices support these mechanisms.	P2P (peer-to-peer)	
	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. **Note:** ▶ Also take the port's VLAN setting (see on page 180 “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.	`none, 0 - 4042`	`none`
VLAN Priority	The VLAN priority (Layer 2, IEEE 802.1p) with which the device sends PTP frames to this port. If you have set the VLAN ID to `none`, the device ignores the VLAN priority.	`0 - 7`	`0`

Table 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 `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 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 135 “Global”).	`E2E` (end-to-end):	
	The device itself measures the runtime to all the PTP devices connected. If a reconfiguration is performed, this eliminates the need to determine the runtime again.	`P2P` (peer-to-peer)	
	For the MACH 104 and MACH 1040 devices: Such as E2E with the following characteristics: ▶ The device only transmits the PTP slaves' delay queries to the master, even though these queries are multicast frames. In this way, the device relieves the other clients from unnecessary multicast queries. ▶ With changes in the PTP master-slave topology, the device relearns the port for the PTP master as soon as it has received a frame from another PTP master. ▶ If the device does not recognize a PTP master, it also floods delay queries received in the `E2E Optimized` mode.	`E2E Optimized` (end-to-end, optimized)	
	For the MACH 104 and MACH 1040 devices: The device does not allow runtime measurement, i.e., it discards frames received, which are used for measuring runtime.	`Disabled`	
Primary Domain	Assignment of the clock to a PTPv2 domain.	0-225	0
Network Protocol	Network protocol for P2P and management messages.	`UDP/IPv4`, `IEEE 802.3`	`UDP/IPv4`

Table 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. **Note:** ▶ Also take the port's VLAN setting (see on page 180 “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.	`none`, `0 - 4042`	`none`
VLAN Priority	The VLAN priority (Layer 2, IEEE 802.1p) with which the device sends tagged PTP frames. If you have set the VLAN ID to `none`, the device ignores the VLAN priority.	`0 - 7`	`0`

Table 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: ▶ 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 `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 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 `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 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.	PowerMICE, MACH 104, MACH 1040, MACH 4000: 10-630 RS30/RS40, MS20/MS30, RSR20/RSR30, MACH 100, MACH 1000, OCTOPUS: 15-3825	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
Frame size	Set the maximum packet size (frame size) in bytes.	MACH 104, MACH 1040: 1522, 1552, 9022 PowerMICE, MACH 4000: 1522, 1552 RS30/RS40, MS20/MS30, RSR20/RSR30, MACH 100, MACH 1000, OCTOPUS: 1522, 1632	1522
Activate Address Relearn Detection	Enable/disable whether the device detects whether it has repeatedly learned the same MAC source addresses at different ports. This process very probably indicates a loop situation in the network. If the device detects this process, it creates an entry in the log file and sends an alarm (trap).	On, Off	Off
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

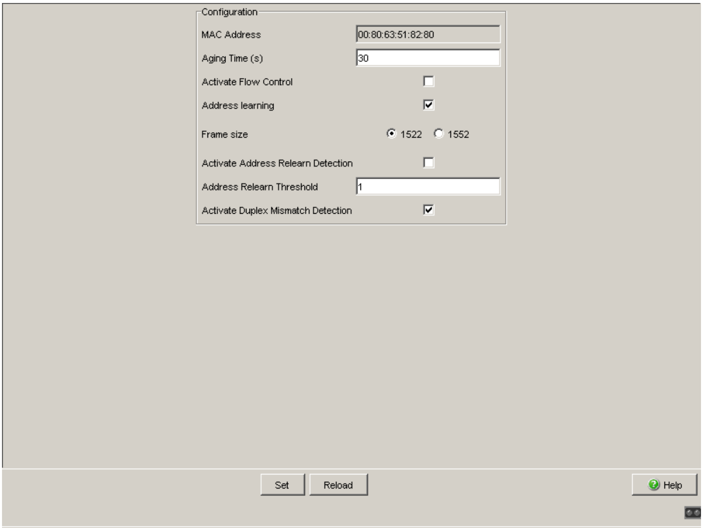
Table 81: Switching:Global dialog

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



Configuration

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

Aging Time (s) 30

Activate Flow Control □

Address learning ☑

Frame size ● 1522 ○ 1552

Activate Address Relearn Detection □

Address Relearn Threshold 1

Activate Duplex Mismatch Detection ☑

Figure 43: 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 `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.

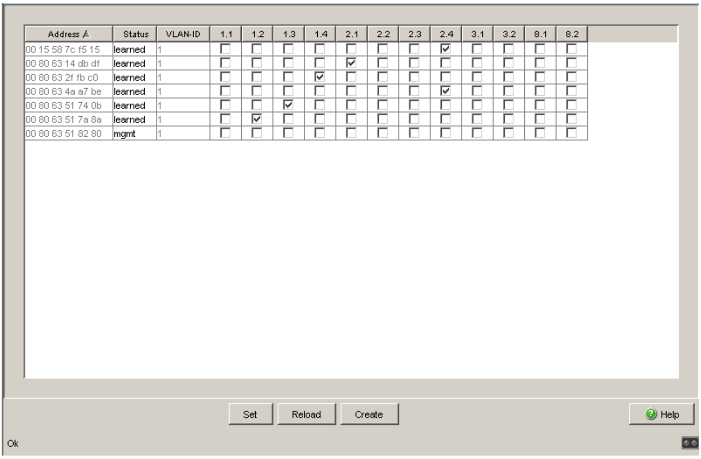
Table 83: Buttons

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

Figure 44: Filter Table dialog

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	Defines the ID of the VLAN to which the table entry applies. Possible values: ▶ All VLAN IDs that are set up
Address	Defines the destination MAC address to which the table entry applies. Possible values: ▶ Valid MAC address Enter the value in one of the following formats: – 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	Defines the device ports to which the device transmits data packets with the destination MAC address: ☐ Select one port if the destination MAC address is a Unicast address. ☐ Select one or more ports if the destination MAC address is a Multicast address. ☐ 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	This column contains the device ports that are assigned to the table entry. ☐ Select one port if the destination MAC address is a Unicast address. ☐ Select one or more ports if the destination MAC address is a Multicast address. ☐ 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 Basic Settings:Load/Save dialog and click "Save".
Reload	Updates the fields with the values that are saved in the volatile memory (RAM) of the device.
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 210 “Link Aggregation”) are excluded from the rate limitation, regardless of the entries in the “Rate Limiter” dialog.

4.3.1 Rate limiter settings for RS20/RS30/RS40, MS20/MS30, RSR20/RSR30, MACH 100, MACH 1000 and OCTOPUS

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

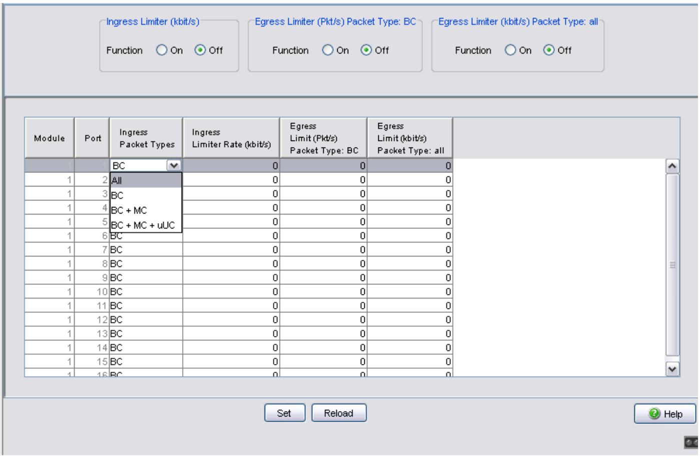
Setting options per port:

- "Inbound Packet Types" allows you to select the packet type for which the limit is to apply:
  - `All`, limits the total inbound data volume at this port.
  - `BC`, limits the broadcast packets received at this port.
  - `BC + MC`, limits broadcast packets and multicast packets received at this port.
  - `BC + MC + uUC`, limits broadcast packets, multicast packets, and unknown unicast packets received at this port.

- Inbound Limiter Rate for the inbound packet type selected:
  - = 0, no inbound limit at this port.
  - > 0, maximum inbound traffic rate in kbit/s that can be received at this port.

- Outbound Limiter Rate for broadcast packets:
  - = 0, no rate limit for outbound broadcast packets at this port.
  - > 0, maximum number of outbound broadcasts per second that can be sent at this port.

- Outbound Limiter Rate for the entire data stream:
  - = 0, no rate limit for outbound data stream at this port.
  - > 0, maximum outbound traffic rate in kbit/s sent at this port.



Ingress Limiter (kbit/s)

Function ○ On ● Off

Egress Limiter (Pkt/s) Packet Type: BC

Function ○ On ● Off

Egress Limiter (kbit/s) Packet Type: all

Function ○ On ● Off

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

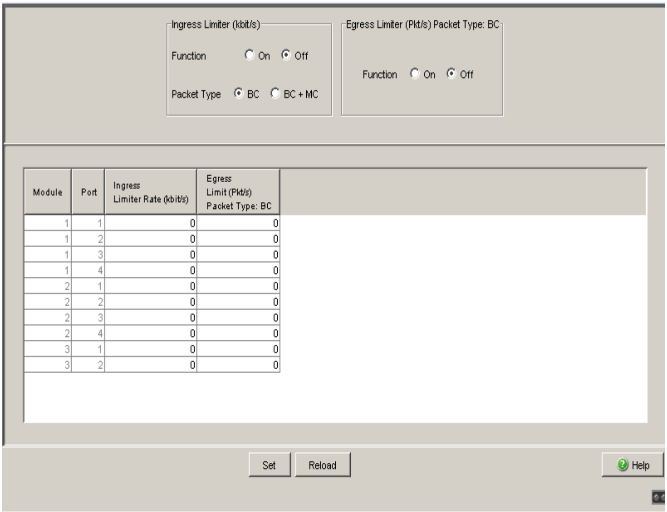
Figure 45: Rate Limiter Dialog

4.3.2 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:

- Inbound Limiter Rate for the packet type selected in the Inbound Limiter frame:
  - = 0, no inbound limit at this port.
  - > 0, maximum outbound traffic rate in kbit/s that can be sent at this port.
- Outbound Limiter Rate for broadcast packets:
  - = 0, no rate limit for outbound broadcast packets at this port.
  - > 0, maximum number of outbound broadcasts per second sent at this port.



Ingress Limiter (kbit/s)

Function ○ On ● Off

Packet Type ● BC ○ BC + MC

Egress Limiter (Pkt/s) Packet Type: BC

Function ○ On ● Off

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 `Basic Settings:Load/Save` dialog and click "Save".
Reload	Updates the fields with the values that are saved in the volatile memory (`RAM`) of the device.
Help	Opens the online help.

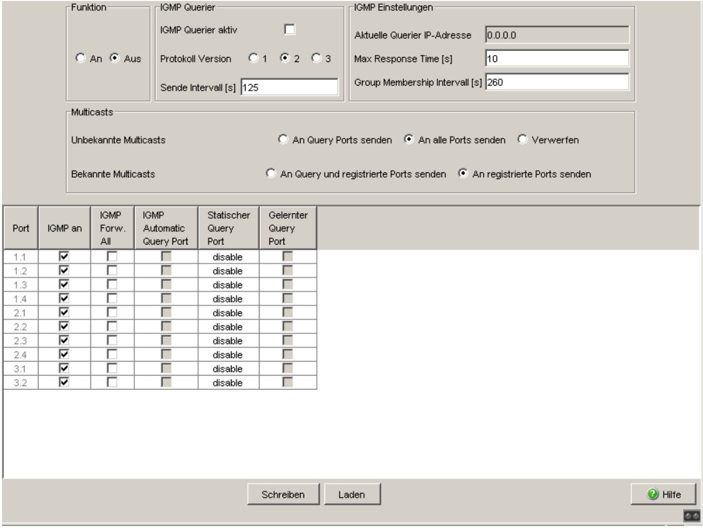
Table 87: Buttons

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.



Funktion

○ An ● Aus

IGMP Querier

IGMP Querier aktiv □

Protokoll Version ○ 1 ● 2 ○ 3

Sende Intervall [s] 125

IGMP Einstellungen

Aktuelle Querier IP-Adresse 0.0.0.0

Max Response Time [s] 10

Group Membership Intervall [s] 260

Multicasts

Unbekannte Multicasts ○ An Query Ports senden ● An alle Ports senden ○ Verwerfen

Bekannte Multicasts ○ An Query und registrierte Ports senden ● An registrierte Ports senden

Port	IGMP an	IGMP Forw. All	IGMP Automatic Query Port	Statischer Query Port	Gelernter Query Port
1.1	☑	□	□	disable	□
1.2	☑	□	□	disable	□
1.3	☑	□	□	disable	□
1.4	☑	□	□	disable	□
2.1	☑	□	□	disable	□
2.2	☑	□	□	disable	□
2.3	☑	□	□	disable	□
2.4	☑	□	□	disable	□
3.1	☑	□	□	disable	□
3.2	☑	□	□	disable	□

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: ▶ 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	▶ Send to Query Ports: The device sends the packets with an unknown MAC/IP Multicast address to all query ports. ▶ Send to All Ports: The device sends the packets with an unknown MAC/IP Multicast address to all ports. ▶ Discard: The device discards all packets with an unknown MAC/IP Multicast address.	Send to Query Ports Send to All Ports Discard	Send to All Ports
Known Multicasts	▶ Send to query and registered ports: The device sends the packets with a known MAC/IP Multicast address to all query ports and to registered ports. The advantage of this 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. **Note:** If a number of routers are connected to a subnetwork, you must use IGMP version 1 so that all the routers receive all the IGMP reports. **Note:** If you use IGMP version 1 in a subnetwork, then you must also use IGMP version 1 in the entire network.	`On` `Off`	`Off`
IGMP Automatic Query Port	Displays which ports the device has learned as query ports if `automatic` is selected in “Static Query Port”. Prerequisite: 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

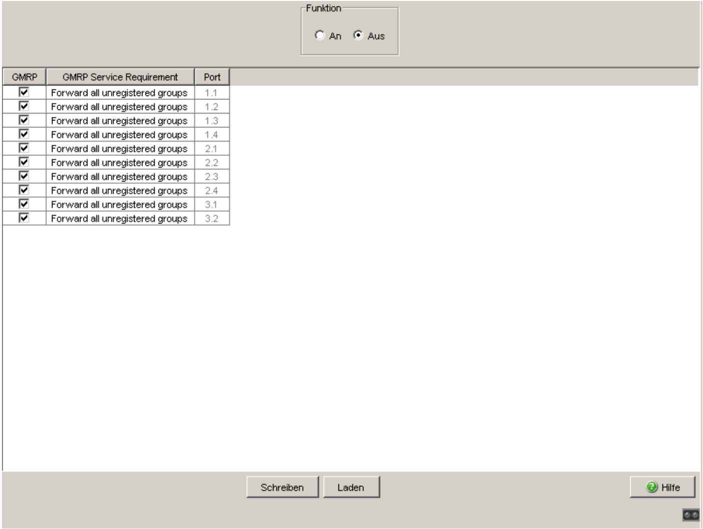
Button	Meaning
Set	Transfers the changes to the volatile memory (`RAM`) of the device. To permanently save the changes afterwards, you open the `Basic Settings:Load/Save` dialog and click "Save".
Reload	Updates the fields with the values that are saved in the volatile memory (`RAM`) of the device.
Help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

Table 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.



Funktion

○ An ● Aus

GMRP	GMRP Service Requirement	Port
☑	Forward all unregistered groups	1.1
☑	Forward all unregistered groups	1.2
☑	Forward all unregistered groups	1.3
☑	Forward all unregistered groups	1.4
☑	Forward all unregistered groups	2.1
☑	Forward all unregistered groups	2.2
☑	Forward all unregistered groups	2.3
☑	Forward all unregistered groups	2.4
☑	Forward all unregistered groups	3.1
☑	Forward all unregistered groups	3.2

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: ▶ 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	▶ 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 `Switching:Multicasts:GMRP` 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 – 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 `Switching:Multicasts:GMRP` 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 `Basic Settings:Load/Save` dialog and click "Save".
Reload	Updates the fields with the values that are saved in the volatile memory (`RAM`) of the device.
Help	Opens the online help.

Table 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 180 “VLAN Static”)
Max. supported VLANs	Displays the maximum number of VLANs (see on page 180 “VLAN Static”).
Number of VLANs	Displays the number of VLANs configured (see on page 180 “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 183 "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 **Note:** This setting is only effective for a core port. Access ports and normal ports ignore this setting and always use 8100_H	0 - 65535	33024 (8100_H)

Table 99: VLAN settings

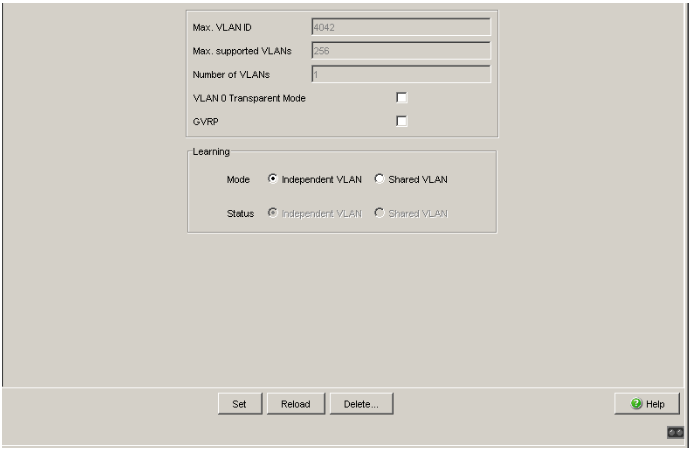
Note: If you are using the GOOSE protocol in accordance with IEC61850-8-1, then you activate the "VLAN 0 transparent mode". In this way, the prioritizing information remains in the data packet in accordance with IEEE802.1D/p when the device forwards the data packet.
This also applies to other protocols 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 RS20/RS30/RS40, MS20/MS30, RSR20/RSR30, MACH 100, MACH 1000 and OCTOPUS:
  In “Transparent mode”, the devices ignore the port VLAN ID set. Set the VLAN membership of the ports of VLAN 1 to `U` (Untagged) or `T` (Tagged), (see on page 180 “VLAN Static”).
- 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	Selecting the VLAN Mode. **“Independent VLAN”** subdivides the forwarding database (see on page 152 “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. **Application area:** Setting up identical networks that use the same MAC addresses. **“Shared VLAN”** uses the same forwarding database for all VLANs (see on page 152 “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. **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 63 “Restart”) is performed on the device, and the changes are then displayed in the line below under “Status”.	Independent VLAN, Shared VLAN	Independent VLAN
Status	Displays the current status. After a warm start (see on page 63 “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



Max. VLAN ID 4042

Max. supported VLANs 256

Number of VLANs 1

VLAN 0 Transparent Mode □

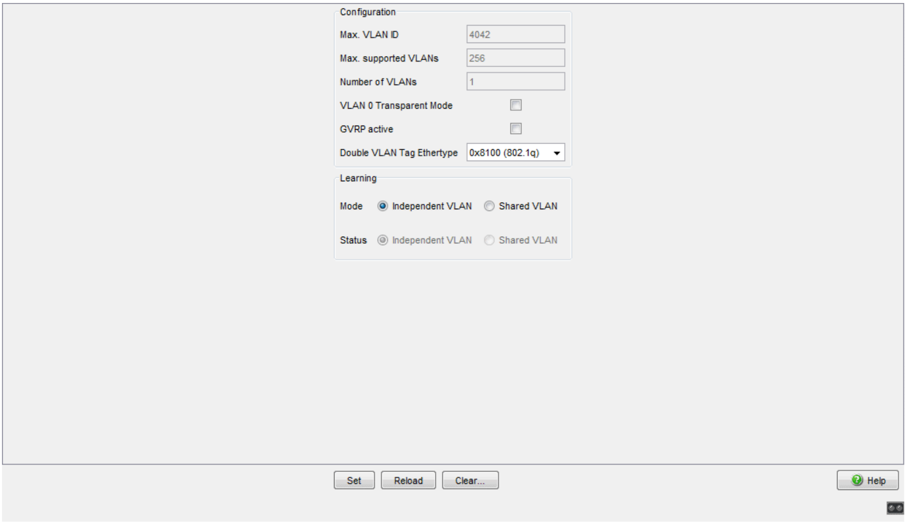
GVRP □

Learning

Mode ● Independent VLAN ○ Shared VLAN

Status ● Independent VLAN ○ Shared VLAN

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

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

Buttons

Button	Meaning
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 `Basic Settings:Network` 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

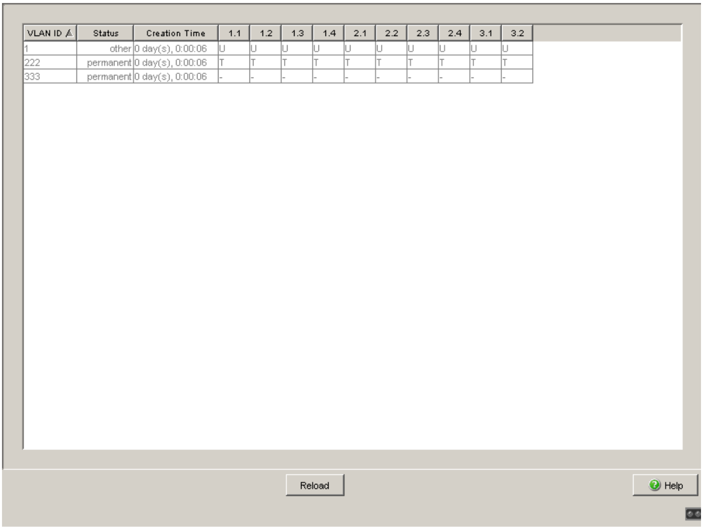
The Current VLAN table shows all
- manually configured VLANs
- VLANs configured via redundancy mechanisms
- VLANs configured via GVRP

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 180 “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.	`other`: This entry solely appears for VLAN 1. The system provides VLAN 1. VLAN 1 is always present. `permanent`: A static entry made by you. This entry is kept when the device is restarted. dynamic: This VLAN was created dynamically via GVRP.
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.	`-` Currently not a member `T` Member of VLAN; send data packets with tag. `U` Member of the VLAN; send data packets without tag (untagged). `F` Membership forbidden, so no entry possible via GVRP either.

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	-	-	-	-	-	-	-	-	-	-

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

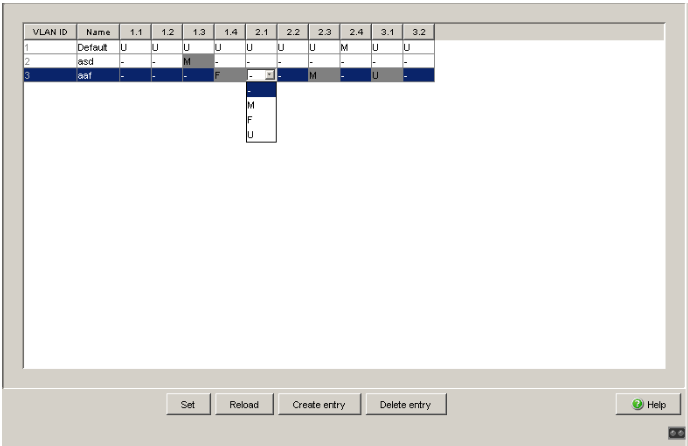
4.5.3 VLAN Static

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



VLAN ID	Name	1.1	1.2	1.3	1.4	2.1	2.2	2.3	2.4	3.1	3.2
1	Default	U	U	U	U	U	U	U	M	U	U
2	asd	-	-	M	-	-	-	-	-	-	-
3	aaf	-	-	-	F	-	-	M	-	U	-

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
Fast HIPER-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 `Basic Settings:Load/Save` dialog and click "Save".
Reload	Updates the fields with the values that are saved in the volatile memory (`RAM`) of the device.
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	- 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	- `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`

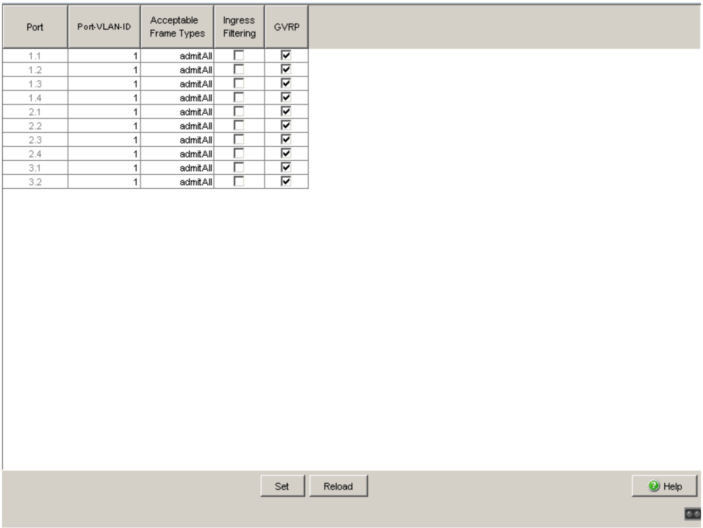
Table 107:`Switching:VLAN:Port` dialog

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:

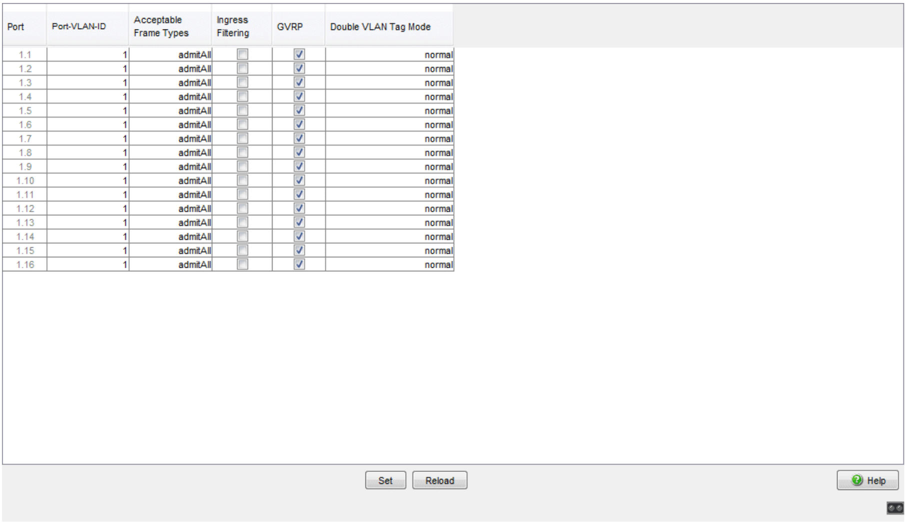
- HIPER-Ring
  Select the port VLAN ID 1 for the ring ports and deactivate “`Ingress Filtering`”.
- MRP-Ring
  - If the MRP-Ring configuration (see on page 220 “Configuring the MRP-Ring”) is not assigned to a VLAN, select the port VLAN ID 1.
  - If the MRP-Ring configuration (see on page 220 “Configuring the MRP-Ring”) is assigned to a VLAN, the device automatically performs the VLAN configuration for this port.

- Fast HIPER-Ring (RSR20, RSR30 and MACH 1000)
  - If the Fast HIPER-Ring configuration (see on page 227 “Configuring the Fast HIPER-Ring (RSR20, RSR30, MACH 1000)”) is not assigned to a VLAN, select the port VLAN ID 1.
  - If the Fast HIPER-Ring configuration (see on page 227 “Configuring the Fast HIPER-Ring (RSR20, RSR30, MACH 1000)”) 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	☐	☑
1.2	1	admitAll	☐	☑
1.3	1	admitAll	☐	☑
1.4	1	admitAll	☐	☑
2.1	1	admitAll	☐	☑
2.2	1	admitAll	☐	☑
2.3	1	admitAll	☐	☑
2.4	1	admitAll	☐	☑
3.1	1	admitAll	☐	☑
3.2	1	admitAll	☐	☑

Figure 53: `Switching:VLAN:Port` *dialog*



Port	Port-VLAN-ID	Acceptable Frame Types	Ingress Filtering	GVRP	Double VLAN Tag Mode
1.1	1	admitAll	☐	☑	normal
1.2	1	admitAll	☐	☑	normal
1.3	1	admitAll	☐	☑	normal
1.4	1	admitAll	☐	☑	normal
1.5	1	admitAll	☐	☑	normal
1.6	1	admitAll	☐	☑	normal
1.7	1	admitAll	☐	☑	normal
1.8	1	admitAll	☐	☑	normal
1.9	1	admitAll	☐	☑	normal
1.10	1	admitAll	☐	☑	normal
1.11	1	admitAll	☐	☑	normal
1.12	1	admitAll	☐	☑	normal
1.13	1	admitAll	☐	☑	normal
1.14	1	admitAll	☐	☑	normal
1.15	1	admitAll	☐	☑	normal
1.16	1	admitAll	☐	☑	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 `Basic Settings:Load/Save` dialog and click "Save".
Reload	Updates the fields with the values that are saved in the volatile memory (`RAM`) of the device.
Help	Opens the online help.

Table 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 301 “LLDP Information from Neighbor Devices”) and the LLDP-MED (see on page 303 “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. **Note:** To transmit the voice VLAN network policy you must have activated both the LLDP (see on page 301 “LLDP Information from Neighbor Devices”) and the LLDP-MED (see on page 303 “LLDP-MED (Media Endpoint Discovery)”).	`On`, `Off`	`Off`

Table 109:Global Settings for the Voice VLAN Dialog

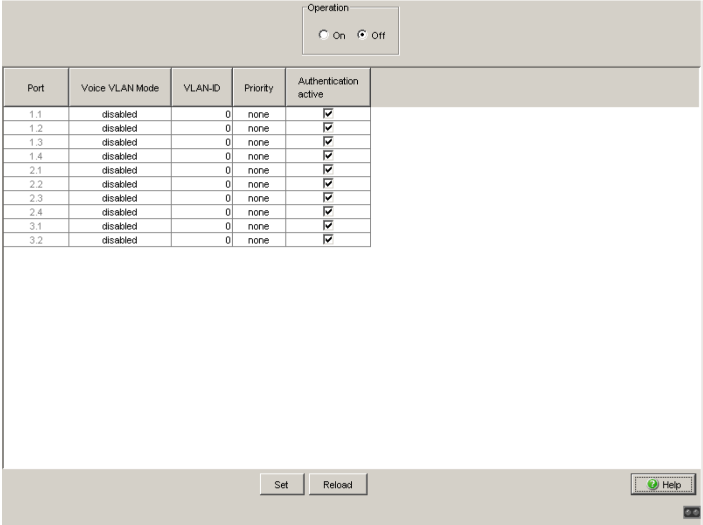
Parameters	Meaning	Possible values	Default setting
Port	Module and port numbers to which this entry applies	-	-
Voice VLAN Mode	Mode of the voice VLAN network policy which the Switch communicates via LLDP-MED to the devices connected. ▶ `disabled`: The Switch does not sent a voice VLAN network policy. ▶ `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. **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.	`0 - 4094`	`0`

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 authentification	▶ `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 - the device has identified itself via LLDP-MED as a voice device, and - the device sends tagged frames with the voice VLAN ID. **Note:** ▶ If you are using the authentication for a port, activate the 802.1X-based port security at this port (see on page 95 “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.	`On` `Off`	`On`

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 `Basic Settings:Load/Save` dialog and click "Save".
Reload	Updates the fields with the values that are saved in the volatile memory (`RAM`) of the device.
Help	Opens the online help.

Table 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

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 118).
- 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 116).

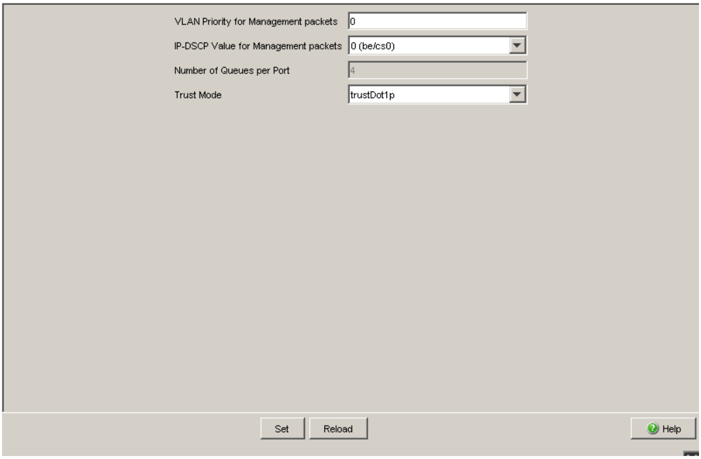
  Note: Certain DSCP values have DSCP names, such as be/cs0 to cs7 (class selector) or af11 to af43 (assured forwarding) and ef (expedited forwarding).

- display the maximum number of queues possible per port.
  The device supports 4 (8 for MACH 4000, MACH 104, MACH 1040 and PowerMICE) priority queues (traffic classes in compliance with IEEE 802.1D).
- select the trust mode globally (RS20/RS30/RS40, MS20/MS30, RSR20/RSR30, MACH 100, MACH 1000 and OCTOPUS). You use this to specify how the device handles received data packets that contain priority information.
  - “untrusted”
    The device ignores the priority information in the packet and always assigns the packets the port priority of the receiving port.
  - “trustDot1p”:
    The device prioritizes received packets that contain VLAN tag information according to this information (assigning them to a traffic class - see “802.1D/p mapping”).
    The device prioritizes received packets that do not contain any tag information (assigning them to a traffic class - see “Entering the port priority”) according to the port priority of the receiving port .
  - “trustIpDscp”:
    The device prioritizes received IP packets (assigning them to a traffic class - see “IP DSCP mapping”) according to their DSCP value.
    The device prioritizes received packets that are not IP packets (assigning them to a traffic class - see “Entering the port priority”) according to the port priority of the receiving port .
    For received IP packets:
    The device also performs VLAN priority remarking.
    In VLAN priority remarking, the device modifies the VLAN priority of the IP packets if the packets are to be sent with a VLAN tag (see on page 180 “VLAN Static”).
    Based on the traffic class to which the IP packet was assigned (see above), the device assigns the new VLAN priority to the IP packet in accordance with table 120.
    Example: A received IP packet with a DSCP value of 32 (cs4) is assigned to traffic class 2 (default setting). The packet was received at a port with port priority 2. Based on table 120, the VLAN priority is set to 4.

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

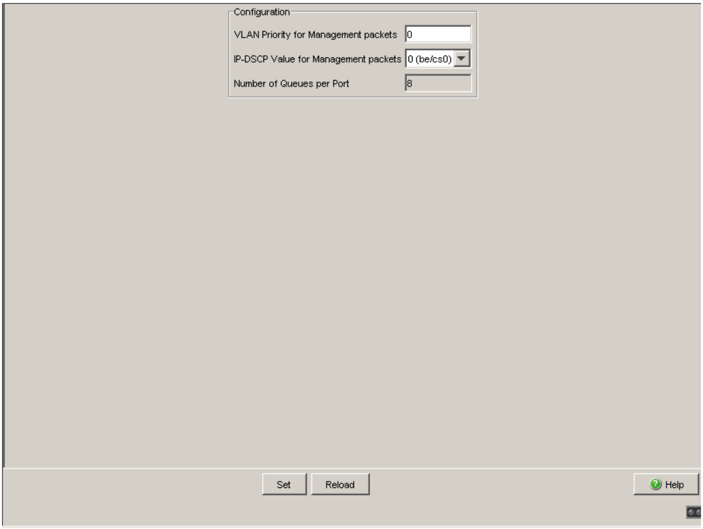
Traffic class	New VLAN priority when receiving port has an even port priority	New VLAN priority when receiving port has an odd port priority
0	0	1
1	2	3
2	4	5
3	6	7

Table 112:VLAN priority remarking



VLAN Priority for Management packets: 0
IP-DSCP Value for Management packets: 0 (be/cs0)
Number of Queues per Port: 4
Trust Mode: trustDot1p

Figure 56: Global dialog (RS20/RS30/RS40, MS20/MS30, RSR20/RSR30, MACH 100, MACH 1000 and OCTOPUS)



Configuration

VLAN Priority for Management packets: 0

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

Number of Queues per Port: 8

Figure 57: Global dialog (PowerMICE, MACH 104, MACH 1040 and MACH 4000)

Buttons

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

Table 113:Buttons

5.2 Port Configuration

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

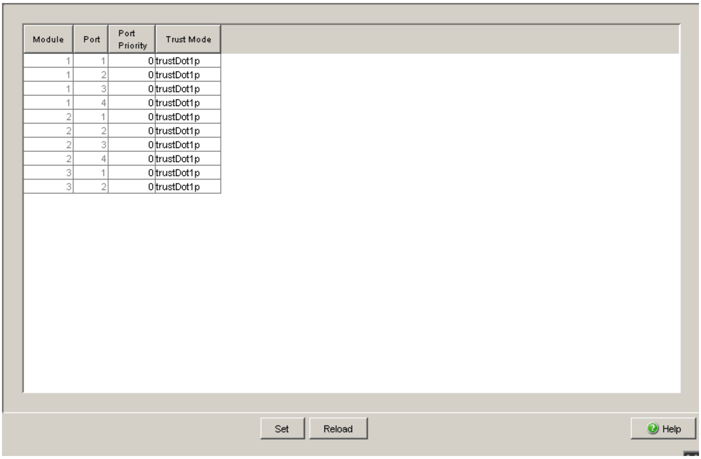
- assign a port priority to a port.
- select the trust mode for a port (PowerMICE, MACH 104, MACH 1040 and MACH 4000),
- display the untrusted traffic class (PowerMICE, MACH 104, MACH 1040 and MACH 4000),

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

Table 114:Port configuration table for RS20/RS30/RS40, MS20/MS30, RSR20/RSR30, MACH 1000 and OCTOPUS

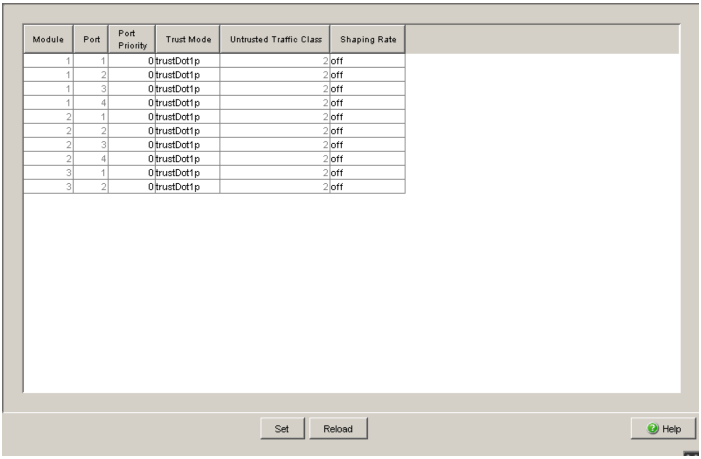
Parameter	Meaning
Module.Port	Port identification using module and port numbers of the device, e.g. 2.1 for port one of module two.
Port priority	Enter the port priority.
Trust mode	Select the trust mode.
Untrusted traffic class	Display the traffic class used in the “untrusted” trust mode.

Table 115:Port configuration table for PowerMICE, MACH 104, MACH 1040 and MACH 4000



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

Figure 58: Port configuration dialog for RS20/RS30/RS40, MS20/MS30, RSR20/RSR30, MACH 1000 and OCTOPUS



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 59: Port configuration dialog for PowerMICE, MACH 104, MACH 1040 and MACH 4000

5.2.1 Entering the port priority

□ RS20/RS30/RS40, MS20/MS30, RSR20/RSR30, MACH 100, MACH 1000 and OCTOPUS:
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 116).
Prerequisite:
Setting in the dialog `Global: Trust Mode: untrusted`(see on page 194 “Global”) or
Setting in the dialog `Global: Trust Mode: trustDot1p`(see on page 194 “Global”) and the data packets do not contain a VLAN tag or
Setting in the dialog `Global: Trust Mode: trustIpDscp`(see on page 194 “Global”) and the data packets are not IP packets.

□ Power MICE, MACH 104, MACH 1040 and MACH 4000:
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 116).
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 for RS20/RS30/RS40, MS20/MS30, RSR20/RSR30, MACH 100 MACH 1000, OCTOPUS (default setting)	Traffic Class for MACH 4000, MACH 104, MACH 1040 and PowerMICE (default setting)	IEEE 802.1D traffic type
0	1	2	Best effort (default)
1	0	0	Background
2	0	1	Standard
3	1	3	Excellent effort (business critical)
4	2	4	Controlled load (streaming multimedia)
5	2	5	Video, < 100 ms of latency and jitter

Table 116:Assigning the port priority to the traffic classes

Port priority	Traffic class for RS20/RS30/RS40, MS20/MS30, RSR20/RSR30, MACH 100 MACH 1000, OCTOPUS (default setting)	Traffic Class for MACH 4000, MACH 104, MACH 1040 and PowerMICE (default setting)	IEEE 802.1D traffic type
6	3	6	Voice, < 10 ms of latency and jitter
7	3	7	Network control reserved traffic

Table 116:Assigning the port priority to the traffic classes

5.2.2 Selecting the Trust Mode (PowerMICE, MACH 104, MACH 1040 and MACH 4000)

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 .
  - 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 120.
    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 120.

5.2.3 Displaying the untrusted traffic class (PowerMICE, MACH 104, MACH 1040 and MACH 4000)

“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 200 “Entering the port priority”), the untrusted traffic class also changes (see table 120).

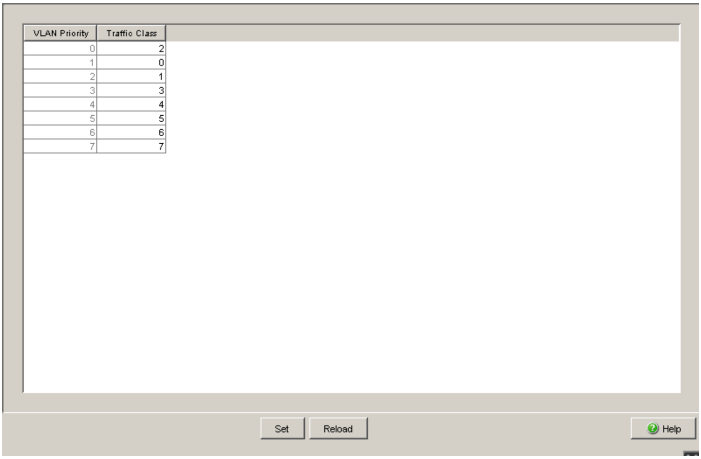
Buttons

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

Table 117:Buttons

5.3 802.1D/p mapping

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



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

Figure 60: 802.1D/p Mapping dialog

□ Enter following desired values in the Traffic Class field for every VLAN priority:

- between 0 and 3 for RS20/RS30/RS40, MS20/MS30, RSR20/RSR30, MACH 100, MACH 1000 and OCTOPUS
- between 0 and 7 for MACH 4000, MACH 104, MACH 1040 and PowerMICE.

VLAN priority	Traffic class for RS20/RS30/RS40, MS20/MS30, RSR20/RSR30, MACH 100, MACH 1000, OCTOPUS (default setting)	Traffic class for MACH 4000, MACH 104, MACH 1040 and PowerMICE (default setting)	IEEE 802.1D traffic type
0	1	2	Best effort (default)
1	0	0	Background
2	0	1	Standard
3	1	3	Excellent effort (business critical)
4	2	4	Controlled load (streaming multimedia)
5	2	5	Video, < 100 ms of latency and jitter
6	3	6	Voice, < 10 ms of latency and jitter
7	3	7	Network control reserved traffic

Table 118:Assigning the VLAN priority to the traffic classes

Note: Network protocols and redundancy mechanisms use the highest traffic classes 3 (RS20/30/40, MS20/30, RSR20/RSR30, MACH 100, MACH 1000, OCTOPUS) or 7 (PowerMICE, MACH 104, MACH 1040, MACH 4000). 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 `Basic Settings:Load/Save` dialog and click "Save".
Reload	Updates the fields with the values that are saved in the volatile memory (`RAM`) of the device.
Help	Opens the online help.

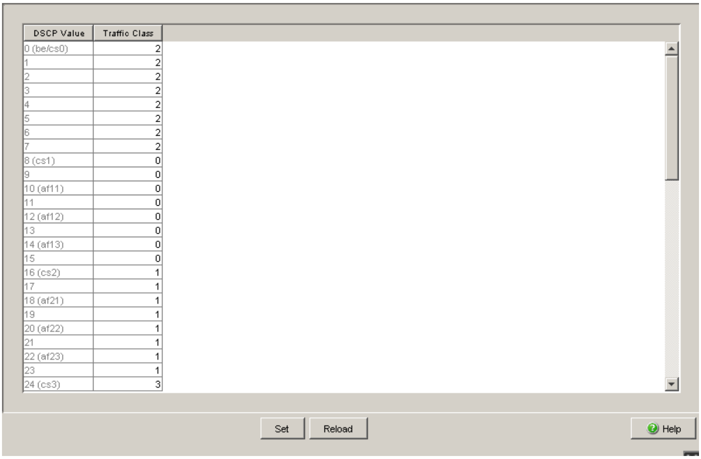
Table 119:Buttons

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 in the Traffic Class field for every DSCP value (0-63)

- ▶ between 0 and 3 for RS20/RS30/RS40, MS20/MS30, RSR20/RSR30, MACH 100, MACH 1000 and OCTOPUS
- ▶ between 0 and 7 for MACH 4000, MACH 104, MACH 1040 and PowerMICE.



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 61: 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 for RS20/RS30/RS40, MS20/MS30, RSR20/RSR30, MACH 100, MACH 1000, OCTOPUS (default setting)	Traffic class for MACH 4000 and PowerMICE (default setting)
0	Best Effort /CS0	1	2
1-7		1	2
8	CS1	0	0
9,11,13,15		0	0
10,12,14	AF11,AF12,AF13	0	0
16	CS2	0	1
17,19,21,23		0	1
18,20,22	AF21,AF22,AF23	0	1
24	CS3	1	3
25,27,29,31		1	3
26,28,30	AF31,AF32,AF33	1	3
32	CS4	2	4
33,35,37,39		2	4
34,36,38	AF41,AF42,AF43	2	4
40	CS5	2	5
41,42,43,44,45,47		2	5
46	EF	2	5
48	CS6	3	6
49-55		3	6

Table 120:Mapping the DSCP values onto the traffic classes

DSCP value	DSCP name	Traffic class for RS20/RS30/RS40, MS20/MS30, RSR20/RSR30, MACH 100, MACH 1000, OCTOPUS (default setting)	Traffic class for MACH 4000 and PowerMICE (default setting)
56	CS7	3	7
57-63		3	7

Table 120: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 Basic Settings:Load/Save dialog and click "Save".
Reload	Updates the fields with the values that are saved in the volatile memory (RAM) of the device.
Help	Opens the online help.

Table 121:Buttons

6 Redundancy

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

- Link Aggregation
- Ring Redundancy
- Sub-Ring
- Ring/Network coupling
- Spanning Tree

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

6.1 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.

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.

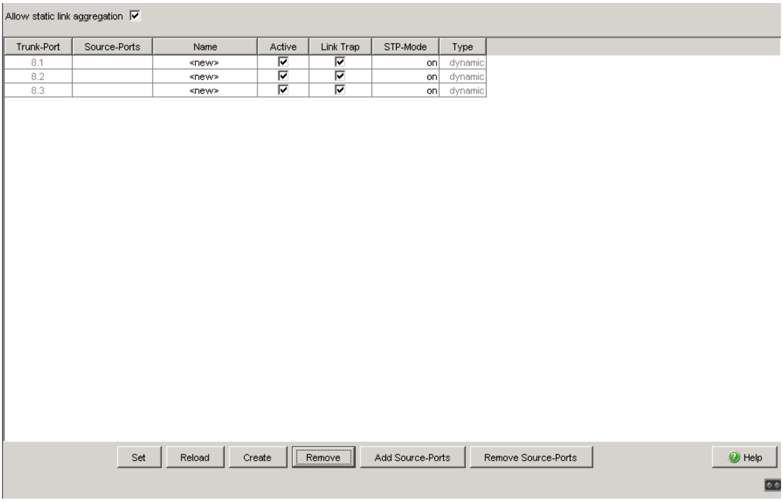
Note: Exclude the combination of a link aggregation with the following redundancy procedures:

- Network/Ring coupling
- MRP-Ring
- Fast HIPER-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 `Allow static link aggregation` 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 `on` if you have integrated the link aggregation into a Spanning Tree, or `off` if you have not.
Type	`- manual` The partner device does not support LACP, and you have selected “Allow static link aggregation”. `- dynamic` Both devices support LACP and you have not selected “Allow static link aggregation”. **Note:** If there are multiple connections between devices that all support LACP, the device displays `dynamic` even if “Allow static link aggregation” was selected. In this case, the devices automatically switch to dynamic.

Table 122:Link Aggregation



Allow static link aggregation ☑

Trunk-Port	Source-Ports	Name	Active	Link Trap	STP-Mode	Type
8.1		<new>	☑	☑	on	dynamic
8.2		<new>	☑	☑	on	dynamic
8.3		<new>	☑	☑	on	dynamic

Figure 62: 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 214 “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 `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.
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 123:Buttons

6.2 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-(**HI**GH **PE**RFORMANCE **R**EDUNDANCY) Ring with up to 50 devices typically transforms back to a line structure within 80 ms (possible settings: standard/accelerated).
- MRP (**M**edia **R**edundancy **P**rotocol) Ring (IEC 62439) of up to 50 devices typically transforms back to a line structure within 80 ms (adjustable to max. 200 ms/500 ms).
- Fast HIPER-Ring of up to 5 devices typically transforms back to a line structure within 5 ms (maximum 10 ms). With a larger number of devices, the reconfiguration time increases.

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

- Within a HIPER-Ring, you can use any combination of the following devices:
  - RS2-./.
  - RS2-16M
  - RS2-4R
  - RS20, RS30, RS40
  - 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 223 “Advanced Ring Configuration/Diagnostics (ARC)”).

Parameter	Meaning

Version	Select the Ring Redundancy version you want to use:
	`HIPER-Ring`
	`MRP`
	`FAST HIPER-Ring` (RSR20/30, MACH 1000)

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 124:Ring Redundancy basic configuration

6.2.1 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)

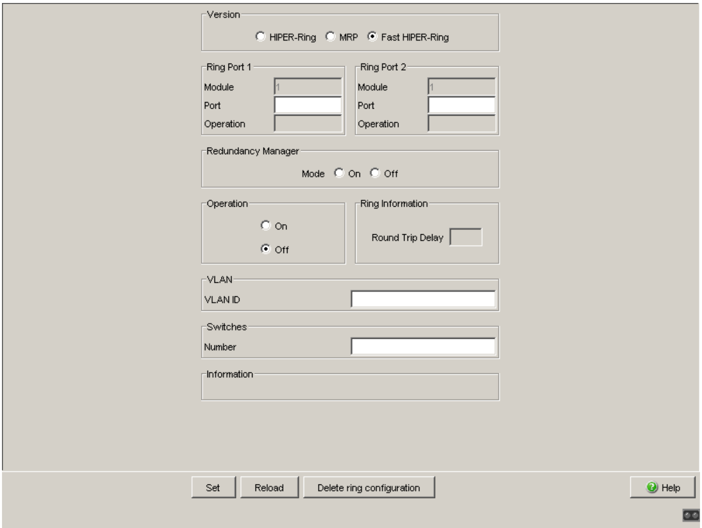
Table 125:Port settings for ring ports

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: `active`: This port is switched on and has a link. `inactive`: This port is switched off or it has no link.
Ring Manager Status	Status information, no input possible: `Active (redundant line)`: The redundant line was closed because a data line or a network component within the ring failed. `Inactive`: The redundant ring is open, and all data lines and network components are working.
Ring Manager Mode	If there is exactly one device, you switch the Ring Manager function on at the ends of the line.
Ring Recovery	The settings in the ”Ring Recovery“ frame are only effective for devices that are ring managers. In the ring manager, select the desired value for the test packet timeout for which the ring manager waits after sending a test packet before it evaluates the test packet as lost. ▶ `Standard`: test packet timeout 480 ms ▶ `Accelerated`: test packet timeout 280 ms **Note:** The settings are especially meaningful if at least one line in the ring consists of a 1,000 MBit/s twisted pair line. The reconfiguration time after connection interruption existing due to the reaction characteristic of 1,000 MBit/s twisted pair ports can thus be accelerated considerably.
Information	If the device is a ring manager: The displays in this frame mean: “Redundancy working”: When a component of the ring is down, the redundant line takes over its function. “Configuration failure”: You have configured the function incorrectly, or there is no ring port connection.

Table 126:HIPER-Ring configuration



Version: ○ HIPER-Ring ○ MRP ● Fast HIPER-Ring

Ring Port 1: Module 1, Port, Operation

Ring Port 2: Module 1, Port, Operation

Redundancy Manager: Mode ○ On ○ Off

Operation: ○ On ● Off

Ring Information: Round Trip Delay

VLAN: VLAN ID

Switches: Number

Information

Figure 63: Selecting HIPER-Ring version, entering ring ports, enabling/disabling ring manager and selecting ring recovery (RSR20, RSR30, MACH 1000)

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` 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.

6.2.2 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 127: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.

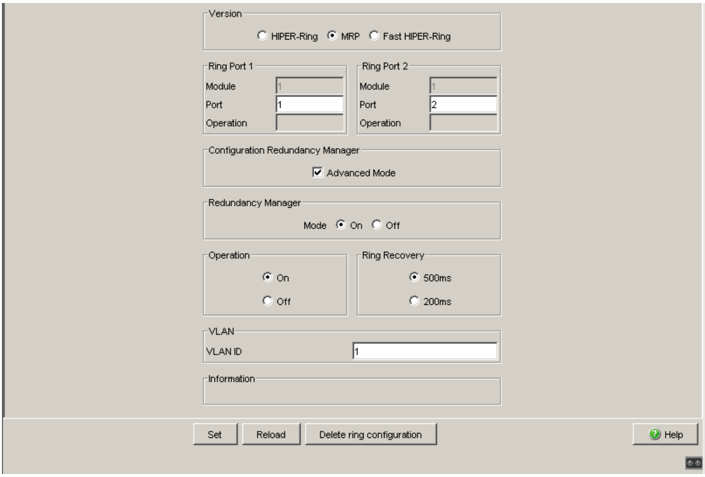
□ Check the VLAN configuration of the ring ports: For all ring ports in this MRP-Ring, select this corresponding VLAN ID and the VLAN membership T in the static VLAN table.

□ 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: `forwarding`: This port is switched on and has a link. `blocked`: This port is blocked and has a link. `disabled`: This port is switched off. `not connected`: This port has no link.
Ring Manager Mode	If there is exactly one device, you switch the Ring Manager function on at the ends of the line.
Operation	When you have configured all the parameters for the MRP-Ring, you switch the operation on with this setting. When you have configured all the devices in the MRP-Ring, you close the redundant line.
Ring Recovery	For the device for which you have activated the ring manager, select the value 200 ms if the stability of the ring meets the requirements for your network. Otherwise select 500 ms. `Note`: Settings in the “Ring Recovery” frame are only effective for devices that are ring managers.
VLAN ID	If you have configured VLANs, then here you select: ▶ `VLAN ID 0` if you do not want to assign the MRP-Ring configuration to any VLAN. Note the VLAN configuration of the ring ports: Select VLAN ID 1 and VLAN membership `U` in the static VLAN table for the ring ports. ▶ `VLAN ID > 0` if you want to assign the MRP-Ring configuration to this VLAN. Select this VLAN ID in the MRP-Ring configuration for all devices in this MRP-Ring.Note the VLAN configuration of the ring ports: For all ring ports in this MRP-Ring, select this corresponding VLAN ID and the VLAN membership `T` 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 128:MRP-Ring configuration



Version: ○ HIPER-Ring ● MRP ○ Fast HIPER-Ring

Ring Port 1

Module	1
Port	1
Operation	

Ring Port 2

Module	1
Port	2
Operation	

Configuration Redundancy Manager: ☑ Advanced Mode

Redundancy Manager: Mode ● On ○ Off

Operation: ● On ○ Off

Ring Recovery: ● 500ms ○ 200ms

VLAN: VLAN ID 1

Information

Figure 64: Selecting MRP-Ring version, entering ring ports and enabling/disabling ring manager (RSR20, RSR30, MACH 1000)

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-volatilely.

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.

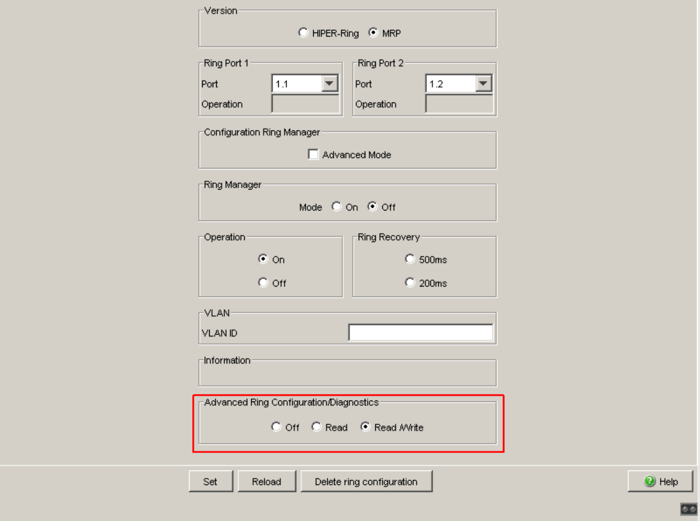
▶ Physical Topology:
- You connected the devices to a physical ring.

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 244 “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 258 “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.



Version
○ HIPER-Ring ● MRP

Ring Port 1
Port 1.1
Operation

Ring Port 2
Port 1.2
Operation

Configuration Ring Manager
□ Advanced Mode

Ring Manager
Mode ○ On ● Off

Operation
● On
○ Off

Ring Recovery
○ 500ms
○ 200ms

VLAN
VLAN ID

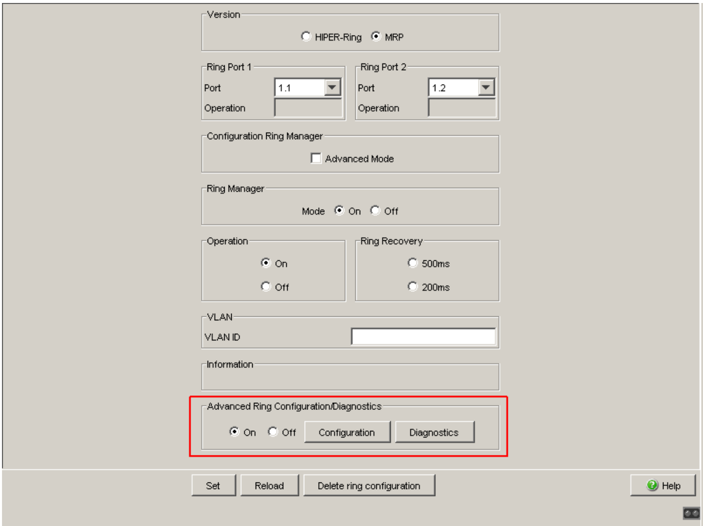
Information

Advanced Ring Configuration/Diagnostics
○ Off ○ Read ● Read /Write

Figure 65: 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.



Version: ○ HIPER-Ring ● MRP

Ring Port 1: Port 1.1, Operation

Ring Port 2: Port 1.2, Operation

Configuration Ring Manager: ☐ Advanced Mode

Ring Manager: Mode ● On ○ Off

Operation: ● On ○ Off

Ring Recovery: ○ 500ms ○ 200ms

VLAN: VLAN ID

Information

Advanced Ring Configuration/Diagnostics: ● On ○ Off

Figure 66: Ring Redundancy Dialog, Advanced Ring Configuration/Diagnostics of an MRP manager.

6.2.3 Configuring the Fast HIPER-Ring (RSR20, RSR30, MACH 1000)

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 129:Port settings for ring ports

Note: Configure all the devices of the Fast HIPER-Ring individually. Before you connect the redundant line, you must have completed the configuration of all the devices of the Fast HIPER-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.

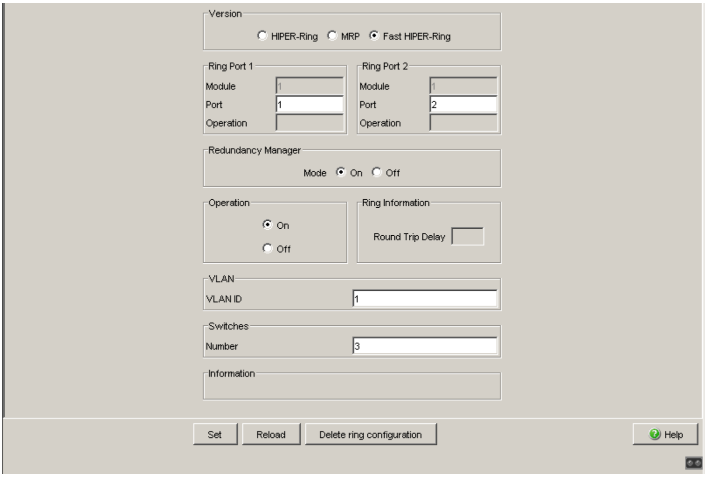
□ Check the VLAN configuration of the ring ports: For all ring ports in this MRP-Ring, select this corresponding VLAN ID and the VLAN membership `T` in the static VLAN table.

□ 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: `forwarding`: This port is switched on and has a link. `blocked`: This port is blocked and has a link. `disabled`: This port is switched off. `not connected`: This port has no link.
Ring Manager 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	`Round Trip Delay`: 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 `VLAN ID 0` 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 `U` in the static VLAN table for the ring ports. `VLAN ID > 0` 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 `T` 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 130:Fast HIPER-Ring configuration



Version: ○ HIPER-Ring ○ MRP ● Fast HIPER-Ring

Ring Port 1: Module 1, Port 1, Operation

Ring Port 2: Module 1, Port 2, Operation

Redundancy Manager: Mode ● On ○ Off

Operation: ● On ○ Off

Ring Information: Round Trip Delay

VLAN: VLAN ID 1

Switches: Number 3

Information

Figure 67: 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 `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.
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 131:Buttons

6.3 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 220 "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.

6.3.1 Sub-Ring configuration

Parameters	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: (8)	-
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.		
Redundancy existing	A symbol displays whether the redundancy exists.		

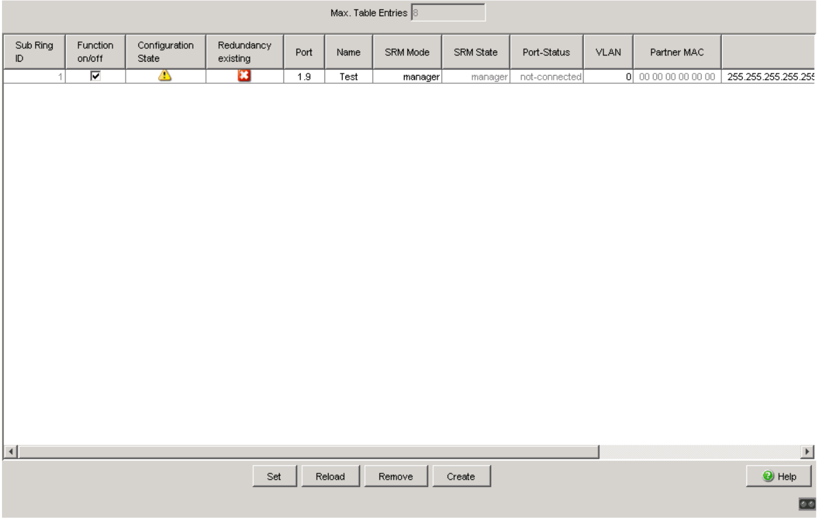
Table 132:Sub-Ring basic configuration

Parameters	Meaning	Possible values	Default setting
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 (`Redundant Manager` mode) 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. `SingleManager` 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
SRM State	Actual state: Shows whether this SRM manages the redundant connection (`Redundant Manager` mode) 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. `SingleManager` 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
Port Status	Connection status of the Sub-Ring port	forwarding disabled blocked not connected	
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	-
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

Table 132:Sub-Ring basic configuration

Parameters	Meaning	Possible values	Default setting
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
Protocol		`standardMRP`	`standardMRP`

Table 132:Sub-Ring basic configuration



Max. Table Entries 8

Sub Ring ID	Function on/off	Configuration State	Redundancy existing	Port	Name	SRM Mode	SRM State	Port-Status	VLAN	Partner MAC	
1	☑	⚠	☒	1.9	Test	manager	manager	not-connected	0	00 00 00 00 00 00	255.255.255.255.255

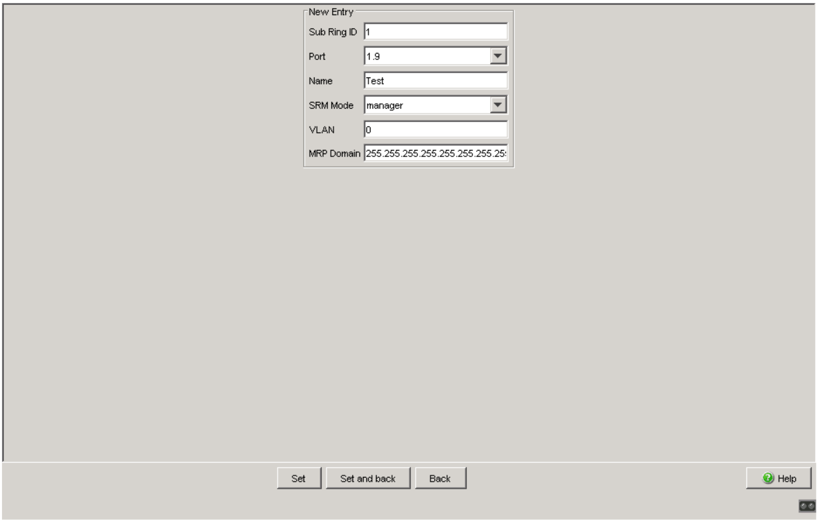
Figure 68: Sub-Ring basic configuration

6.3.2 Sub-Ring – New Entry

Parameters	Meaning	Possible values	Default setting
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 (`Redundant Manager` mode) 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. `SingleManager` 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. 255.255.255. 255

Table 133:Sub-Ring - New Entry

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



New Entry

Sub Ring ID	1
Port	1.9
Name	Test
SRM Mode	manager
VLAN	0
MRP Domain	255.255.255.255.255.255.255.25

Figure 69: 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 `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.
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 134:Buttons

6.4 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

6.4.1 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.

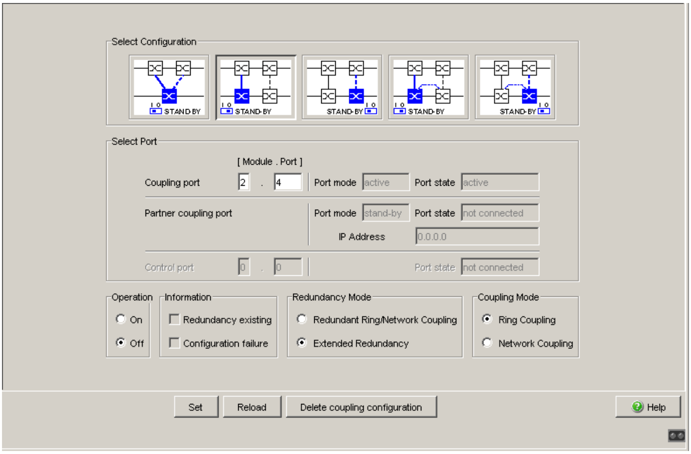
Device type	STAND-BY switch type
RS2-./.	DIP switch
RS2-16M	DIP switch
RS20/RS30/RS40	Selectable: DIP switch and software setting
MICE/Power MICE	Selectable: DIP switch and software setting
MS20/MS30	Selectable: DIP switch and software setting
OCTOPUS	Software switch
RSR20/RSR30	Software switch
MACH 100	Software switch
MACH 1000	Software switch
MACH 3000/MACH 4000	Software switch

Table 135: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 - `Redundancy:Ring/Network Coupling` 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 `Redundancy:Ring/Network Coupling` dialog

Table 136:Setting the STAND-BY switch



Select Port

[Module . Port]

Coupling port 2 . 4 Port mode active Port state active

Partner coupling port Port mode stand-by Port state not connected

IP Address 0.0.0.0

Control port 0 . 0 Port state not connected

Operation: ○ On ● Off

Information: □ Redundancy existing □ Configuration failure

Redundancy Mode: ○ Redundant Ring/Network Coupling ● Extended Redundancy

Coupling Mode: ● Ring Coupling ○ Network Coupling

Figure 70: 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
Coupling port	This is the port to which you have connected a redundant connection. **Note:** Configure the coupling port and the ring ports, if there are any ring ports, on different ports. **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.
Port mode	- `active:` You have switched the port on. - `stand-by:` The port is in stand-by mode.
Port State	- `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	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. **Note:** Configure the partner coupling port and the ring ports, if there are any ring ports, on different ports.
IP address	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.
Control port	This is the port to which you connect the control line.
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 Fast HIPER-Ring), or network segments.

Table 137: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 138: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 `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.

Table 139:Buttons

Button	Meaning
Delete Coupling configuration	Removes the coupling configuration.
Help	Opens the online help.

Table 139:Buttons (cont.)

6.5 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 a 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.

6.5.1 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 Tress settings for the bridge.

Parameter s	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 140: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 s	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 141:Global Spanning Tree settings, local bridge parameters

Parameter s	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 ≤ n*4096 ≤ 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 141:Global Spanning Tree settings, local bridge parameters

Parameters	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 152). 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 141: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:

Forward Delay ≥ (Max Age/2) + 1

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

Parameter s	Meaning	Possible values	Default setting
Column „Root“	**Information on the device that is currently the root bridge**		
Bridge ID	The Bridge ID 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 Priority of the current root bridge.	0 ≤ n*4096 ≤ 61440	32768
Hello Time	The Hello Time of the current root bridge.	1 - 2	2
Forward Delay	The Forward Delay of the current root bridge.	4 - 30 s	15 s
Max Age	The Max Age of the current root bridge.	6 - 40 s	20 s

Table 142: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 143:Global Spanning Tree settings, topology information

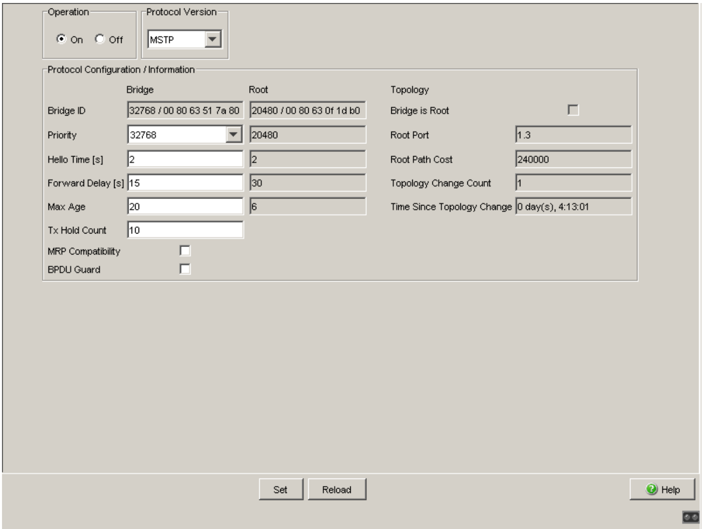
Parameters	Meaning	Possible values
Topology change count	Counts how often the device has put a port into the `Forwarding` status via Spanning Tree since it was started.	
Time since last change	Time since the last topology change.	

Table 143: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:

Parameters	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 144:Global Spanning Tree settings, Information frame



Operation: ● On ○ Off

Protocol Version: MSTP

Protocol Configuration / Information

	Bridge	Root
Bridge ID	32768 / 00 80 63 51 7a 80	20480 / 00 80 63 0f 1d b0
Priority	32768	20480
Hello Time [s]	2	2
Forward Delay [s]	15	30
Max Age	20	6
Tx Hold Count	10	
MRP Compatibility	□	
BPDU Guard	□	

Topology	
Bridge is Root	□
Root Port	1.3
Root Path Cost	240000
Topology Change Count	1
Time Since Topology Change	0 day(s), 4:13:01

Figure 71: 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 `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 145:Buttons

6.5.2 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 146: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 `Bridge ID` 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 `Bridge ID` 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 147:Dialog Multiple Spanning Tree settings, MST Global (CIST), Global MST parameters

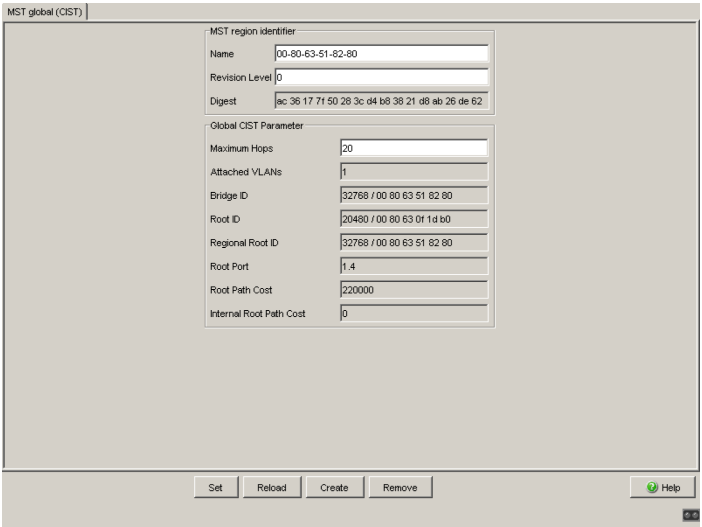
Parameters	Meaning	Possible values	Default setting
Root path costs	External path costs from the regional root bridge of the MST region of the device to the current root bridge of the entire layer 2 network (CIST root).[c] These are the same for all devices within an MST region. 0: Regional root bridge 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 147: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).



MST region identifier

Name: 00-80-63-51-82-80

Revision Level: 0

Digest: ac 36 17 7f 50 28 3c d4 b8 38 21 d8 ab 26 de 62

Global CIST Parameter

Maximum Hops: 20

Attached VLANs: 1

Bridge ID: 32768 / 00 80 63 51 82 80

Root ID: 20480 / 00 80 63 0f 1d b0

Regional Root ID: 32768 / 00 80 63 51 82 80

Root Port: 1.4

Root Path Cost: 220000

Internal Root Path Cost: 0

Figure 72: 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 148: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	

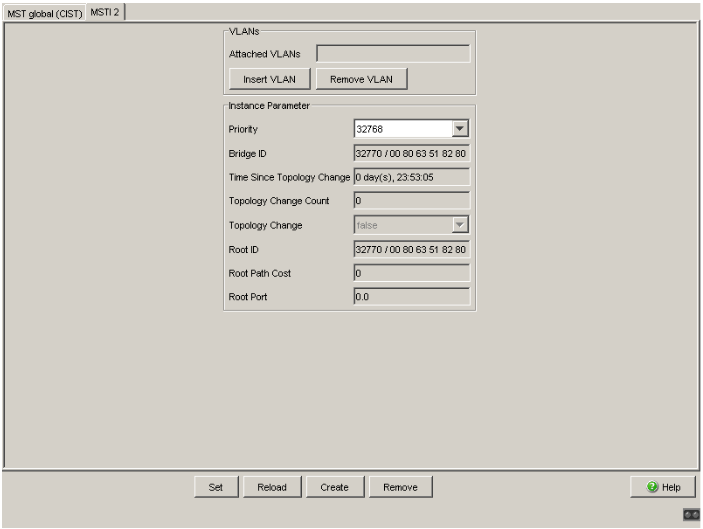
Table 148:Multiple Spanning Tree settings, MST Instance, VLANs

Parameters	Meaning	Possible values	Default setting
Frame „Instance Parameters“	Detailed information on the selected Multiple Spanning Tree Instance.		
Priority	The local bridge `Priority` for the selected MST Instance. The bridge priority and its own MAC address make up this separate `Bridge ID`. 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 `Bridge ID` among all the devices in the selected MST region. Enter the value as a multiple of 4096.	0 ≤ n*4096 ≤ 61440	32768
Bridge ID	The local `Bridge ID`, made up of the local `priority` + MSTI, following by its own MAC address. The format is ppppp / mm mm mm mm mm mm, with: ppppp: priority+MSTI (decimal) and mm: the respective byte of the MAC address (hexadecimal).	0 - 65534; sum of priority (0 - 61440 in steps of 4096) and MSTI (1 - 4094)	32768 + MSTI
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 `Forwarding` status via Spanning Tree since the selected MST Instance was started.		
Root ID	The `Bridge ID` of the current root bridge of the selected MST region. The format is ppppp / mm mm mm mm mm mm, with: ppppp: priority (decimal) and mm: the respective byte of the MAC address (hexadecimal).	0 - 65534; sum of priority (0 - 61440 in steps of 4096) and MSTI (1 - 4094)	

Table 149: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 149:Multiple Spanning Tree settings, MST Instance, parameters



Attached VLANs:

Priority: 32768

Bridge ID: 32770 / 00 80 63 51 82 80

Time Since Topology Change: 0 day(s), 23:53:05

Topology Change Count: 0

Topology Change: false

Root ID: 32770 / 00 80 63 51 82 80

Root Path Cost: 0

Root Port: 0.0

Figure 73: 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 `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.
Create	Adds a MSTP instance.
Remove	Removes a MSTP instance.
Help	Opens the online help.

Table 150:Buttons

6.5.3 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. **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.	`On`, `Off`	`On`
Port status (read only)	Displays the STP port status with regard to the global MSTI (IST).	`discarding`, `learning`, `forwarding`, `disabled`, `manualForwarding`, `notParticipate`	-

Table 151: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 ≤ n·16 ≤ 240	128
Received bridge ID (read only)	Displays the remote bridge ID from which this port last received an STP-BPDU.[a]	Bridge identification (format ppppp / mm mm mm mm mm mm)	-
Received port ID (read only)	Displays the port ID at the remote bridge from which this port last received an STP-BPDU.[a]	Port ID, format pn nn, with p: port priority / 16, nnn: port No., (both hexadecimal)	-
Received path costs (read only)	Displays the path costs of the remote bridge from its root port to the CIST root bridge.[a]	0-200000000	-

Table 151:Port-related STP settings and displays, CIST

Parameters	Meaning	Possible values	Default setting
Admin Edge Port	Only activate this setting when a terminal device is connected to the port (administrative: default setting). Then the port immediately has the forwarding status after a link is set up, without first going through the STP statuses. If the port still receives an STP-BPDU, the device blocks the port and clarifies its STP port role. In the process, the port can switch to a different status, e.g. `forwarding`, `discarding`, `learning`. Deactivate the setting when the port is connected to a bridge. After a link is set up, the port then goes through the STP statuses first before taking on the `forwarding` status, if applicable. This setting applies to all MSTIs.	`active` (box selected), `inactive` (box empty)	`inactive`
Auto Edge Port	The device only considers the Auto Edge Port setting when the Admin Edge Port parameter is deactivated. If Auto Edge Port is active, after a link is set up the device sets the port to the forwarding status after 1.5 · `Hello Time` (in the default setting 3 s). If Auto Edge Port is deactivated, the device waits for the `Max Age` instead (in the default setting 20 s). This setting applies to all MSTIs.	`active` (box selected), `inactive` (box empty)	`active`

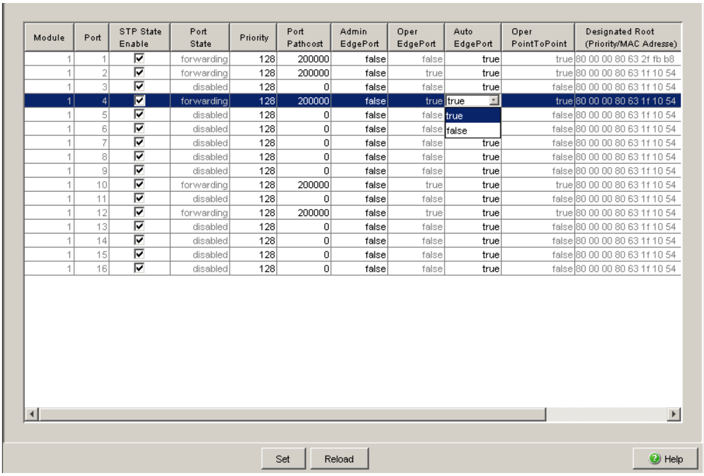
Table 151:Port-related STP settings and displays, CIST

Parameters	Meaning	Possible values	Default setting
Oper Edge Port	The device sets the “Oper Edge Port” condition to `true` if it has not received any STP-BPDUs, i.e. a terminal device is connected. It sets the condition to `false` if it has received STP-BPDUs, i.e. a bridge is connected. This condition applies to all MSTIs.	`true`, `false`	-
Oper PointToPoint	The device sets the “Oper point-to-point” condition to `true` if this port has a full duplex condition to an STP device. Otherwise it sets the condition to `false` (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.	`true`, `false` The device determines this condition from the duplex mode: FDX: `true` HDX: `false`	

Table 151: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	☑	forwarding	128	200000	false	false	true	true	80 00 00 80 63 2f fb b8
1	2	☑	forwarding	128	200000	false	true	true	true	80 00 00 80 63 1f 10 54
1	3	☑	disabled	128	0	false	false	true	false	80 00 00 80 63 1f 10 54
1	4	☑	forwarding	128	200000	false	true	true	true	80 00 00 80 63 1f 10 54
1	5	☑	disabled	128	0	false	false	true	false	80 00 00 80 63 1f 10 54
1	6	☑	disabled	128	0	false	false	false	false	80 00 00 80 63 1f 10 54
1	7	☑	disabled	128	0	false	false	true	false	80 00 00 80 63 1f 10 54
1	8	☑	disabled	128	0	false	false	true	false	80 00 00 80 63 1f 10 54
1	9	☑	disabled	128	0	false	false	true	false	80 00 00 80 63 1f 10 54
1	10	☑	forwarding	128	200000	false	true	true	true	80 00 00 80 63 1f 10 54
1	11	☑	disabled	128	0	false	false	true	false	80 00 00 80 63 1f 10 54
1	12	☑	forwarding	128	200000	false	true	true	true	80 00 00 80 63 1f 10 54
1	13	☑	disabled	128	0	false	false	true	false	80 00 00 80 63 1f 10 54
1	14	☑	disabled	128	0	false	false	true	false	80 00 00 80 63 1f 10 54
1	15	☑	disabled	128	0	false	false	true	false	80 00 00 80 63 1f 10 54
1	16	☑	disabled	128	0	false	false	true	false	80 00 00 80 63 1f 10 54

Figure 74: 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 152:Port-related STP settings and displays, guards

Parameters	Meaning	Possible values	Default setting
Root Guard	The “Root Guard” setting is only relevant for ports with the STP role `designated`. If such a port receives an STP-BPDU with better path information on the root that what the device knows, the device discards the BPDU and sets the port status to `discarding`, instead of assigning the port the STP port role `root`. 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. **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.	`active` (box selected), `inactive` (box empty)	`inactive`
TCN Guard	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. **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.	`active` (box selected), `inactive` (box empty)	`inactive`

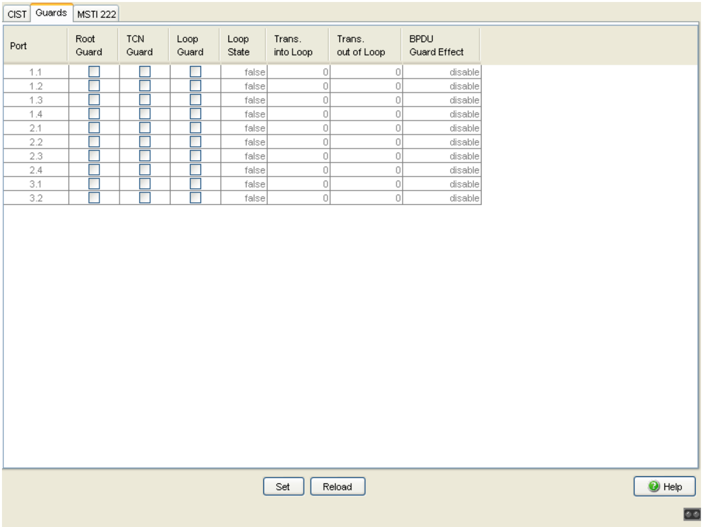
Table 152:Port-related STP settings and displays, guards

Parameters	Meaning	Possible values	Default setting
Loop Guard	The “Loop Guard” setting is only meaningful for ports with the STP role alternate, backup or root. 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 discarding condition (port sends no more data). The device also sets the port to what is known as the “loop inconsistent status” and displays this in the “Loop Status” column. 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. When the port receives BPDUs again, the device resets the loop status of the port to false, and the transmission status of the port according to the port role. If the “Loop Guard” setting is inactive, however, the device sets the port to the forwarding status when STP-BPDUs have not been received. **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.	active (box selected), inactive (box empty)	inactive
Loop State (read only)	Display the status of the Loop Status. The device sets the loop status of the port to true if the “Loop Guard” setting is active at the port and the port is not receiving any more STP-BPDUs. Here the device leaves the port in the discarding transmission status, thus helping to prevent a potential loop. When the port receives STP-BPDUs again, the device resets the loop status to false.	true, false	-
Transitions to Loop Status (read only)	Counts how often the device has set the port to the loop status (“Loop Status” column true).	0 - 4294967295 (2^{32}-1)	0

Table 152: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 `true`).	0 - 4294967295 (2^{32}-1)	0
BPDU Guard Effect (read only)	The “BPDU Guard Effect” status is only relevant for edge ports (ports with the “Admin Edge Port” status `true`), and only if the “BPDU Guard” global function is active (see table 141). When such a port receives any random STP-BPDU, the device sets the port's “BPDU Guard Effect” status to `true` and its transmission status to `discarding`. 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. 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.	`true`, `false`	-

Table 152:Port-related STP settings and displays, guards



Port	Root Guard	TCN Guard	Loop Guard	Loop State	Trans. into Loop	Trans. out of Loop	BPDU Guard Effect
1.1	☐	☐	☐	false	0	0	disable
1.2	☐	☐	☐	false	0	0	disable
1.3	☐	☐	☐	false	0	0	disable
1.4	☐	☐	☐	false	0	0	disable
2.1	☐	☐	☐	false	0	0	disable
2.2	☐	☐	☐	false	0	0	disable
2.3	☐	☐	☐	false	0	0	disable
2.4	☐	☐	☐	false	0	0	disable
3.1	☐	☐	☐	false	0	0	disable
3.2	☐	☐	☐	false	0	0	disable

Figure 75: 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`	-

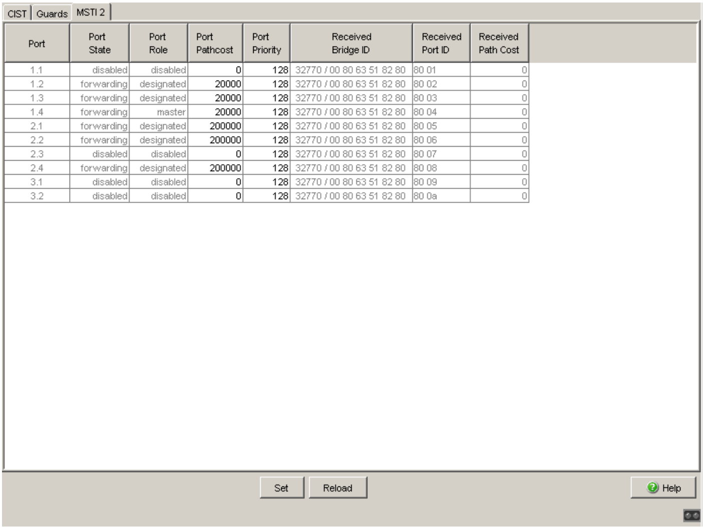
Table 153:Port-related STP settings and displays, per MSTI

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 ≤ n*16 ≤ 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 153: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 76: 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 `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 154:Buttons

7 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
- Service Mode

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

7.1 Syslog

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

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

Note: You will find the actual events that the device has logged in the “Trap Log” dialog (see on page 276 “Trap log”) and in the log file (see on page 323 “Event Log”). The device evaluates SNMP requests as events if you have activated “Log SNMP Set/Get Request” (see table 156).

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 155: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 155: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`
		`emercency`
			critical

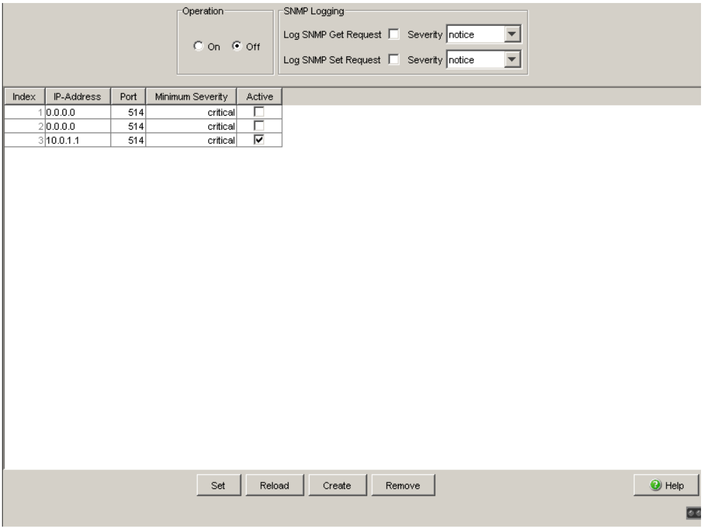
Active	Activate or deactivate the current syslog server entry in the table.	`active` (box selected) `inactive` (box empty)	inactive

Table 156: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.
- Only 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.
- Only set the minimum severity for one or more syslog server entries to `notice` or lower. Then it may happen that the device sends a large number of 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	□
2	0.0.0.0	514	critical	□
3	10.0.1.1	514	critical	☑

Figure 77: Syslog dialog

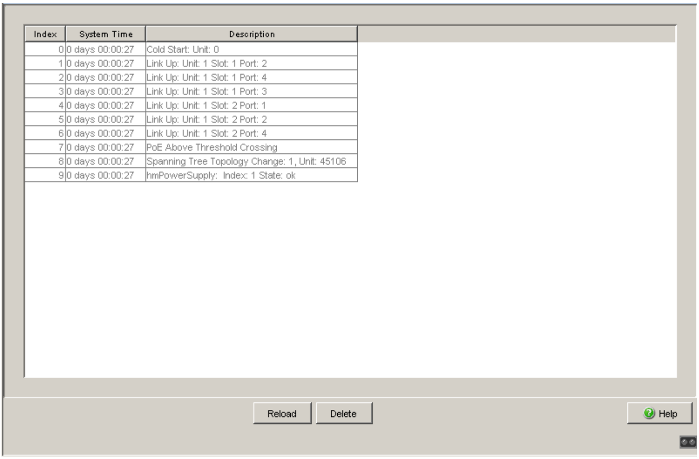
Buttons

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.
Create	Adds a new table entry.
Remove	Removes the selected table entry.
Help	Opens the online help.

Table 157:Buttons

7.2 Trap log

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



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

Figure 78: 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 which went bysince the logged event.	d days hh:mm:ss	
Description	Displays a short description of the logged event.	-	

Table 158:Trap log table

You have the option to also send the logged events to one or more syslog servers (see on page 272 “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 159:Buttons

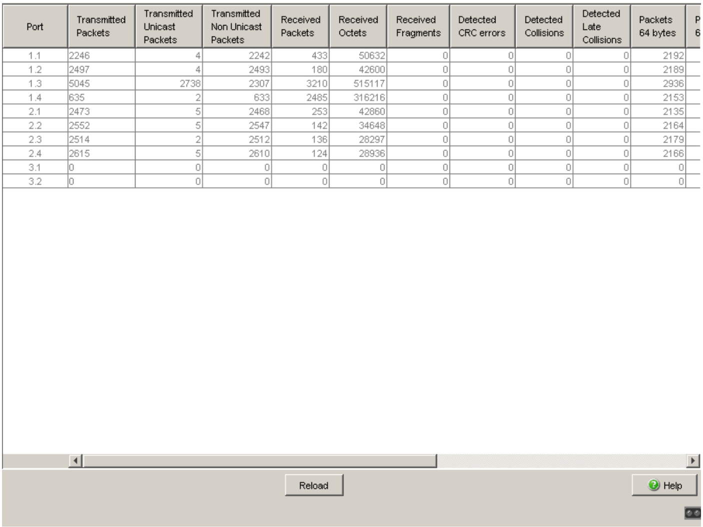
7.3 Ports

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

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

7.3.1 Statistics table

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



Port	Transmitted Packets	Transmitted Unicast Packets	Transmitted Non Unicast Packets	Received Packets	Received Octets	Received Fragments	Detected CRC errors	Detected Collisions	Detected Late Collisions	Packets 64 bytes	P 6
1.1	2246	4	2242	433	50632	0	0	0	0	2192	
1.2	2497	4	2493	180	42600	0	0	0	0	2189	
1.3	5045	2738	2307	3210	515117	0	0	0	0	2936	
1.4	635	2	633	2485	316216	0	0	0	0	2153	
2.1	2473	5	2468	253	42860	0	0	0	0	2135	
2.2	2552	5	2547	142	34648	0	0	0	0	2164	
2.3	2514	2	2512	136	28297	0	0	0	0	2179	
2.4	2615	5	2610	124	28936	0	0	0	0	2166	
3.1	0	0	0	0	0	0	0	0	0	0	
3.2	0	0	0	0	0	0	0	0	0	0	

Figure 79: Port statistics, table

Buttons

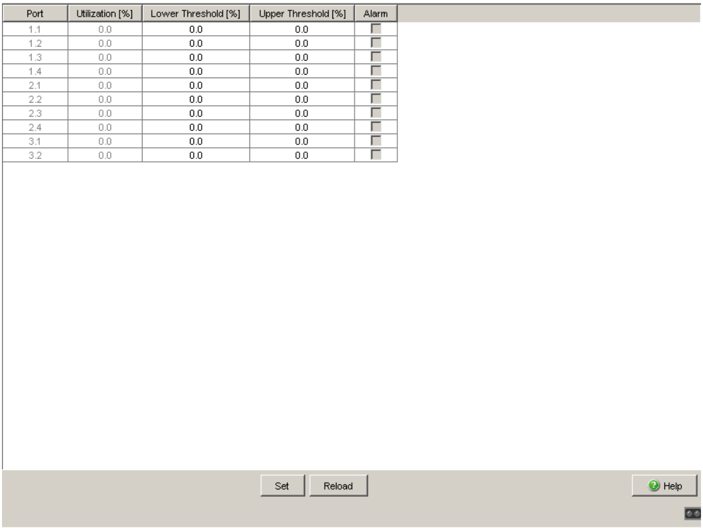
Button	Meaning
Reload	Updates the fields with the values that are saved in the volatile memory (`RAM`) of the device.
Reset port counters	Resets the counter for the port statistics to `0`.
Help	Opens the online help.

Table 160:Buttons

7.3.2 Network load (Utilization)

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

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



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

Figure 80: 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 161: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 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.

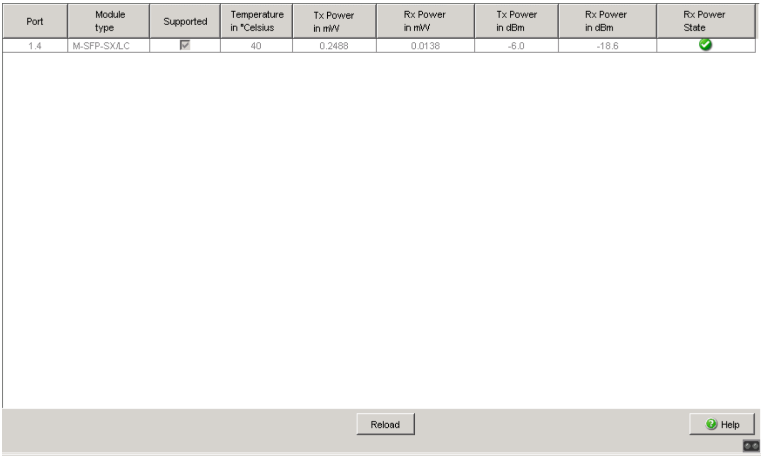
Table 162:Buttons

7.3.3 SFP Transceiver

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

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

Table 163:SFP Modules dialog



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

Figure 81: 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 164:Buttons

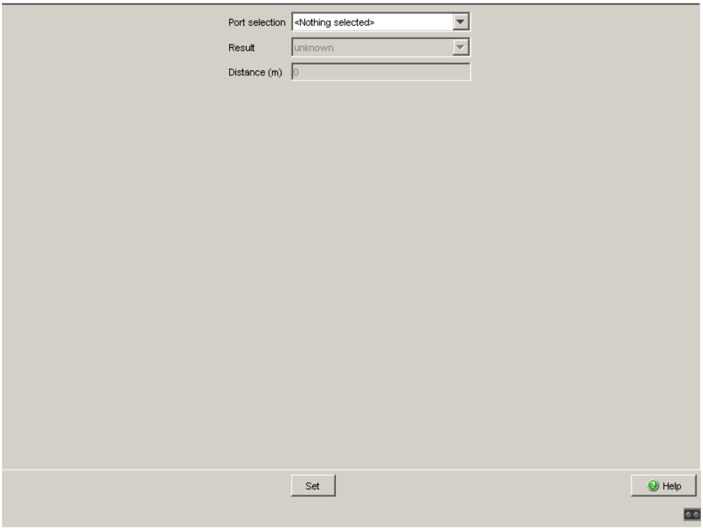
7.3.4 TP Cable Diagnosis

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.



Port selection <Nothing selected>

Result unknown

Distance (m) 0

Figure 82: 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 165: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 `Basic Settings:Load/Save` dialog, select the location to save the configuration, and click "Save".
Help	Opens the online help.

Table 166:Buttons

7.3.5 Port Monitor

The Port Monitor dialog enables you to monitor ports. When particular conditions occur, such as connection problems due to a loose connection, the device performs a pre-defined action, e.g. it deactivates the port.

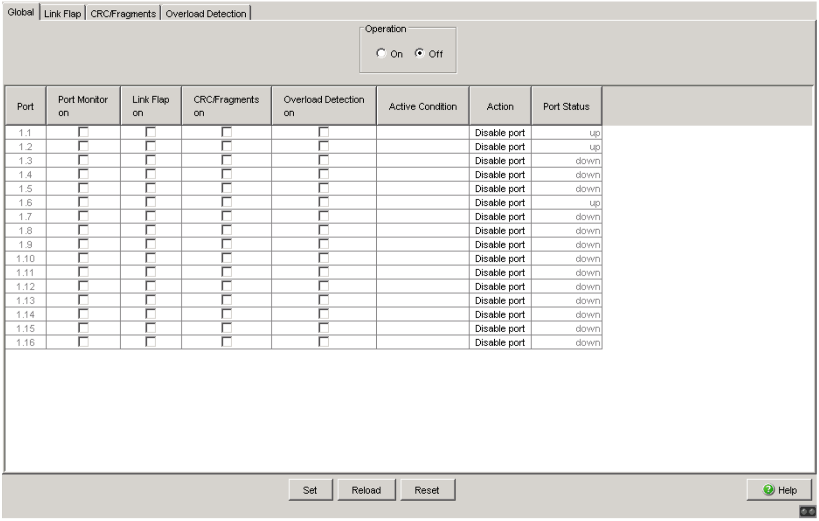
This dialog provides you with the following functions:

- Activating or deactivating the port monitor globally
- Activating or deactivating the port monitor for individual ports
- Activating one or several conditions for any port, during which the device performs an action
- Defining this action for every port
- Saving the current settings of every card index simultaneously using the "Set" button.
- Updating the content of every card index using the "Reload" button.
- Resetting the status and the counter of ports selected:
  - Reactivating the ports that the device had deactivated due to an action performed.
  - Deleting the corresponding numbers on the counters in every card index.

This is how you activate a "Global" card index action:

□ Activate the function globally.
□ Activate the ports wanted in the "Port monitor on" column.
□ Select the triggering conditions in the corresponding columns.
□ Select the action to be performed in the "Action" column.
"Disable port" is the default setting.
□ Save the values entered using the "Set" button.

Note: Set the appropriate parameters in the corresponding card index. Using the "Reload" button, you discard unsaved changes in every card index. Using the "Set" button, you save the settings of every card index.



Operation
○ On ● Off

Port	Port Monitor on	Link Flap on	CRC/Fragments on	Overload Detection on	Active Condition	Action	Port Status
1.1	☐	☐	☐	☐		Disable port	up
1.2	☐	☐	☐	☐		Disable port	up
1.3	☐	☐	☐	☐		Disable port	down
1.4	☐	☐	☐	☐		Disable port	down
1.5	☐	☐	☐	☐		Disable port	down
1.6	☐	☐	☐	☐		Disable port	up
1.7	☐	☐	☐	☐		Disable port	down
1.8	☐	☐	☐	☐		Disable port	down
1.9	☐	☐	☐	☐		Disable port	down
1.10	☐	☐	☐	☐		Disable port	down
1.11	☐	☐	☐	☐		Disable port	down
1.12	☐	☐	☐	☐		Disable port	down
1.13	☐	☐	☐	☐		Disable port	down
1.14	☐	☐	☐	☐		Disable port	down
1.15	☐	☐	☐	☐		Disable port	down
1.16	☐	☐	☐	☐		Disable port	down

Figure 83: Global Port Monitor Dialog

Parameters	Meaning
“Operation” Frame	Switches the “Port monitor” function for the device on or off.
Port table	
Port	List of the device's available ports.
Port Monitor on	You select the ports to be monitored here.
Link Flap on	You select here whether link changes trigger an action. Switchovers from the “Link down” state following “Link up” are considered as a link changes.
CRC/Fragments 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.
Active Condition	Shows the condition on the basis of which the device performed an action on this port.

Table 167:Global Port Monitor Table

Parameters	Meaning
Action	You select the action here, which the device performs when a condition occurs. The following actions are possible: – Deactivating the port – Sending a trap.
Port Status	Displays the current port status. – up: Data transmission via the port is possible. – down: Data transmission via the ports is interrupted.

Table 167:Global Port Monitor Table

Note: If the device deactivates a port after an interface disable condition occurs, use the auto disable function to recover this deactivation.

You set the parameters for the "Link Change" conditions as follows:

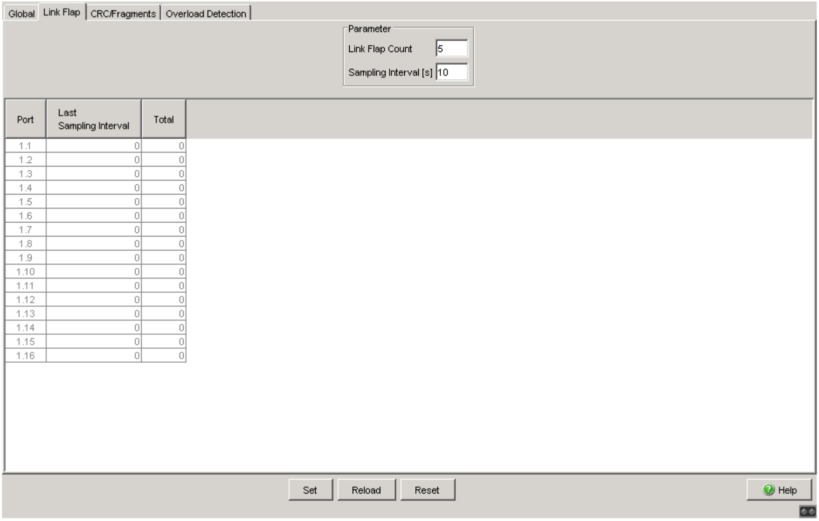
☐ Select the "Link Change" card index.

☐ Enter the number of link changes. Possible values are 1 - 100, the default is 5. When the value is reached, the device performs the action preset in the "Global" card index.

☐ Enter the length of the sampling interval. The sampling interval length is selectable within the range of 0 to 180 s. The default setting is 10 s.

☐ Save the values entered using the "Set" button.

Note: The parameters set apply to every port that you have activated the "Link Change on" setting in the "Global" card index for.
Using the "Reload" button, you discard unsaved changes in every card index.
Using the "Set" button, you save the settings of every card index.



Parameter

Link Flap Count 5

Sampling Interval [s] 10

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 84: 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 49 “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 168:Link Changes Port Monitor Table

You set the parameters for the “CRC/Fragments” conditions as follows:

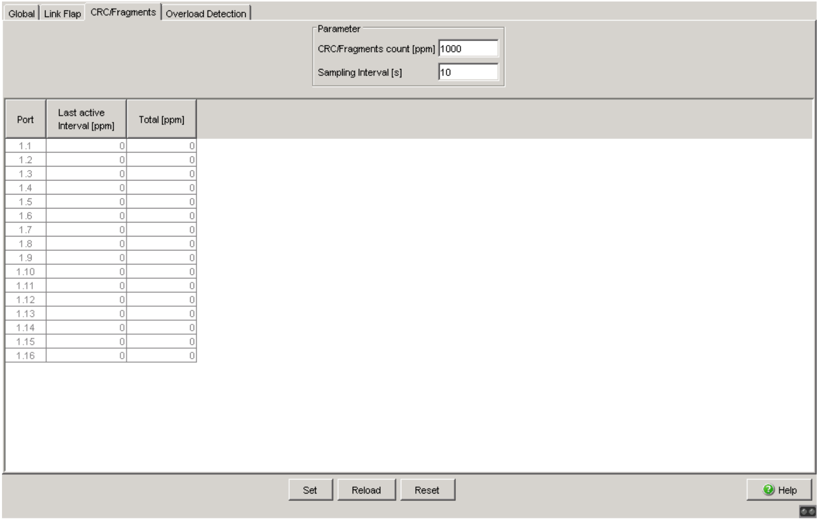
☐ Select the “CRC/Fragments” card index.

☐ Enter the CRC/fragment error rate. Possible values are 1 - 1,000,000 ppm. The default setting is 1,000 ppm. When the value is reached, the device performs the action preset in the “Global” card index.

☐ Enter the length of the sampling interval. The sampling interval length is selectable within the range of 0 to 180 s. The default setting is 10 s.

☐ Save the values entered using the “Set” button.

Note: The parameters set apply to every port that you have activated the "CRC/Fragments" setting in the "Global" card index for.
Using the "Reload" button, you discard unsaved changes in every card index.
Using the "Set" button, you save the settings of every card index.
To reset the values in the table to `0`, click the "Reset“button.



Parameter

CRC/Fragments count [ppm] 1000

Sampling Interval [s] 10

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 85: CRC/Fragment Error Port Monitor Dialog

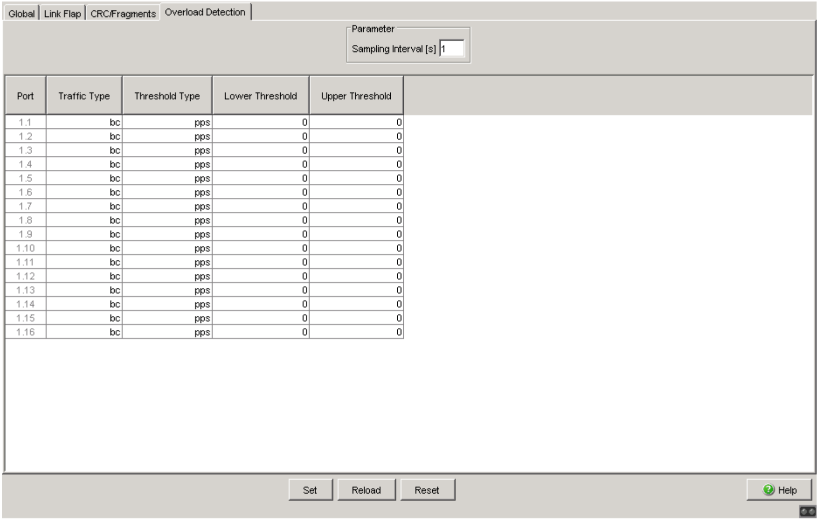
Parameters	Meaning
CRC/Fragments count [ppm]	Fragment error rate in the completed sampling interval that leads to an action by the device.
Sampling Interval [s]	Length of the sampling interval in which the device determines the CRC/fragment error rate.
Port table	
Port	List of the device's available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

You set the parameters for the overload conditions as follows:

☐ Select the "Overload Detection" card index.
☐ Enter the "Traffic Type" for sampling. The default setting is `bc`.
☐ On the MACH104 and MACH1040 devices, enter the "Threshold Type" for sampling. The default setting is `pps`.
The threshold range for `pps` and `kbps` is `0-10000000`.
The threshold range for `link-capacity` is `0-100`.
☐ Enter the "Lower Threshold". When the counters reach this value, the overload function enables the port when auto-disabled. The default setting is `0`.
☐ Enter the "Upper Threshold". When the counters reach this value, the device either sends a trap or disables the port according to the action configured in the "Global" card index. The default setting is `0`.
☐ Enter the length of the "Sampling Interval [s]". The sampling interval length is selectable within the range of `1-20` s. The default setting is `1` s.
☐ Save the values entered using the "Set" button.

Note: The parameters set apply to every port that you have activated the "Overload Detection" setting in the "Global" card index for.
Using the "Reload" button, you discard unsaved changes in every card index.
Using the "Set" button, you save the settings of every card index.



Sampling Interval [s] 1

Port	Traffic Type	Threshold Type	Lower Threshold	Upper Threshold
1.1	bc	pps	0	0
1.2	bc	pps	0	0
1.3	bc	pps	0	0
1.4	bc	pps	0	0
1.5	bc	pps	0	0
1.6	bc	pps	0	0
1.7	bc	pps	0	0
1.8	bc	pps	0	0
1.9	bc	pps	0	0
1.10	bc	pps	0	0
1.11	bc	pps	0	0
1.12	bc	pps	0	0
1.13	bc	pps	0	0
1.14	bc	pps	0	0
1.15	bc	pps	0	0
1.16	bc	pps	0	0

Figure 86: 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.
Traffic Type	Defines the overload detection traffic type. The following types are possible: – 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	Defines the overload detection threshold type. The following types are possible: – pps - packets per second Available on the MACH1040 and MACH104: – kbps - kilobits per second – link-capacity - percent of the link capacity

Table 170:CRC/Fragments Port Monitor Table

Parameters	Meaning
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 170:CRC/Fragments Port Monitor Table

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.
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 171:Buttons

7.3.6 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 the device auto-disables a port, it effectively shuts down the port and the port blocks traffic. The port LED blinks green 3 times per period. In addition, the device generates a log entry listing the reason for the auto-disable after re-enabling the port.

This feature provides a recovery function which automatically enables an auto-disabled port after a user-defined time. The range of the recovery timer is 30 – 2,147,483 s. The function allows you to set the recovery timer per interface. The device allows you to enable port recovery for specific reasons. To recover the port automatically, set the reason and recovery timer. Default state: disabled

In the cases where the recovery timer is still counting down, the device allows the administrator to re-enable an auto disabled port with the "Reset" button.

The auto-disable function serves 2 purposes:

- It assists the administrator in port analysis.
- It eliminates the possibility that this port causes other ports on the module (or the entire module) to shut down.

Configuration

Parameters	Meaning
Link Flap	Defines whether the device enables a port after a Link Flap condition produces a disable port action. Possible values: ▶ `Selected` Enables the ports after the user-defined time elapses. ▶ `Not selected` (default setting) The ports remain disabled.
CRC Error	Defines whether the device enables a port after a CRC/Fragments condition produces a disable port action. Possible values: ▶ `Selected` Enables the ports after the user-defined time elapses. ▶ `Not selected` (default setting) The ports remain disabled.
Overload Detection	Defines whether the device enables a port after an Overload Detection condition produces a disable port action. Possible values: ▶ `Selected` Enables the ports after the user-defined time elapses. ▶ `Not selected` (default setting) The ports remain disabled.

Table 172:"Configuration" frame in the `Diagnostics:Ports:Auto Disable` dialog

Table

Parameters	Meaning
Port	Shows the number of the device port to which the table entry relates.
Reset Timer[s]	Timer value in seconds after which the device reactivates a deactivated port. Possible values: ▶ `30...2147483` ▶ `0` (default setting) A value of 0 disables the timer.
Remaining Time [s]	Remaining time in seconds until the reactivation of the port.
Component	Shows the name of the component that caused the port to disable itself.
Reason	Shows the reason the port disabled itself.
Active	Shows the operational status of the function for the port. Possible values: ▶ `Selected` The Auto Disable function shuts down the port. ▶ `Not selected` (default setting) The Auto Disable function is inactive for this port.

Table 173:Table in the `Diagnostics:Ports:Auto Disable` dialog

Buttons

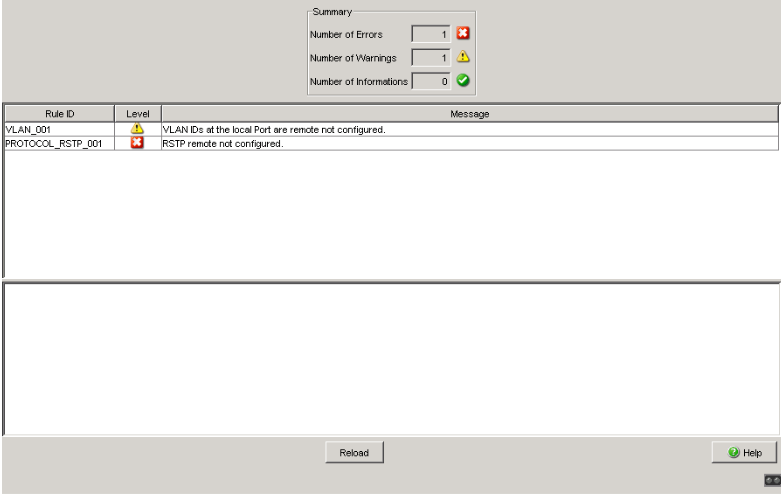
Button	Meaning
Set	Transfers the changes to the volatile memory (`RAM`) of the device. To permanently save the changes afterwards, you open the `Basic Settings:Load/Save` dialog and click "Save".
Reload	Updates the fields with the values that are saved in the volatile memory (`RAM`) of the device.
Reset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

Table 174:Buttons

7.4 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.

Figure 87: Configuration Check Dialog

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

Table 175: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	Level of deviation between this device's configuration and the recognized neighboring devices. The rule level can have 3 statuses: ! 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 176: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 switch port, even though they are connected to the neighboring device.

Note: If you have more than 39 VLANs configured on the device, the dialog always shows 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
Set	Transfers the changes to the volatile memory (RAM) of the device. To permanently save the changes afterwards, you open the Basic Settings:Load/Save dialog and click "Save".
Reload	Updates the fields with the values that are saved in the volatile memory (RAM) of the device.
Reset	Enables the port when disabled by the Port Monitor function.
Help	Opens the online help.

Table 177:Buttons

7.5 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.

7.5.1 LLDP Information from Neighbor Devices

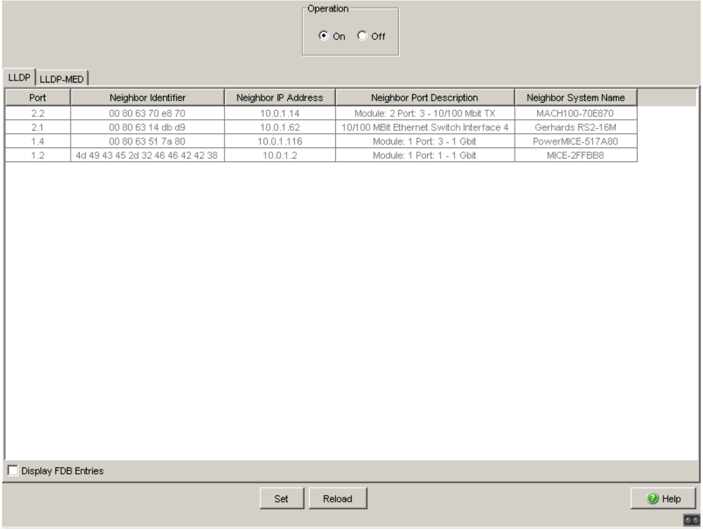
The table on the “LLDP” tab page shows you the collected LLDP information for neighboring devices. This information enables the network management station to map the structure of your network.

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

Table 178:Topology discovery (LLDP information)



Operation

● On ○ Off

Port	Neighbor Identifier	Neighbor IP Address	Neighbor Port Description	Neighbor System Name
2.2	00 80 63 70 e8 70	10.0.1.14	Module: 2 Port: 3 - 10/100 Mbit TX	MACH100-70E870
2.1	00 80 63 14 db d9	10.0.1.62	10/100 MBit Ethernet Switch Interface 4	Gerhards RS2-16M
1.4	00 80 63 51 7a 80	10.0.1.116	Module: 1 Port: 3 - 1 Gbit	PowerMICE-517A80
1.2	4d 49 43 45 2d 32 46 46 42 42 38	10.0.1.2	Module: 1 Port: 1 - 1 Gbit	MICE-2FFBB8

□ Display FDB Entries

Figure 88: 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 152 “Filter for MAC addresses”).

7.5.2 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 301 “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
Module.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: – 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	– `true`: 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. – false: The network policy for the remote device's application type is known.
Tagged Bit Status	– `true`: The remote device's application uses VLAN-tagged frames – `false`: 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)

Table 179:Topology discovery (LLDP-MED information)

Parameters	Meaning
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 179: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 187 “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.

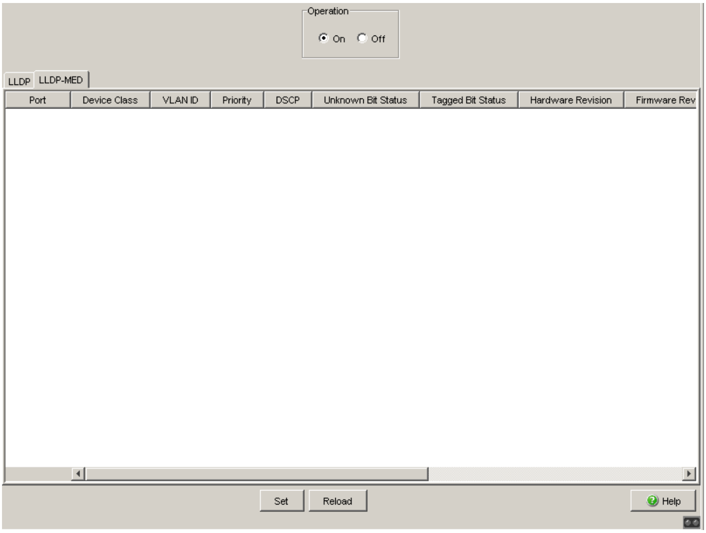


Figure 89: LLDP-MED Information

Buttons

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

Table 180:Buttons

7.6 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.

Selecting "RX" as the monitoring direction on a source port determines the destination port mirror (copy from the selected source interface) only frames received on the source interface (monitoring ingress).
Selecting "TX" as the monitoring direction on a source port determines the destination port mirror (copy from the selected source interface) only frames sent from the source interface (monitoring egress).

With port mirroring active, the device copies the traffic received and/or forwarded on a source port to the destination port.

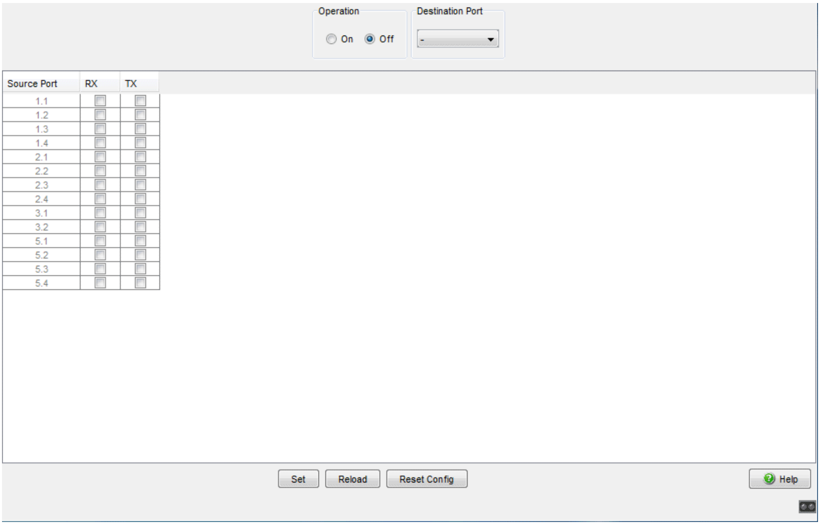
The PowerMICE and MACH4000 devices use the destination port for the port mirroring task exclusively. The source port forwards and receives traffic as normal.

☐ 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`.



Operation ○ On ● Off

Destination Port -

Source Port	RX	TX
1.1	□	□
1.2	□	□
1.3	□	□
1.4	□	□
2.1	□	□
2.2	□	□
2.3	□	□
2.4	□	□
3.1	□	□
3.2	□	□
5.1	□	□
5.2	□	□
5.3	□	□
5.4	□	□

Figure 90: `Diagnostics:Port Mirroring N:1` *dialog*

Buttons

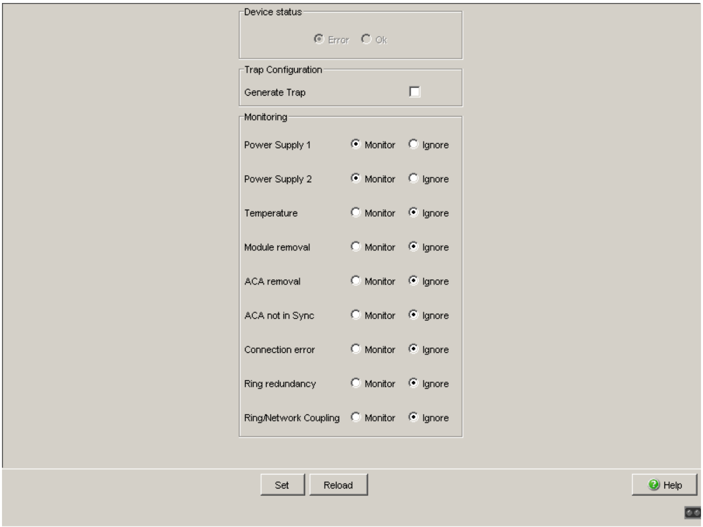
Button	Meaning
Set	Transfers the changes to the volatile memory (`RAM`) of the device. To permanently save the changes afterwards, you open the `Basic Settings:Load/Save` dialog and click "Save".
Reload	Updates the fields with the values that are saved in the volatile memory (`RAM`) of the device.
Reset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

Table 181:Buttons

7.7 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.



Device status

● Error ○ Ok

Trap Configuration

Generate Trap □

Monitoring

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

Figure 91: Device State dialog (for PowerMICE)

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

The events which can be selected are:

Name	Meaning
“Device Status” Frame	The device determines this status from the individual monitoring results. It can have the values “Error” or “OK”.
“Trap Configuration” Frame	-
Generate Trap	Activate this setting so the device sends a trap if it changes its device status.
“Monitoring” Frame	-
Power supply ...	Monitor/ignore supply voltage(s).
Temperature (°C)	Monitor/ignore temperature thresholds set (see on page 20 “System”) for temperatures that are too high/too low
Module removal	Monitor/ignore the removal of a module (for modular devices).
ACA removal	Monitor/ignore the removal of the ACA.
ACA not in sync	Monitor/ignore non-matching of the configuration on the device and on the ACA[a] .
Connection error	Monitor/ignore the link status (Ok or inoperable) of at least one port. The reporting of the link status can be masked for each port by the management (see on page 34 “Port Configuration”). Link status is not monitored in the state on delivery.
Ring Redundancy	Monitor/ignore ring redundancy (for HIPER-Ring only in Ring Manager mode). On delivery, ring redundancy is not monitored. If the device is a normal ring subscriber and not the ring manager, it reports the following: ▶ nothing (for the HIPER-Ring) ▶ detected errors in the local configuration (for Fast HIPER-Ring and for MRP)
Ring/Network coupling	Monitor/ignore the redundant coupling operation. On delivery, no monitoring of the redundant coupling is set. For two-Switch coupling with control line, the slave additionally reports the following conditions: – Incorrect link status of the control line – Partner device is also a slave (in standby mode). **Note:** In two-Switch coupling, both Switches must have found their respective partners.
Fan	Monitor/ignore fan function (for devices with fan).

Table 182: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 312 “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 Basic Settings:Load/Save dialog and click "Save".
Reload	Updates the fields with the values that are saved in the volatile memory (RAM) of the device.
Help	Opens the online help.

Table 183:Buttons

7.8 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.

7.8.1 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.

7.8.2 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 21 “System Data”). Select “Monitor” for the temperature if the signal contact should report an impermissible temperature.

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

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

▶ The 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 214 “Ring Redundancy”). Select “Monitor” for the ring redundancy if the signal contact is to report the elimination of the reserve redundancy in the redundant ring.
  Default setting: no monitoring.

  Note: If the device is a normal ring member and not a ring manager, it doesn't report anything for the HIPER-Ring; for the 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 214 “Ring Redundancy”).
  Default setting: no monitoring.

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

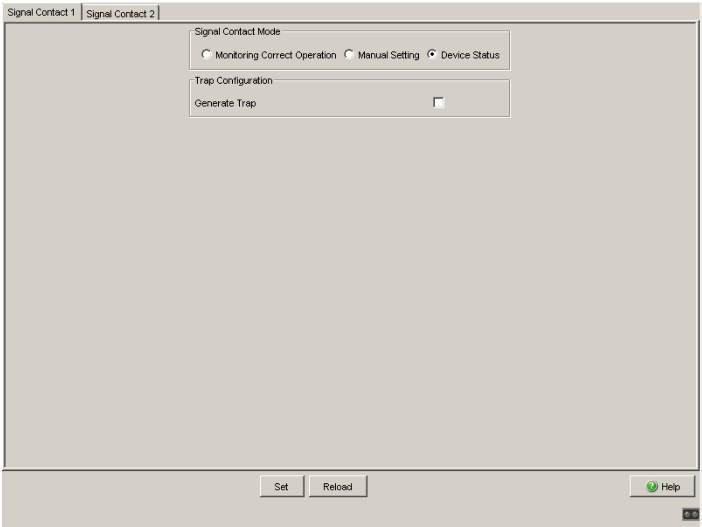
7.8.3 Device status

☐ 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 20 “Device Status”) and thereby offers remote diagnosis.
The device status “Error detected” (see on page 20 “Device Status”) is reported by means of a break in the contact via the potential-free signal contact (relay contact, closed circuit).

7.8.4 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.



Signal Contact Mode

○ Monitoring Correct Operation ○ Manual Setting ● Device Status

Trap Configuration

Generate Trap □

Figure 92: 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 `Basic Settings:Load/Save` dialog and click "Save".

Table 184: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 184:Buttons (cont.)

7.9 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 10 trap destinations:

- RS20, RS30, RS40
- MS20, MS30
- OCTOPUS
- MACH 102
- RSR20, RSR30
- MACH 1020, MACH 1030

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 on "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.

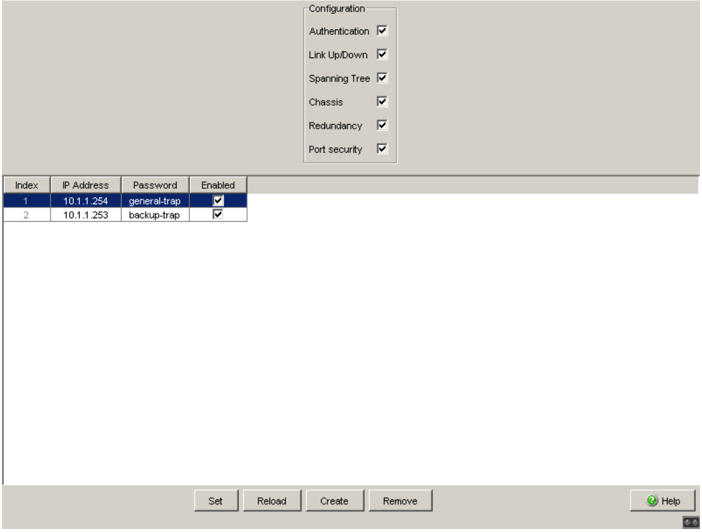
The events which can be selected are:

Name	Meaning
Authentication	The device has rejected an unauthorized access attempt (see on page 72 “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 185:Trap categories

Name	Meaning
Chassis	Summarizes the following events: ▶ The status of a supply voltage has changed (see the `System` dialog). ▶ The status of the signal contact has changed. To take this event into account, you activate “Create trap when status changes” in the `Diagnostics:Signal Contact 1/2` dialog. ▶ The AutoConfiguration Adapter (ACA) has been added or removed. ▶ – 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 `Diagnosis:Ports:SFP Modules`). ▶ 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 `Port Security` dialog).

Table 185:Trap categories



Configuration

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

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

Figure 93: 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 `Basic Settings:Load/Save` dialog and click "Save".
Reload	Updates the fields with the values that are saved in the volatile memory (`RAM`) of the device.
Create	Adds a new table entry.
Remove	Removes the selected table entry.
Help	Opens the online help.

Table 186:Buttons

7.10 Report

The following reports are available for the diagnostics:

- System Information (see on page 322 “System Information”).
  The System Information is an HTML file with system-relevant data. The device displays the system information in an own dialog.
- Event Log (see on page 323 “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 an own dialog.

Note: You have the option to also send the logged events to one or more syslog servers (see on page 272 “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 187).

  □ 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”.

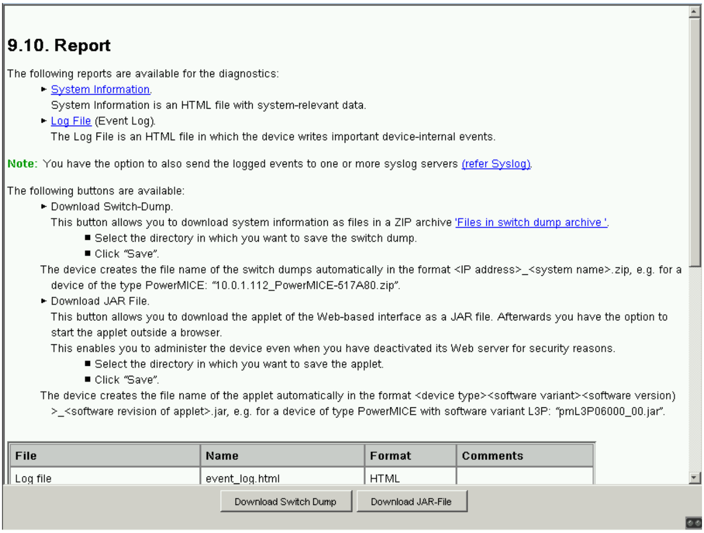
The device creates the file name of the applet automatically in the format <device type><software variant><software version)>_<software revision of applet>.jar, e.g. for a device of type PowerMICE with software variant L3P: “pmL3P06000_00.jar”.

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 187:Files in switch dump archive

a: Prerequisite: a Telnet connection is available.

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



9.10. Report

The following reports are available for the diagnostics:

- System Information.
  System Information is an HTML file with system-relevant data.
- Log File (Event Log).
  The Log File is an HTML file in which the device writes important device-internal events.

Note: You have the option to also send the logged events to one or more syslog servers (refer Syslog).

The following buttons are available:

- Download Switch-Dump.
  This button allows you to download system information as files in a ZIP archive 'Files in switch dump archive '.
  - 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	

Figure 94: Report dialog

7.10.1 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 188: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 188:Buttons (cont.)

7.10.2 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 189:Buttons

7.11 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 190). 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.

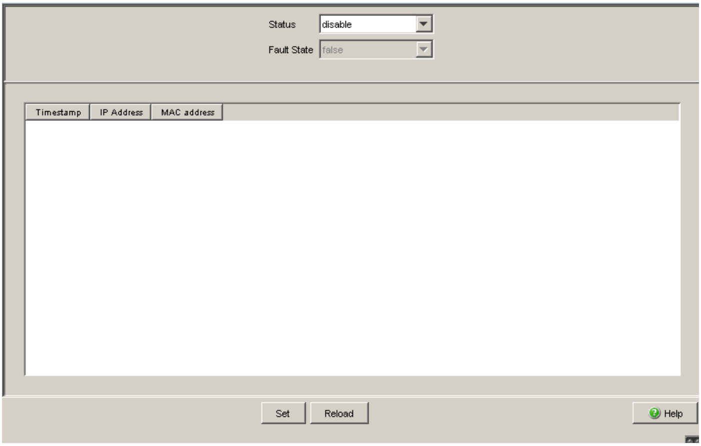
Mode	Meaning
Field „Status“	Defines the status for the IP address conflict detection. The value of the status field can be „enable“, „disable“, „activeDetectionOnly“ or „passiveDetectionOnly“.
`enable`	Enables active and passive detection.
`disable`	Disables the function
`activeDetectionOnly`	Enables 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.
`passiveDetectionOnly`	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 190: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.



Status: disable

Fault State: false

Figure 95: 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 `Basic Settings:Load/Save` dialog and click "Save".
Reload	Updates the fields with the values that are saved in the volatile memory (`RAM`) of the device.
Help	Opens the online help.

Table 191:Buttons

7.12 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 intended use of this function is for end device ports, where few MAC address changes occur.

7.12.1 Operation

Parameters	Meaning
Operation	Activates/deactivates the MAC Notification function globally on the device. Possible values: ▶ `On` The device sends traps for the active rows to the active management stations in `Diagnostics:Status Configuration:Alarms (Traps).` ▶ `Off` (default setting)

Table 192:"Operation" frame in the `Diagnostics:Status Configuration:MAC Notification` dialog

7.12.2 Configuration

Parameters	Meaning
Intervals [s]	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. Possible values: ▶ 0..2147483647

Table 193:"Configuration" frame in the Diagnostics:Status Configuration:MAC Notification dialog

7.12.3 Table

Parameters	Meaning
Port	Shows the number of the device port to which the table entry relates.
Enable	Activates/deactivates the MAC Notification function on this port. Possible values: ▶ Selected When globally activated, the device sends traps for this row to the active management stations in Diagnostics:Status Configuration:Alarms (Traps). ▶ Not selected (default setting)

Table 194:Table in the Diagnostics:Status Configuration:MAC Notification dialog

Parameters	Meaning
Mode	Defines when the device sends a trap for MAC address events on a specific interface. Possible values: ▶ `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	Shows the status of the last MAC address on this interface. Possible values: ▶ `other` ▶ `added` ▶ `removed`

Table 194:Table in the `Diagnostics:Status Configuration:MAC Notification` dialog (cont.)

■ Buttons

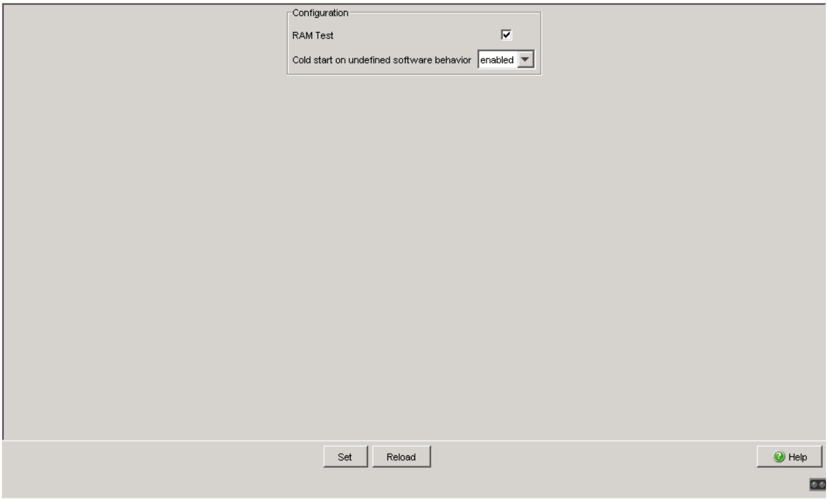
Button	Meaning
Set	Transfers the changes to the volatile memory (`RAM`) of the device. To permanently save the changes afterwards, you open the `Basic Settings:Load/Save` dialog and click "Save".
Reload	Updates the fields with the values that are saved in the volatile memory (`RAM`) of the device.
Help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

Table 195:Buttons

7.13 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.



Configuration

RAM Test ☑

Cold start on undefined software behavior: enabled

Figure 96: 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 `Basic Settings:Load/Save` dialog and click "Save".
Reload	Updates the fields with the values that are saved in the volatile memory (`RAM`) of the device.
Help	Opens the online help.

Table 196:Buttons

7.14 Service Mode

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

The service mode enables you to divide the device into 2 transmission areas. You can thus, for example, perform test or service configurations in the field area of a network while the ongoing operation continues in the backbone area.

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

- resets the port VLAN IDs for all the ports of this VLAN to the new VLAN ID
- deactivates GVRP at all ports of this VLAN. The device prevents GVRP from dynamically changing the service mode port settings as a result.
- activates “Ingress Filtering” at all ports of this VLAN. As a consequence, the device only transmits packets when the input and output ports belong to this VLAN.

Buttons

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

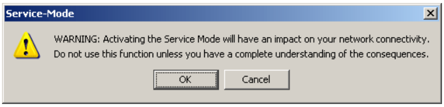
Table 197:Buttons

7.14.1 Activating the service mode

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

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

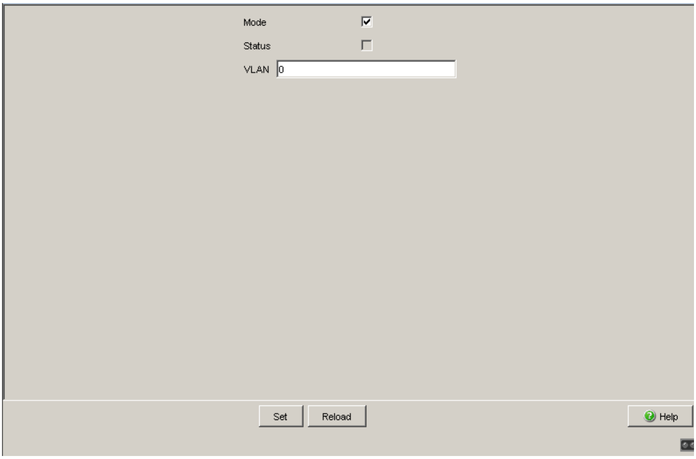
□ Select the `Diagnostics:Service Mode` dialog.
□ Activate “Mode”.
□ Enter a number other than 0 or 1 in the “VLAN” field. Enter a VLAN ID for a new VLAN in order to keep the settings for existing VLANs.
□ Click “Set”. The device outputs the following system message:



WARNING: Activating the Service Mode will have an impact on your network connectivity.
Do not use this function unless you have a complete understanding of the consequences.

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

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



Mode ☑

Status □

VLAN 0

Figure 97: Service Mode dialog - mode activated

□ Deactivate the redundant supply voltage.

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

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

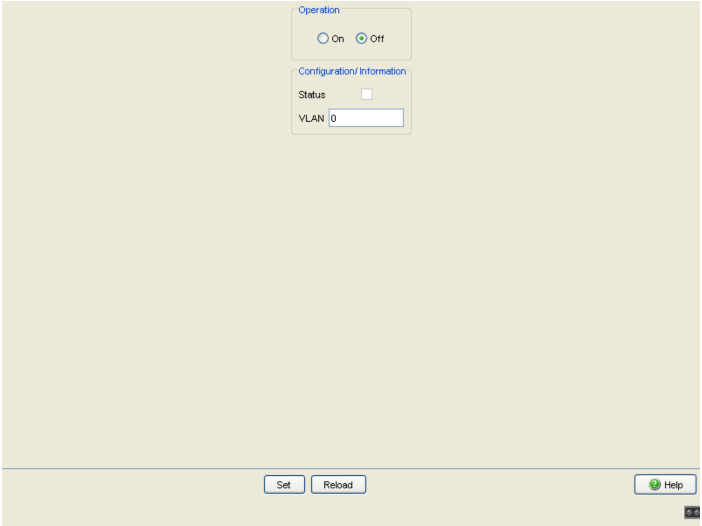
7.14.2 Deactivating the service mode

□ Reactivate the redundant voltage.

The service mode is now deactivated.

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

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



Operation

○ On ● Off

Configuration/ Information

Status □

VLAN 0

Figure 98: Service Mode dialog - mode deactivated

8 Advanced

The menu contains the dialogs, displays and tables for:

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

8.1 DHCP Relay Agent

This dialog allows you to configure the DHCP relay agent.

□ Enter the DHCP server IP address.
If one DHCP server is not available, you can enter up to 3 additional DHCP server IP addresses so that the device can change to another DHCP server.

□ With Option 82, a DHCP relay agent which receives a DHCP request adds an “Option 82” field to the request, as long as the request received does not already have such a field.
When you switch the function off, the device forwards attached “Option 82” fields. Under “Type”, you specify the format in which the device enters the device recognition in the “Option 82” field by the DHCP relay agent.
The options are:

- IP address
- MAC Address (default setting)
- System name (Client ID)
- Other (freely definable ID)
  Enter a freely definable character string in the "Manual Value (Type other)" text box for the DHCP Relay Agent unique identification.

“DHCP Server Remote ID entry” shows you the value which you enter when configuring your DHCP server. “Type display” shows the device recognition in the selected form.

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

Note: The VLAN ID is 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`

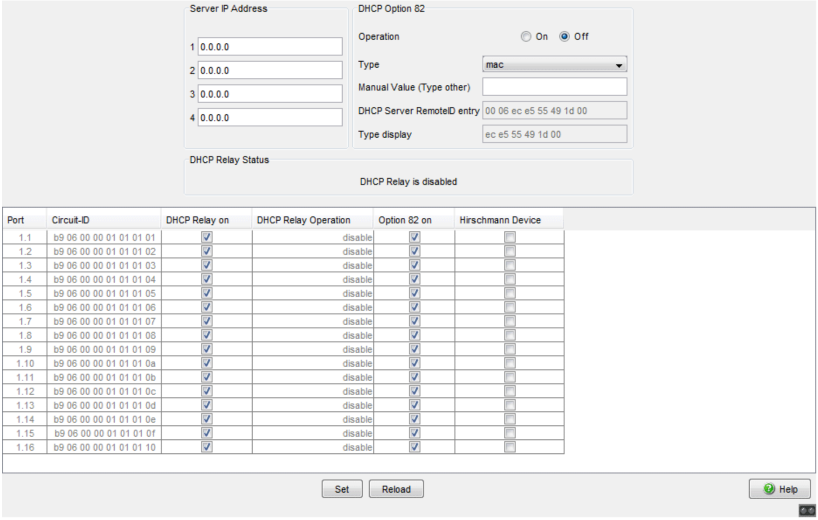
☐ The "DHCP-Relay on" activates the relay on the port. Clients connected to an activated port communicate directly with a DHCP Server.

☐ 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.



Server IP Address

1 0.0.0.0

2 0.0.0.0

3 0.0.0.0

4 0.0.0.0

DHCP Option 82

Operation ○ On ● Off

Type: mac

Manual Value (Type other):

DHCP Server RemoteID entry: 00 06 ec e5 55 49 1d 00

Type display: ec e5 55 49 1d 00

DHCP Relay Status

DHCP Relay is disabled

Port	Circuit-ID	DHCP Relay on	DHCP Relay Operation	Option 82 on	Hirschmann Device
1.1	b9 06 00 00 01 01 01 01	☑	disable	☑	□
1.2	b9 06 00 00 01 01 01 02	☑	disable	☑	□
1.3	b9 06 00 00 01 01 01 03	☑	disable	☑	□
1.4	b9 06 00 00 01 01 01 04	☑	disable	☑	□
1.5	b9 06 00 00 01 01 01 05	☑	disable	☑	□
1.6	b9 06 00 00 01 01 01 06	☑	disable	☑	□
1.7	b9 06 00 00 01 01 01 07	☑	disable	☑	□
1.8	b9 06 00 00 01 01 01 08	☑	disable	☑	□
1.9	b9 06 00 00 01 01 01 09	☑	disable	☑	□
1.10	b9 06 00 00 01 01 01 0a	☑	disable	☑	□
1.11	b9 06 00 00 01 01 01 0b	☑	disable	☑	□
1.12	b9 06 00 00 01 01 01 0c	☑	disable	☑	□
1.13	b9 06 00 00 01 01 01 0d	☑	disable	☑	□
1.14	b9 06 00 00 01 01 01 0e	☑	disable	☑	□
1.15	b9 06 00 00 01 01 01 0f	☑	disable	☑	□
1.16	b9 06 00 00 01 01 01 10	☑	disable	☑	□

Figure 99: 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 198:Buttons

8.2 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.

8.2.1 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`

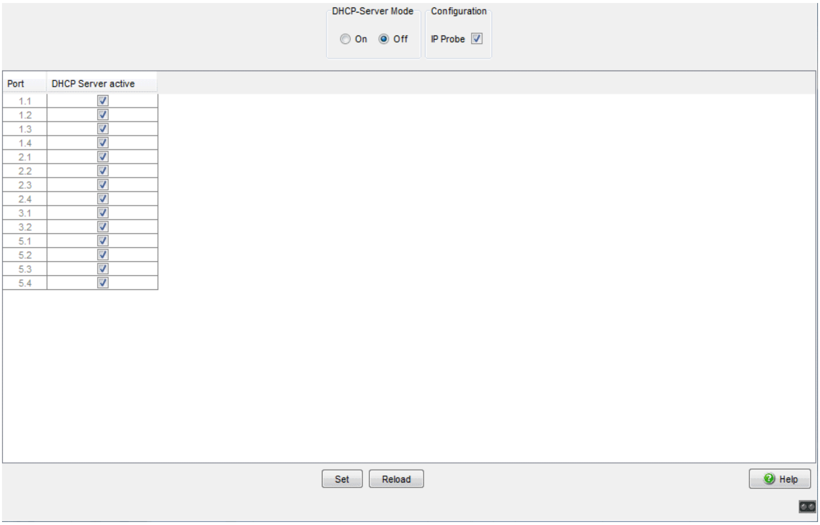
Table 199:"DHCP-Server Mode" frame in the `Advanced:DHCP Server:Global` dialog

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 200:"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 201:Table in the `Advanced:DHCP Server:Global` dialog



DHCP-Server Mode: ○ On ● Off

Configuration: IP Probe ☑

Port	DHCP Server active
1.1	☑
1.2	☑
1.3	☑
1.4	☑
2.1	☑
2.2	☑
2.3	☑
2.4	☑
3.1	☑
3.2	☑
5.1	☑
5.2	☑
5.3	☑
5.4	☑

Figure 100: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 `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 202:Buttons

8.2.2 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 64 pool entries (128 for the PowerMICE and MACH devices).

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	▶ 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	Module and port numbers to which this entry applies. ▶ For a dynamic address entry select all. ▶ For a static address entry select all or one valid module and port number.	Valid module and port number or all.	all
VLAN	VLAN number to which this entry applies. **Note:** This column is available on the MS, Octopus, RS, RSR, MACH102, and MACH1020/10130 devices.	Valid VLAN No.	-
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 203:DHCP server pool settings, IP address basic settings

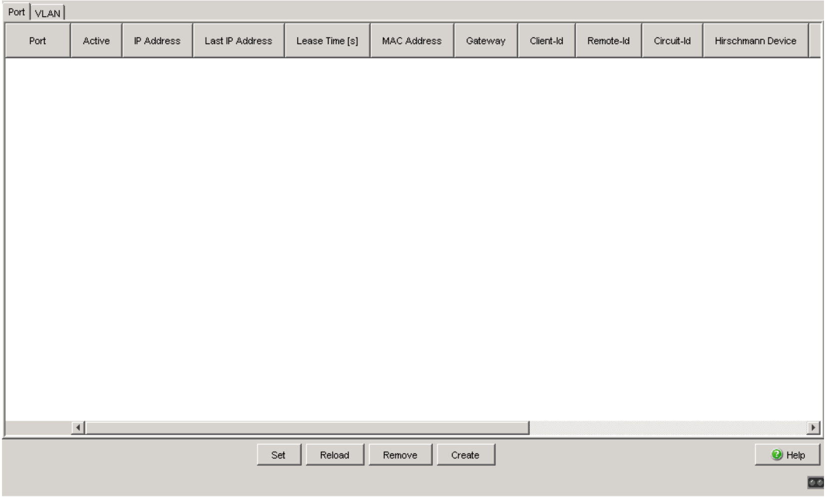
Parameter	Meaning	Value range	Default setting
Remote ID	For a static address entry: Remote ID with which the client identifies itself.	Remote ID of the client that contains the static IP address[a]	-
Circuit ID	For a static address entry: Circuit ID with which the client identifies itself.	Circuit ID 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 tftp://server name or ip address/directory/file.	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 203: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 21 “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. **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.	Valid hex string.	-

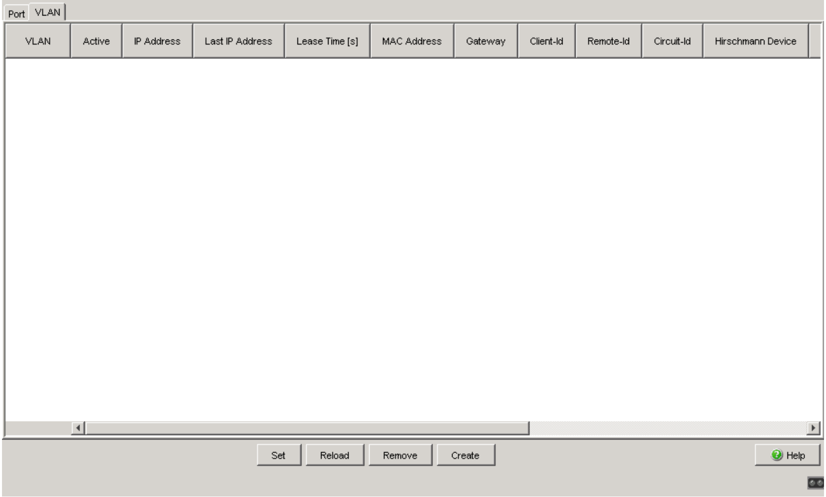
Table 203:DHCP server pool settings, IP address basic settings

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



Port	Active	IP Address	Last IP Address	Lease Time [s]	MAC Address	Gateway	Client-Id	Remote-Id	Circuit-Id	Hirschmann Device

Figure 101:DHCP Server Pool per Port dialog



VLAN	Active	IP Address	Last IP Address	Lease Time [s]	MAC Address	Gateway	Client-Id	Remote-Id	Circuit-Id	Hirschmann Device

Figure 102: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 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.
Create	Adds a new table entry.
Remove	Removes the selected table entry.
Help	Opens the online help.

Table 204:Buttons

8.2.3 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 205: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 205:DHCP lease table

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

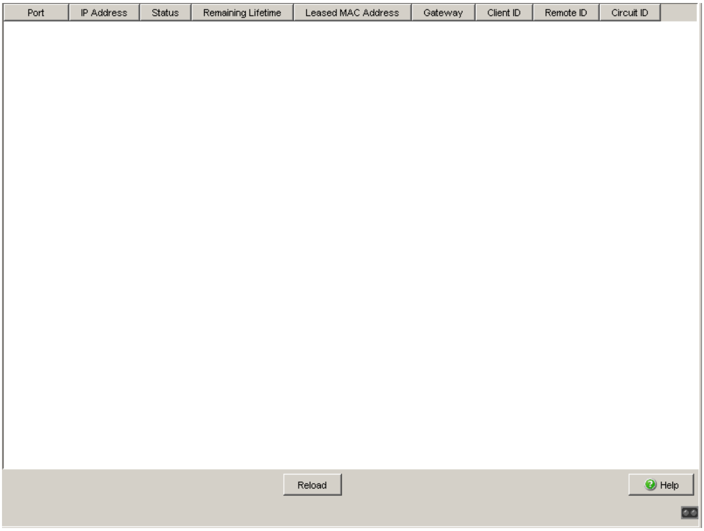


Figure 103:DHCP Server Lease Table dialog

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 206:Buttons

8.3 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“.

8.3.1 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:Network` dialog, check whether `Local` is selected in the “Mode” frame (see on page 27 “Network”).

□ In the `Switching:VLAN:Global` dialog, check whether “VLAN 0 Transparent Mode” is selected (see on page 172 “VLAN Global”).

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

□ Configure the alarm settings and the threshold values for the alarms you want to monitor (see on page 309 “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:

□ Select the port for which you want to set the DCP mode in detail, and in the column `DCP Mode`, select

- `none`:
  The device sends received DCP frames. However, the CPU does not process them yet, it still generates DPC frames. The port does not send any DCP frames which were received at another port.
- `ingress`:
  The device sends received DCP frames. The CPU processes received DCP frames from this port, but does not generate any. The port does not send any DCP frames which were received at another port.
- `egress`:
  The device sends received DCP frames. The CPU ignores frames received from this port and generates them as needed.
- `both`:
  The device sends received DCP frames. The CPU processes received frames and generates them as needed.

The default setting is `both`.

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

□ Select the port for which you want to set its PHY module to the fast start mode, and select from the following in the column `Fast Start Up`:

▶ `disable` to set the normal start mode,
▶ `enable` to set the fast start mode.

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

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

Settings for the PLC:

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

■ Buttons

Button	Meaning
Set	Transfers the changes to the volatile memory (`RAM`) of the device. To permanently save the changes, open the `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 207:Buttons

8.3.2 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 161 “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 `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 208:Buttons

8.3.3 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

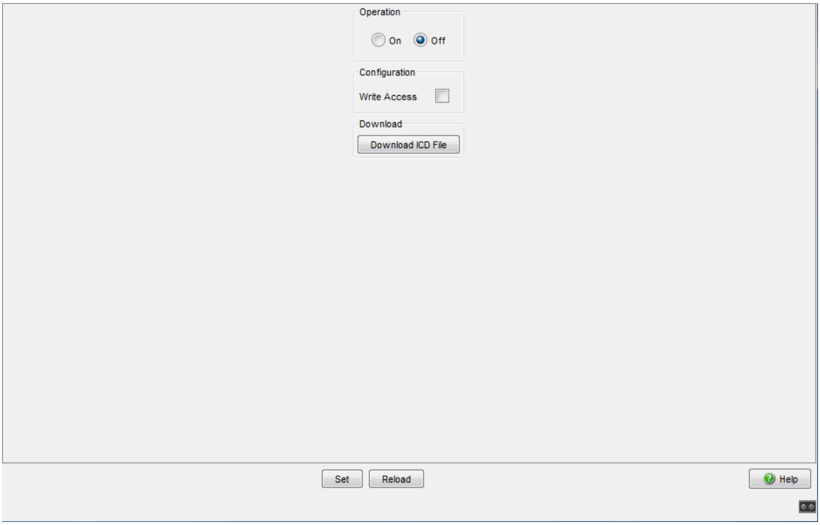
Table 209:"Operation" frame in the `Advanced:Industrial Protocols:IEC61850` *dialog*

Parameter	Meaning	Value range	Default setting
Write Access	Activate/deactivate the MMS server.	select, not selected	not selected

Table 210:"Configuration" frame in the `Advanced:Industrial Protocols:IEC61850` *dialog*

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

Table 211:"Download" frame in the `Advanced:Industrial Protocols:IEC61850` *dialog*



Operation

○ On ● Off

Configuration

Write Access □

Download

Figure 104:`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 `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 212:Buttons

8.3.4 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:

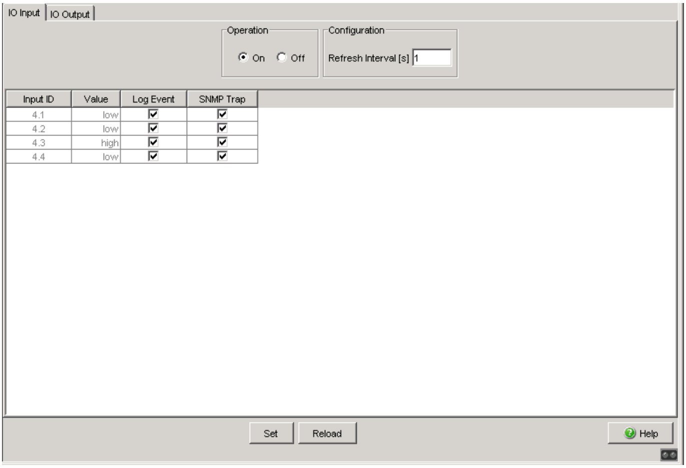
- safety instructions
- a description of the device
- information about assigning the Digital I/O MICE Media module connection terminals
- a description of the display elements
- and other information that you need for installing the device prior to your configuring it

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.



Operation: ● On ○ Off

Configuration: Refresh Interval [s] 1

Input ID	Value	Log Event	SNMP Trap
4.1	low	☑	☑
4.2	low	☑	☑
4.3	high	☑	☑
4.4	low	☑	☑

Figure 105: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 213: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 214: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 – `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

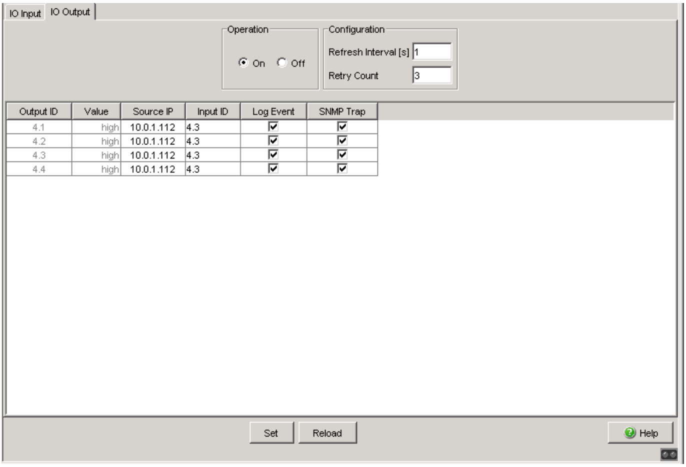
Table 215:IO Input Table

Parameter	Meaning	Value Range	Default Setting
Log Event	Activates/deactivates the logging function for input status changes. – `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 `Diagnostics:Report:EventLog` 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	Activates or deactivates the transmission of SNMP traps in the course of an input status changes. – 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 Diagnostics:Trap Log 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 215: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 218).



Operation: ● On ○ Off

Configuration:
Refresh Interval [s] 1
Retry Count 3

Output ID	Value	Source IP	Input ID	Log Event	SNMP Trap
4.1	high	10.0.1.112	4.3	☑	☑
4.2	high	10.0.1.112	4.3	☑	☑
4.3	high	10.0.1.112	4.3	☑	☑
4.4	high	10.0.1.112	4.3	☑	☑

Figure 106: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 216: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 217: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 s	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. – `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 218:IO Output Table

Parameters	Meaning	Value range	Default setting
Log Event	Activates/deactivates the logging function for output status changes. – `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 `Diagnostics:Report:EventLog` 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	Activates or deactivates the transmission of SNMP traps in the course of an output status changes. – 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 218: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.

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

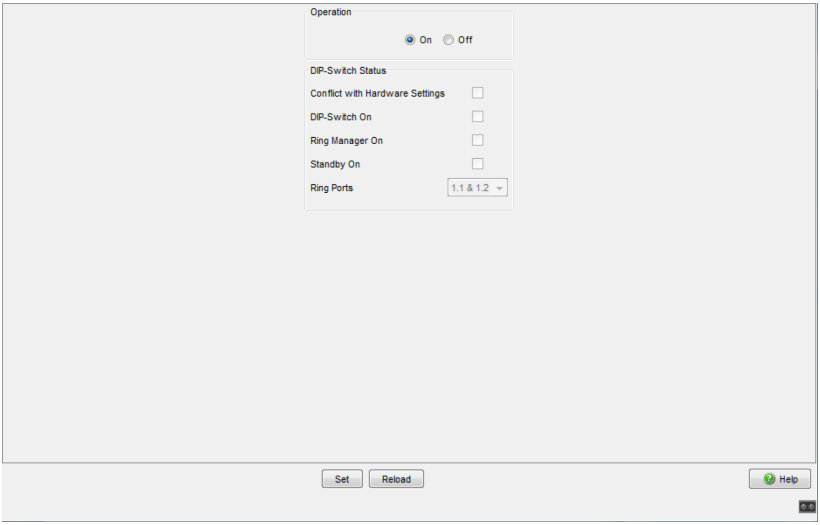
This feature introduces the possibility to disable the DIP switches using software.

Parameter	Meaning	Value range	Default setting
Operation	Activates/deactivates the DIP switches physically located on the device. `On`: activates hardware DIP switch configuration	`On`, `Off`	`On`

Table 219:"Operation" frame in the `Advanced:DIP-Switch` dialog

Parameter	Meaning	Value range	Default setting
Conflict with Hardware Settings	Displays a conflict between the software and hardware DIP switch settings. `active`: the software DIP switch "Operation" is `Off` and the hardware DIP switch is active.	`active`, `inactive`	-

Table 220:"DIP-Switch Status" frame in the `Advanced:DIP-Switch` dialog



Operation

● On ○ Off

DIP-Switch Status

Conflict with Hardware Settings □

DIP-Switch On □

Ring Manager On □

Standby On □

Ring Ports 1.1 & 1.2

Figure 107:`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 `Basic Settings:Load/Save` dialog and click "Save".
Reload	Updates the fields with the values that are saved in the volatile memory (`RAM`) of the device.
Help	Opens the online help.

Table 221:Buttons

8.5 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 222:Buttons

A Appendix

A.1 Technical Data

Switching	
Size of MAC address table (incl. static filters)	8,000 (16,000 for PowerMICE and MACH 4000)
Max. number of statically configured MAC address filters	100
Max. number of MAC address filters learnable via GMRP/IGMP Snooping	512 (RS20/RS30/RS40, RSR20/RSR30, MS20/MS30, OCTOPUS, MACH 100, MACH 1000) 1,000 (PowerMICE, MACH 104, MACH 1040, MACH 4000)
Max. length of over-long packets	– 1,632 bytes (RS20/RS30/RS40, RSR20/RSR30, MS20/MS30, OCTOPUS, MACH 100, MACH 1000) – 1,552 bytes (PowerMICE) – 9,022 Bytes (MACH 104, MACH 1040, MACH 4000)

VLAN	
VLAN ID	1 to 4,042
Number of VLANs	max. 255 simultaneously per device (PowerMICE, MACH 104, MACH 1040, MACH 4000: 256 simultaneously per device) max. 255 simultaneously per port (PowerMICE, MACH 104, MACH 1040, MACH 4000: 256 simultaneously per port)
Number of VLANs in GMRP in VLAN 1	max. 255 simultaneously per device (PowerMICE, MACH 104, MACH 1040, MACH 4000: 256 simultaneously per device) max. 255 simultaneously per port (PowerMICE, MACH 104, MACH 1040, MACH 4000: 256 simultaneously per port)

A.2 List of RFCs

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

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

A.7.2 Broadcom Corporation

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

B Index

C Readers’ Comments

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

Your assessment of this manual:

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

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

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

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