HIRSCHMANN
A Belden Company

User Manual

Basic Configuration
Industrial ETHERNET (Gigabit-)Switch
RS20/RS30/RS40, MS20/MS30, OCTOPUS, Power MICE, RSR20/RSR30, MACH 1000, MACH 4000

Technical Support
HAC-Support@hirschmann.de

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

The performance features described here are binding only if they have been expressly guaranteed in the contract. This publication has been created by Hirschmann Automation and Control GmbH according to the best of our knowledge. Hirschmann reserves the right to change the contents of this manual without prior notice. Hirschmann can give no guarantee in respect of the correctness or accuracy of the details in this publication.

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

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

Content

Content 3

About this Manual 9

Key 11

Introduction 13

1 Access to the user interfaces 15

1.1 System Monitor 16

1.2 Command Line Interface 18

1.3 Web-based Interface 21

2 Entering the IP Parameters 25

2.1 IP Parameter Basics 27
2.1.1 IP address (version 4) 27
2.1.2 Network mask 28

2.2 Entering IP parameters via CLI 32

2.3 Entering the IP Parameters via HiDiscovery 35

2.4 Loading the system configuration from the ACA 38

2.5 System configuration via BOOTP 40

2.6 System configuration via DHCP 45

2.7 System configuration via DHCP Option 82 48

2.8 Web-based IP configuration 49

2.9 Faulty device replacement 51

3 Loading/saving settings 53

3.1 Loading settings 54
3.1.1 Loading from the local non-volatile memory 55
3.1.2 Loading from the AutoConfiguration Adapter 55
3.1.3 Loading from a file 56
3.1.4 Resetting the configuration to the state on delivery 58

3.2 Saving settings 59
3.2.1 Saving locally (and on the ACA) 59
3.2.2 Saving in a file on URL 60
3.2.3 Saving in a binary file on the PC 61
3.2.4 Saving as a script on the PC 61

4 Loading software updates 63

4.1 Loading the software from the ACA 65
4.1.1 Selecting the software to be loaded 66
4.1.2 Starting the software 67
4.1.3 Performing a cold start 67

4.2 Loading the software from the tftp server 68

4.3 Loading the software via file selection 70

5 Configuring the ports 71

6 Protection from unauthorized access 75

6.1 Password for SNMP access 76
6.1.1 Description of password for SNMP access 76
6.1.2 Entering the password for SNMP access 77

6.2 Telnet/Web/SSH access 81
6.2.1 Description of Telnet access 81
6.2.2 Description of Web access 81
6.2.3 Description of SSH access 82
6.2.4 Enabling/disabling Telnet/Web/SSH access 83

6.3 Disabling the HiDiscovery function 84
6.3.1 Description of the HiDiscovery protocol 84
6.3.2 Enabling/disabling the HiDiscovery function 84

6.4 Port access control 85
6.4.1 Port access control 85
6.4.2 Defining port access control 86

6.5 Port authentication acc. to 802.1X 88
6.5.1 Description of port authentication according to 802.1X 88
6.5.2 Authentication process according to 802.1X 89
6.5.3 Preparing the device for the 802.1X port authentication 89
6.5.4 Setting 802.1X 90

7 Network load control 91

7.1 Direct packet distribution 92
7.1.1 Store-and-forward 92
7.1.2 Multi-address capability 92
7.1.3 Aging of learned addresses 93
7.1.4 Entering static address entries 94
7.1.5 Disabling the direct packet distribution 95

7.2 Multicast application 96
7.2.1 Description of the Multicast application 96
7.2.2 Example of a Multicast application 97
7.2.3 Description of IGMP Snooping 98
7.2.4 Description of GMRP 99
7.2.5 Setting up the Multicast application 100

7.3 Rate Limiter 106
7.3.1 Description of the Rate Limiter 106
7.3.2 Rate Limiter settings for MACH 4000 and Power MICE 106
7.3.3 Rate Limiter settings for RS20/RS30/40, MS20/MS30, MACH 1000 and OCTOPUS 107

7.4 QoS/Priority 110
7.4.1 Description of Prioritization 110
7.4.2 VLAN tagging 111
7.4.3 IP ToS / DiffServ 113
7.4.4 Management prioritizing 116
7.4.5 Handling of received priority information 116
7.4.6 Handling of traffic classes 117
7.4.7 Setting prioritization 117

7.5 Flow control 122
7.5.1 Description of flow control 122
7.5.2 Setting the flow control 124

7.6 VLANs 125
7.6.1 Description of VLANs 125
7.6.2 Configuring VLANs 128
7.6.3 Example of a simple VLAN 131

8 Synchronizing the system time in the network 139

8.1 Entering the time 140

8.2 SNTP 142

8.2.1 Description of SNTP 142
8.2.2 Preparing the SNTP coordination 143
8.2.3 Configuring SNTP 144

8.3 Precision Time Protocol 148
8.3.1 Description of PTP functions 148
8.3.2 Preparing the PTP configuration 152
8.3.3 Configuring PTP 153

8.4 Interaction of PTP and SNTP 156

9 Operation diagnosis 159

9.1 Sending traps 160
9.1.1 SNMP trap listing 161
9.1.2 SNMP traps when booting 162
9.1.3 Configuring traps 163

9.2 Monitoring the device status 165
9.2.1 Configuring the device status 166
9.2.2 Displaying the device status 166

9.3 Out-of-band signaling 168
9.3.1 Controlling the signal contact 169
9.3.2 Monitoring correct operation via the signal contact 170
9.3.3 Monitoring the device status via the signal contact 171

9.4 Port status indication 172

9.5 Event counter at port level 173

9.6 Displaying the SFP status 175

9.7 TP cable diagnosis 176

9.8 Topology discovery 177
9.8.1 Description of topology discovery 177
9.8.2 Displaying the topology discovery 178

9.9 Detecting IP address conflicts 181
9.9.1 Description of IP address conflicts 181
9.9.2 Configuring ACD 182
9.9.3 Displaying ACD 182

9.10 Reports 184

9.11 Monitoring port traffic (port mirroring) 186

A Setting up configuration environment 189

A.1 Setting up DHCP/BOOTP server 190

A.2 Setting up DHCP Server Option 82 196

A.3 tftp server for software updates 200
A.3.1 Setting up the tftp process 201
A.3.2 Software access rights 204

A.4 Preparing access via SSH 205
A.4.1 Generating a key 205
A.4.2 Uploading the key 206
A.4.3 Access via SSH 207

B General information 209

B.1 Management Information Base (MIB) 210

B.2 Abbreviations used 213

B.3 List of RFC's 214

B.4 Based specifications and standards 216

B.5 Technical Data 217

B.6 Copyright of integrated software 218
B.6.1 Bouncy Castle Crypto APIs (Java) 218
B.6.2 LVL7 Systems, Inc. 219

B.7 Reader´s comments 220

C Index 223

D Further support 227

About this Manual

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

The following thematic sequence has proven itself in practice:

- Set up device access for operation by entering the IP parameters
- Check the status of the software and update it if necessary
- Load/store the configuration
- Configure the ports
- Set up protection from unauthorized access
- Optimize the data transmission with network load control
- Synchronize system time in the network
- Function diagnosis

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

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

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

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

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

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

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

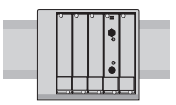
Key

The designations used in this manual have the following meanings:

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

Symbols used:

	Router with firewall
	Switch with firewall
	Router
	Switch
	Bridge
	Hub

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

Introduction

The device has been developed for practical application in a harsh industrial environment. Accordingly, the installation process has been kept simple. Thanks to the selected default settings, you only have to enter a few settings before starting to operate the device.

1 Access to the user interfaces

The device has three user interfaces, which you can access via different interfaces:

- System monitor via the V.24 interface (out-of-band)
- Command Line Interface (CLI) via the V.24 connection (out-of-band) and Telnet (in-band)
- Web-based interface via Ethernet (in-band).

1.1 System Monitor

The system monitor enables you to

- select the software to be loaded
- perform a software update
- start the selected software
- shut down the system monitor
- delete the configuration saved and
- display the boot code information.

Opening the system monitor

☐ Use the terminal cable (see accessories) to connect
  – the V.24 socket (RJ11) to
  – a terminal or a COM port of a PC with terminal emulation based on VT100
  (for the physical connection, see the "Installation" user manual).

Speed	9,600 Baud
Data	8 bit
Parity	none
Stopbit	1 bit
Handshake	off

Table 1: Data transfer parameters

☐ Start the terminal program on the PC and set up a connection with the device.

When you boot the device, the message
"Press <1> to enter System Monitor 1"
appears on the terminal.

```
< PowerMICE MS4128-5  (Boot) Release: 1.00 Build: 2005-09-17 15:36 >

Press <1> to enter System Monitor 1 ...
 1
```

Figure 1: Screen display during the boot process

☐ Press the <1> key within one second to start system monitor 1.

```
   System Monitor

   (Selected OS: L3P-01.0.00-K16 (2005-10-31 19:32))

   1  Select Boot Operating System
   2  Update Operating System
   3  Start Selected Operating System
   4  End (reset and reboot)
   5  Erase main configuration file



sysMon1>
```

Figure 2: System monitor 1 screen display

☐ Select a menu item by entering the number.
☐ To leave a submenu and return to the main menu of system monitor 1, press the <ESC> key.

1.2 Command Line Interface

The Command Line Interface enables you to use all the functions of the device via a local or remote connection.
The Command Line Interface provides IT specialists with a familiar environment for configuring IT devices.
The script compatibility of the Command Line Interface enables you, among other things, to feed multiple devices with the same configuration data.

You will find a detailed description of the Command Line Interface in the "Command Line Interface" reference manual.

Note: To facilitate making entries, CLI gives you the option of abbreviating keywords. Type in the beginning of a keyword. When you press the tab key, CLI completes the keyword.

Opening the Command Line Interface

☐ Connect the device to a terminal or to the COM port of a PC using terminal emulation based on VT100 and press any key (see on page 16 „Opening the system monitor“) or
call up the Command Line Interface via Telnet.
A window for entering the user name appears on the screen.
Up to five users can access the Command Line Interface.

```
        Copyright (c) 2004-2005 Hirschmann Automation and Control GmbH
                            All rights reserved

                         PowerMICE Release L3P-01.0.00-K16

                         (Build date 2005-10-31 19:32)



                        System Name:  PowerMICE
                        Mgmt-IP    :  149.218.112.105
                        1.Router-IP:  0.0.0.0
                        Base-MAC   :  00:80:63:51:74:00
                        System Time:  2005-11-01 16:00:59


User:
```

Figure 3: Logging in to the Command Line Interface program

- ☐ Enter a user name. The default setting for the user name is **admin**. Press the Enter key.
- ☐ Enter the password. The default setting for the password is **private**. Press the Enter key.
  You can change the user name and the password later in the Command Line Interface.
  Please note that these entries are case-sensitive.

The start screen appears.

```
NOTE: Enter '?' for Command Help. Command help displays all options
      that are valid for the 'normal' and 'no' command forms.  For
      the syntax of a particular command form, please consult the
      documentation.


(Hirschmann PowerMICE) >
```

Figure 4: CLI screen after login

1.3 Web-based Interface

The user-friendly Web-based interface gives you the option of operating the device from any location in the network via a standard browser such as Mozilla Firefox or Microsoft Internet Explorer.
As a universal access tool, the Web browser uses an applet which communicates with the device via the Simple Network Management Protocol (SNMP).
The Web-based interface allows you to graphically configure the device..

Opening the Web-based Interface

To open the Web-based interface, you will need a Web browser (a program that can read hypertext), for example Mozilla Firefox version 1 or later, or Microsoft Internet Explorer version 6 or later.

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

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

Figure 5: Installing Java

- ☐ Start your Web browser.
- ☐ Make sure that you have activated JavaScript and Java in the security settings of your browser.
- ☐ Establish the connection by entering the IP address of the device which you want to administer via the Web-based management in the address field of the Web browser. Enter the address in the following form:
  `http://xxx.xxx.xxx.xxx`

  The login window appears on the screen.

Figure 6: Login window

- ☐ Select the desired language.
- ☐ In the drop-down menu, you select
  – user, to have read access, or
  – admin, to have read and write access

  to the device.
- ☐ The password "public", with which you have read access, appears in the password field. If you wish to have write access to the device, then highlight the contents of the password field and overwrite it with the password "private" (default setting).
- ☐ Click on OK.

The website of the device appears on the screen.

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

Note: You can block your access to the device by entering an incorrect configuration.
Activating the function "Cancel configuration change" in the "Load/Save" dialog enables you to return automatically to the last configuration after a set time period has elapsed. This gives you back your access to the device.

2 Entering the IP Parameters

The IP parameters must be entered when the device is installed for the first time.

The device provides 6 options for entering the IP parameters during the first installation:

- Using the Command Line Interface (CLI). Choose this "out of band" method if
  - you preconfigure your device outside its operating environment
  - you do not have network access ("in-band") to the device

  (see page 32 „Entering IP parameters via CLI“).
- Using the HiDiscovery protocol. Choose this "in band" method if the device is already installed in the network or if you have another Ethernet connection between your PC and the device (see page 35 „Entering the IP Parameters via HiDiscovery“).
- Using the AutoConfiguration Adapter (ACA). Choose this method if you are replacing a device with a device of the same type and have already saved the configuration on an ACA (see page 38 „Loading the system configuration from the ACA“).
- Using BOOTP. Choose this "in band" method if you want to configure the installed device using BOOTP. You need a BOOTP server for this. The BOOTP server assigns the configuration data to the device using its MAC address (see page 40 „System configuration via BOOTP“). Because the device is delivered with "DHCP mode" as the setting for the configuration data reference, you have to reset this to the BOOTP mode for this method.
- Using DHCP. Choose this "in band" method if you want to configure the installed device using DHCP. You need a DHCP server for this. The DHCP server assigns the configuration data to the device using its MAC address or its system name (see page 45 „System configuration via DHCP“).
- Using DHCP Option 82. Choose this "in band" method if you want to configure the installed device using DHCP Option 82. You need a DHCP server with Option 82 for this. The DHCP server assigns the configuration data to the device using its physical connection (see page 48 „System configuration via DHCP Option 82“).

If the device already has an IP address and can be reached via the network, then the Web-based interface provides you with another option for configuring the IP parameters.

2.1 IP Parameter Basics

2.1.1 IP address (version 4)

The IP addresses consist of 4 bytes. These 4 bytes are written in decimal notation, separated by a decimal point.

Since 1992, five classes of IP address have been defined in the RFC 1340.

Class	Network address	Host address	Address range
A	1 byte	3 bytes	1.0.0.0 to 126.255.255.255
B	2 bytes	2 bytes	128.0.0.0 to 191.255.255.255
C	3 bytes	1 byte	192.0.0.0 to 223.255.255.255
D			224.0.0.0 to 239.255.255.255
E			240.0.0.0 to 255.255.255.255

Table 2: IP address classes

The network address is the fixed part of the IP address. The worldwide leading regulatory board for assigning network addresses is the IANA (Internet Assigned Numbers Authority). If you require an IP address block, contact your Internet service provider. Internet service providers should contact their local higher-level organization:

- APNIC (Asia Pacific Network Information Center) - Asia/Pacific Region
- ARIN (American Registry for Internet Numbers) - Americas and Sub-Sahara Africa
- LACNIC (Regional Latin-American and Caribbean IP Address Registry) – Latin America and some Caribbean Islands
- RIPE NCC (Réseaux IP Européens) - Europe and Surrounding Regions

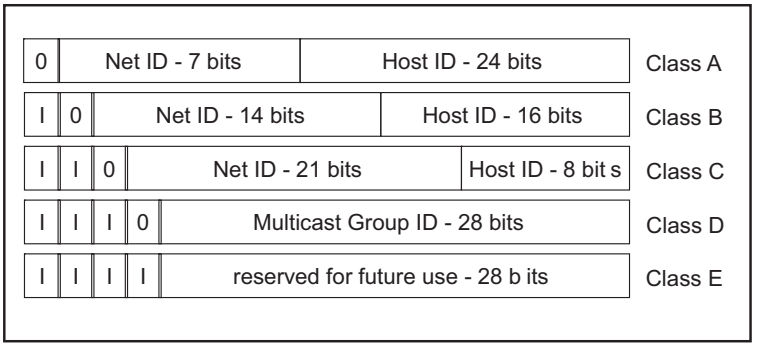


Figure 7: Bit representation of the IP address

An IP address belongs to class A if its first bit is a zero, i.e. the first decimal number is less than 128. The IP address belongs to class B if the first bit is a one and the second bit is a zero, i.e. the first decimal number is between 128 and 191. The IP address belongs to class C if the first two bits are a one, i.e. the first decimal number is higher than 191.

Assigning the host address (host id) is the responsibility of the network operator. He alone is responsible for the uniqueness of the IP addresses he assigns.

2.1.2 Network mask

Routers and gateways subdivide large networks into subnetworks. The network mask assigns the IP addresses of the individual devices to a particular subnetwork.

The division into subnetworks with the aid of the network mask is performed in much the same way as the division of the network addresses (net id) into classes A to C.

In bits of the host address (host id) that represent the mask are set to one. The remaining bits of the host address in the network mask are set to zero (see the following examples).

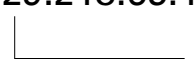
Example of a network mask:

Decimal notation
255.255.192.0

Binary notation
11111111.11111111.11000000.00000000

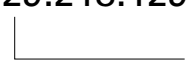
Example of IP addresses with subnetwork assignment when the above subnet mask is applied:

Decimal notation
129.218.65.17

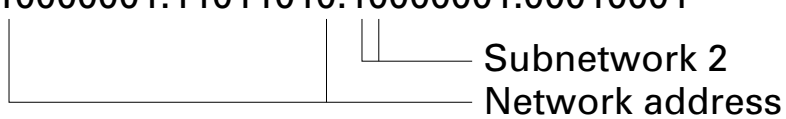


binary notation
10000001.11011010.01000001.00010001

Decimal notation
129.218.129.17



binary notation
10000001.11011010.10000001.00010001



Example of how the network mask is used

In a large network it is possible that gateways and routers separate the management agent from its management station. How does addressing work in such a case?

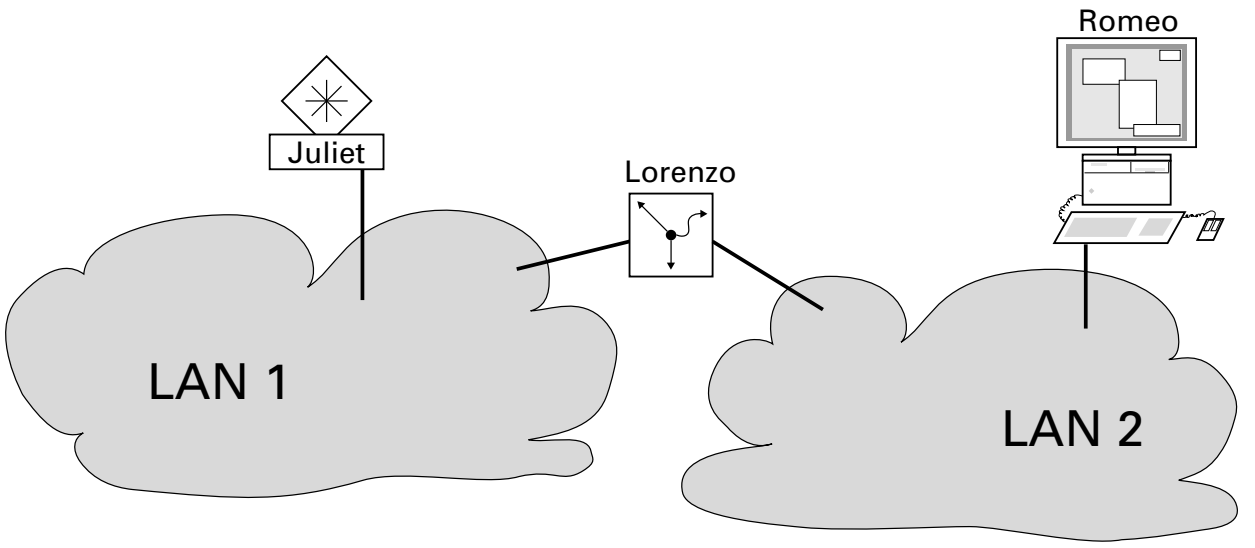


Figure 8: Management agent that is separated from its management station by a router

The management station "Romeo" wants to send data to the management agent "Juliet". Romeo knows Juliet's IP address and also knows that the router "Lorenzo" knows the way to Juliet.

Romeo therefore puts his message in an envelope and writes Juliet's IP address as the destination address. For the source address he writes his own IP address on the envelope.

Romeo then places this envelope in a second one with Lorenzo's MAC address as the destination and his own MAC address as the source. This process is comparable to going from layer 3 to layer 2 of the ISO/OSI base reference model.

Finally, Romeo puts the entire data packet into the mailbox. This is comparable to going from layer 2 to layer 1, i.e. to sending the data packet over the Ethernet.

Lorenzo receives the letter and removes the outer envelope. From the inner envelope he recognizes that the letter is meant for Juliet. He places the inner envelope in a new outer envelope and searches his address list (the ARP table) for Juliet's MAC address. He writes her MAC address on the outer envelope as the destination address and his own MAC address as the source address. He then places the entire data packet in the mail box.

Juliet receives the letter and removes the outer envelope. She finds the inner envelope with Romeo's IP address. Opening the inner envelope and reading its contents corresponds to transferring the message to the higher protocol layers of the SO/OSI layer model.

Juliet would now like to send a reply to Romeo. She places her reply in an envelope with Romeo's IP address as destination and her own IP address as source. But where is she to send the answer? For she did not receive Romeo's MAC address. It was lost when Lorenzo replaced the outer envelope.

In the MIB, Juliet finds Lorenzo listed under the variable hmNetGatewayIPAddr as a means of communicating with Romeo. She therefore puts the envelope with the IP addresses in a further envelope with Lorenzo's MAC destination address.

The letter now travels back to Romeo via Lorenzo, the same way the first letter traveled from Romeo to Juliet.

2.2 Entering IP parameters via CLI

If you do not configure the system via BOOTP/DHCP, DHCP Option 82, the HiDiscovery protocol or the ACA auto configuration adapter, then you perform the configuration via the V.24 interface using the CLI.

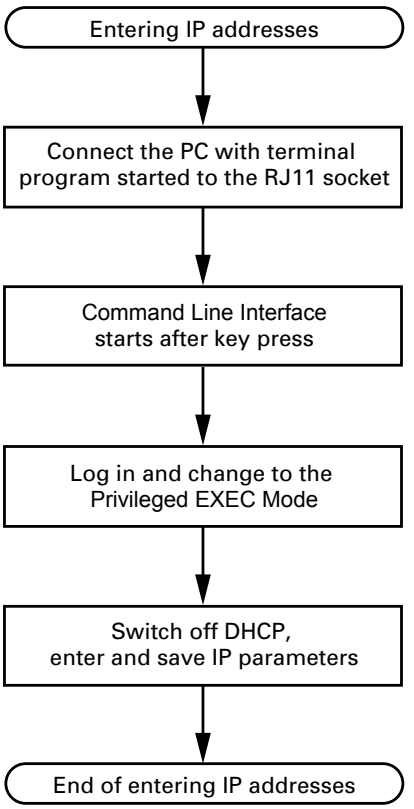


Figure 9: Flow chart for entering IP addresses

If there is no terminal or PC with terminal emulation available in the vicinity of the installation location, you can enter the IP parameters at your own workstation prior to the ultimate installation.

☐ In accordance with the „Opening the Command Line Interface“ dialog on page 18, set up a connection with the device.

The start screen appears.

```
NOTE: Enter '?' for Command Help. Command help displays all options
      that are valid for the 'normal' and 'no' command forms.  For
      the syntax of a particular command form, please consult the
      documentation.


(Hirschmann PowerMICE) >
```

☐ Change to the Privileged EXEC mode by entering `enable` and pressing the Enter key.

☐ Disable DHCP by entering `network protocol none` and then pressing the Enter key.

☐ Enter the IP parameters with `network parms <IP address> <network mask> [<Gateway>]` and press the Enter key.

- Local IP address
  On delivery, the device has the local IP address 0.0.0.0.
- Network mask
  If your network has been divided up into subnetworks, and if these are identified with a network mask, then the network mask is to be entered here.
  The default setting of the network mask is 0.0.0.0.
- IP address of the gateway
  This entry is only required if the device and the management station or tftp server are located in different subnetworks (see page 30 „Example of how the network mask is used“).
  Enter the IP address of the gateway between the subnetwork with the device and the path to the management station.
  The default setting of the IP address is 0.0.0.0.

☐ Save the configuration entered using
`copy system:running-config nvram:startup-config`
and press the Enter key.
Confirm that you want to save it by pressing `y`.

```
NOTE: Enter '?' for Command Help. Command help displays all options
that are valid for the 'normal' and 'no' command forms.  For      the
syntax of a particular command form, please consult the      documen-
tation.


(Hirschmann PowerMICE) >en

(Hirschmann PowerMICE) #network protocol none
(Hirschmann PowerMICE) #network parms 149.218.112.105 255.255.255.0

(Hirschmann PowerMICE) #copy system:running-config nvram:startup-con-
fig

Are you sure you want to save? (y/n) y
Copy OK: 15811 bytes copied

Configuration Saved!

(Hirschmann PowerMICE) #
```

After entering the IP parameters, you can easily configure the device via the Web-based interface (see the “Web-based Interface” reference manual).

2.3 Entering the IP Parameters via HiDiscovery

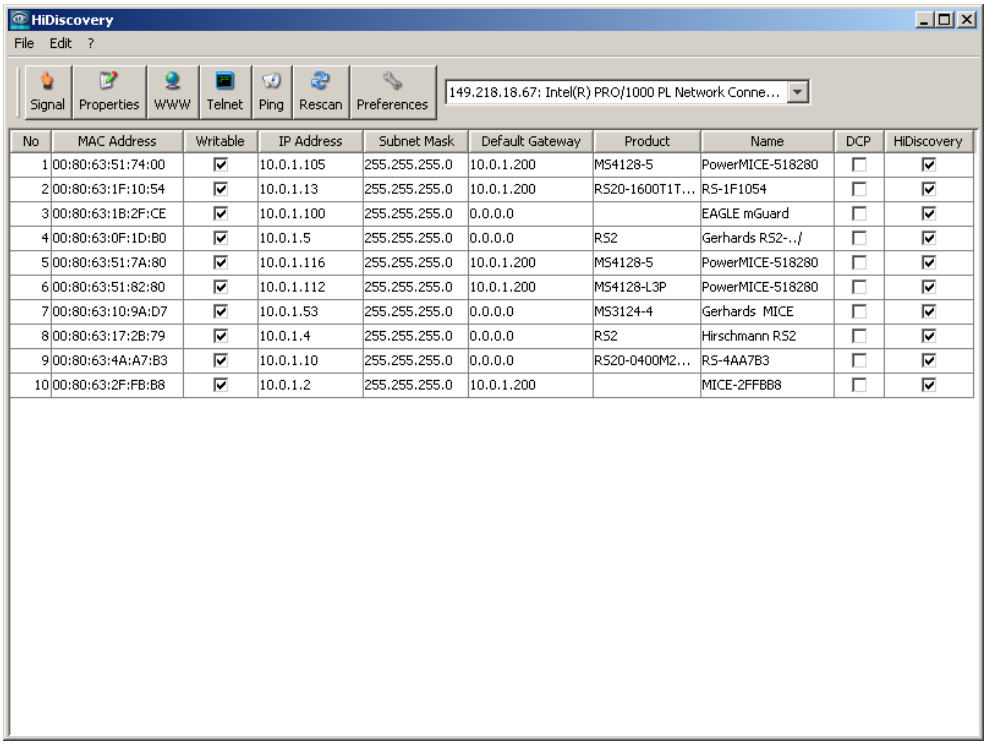
The HiDiscovery protocol enables you to assign IP parameters to the device via the Ethernet.
You can easily configure other parameters via the Web-based interface (see the "Web-based Interface" reference manual).

Install the HiDiscovery software on your PC. The software is on the CD supplied with the device.

☐ To install it, you start the installation program on the CD.

Note: The installation of HiDiscovery involves installing the WinPcap Version 3.0 software package.
If an earlier version of WinPcap is already installed on the PC, then you must first uninstall it. A newer version remains intact when you install HiDiscovery. However, this cannot be guaranteed for all future versions of WinPcap. In the event that the installation of HiDiscovery has overwritten a newer version of WinPcap, you uninstall WinPcap 3.0 and then re-install the new version.

☐ Start the HiDiscovery program.



No	MAC Address	Writable	IP Address	Subnet Mask	Default Gateway	Product	Name	DCP	HiDiscovery
1	00:80:63:51:74:00	☑	10.0.1.105	255.255.255.0	10.0.1.200	MS4128-5	PowerMICE-518280	☐	☑
2	00:80:63:1F:10:54	☑	10.0.1.13	255.255.255.0	10.0.1.200	RS20-1600T1T...	RS-1F1054	☐	☑
3	00:80:63:1B:2F:CE	☑	10.0.1.100	255.255.255.0	0.0.0.0		EAGLE mGuard	☐	☑
4	00:80:63:0F:1D:B0	☑	10.0.1.5	255.255.255.0	0.0.0.0	RS2	Gerhards RS2-../	☐	☑
5	00:80:63:51:7A:80	☑	10.0.1.116	255.255.255.0	10.0.1.200	MS4128-5	PowerMICE-518280	☐	☑
6	00:80:63:51:82:80	☑	10.0.1.112	255.255.255.0	10.0.1.200	MS4128-L3P	PowerMICE-518280	☐	☑
7	00:80:63:10:9A:D7	☑	10.0.1.53	255.255.255.0	0.0.0.0	MS3124-4	Gerhards MICE	☐	☑
8	00:80:63:17:2B:79	☑	10.0.1.4	255.255.255.0	0.0.0.0	RS2	Hirschmann RS2	☐	☑
9	00:80:63:4A:A7:B3	☑	10.0.1.10	255.255.255.0	0.0.0.0	RS20-0400M2...	RS-4AA7B3	☐	☑
10	00:80:63:2F:FB:B8	☑	10.0.1.2	255.255.255.0	10.0.1.200		MICE-2FFBB8	☐	☑

Figure 10: HiDiscovery

When HiDiscovery is started, it automatically searches the network for those devices which support the HiDiscovery protocol.
HiDiscovery uses the first PC network card found. If your computer has several network cards, you can select these in HiDiscovery on the toolbar.

HiDiscovery displays a line for every device which reacts to the HiDiscovery protocol.

HiDiscovery enables you to identify the devices displayed.

☐ Select a device line.

☐ Click on the symbol with the two green dots in the tool bar to set the LEDs for the selected device flashing. To switch off the flashing, click on the symbol again.

☐ By double-clicking a line, you open a window in which you can enter the device name and the IP parameters.

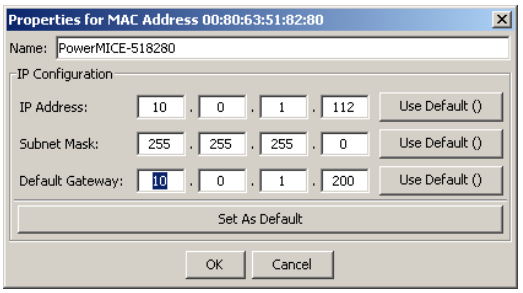


Figure 11: HiDiscovery - assigning IP parameters

Note: When the IP address is entered, the device copies the local configuration settings (see on page 53 „Loading/saving settings“).

Note: For security reasons, switch off the HiDiscovery function for the device in the Web-based interface, after you have assigned the IP parameters to the device (see page 49 „Web-based IP configuration“).

Note: Save the settings so that you will still have the entries after a restart (see on page 53 „Loading/saving settings“).

2.4 Loading the system configuration from the ACA

The AutoConfiguration Adapter (ACA) is a device for

- storing the configuration data of a device and
- storing the device software.

In the case of a device failure, the ACA makes it possible to easily transfer the configuration data by means of a substitute device of the same type.

When you start the device, it checks for an ACA. If it finds an ACA with a valid password and valid software, the device loads the configuration data from the ACA.

The password is valid if

- the password in the device matches the password in the ACA or
- the preset password is entered in the device.

To save the configuration data in the ACA, see „Saving locally (and on the ACA)“ on page 59.

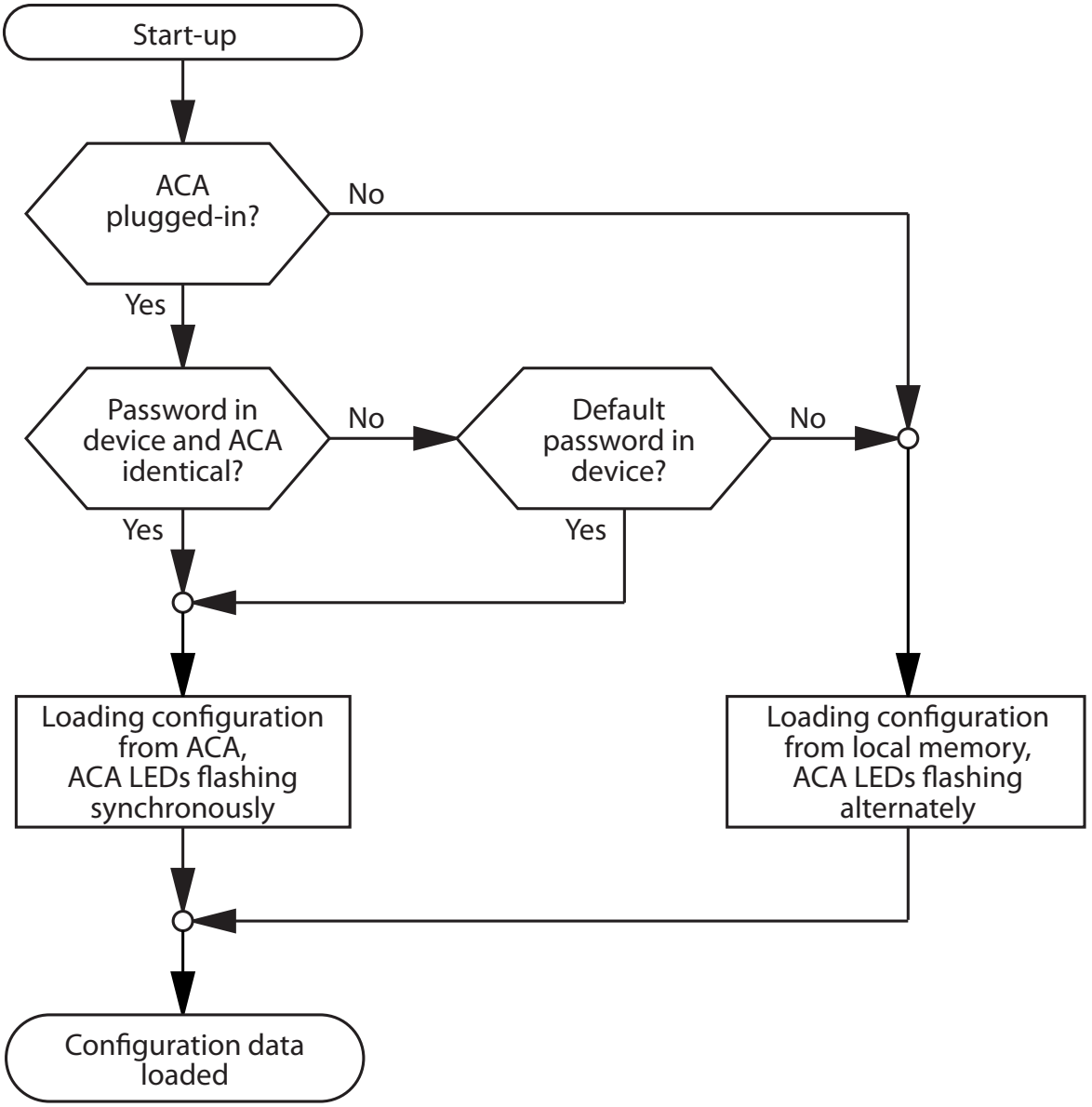


Figure 12: Flow chart of loading configuration data from the ACA

2.5 System configuration via BOOTP

When it is started up via BOOTP (bootstrap protocol), a device receives its configuration in accordance with the "BOOTP process" flow chart (see fig. 13).

Note: In its delivery state, the device gets its configuration data from the DHCP server.

☐ Activate BOOTP to receive the configuration data (see on page 49 „Web-based IP configuration“) or see in the CLI:

`enable`	Switch to the Priviledged EXEC mode.
`configure protocol bootp`	Activate BOOTP.
`copy system:running-config nvram:startup-config`	Activate BOOTP.
`y`	Confirm save..

☐ Provide the BOOTP server with the following data for a device:

```
# /etc/bootptab for BOOTP-daemon bootpd
#
# gw -- gateway
# ha -- hardware address
# ht -- hardware type
# ip -- IP address
# sm -- subnet mask
# tc -- template

.global:\
:gw=0.0.0.0:\
:sm=255.255.240.0:
```

```
switch_01:ht=ethernet:ha=008063086501:ip=149.218.112.83:tc=.global:
switch_02:ht=ethernet:ha=008063086502:ip=149.218.112.84:tc=.global:
.
.
```

Lines that start with a '#' character are comment lines.

The lines under ".global:" make the configuration of several devices easier. With the template (tc) you allocate the global configuration data (tc=.global:) to each device .
The direct allocation of hardware address and IP address occurs in the device lines (switch-0...).

☐ Enter one line for each device.
☐ After ha= enter the hardware address of the device.
☐ After ip= enter the IP address of the device.

In the appendix under „Setting up DHCP/BOOTP server“ on page 190 you will find an example for the configuration of a BOOTP/DHCP server.

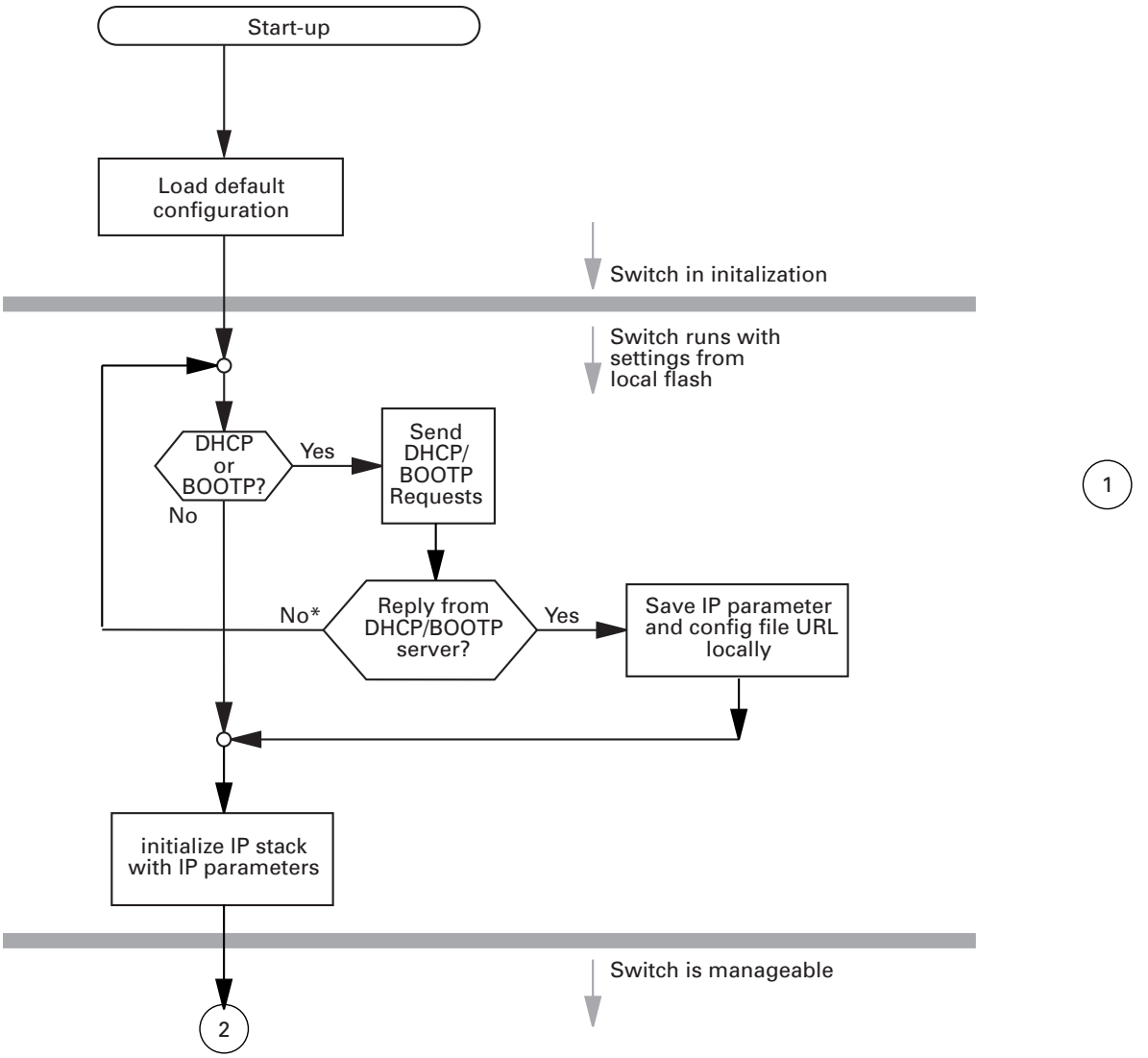


Figure 13: Flow chart for the BOOTP/DHCP process, part 1
** see note fig. 14*

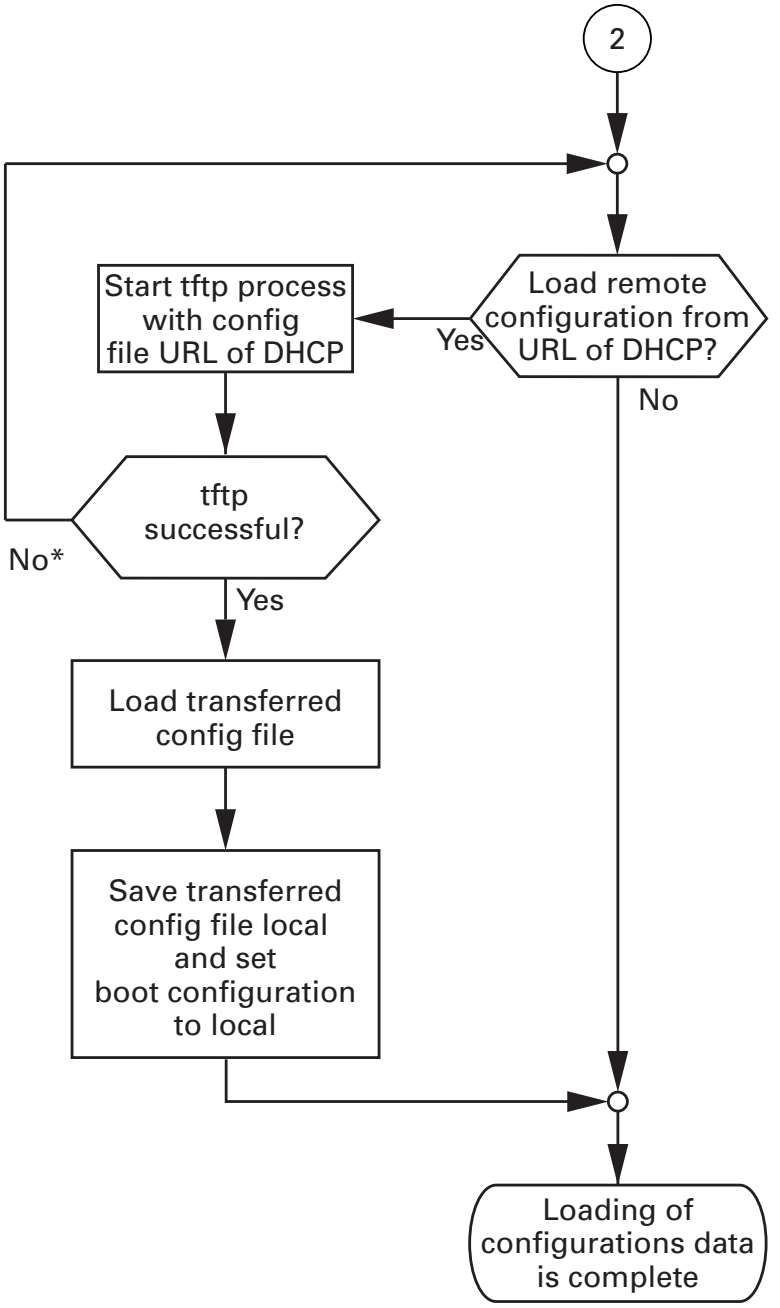


Figure 14: Flow chart for the BOOTP/DHCP process, part 2
** see note*

Note: The loading process started by DHCP/BOOTP (see on page 40 „System configuration via BOOTP“) shows the selection of "from URL & save locally" in the "Load" frame. If you get an error message when saving a configuration, this could be due to an active loading process. DHCP/BOOTP only finishes a loading process when a valid configuration has been loaded. If DHCP/BOOTP does not find a valid configuration, then finish the loading process by loading the local configuration in the "Load" frame.

2.6 System configuration via DHCP

The DHCP (dynamic host configuration protocol) responds similarly to the BOOTP and additionally offers the configuration of a DHCP client via a name instead of via the MAC address. For the DHCP, this name is known as the "client identifier" in accordance with rfc 2131.
The device uses the name entered under sysName in the system group of the MIB II as the client identifier. You can enter this system name directly via SNMP, the Web-based management (see system dialog), or the Command Line Interface.

On startup, a device receives its configuration data according to the "BOOTP/DHCP process" flow chart (see fig. 13).

The device sends its system name to the DHCP server. The DHCP server can then use the system name to assign an IP address as an alternative to the MAC address.
In addition to the IP address, the DHCP server sends
– the tftp server name (if available),
– the name of the configuration file (if available).
The device accepts this data as configuration parameters (see on page 49 „Web-based IP configuration“). If an IP address was assigned by a DHCP server, it will be permanently saved locally.

Option	Meaning
1	Subnet mask
2	Time offset
3	Router
4	Time server
12	Host name
61	Client identifier
66	TFTP server name
67	Bootfile name

Table 3: DHCP options which the device requests

The special feature of DHCP in contrast to BOOTP is that the DHCP server can only provide the configuration parameters for a certain period of time ("lease"). When this time period ("lease duration") expires, the DHCP client must attempt to renew the lease or negotiate a new one. A response similar to BOOTP can be set on the server (i.e. the same IP address is always assigned to a particular client using the MAC address), but this requires the explicit configuration of a DHCP server in the network. If this configuration was not performed, a random IP address – whichever one happens to be available – is assigned.

On delivery, DHCP is activated.
As long as DHCP is activated, the device attempts to obtain an IP address. If it cannot find a DHCP server after restarting, it will not have an IP address.
To activate/deactivate DHCP (see on page 49 „Web-based IP configuration“).

Note: When using HiVision network management, ensure that DHCP always assigns the original IP address to each device.

In the appendix under „Setting up DHCP/BOOTP server“ on page 190 you will find an example for the configuration of a BOOTP/DHCP server.

Example of a DHCP configuration file:

```
# /etc/dhcpd.conf for DHCP Daemon
#
subnet 149.218.112.0 netmask 255.255.240.0 {
option subnet-mask 255.255.240.0;
option routers 149.218.112.96;
}
#
# Host berta requests IP configuration
# with her MAC address
#
host berta {
hardware ethernet 00:80:63:08:65:42;
fixed-address 149.218.112.82;
}
#
# Host hugo requests IP configuration
# with his client identifier.
```

```
#
host hugo {
#  option dhcp-client-identifier "hugo";
option dhcp-client-identifier 00:68:75:67:6f;
fixed-address 149.218.112.83;
server-name "149.218.112.11";
filename "/agent/config.dat";
}
```

Lines that start with a '#' character are comment lines.
The lines preceding the individually listed devices refer to settings that apply to all the following devices.
The fixed-address line assigns a permanent IP address to the device.
For further information, please refer to the DHCP server manual.

2.7 System configuration via DHCP Option 82

As with the classic DHCP, on startup an agent receives its configuration data according to the "BOOTP/DHCP process" flow chart (see fig. 13).

While the system configuration is based on the classical DHCP protocol (see on page 45 „System configuration via DHCP“) on the device being configured, Option 82 is based on the network topology. This procedure gives you the option of always assigning the same IP address to any device which is connected to a particular location (port of a device) on the LAN.
The installation of a DHCP server is described in the chapter „Setting up DHCP Server Option 82“ on page 196.

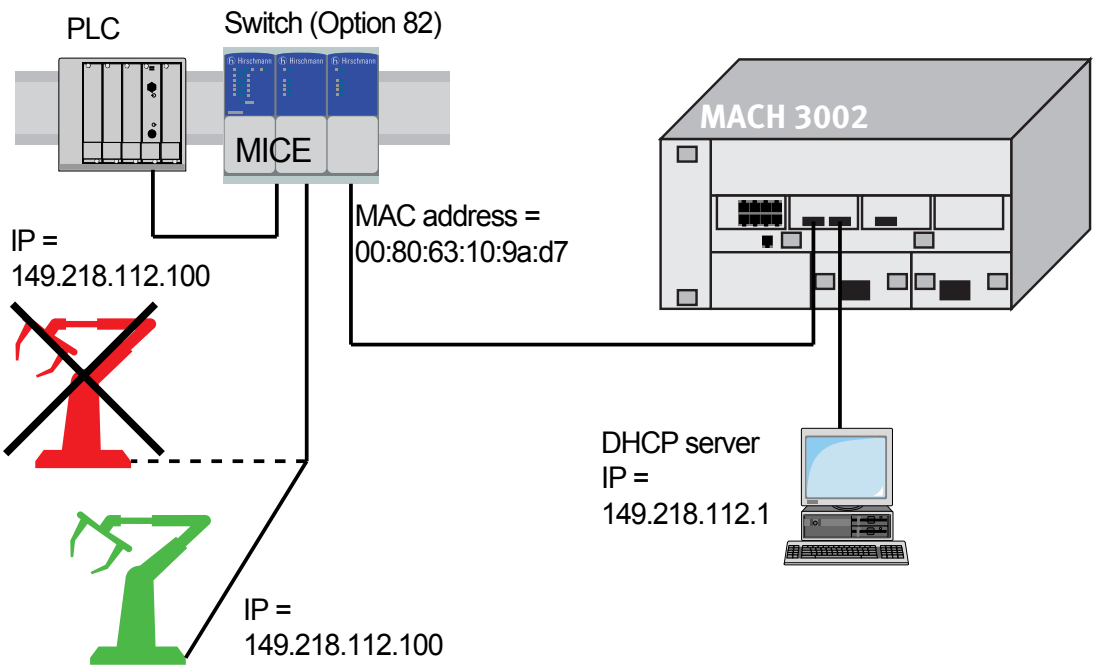


Figure 15: Application example of using Option 82

2.8 Web-based IP configuration

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

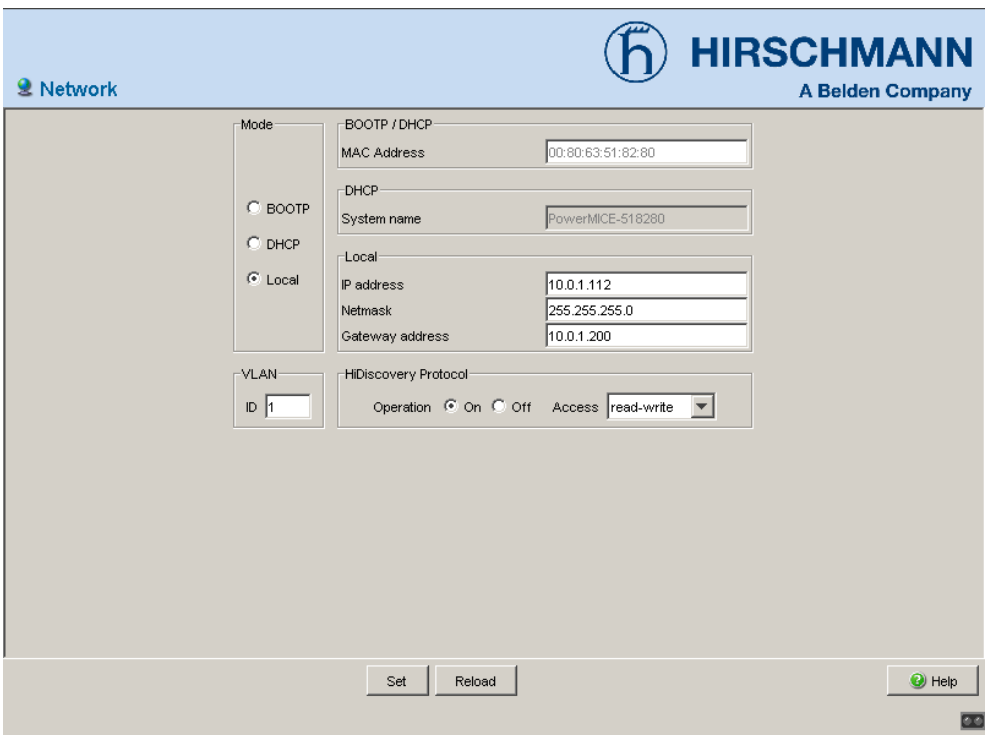


Figure 16: Network parameters dialog

☐ Under "Mode", enter where the device is to obtain its IP parameters:
- ▶ In the BOOTP mode, the configuration is via a BOOTP or DHCP server on the basis of the MAC address of the device (see page 190 „Setting up DHCP/BOOTP server“).
- ▶ In the DHCP mode, the configuration is via a DHCP server on the basis of the MAC address or the name of the device (see page 190 „Setting up DHCP/BOOTP server“).
- ▶ In the local mode the net parameters in the device memory are used.

☐ Enter the parameters on the right according to the selected mode.

- ☐ You enter the name applicable to the DHCP protocol in the "Name" line in the system dialog of the Web-based interface.
- ☐ The "VLAN ID" frame enables you to assign a VLAN to the agent. If you enter the illegal VLAN ID "0" here, the agent can be accessed by all VLANs.
- ☐ The HiDiscovery protocol allows you to assign an IP address to the device on the basis of its MAC address. Activate the HiDiscovery protocol if you want to assign an IP address to the device from your PC with the enclosed HiDiscovery software (setting on delivery: active).

Note: Save the settings so that you will still have the entries after a restart (see page 53 „Loading/saving settings“).

2.9 Faulty device replacement

The device provides two plug-and-play solutions for replacing a faulty device with a device of the same type (faulty device replacement):

- Configuring the new device via an AutoConfiguration Adapter (see on page 38 „Loading the system configuration from the ACA“) or
- Configuration via DHCP Option 82 (see on page 196 „Setting up DHCP Server Option 82“).

In both cases, when the new device is started, it is given the same configuration data that the faulty device had.

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

3 Loading/saving settings

The device saves settings such as the IP parameters and the port configuration in the temporary memory. These settings are lost when you switch off or reboot the device.
The device enables you to

- load settings from a non-volatile memory into the temporary memory
- save settings from the temporary memory in a non-volatile memory.

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

3.1 Loading settings

When it is restarted, the device loads its configuration data from the local non-volatile memory, once you have not activated BOOTP/DHCP and no ACA is connected to the device.

During operation, the device allows you to load settings from the following sources:

- the local non-volatile memory
- the AutoConfiguration Adapter. If an ACA is connected to the device, the device always loads its configuration from the ACA.
- a file in the connected network (= state on delivery)
- a binary file or an editable and readable script on the PC and
- the firmware.

Note: When loading a configuration, do not access the device until it had loaded the configuration file and has made the new configuration settings. Depending on the complexity of the configuration settings, this procedure can take 10-200 seconds.

3.1.1 Loading from the local non-volatile memory

When loading the configuration data locally, the device loads the configuration data from the local non-volatile memory if no ACA is connected to the device.

- ☐ Select the `Basics: Load/Save` dialog.
- ☐ In the "Load" frame, click "Local".
- ☐ Click "Load configuration".

`enable`	Switch to the Priviledged EXEC mode.
`copy nvram:startup-config system:running-config`	The device loads the configuration data from the local non-volatile memory.

3.1.2 Loading from the AutoConfiguration Adapter

If an ACA is connected to the device, the device always loads its configuration from the ACA.
The chapter „Saving locally (and on the ACA)“ dialog on page 59 describes how to save a configuration file on an ACA.

3.1.3 Loading from a file

The device allows you to load the configuration data from a file in the connected network if there is no AutoConfiguration Adapter connected to the device.

- ☐ Select the `Basics: Load/Save` dialog.
- ☐ In the "Load" frame, click
  - ▶ "from URL" if you want the device to load the configuration data from a file and retain the locally saved configuration.
  - ▶ "from URL & save to Switch" if you want the device to load the configuration data from a file and save this configuration locally.
  - ▶ "via PC" if you want the device to load the configuration data from a file from the PC and retain the locally saved configuration.
- ☐ In the "URL" frame, enter the path under which the device will find the configuration file, if you want to load from the URL.
- ☐ Click "Load configuration".

The URL identifies the path to the tftp server from which the device loads the configuration file. The URL is in the format tftp://IP address of the tftp server/path name/file name (e.g. `tftp://149.218.112.5/switch/config.dat`).

Example of loading from a tftp server

- ☐ Before downloading a file from the tftp server, you have to save the configuration file in the corresponding path of the tftp servers with the file name, e.g. `switch/switch_01.cfg` (see on page 60 „Saving in a file on URL“)
- ☐ In the "URL" line, enter the path of the tftp server, e.g. `tftp://149.218.112.214/switch/switch_01.cfg`.

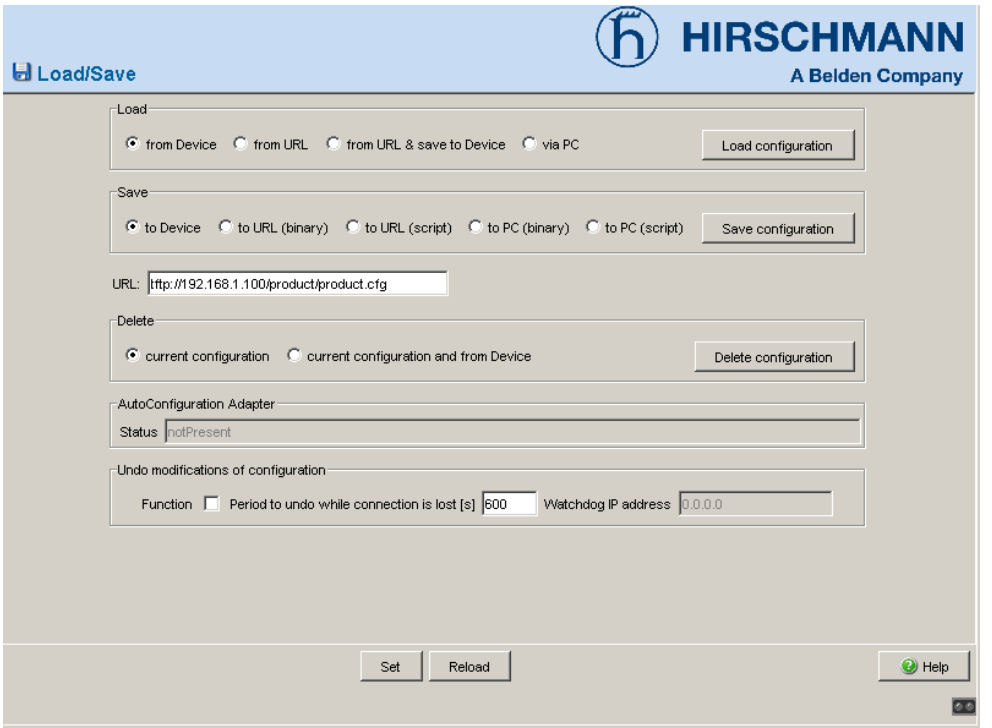


Figure 17: Load/store dialog

`enable`	Switch to the Priviledged EXEC mode.
`copy tftp://149.218.112.159/switch/config.dat nvram:startup-config`	The device loads the configuration data from a tftp server in the connected network.

Note: The loading process started by DHCP/BOOTP (see on page 40 „System configuration via BOOTP“) shows the selection of "from URL & save locally" in the "Load" frame. If you get an error message when saving a configuration, this could be due to an active loading process. DHCP/BOOTP only finishes a loading process when a valid configuration has been loaded. If DHCP/BOOTP does not find a valid configuration, then finish the loading process by loading the local configuration in the "Load" frame.

3.1.4 Resetting the configuration to the state on delivery

The device enables you to

- reset the current configuration to the state on delivery. The locally saved configuration is kept.
- reset the device to the state on delivery. After the next restart, the IP address is also in the state on delivery.

☐ Select the `Basics: Load/Save` dialog.
☐ Make your selection in the "Delete" frame.
☐ Click "Delete configuration".

Setting in the system monitor:

☐ Select `5` "Erase main configuration file"
This menu item allows you to reset the device to its state on delivery. The device saves configurations that differ from the state on delivery in the `switch.cfg` file in the flash memory.
☐ Press the Enter key to delete the switch.cfg file.

3.2 Saving settings

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

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

3.2.1 Saving locally (and on the ACA)

The device allows you to save the current configuration data in the local non-volatile memory and in the ACA.

☐ Select the `Basics: Load/Save` dialog.
☐ In the "Save" frame, click "on the Switch".
☐ Click "Save configuration". The device saves the current configuration data in the local non-volatile memory and, if an ACA is connected, also in the ACA.

```
enable
copy system:running-config
nvram:startup-config
```

Switch to the Priviledged EXEC mode.

The device saves the current configuration data in the local non-volatile memory and, if an ACA is connected, also in the ACA

3.2.2 Saving in a file on URL

The device allows you to save the current configuration data in a file in the connected network.

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

- ☐ Select the `Basics: Load/Save` dialog.
- ☐ In the "Save" frame, click "on URL (binary)" to receive a binary file, or "on URL (script)" to receive an editable and readable script.
- ☐ In the "URL" frame, enter the path under which you want the device to save the configuration file.

The URL identifies the path to the tftp server on which the device saves the configuration file. The URL is in the format tftp://IP address of the tftp server/path name/file name (e.g. `tftp://149.218.112.5/switch/config.dat`).

- ☐ Click "Save configuration".

`enable`	Switch to the Priviledged EXEC mode.
`copy nvram:startup-config tftp://149.218.112.159/switch/config.dat`	The device saves the configuration data in a binary file on a tftp server in the connected network
`copy nvram:script tftp://10.0.1.159/switch/config.txt`	The device saves the configuration data in a script file on a tftp server in the connected network

3.2.3 Saving in a binary file on the PC

The device allows you to save the current configuration data in a binary file on your PC.

- ☐ Select the `Basics: Load/Save` dialog.
- ☐ In the "Save" frame, click "on the PC (binary)".
- ☐ In the save dialog, enter the name of the file in which you want the device to save the configuration file.
- ☐ Click "Save configuration".

3.2.4 Saving as a script on the PC

The device allows you to save the current configuration data in an editable and readable file on your PC.

- ☐ Select the `Basics: Load/Save` dialog.
- ☐ In the "Save" frame, click "on the PC (script)".
- ☐ In the save dialog, enter the name of the file in which you want the device to save the configuration file.
- ☐ Click "Save configuration".

4 Loading software updates

Hirschmann never stops working on improving the performance of its products. So it is possible that you may find a more up to date release of the device software on the Hirschmann Internet site (www.hirschmann.com) than the release saved on your device.

Checking the software release installed

- ☐ Select the `Basics:Software` dialog.
- ☐ This dialog shows you the release number of the software saved on the device.

`enable`	Switch to the Priviledged EXEC mode.
`show sysinfo`	Display the system information.

```
Alarm..................................... None

System Description........................ Hirschmann
Railswitch
System Name............................... RS-1F1054
System Location........................... Hirschmann
Railswitch
System Contact............................ Hirschmann Automa-
tion and Control GmbH
System Up Time............................ 0 days 0 hrs 45
mins 57 secs
System Date and Time (local time zone)..... 2007-04-21 08:00:06
System IP Address......................... 10.0.1.13
Boot Software Release..................... L2E-01.0.00
Boot Software Build Date.................. 2005-11-03 13:50
OS Software Release....................... L2E-03.1.00
OS Software Build Date.................... 2007-06-21 06:14
Hardware Revision......................... 1.22 / 4 / 0103
Hardware Description...................... RS20-
1600T1T1SDAEHH
Serial Number............................. 943434023000001191
Base MAC Address.......................... 00:80:63:1f:10:54
Number of MAC Addresses................... 32 (0x20)
```

Loading the software

The device gives you three options for loading the software:

- From the ACA 21 USB (out-of-band)
- Via tftp from a tftp server (in-band)
- Via a file selection dialog from your PC.

Note: The existing configuration of the device is still there after the new software is installed.

4.1 Loading the software from the ACA

You can connect the ACA 21-USB to a USB port of your PC like a conventional USB stick and copy the device software into the main directory of the ACA 12-USB.

☐ Connect the ACA 21-USB onto which you copied the device software with the USB port of the device.

☐ Open the system monitor (see page 16 „Opening the system monitor“).

☐ Select 2 and press the Enter key to copy the software from the ACA 21-USB into the local memory of the device. At the end of the update, the system monitor asks you to press any key to continue.

☐ Select 3 to start the new software on the device.

The system monitor offers you additional options in connection with the software on your device:

- selecting the software to be loaded
- starting the software
- performing a cold start

4.1.1 Selecting the software to be loaded

In this menu item of the system monitor, you select one of two possible software releases that you want to load.
The following window appears on the screen:

```
   Select Operating System Image

   (Available OS: Selected: 1.00 (2004-08-26 07:15), Backup: 1.00
(2004-08-26 07
:15(Locally selected: 1.00 (2004-08-26 07:15))

   1  Swap OS images
   2  Copy image to backup
   3  Test stored images in Flash mem.
   4  Test stored images in USB mem.
   5  Apply and store selection
   6  Cancel selection
```

Figure 18: Update operating system screen display

- **Swap OS images**
  The memory of the device provides space for two images of the software. Thus, for example, you have the option to load a new version of the software without deleting the existing one.
  ☐ Select `1` to load the other software in the next booting process.

- **Copy image to backup**
  ☐ Select `2` to save a copy of the active software.

- **Test stored images in flash memory**
  ☐ Select `3` to check whether the images of the software stored in the flash memory contain valid codes.

Test stored images in USB memory

☐ Select 4 to check whether the images of the software stored in the ACA 21-USB contain valid codes.

Apply and store selection

☐ Select 5 to confirm the software selection and to save it.

Cancel selection

☐ Select 6 to leave this dialog without making any changes.

4.1.2 Starting the software

This menu item (Start Selected Operating System) of the system monitor allows you to start the software selected.

4.1.3 Performing a cold start

This menu item (End (reset and reboot)) of the system monitor allows you to reset the hardware of the device and perform a restart.

4.2 Loading the software from the tftp server

For a tftp update, you need a tftp server on which the software to be loaded is stored (see on page 200 „tftp server for software updates“).

☐ Select the `Basics:Software` dialog.

The URL identifies the path to the software stored on the tftp server. The URL is in the format tftp://IP address of the tftp server/path name/file name (e.g. `tftp://149.218.112.5/mice/mice.bin`).

☐ Enter the path of the device software.

☐ Click on "tftp-Update" to load the software from the tftp server to the device.

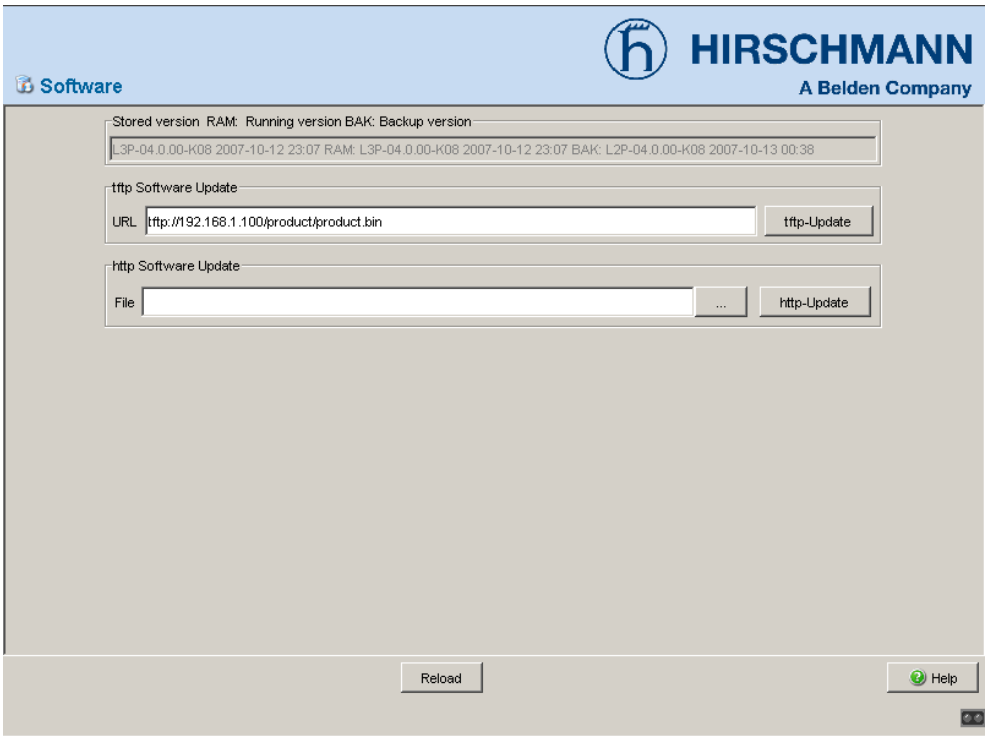


Figure 19: Software update dialog

☐ After successfully loading it, you activate the new software: Select the dialog `Basic Settings:Restart` and perform a cold start.

☐ After booting the device, click "Reload" in your browser to access the device again.

```
enable
copy tftp://10.0.1.159/
rsL2E.bin system:image
```

Switch to the Priviledged EXEC mode.

Transfer the "rsL2E.bin" software file to the device from the tftp server with the IP address 10.0.1.159.

4.3 Loading the software via file selection

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

- ☐ Select the `Basics:Software` dialog.
- ☐ In the file selection frame, click on "...".
- ☐ In the file selection window, select the device software (device.bin) and click on "Open".
- ☐ Click on "Update" to transfer the software to the device.

The end of the update is indicated by one of the following messages:

- ▶ Update completed successfully.
- ▶ Update failed. Reason: incorrect file.
- ▶ Update failed. Reason: error when saving.

- ☐ After loading successfully, activate the new software:
  Select the dialog `Basic Settings: Restart` and perform a cold start.
  In a cold start, the device reloads the software from the non-volatile memory, restarts, and performs a self-test.
- ☐ In your browser, click on "Reload" so that you can access the device again after it is booted.

5 Configuring the ports

The port configuration consists of:

- Switching the port on and off
- Selecting the operating mode
- Activating the display of connection error messages
- Configuring Power over ETHERNET.

Switching the port on and off

In the state on delivery, all the ports are switched on. For a higher level of access security, switch off the ports at which you are not making any connection.

☐ Select the `Basics:Port Configuration` dialog.
☐ In the "Port on" column, select the ports that are connected to another device.

Selecting the operating mode

In the state on delivery, all the ports are set to the “Automatic configuration” operating mode.

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

☐ Select the `Basics:Port Configuration` dialog.
☐ If the device connected to this port requires a fixed setting
– select the operating mode (transmission rate, duplex mode) in the "Manual configuration" column and
– deactivate the port in the "Automatic configuration" column.

Displaying connection error messages

In the state on delivery, the device displays connection errors via the signal contact and the LED display. The device allows you to suppress this display, because you do not want to interpret a switched off device as an interrupted connection, for example.

- ☐ Select the `Basics:Port Configuration` dialog.
- ☐ In the "Signal contact mask" column, select the ports for which you want to have link monitoring.

Configuring Power over ETHERNET

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

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

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

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.

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

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

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

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

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

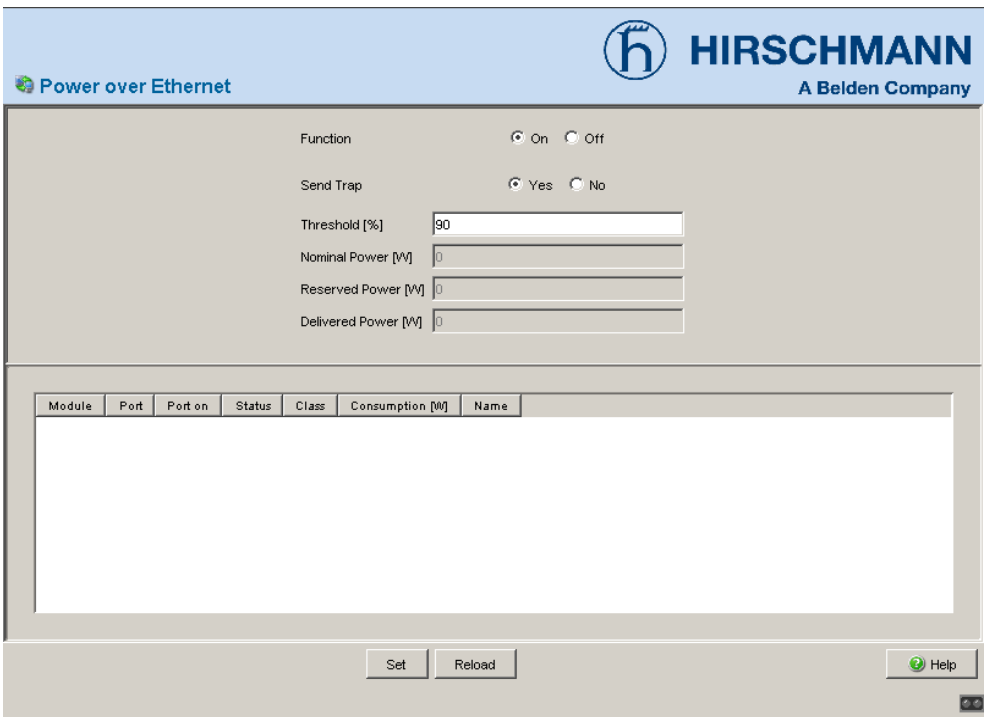


Figure 20: Power over Ethernet dialog

6 Protection from unauthorized access

Protect your network from unauthorized access. The device provides you with the following functions for protecting against unauthorized access.

- Password for SNMP access
- Telnet/Web/SSH access disabling
- HiDiscovery function disabling
- Port access control via IP or MAC address
- Port authentication according to 802.1X

6.1 Password for SNMP access

6.1.1 Description of password for SNMP access

A network management station communicates with the device via the Simple Network Management Protocol (SNMP).
Every SNMP packet contains the IP address of the sending computer and the password with which the sender of the packet wants to access the device MIB.

The device receives the SNMP packet and compares the IP address of the sending computer and the password with the entries in the device MIB (see on page .210 „Management Information Base (MIB)“).
If the password has the appropriate access right, and if the IP address of the sending computer has been entered, then the device will allow access.

In the delivery state, the device is accessible via the password "public" (read only) and "private" (read and write) to every computer.

To protect your device from unwanted access:

☐ First define a new password with which you can access from your computer with all rights.

☐ Treat this password as confidential. Because everyone who knows the password can access the device MIB with the IP address of your computer.

☐ Limit the access rights of the known passwords or delete their entries.

6.1.2 Entering the password for SNMP access

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

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

☐ Select "Modify read-only password" to enter the read password.
☐ Enter the new read password in the "New password" line and repeat your entry in the "Please retype" line.

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

☐ "Data encryption" encrypts the data of the Web-based management that is transferred between your PC and the device with SNMP V3. You can set the "Data encryption" differently for access with a read password and access with a read/write password.

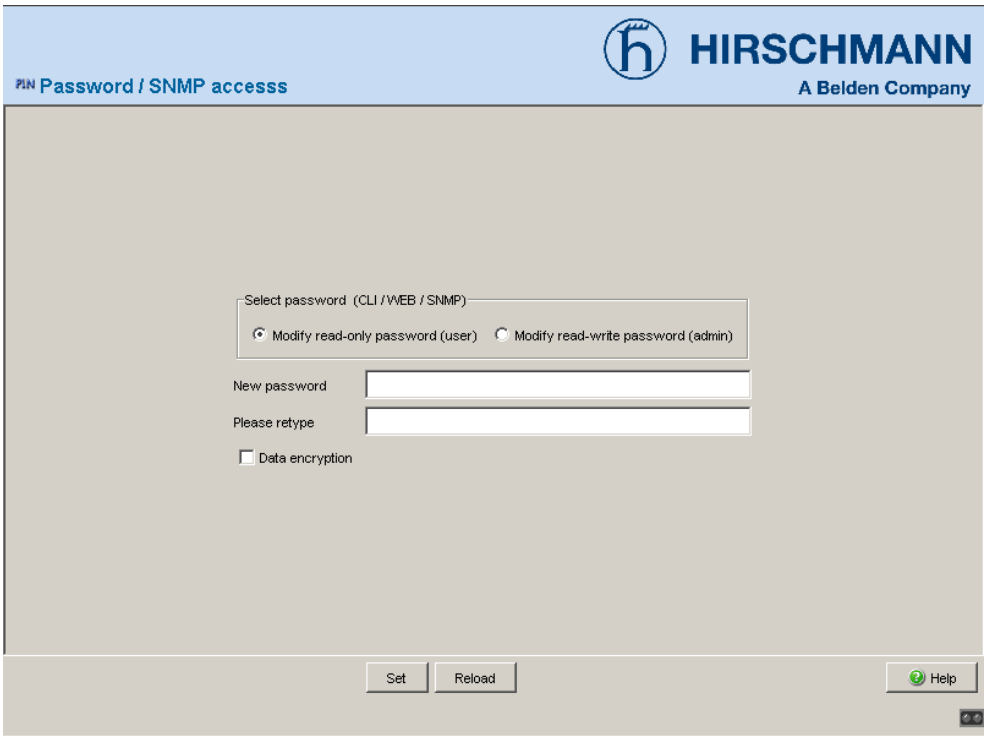


Figure 21: Password dialog

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

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

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

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

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

☐ Select the Security:SNMPv1/v2 access dialog.
With this dialog you can select the access via SNMPv1 or SNMPv2. In the state on delivery, both protocols are activated. You can thus manage the device with HiVision and communicate with earlier versions of SNMP.

If you select SNMPv1 or SNMPv2, you can specify in the table via which IP addresses the device may be accessed, and what kinds of passwords are to be used.
Up to 8 entries can be made in the table.
For security reasons, the read password and the read/write password must not be identical.
Please note that passwords are case-sensitive.

Index Serial number for this table entry

Password	Password with which this computer can access the device. This password is independent of the SNMPv2 password.
IP address	IP address of the computer that can access the device.
IP mask	IP mask for the IP address
Access mode	The access mode determines whether the computer has read-only or read-write access.
Active	Enable/disable this table entry.

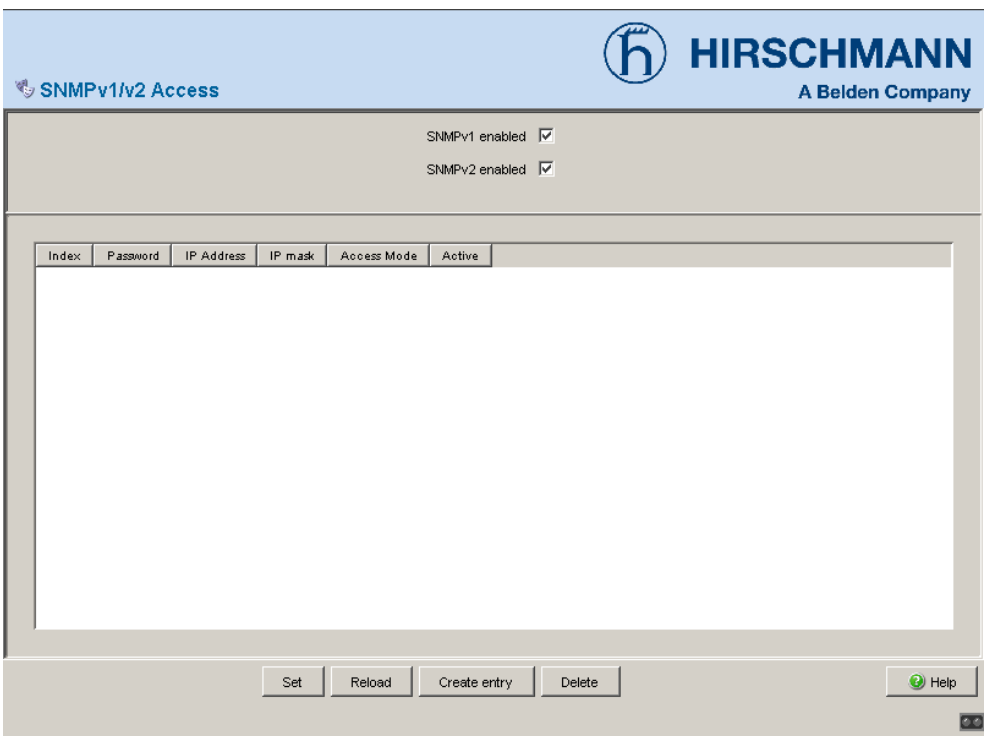


Figure 22: SNMPv1/v2 access dialog

☐ To create a new line in the table click "Create entry".
☐ To delete an entry, select the line in the table and click "Delete".

6.2 Telnet/Web/SSH access

6.2.1 Description of Telnet access

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

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

6.2.2 Description of Web access

The Web server of the device allows you to configure the device by using the Web-based interface. You can deactivate the Web server to prevent Web access to the device.
On delivery, the server is activated.

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

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

6.2.3 Description of SSH access

The SSH server of the device allows you to configure the device by using the Command Line Interface (in-band). You can deactivate the SSH server to prevent SSH access to the device.
On delivery, the server is deactivated.
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 kept.

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

Note: To be able to access the device via SSH, you require a key that has to be installed on the device (see the "Basic Configuration" user manual).

6.2.4 Enabling/disabling Telnet/Web/SSH access

☐ Select the `Security:Telnet/Web/SHH access` dialog.

☐ Disable the server to which you want to refuse access.

`enable`	Switch to the Priviledged EXEC mode.
`transport input telnet`	Enable Telnet server.
`no transport input telnet`	Disable Telnet server.
`ip http server`	Enable Web server.
`no ip http server`	Disable Web server.

6.3 Disabling the HiDiscovery function

6.3.1 Description of the HiDiscovery protocol

The HiDiscovery protocol allows you to assign the device an IP address based on its MAC address (see on page 35 „Entering the IP Parameters via HiDiscovery“). HiDiscovery is a layer 2 protocol.

Note: For security reasons, restrict the HiDiscovery function for the device or disable it after you have assigned the IP parameters to the device.

6.3.2 Enabling/disabling the HiDiscovery function

☐ Select the `Basics:Network` dialog.

☐ Disable the HiDiscovery function in the "HiDiscovery Protocol" frame or limit the access to "read-only".

`enable`	Switch to the Priviledged EXEC mode.
`network protocol hidiscovery off`	Disable HiDiscovery function.
`network protocol hidiscovery read-only`	Enable HiDiscovery function with "read-only" access
`network protocol hidiscovery read-write`	Enable HiDiscovery function with "read-write" access

6.4 Port access control

6.4.1 Port access control

The device protects every port from unauthorized access. Depending on your selection, the device checks the MAC address or the IP address of the connected device.
The following functions are available for monitoring every individual port:

- Who has access to this port?
  The device recognizes 2 classes of access control:
  - All:
    – no access restriction.
    – MAC address 00:00:00:00:00:00 or
    – IP address 0.0.0.0.
  - User:
    – only one assigned user has access.
    – you define the user via his/her MAC or IP address.

- What should happen after an unauthorized access attempt?
  The device can respond in three selectable ways to an unauthorized access attempt:
  - non: no response
  - trapOnly: message by sending a trap
  - portDisable:message by sending a trap and disabling the port

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

6.4.2 Defining port access control

☐ Select the `Security:Port Security` dialog.

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

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

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

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

☐ In the "Action" column you select whether an unauthorized access bid should be followed by
- ▶ no action (none) or
- ▶ the sending of an alarm (trap) (trapOnly) or
- ▶ the disabling of the port by the corresponding entry in the port configuration table (see on page 71 „Configuring the ports“) and the sending of an alarm (trap) (portDisable).

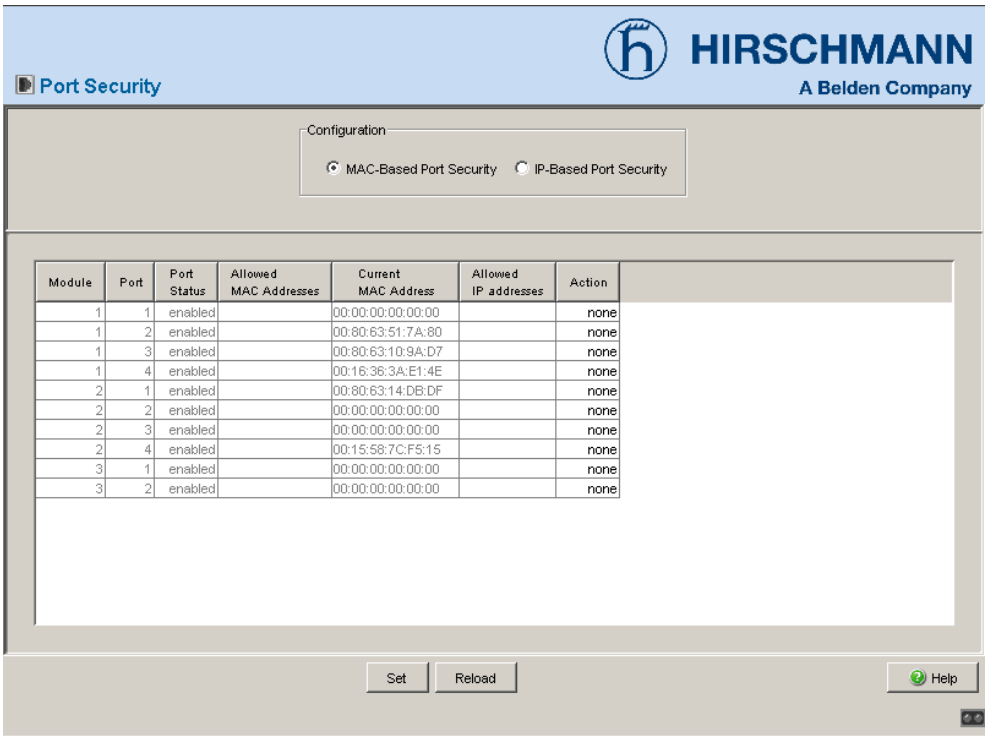


Figure 23: Port Security dialog

Note: This entry in the port configuration table is part of the configuration (see on page 53 „Loading/saving settings“) and is saved together with the configuration.

Note: Prerequisites for the device to be able to send an alarm (trap) (see on page 163 „Configuring traps“):

– at least one recipient is entered
– the corresponding status (“active”) is selected
– “port security” is selected.

6.5 Port authentication acc. to 802.1X

6.5.1 Description of port authentication according to 802.1X

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 at a port by authenticating and authorizing a device that is connected to this port of the device.

The authentication and authorization is carried out by the authenticator, in this case the device. The device authenticates (or does not authenticate) 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 and the server via the Extensible Authentication Protocol over LANs (EAPOL) and the RADIUS protocol respectively.

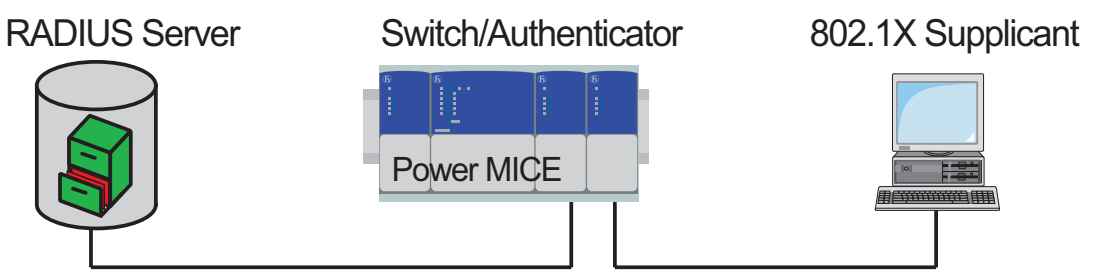


Figure 24: Radius server connection

6.5.2 Authentication process according to 802.1X

A supplicant attempts to communicate via a device port.

- The device requests authentication from the supplicant. At this time, only EAPOL traffic is allowed between the supplicant and the device.
- The supplicant replies with its identification data.
- The device forwards the identification data to the authentication server.
- The authentication server responds to the request in accordance with the access rights.
- The device evaluates this response and provides the supplicant with access to this port (or leaves the port in the blocked state).

6.5.3 Preparing the device for the 802.1X port authentication

- ☐ Configure your own IP parameters (for the device).
- ☐ Globally enable the 802.1X port authentication function.
- ☐ Set the 802.1X port control to "auto". The default setting is "force-authorized".
- ☐ Enter the "shared secret" between the authenticator and the Radius server. The shared secret is a text string specified by the RADIUS server administrator.
- ☐ Enter the IP address and the port of the RADIUS server. The default UDP port of the RADIUS server is port 1812.

6.5.4 Setting 802.1X

Configurating the RADIUS server

☐ Select the `Security:802.1x Port Authentication:RADIUS Server` dialog.

This dialog allows you to enter the data for one, two or three RADIUS servers.

☐ Click "Create entry" to open the dialog window for entering the IP address of a RADIUS server.
☐ Confirm the IP address entered using "OK".
You thus create a new row in the table for this RADIUS server.
☐ In the "Shared secret" column you enter the character string which you get as a key from the administrator of your RADIUS server.
☐ With "Primary server" you name this server as the first server which the device should contact for port authentication queries. If this server is not available, the device contacts the next server in the table.
☐ "Selected server" shows which server the device actually sends its queries to.
☐ With "Delete entry" you delete the selected row in the table.

Selecting ports

☐ Select the `Security:802.1x Port Authentication:Port Configuration` dialog.
☐ In the "Port control" column you select "auto" for the ports for which you want to activate the port-related network access control.

Activating access control

☐ Select the `Security:802.1x Port Authentication:Global` dialog.
☐ With "Function" you enable the function.

7 Network load control

To optimize the data transmission, the device provides you with the following functions for controlling the network load:

- Settings for direct packet distribution (MAC address filter)
- Multicast settings
- Rate limiter
- Prioritization - QoS
- Flow control
- Virtual LANs

7.1 Direct packet distribution

With direct packet distribution, you protect the device from unnecessary network loads. The device provides you with the following functions for direct packet distribution:

- Store-and-forward
- Multi-address capability
- Aging of learned addresses
- Static address entries
- Disabling the direct packet distribution

7.1.1 Store-and-forward

All data received by the device is stored, and its validity is checked. Invalid and defective data packets (> 1,502 bytes or CRC errors) as well as fragments (< 64 bytes) are rejected. Valid data packets are forwarded by the device.

7.1.2 Multi-address capability

The device learns all the source addresses for a port. Only packets with

- unknown addresses
- these addresses or
- a multi/broadcast address

in the destination address field are sent to this port. The device enters learned source addresses in its filter table (see on page 94 „Entering static address entries“).

The device can learn up to 8000 addresses. This is necessary if more than one terminal device is connected to one or more ports. It is thus possible to connect several independent subnetworks to the device.

7.1.3 Aging of learned addresses

The device monitors the age of the learned addresses. Address entries which exceed a certain age (30 seconds, aging time), are deleted by the device from its address table.
The device floods data packets with an unknown destination address.
The device directly distributes data packets with a known destination address.

Note: A reboot deletes the learned address entries.

- ☐ Select the `Switching:Global` dialog.
- ☐ Enter the aging time for all dynamic entries in the range from 10 to 630 seconds (unit: 1 second; default setting: 30). In connection with the router redundancy (see MACH 3000), select a time greater than/ equal to 30 seconds.

7.1.4 Entering static address entries

An important function of the device is the filter function. It selects data packets according to defined patterns, known as filters. These patterns are assigned distribution rules. This means that a data packet received by a device at a port is compared with the patterns. If there is a pattern that matches the data packet, a device then sends or blocks this data packet according to the distribution rules at the relevant ports.

The following are valid filter criteria:

- Destination address
- Broadcast address
- Multicast address
- VLAN membership

The individual filters are stored in the filter table (Forwarding Database, FDB). It consists of three parts: a static part and two dynamic parts.

- The management administrator describes the static part of the filter table (`dot1qStaticTable`).
- During operation, the device is capable of learning which of its ports receive data packets from which source address (see on page 92 „Multi-address capability“). This information is written to a dynamic part (`dot1qTpFdbTable`).
- Addresses learned dynamically from neighboring agents and those learned via GMRP are written to the other dynamic part.

Addresses already located in the static filter table are automatically transferred to the dynamic part by the device.
An address entered statically cannot be overwritten through learning.

Note: If the redundancy manager is active, it is not possible to make permanent unicast entries.

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

☐ Select the `Switching:Filters for MAC Addresses` dialog.

Each row of the filter table represents one filter. Filters specify the way in which data packets are sent. They are set automatically by the Switch (learned status) or created manually. Data packets whose destination address is entered in the table are sent from the receiving port to the ports marked in the table. Data packets whose destination address is not in the table are sent from the receiving port to all other ports. In the "Create filter" dialog you can set up new filters. The following status settings are possible:

- `learned`: the filter was created automatically by the device.
- `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 59 „Saving settings“).
- `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.

To delete entries with the "learned" status from the filter table, select the `Basics:Restart` dialog and click "Reset MAC address table".

7.1.5 Disabling the direct packet distribution

To enable you to observe the data at all the ports, the device allows you to disable the learning of addresses. When the learning of addresses is disabled, the device transfers all the data from all ports to all ports.

☐ Select the `Switching:Global` dialog.

Checkmark "Address Learning" to observe the data at all ports.

7.2 Multicast application

7.2.1 Description of the Multicast application

The data distribution in the LAN differentiates between three distribution classes on the basis of the addressed recipients:

- Unicast - one recipient
- Multicast - a group of recipients
- Broadcast - every recipient that can be reached

In the case of a Multicast address, the device forwards all data packets with a Multicast address to all ports. This leads to an increased bandwidth requirement. Protocols such as GMRP and procedures such as IGMP Snooping enable the device to exchange information via the direct distribution of Multicast data packets. The bandwidth requirement can be reduced by distributing the Multicast data packets only to those ports to which recipients of these Multicast packets are connected.

You can recognize IGMP Multicast addresses by the range in which the address lies:

- MAC Multicast address 01:00:5E:00:00:00 - 01:00:5E:FF:FF:FF
- Class D IP Multicast address 224.0.0.0 - 239.255.255.255

7.2.2 Example of a Multicast application

The cameras for monitoring machines normally transmit their images to monitors located in the machine room and to the monitoring room. In an IP transmission, a camera sends its image data with a Multicast address via the network.
To prevent all the image data from slowing down the entire network, the device uses the GMRP to distribute the Multicast address information. As a result, the image data with a Multicast address is only distributed to those ports that are connected to the associated monitors for surveillance.

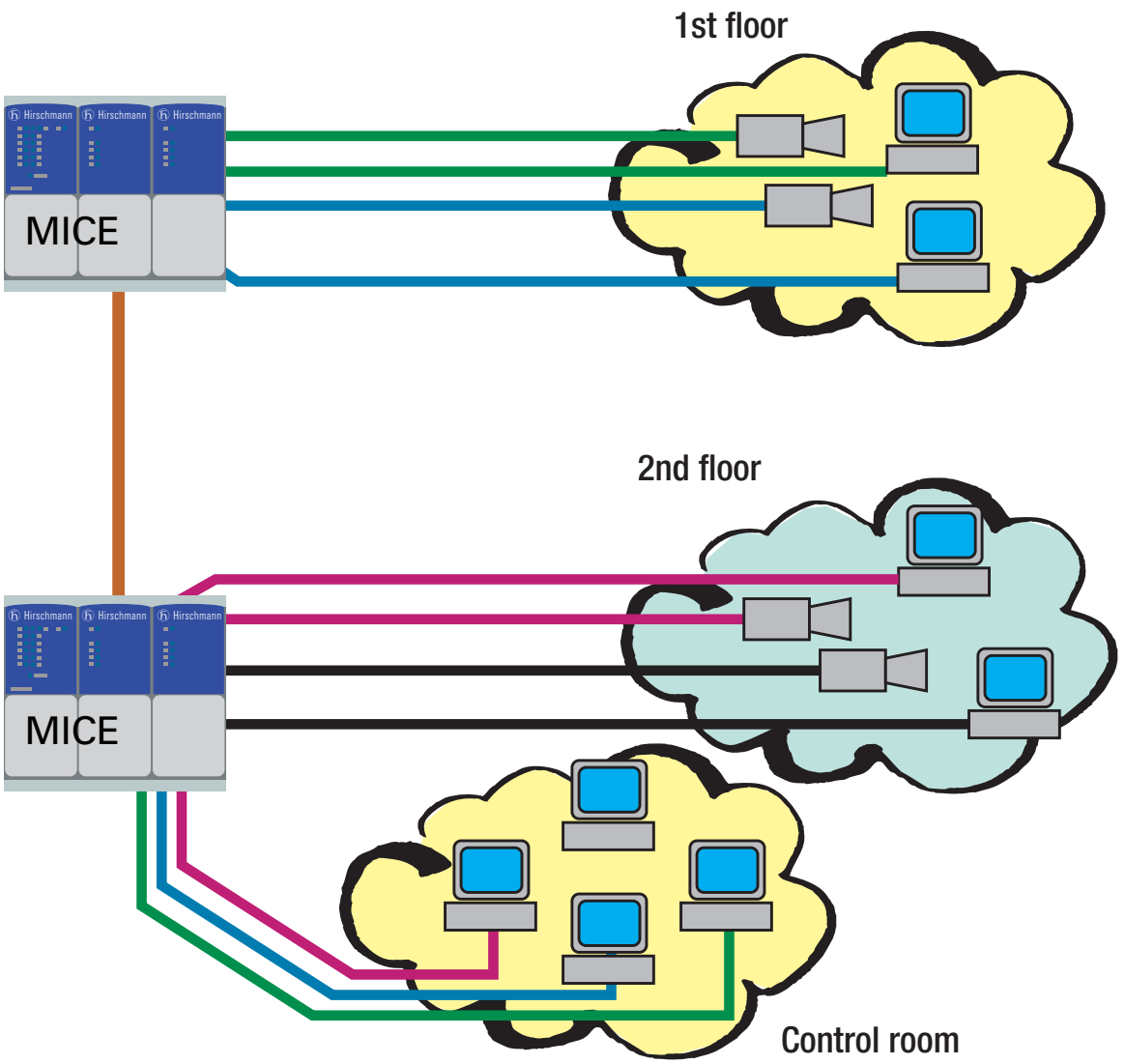


Figure 25: Example: Video surveillance in machine rooms

7.2.3 Description of IGMP Snooping

The Internet Group Management Protocol (IGMP) describes the distribution of Multicast information between routers and terminal devices on the Layer 3 level.

Routers with an active IGMP function periodically send queries to find out which IP Multicast group members are connected to the LAN. Multicast group members reply with a Report message. This Report message contains all the parameters required by the IGMP. The router records the IP Multicast group address from the Report message in its routing table. The result of this is that it transfers frames with this IP Multicast group address in the destination field only in accordance with the routing table.

Devices which no longer want to be members of a Multicast group can cancel their membership by means of a Leave message (from IGMP version 2), and they do not transmit any more Report messages. In IGMP versions 1 and 2, the router removes the routing table entry if it does not receive any Report messages within a specified period of time (aging time).

If there are a number of routers with an active IGMP function in the network, then they work out among themselves (in IGMP version 2) which router carries out the Query function. If there is no router in the network, then a suitably equipped switch can perform the Query function.

A switch that connects a Multicast receiver with a router can evaluate the IGMP information with the aid of the IGMP Snooping procedure.

IGMP Snooping translates IP Multicast group addresses into MAC Multicast addresses, so that the IGMP functions can also be used by Layer 2 switches. The switch records the MAC addresses of the Multicast receivers, with are obtained via IGMP Snooping from the IP addresses, in the static address table. Thus the switch blocks Multicast packets at the ports at which no Multicast receivers are connected.

7.2.4 Description of GMRP

The GARP Multicast Registration Protocol (GMRP) describes the distributionof data packets with a Multicast address as the destination address on layer 2.

Devices that want to receive data packets with a Multicast address as the use the GMRP to perform the registration of the Multicast address. For a Switch, registration involves entering the Multicast address in the . When a Multicast address is entered in the filter table, the Switch sends this information in a GMRP packet to all the ports. Thus the connected Switches know that they have to forward this Multicast address to this Switch. The GMRP enables packets with a Multicast address in the destination address field to be sent to the ports entered. The other ports are not affected by these packets.

Data packets with unregistered Multicast addresses are sent to all ports by the Switch.

Basic setting: "Global setting": disabled

7.2.5 Setting up the Multicast application

☐ Select the `Switching:Multicasts` dialog.

Global settings

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

- the device does not evaluate Query and Report packets received, and
- it sends (floods) received data packets with a Multicast address as the destination address to all ports.

"GMRP" allows you to enable GMRP globally for the entire device.

It GMRP is disabled, then

- the device does not generate any GMRP packets,
- does not evaluate any GMRP packets received, and
- sends (floods) received data packets to all ports.

The device is transparent for received GMRP packets, regardless of the GMRP setting.

"inactive" disables GMRP and IGMP Snooping.

IGMP Querier

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

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

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

IGMP settings

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

In "Response Time" you specify the period within which the Multicast group members respond to a query (valid values: 1-3598 s, default setting: 10 s).
The Multicast group members select a random value within the response time for their response, to prevent all the Multicast group members responding to the query at the same time.
Select a large value if you want to reduce the load on your network and can accept the resulting longer switching times.
Select a small value if you require short switching times and can accept the resulting network load.

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

Unknown Multicasts

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

- "Send to Query Ports".
  The device sends the packets with an unknown MAC/IP Multicast address to all query ports.
- "Send to All Ports".
  The device sends the packets with an unknown MAC/IP Multicast address to all ports.
- "Discard".
  The device discards all packets with an unknown MAC/IP Multicast address.

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

Known Multicasts

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

- "Send to query and registered ports".
  The device sends the packets with a known MAC/IP Multicast address to all query ports and to registered ports.
  This standard setting sends all Multicasts to all query ports and to registered ports. The advantage of this is that it works in most applications without any additional configuration.
  Application: "Flood and Prune" routing in PIM-DM.
- "Send to registered ports".
  The device sends the packets with a known MAC/IP Multicast address to registered ports.
  The advantage of this setting, which deviates from the standard, is that it uses the available bandwidth optimally through direct distribution. It requires additional port settings.
  Application: Routing protocol PIM-SM.

Settings per port (table)

- IMGP on per port
  This table column enables you to enable/disable the IGMP for each port when the global IGMP Snooping is enabled. Disabling the IGMP at a port prevents registration for this port.

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

  Note: If a number of routers are connected to a subnetwork, you must use IGMP version 1 so that all the routers receive all the IGMP reports.

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

- IGMP Automatic Query Port
  This table column shows you which ports the device has learned as query ports, if "automatic" is selected in "Static Query Port".

- Static Query Port
  The device sends IGMP report messages to the ports at which it receives IGMP queries (disable = default setting).
  This column allows you to also send IGMP report messages to other selected ports (enable) or
  to connected Hirschmann devices (automatic).

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

- GMRP per Port
  This table column enables you to enable/disable the GMRP for each port when the global GMRP is enabled. When you disable the GMRP at a port, no registrations can be made for this port, and GMRP packets cannot be sent out of this port.

- GMRP Service Requirements
  Devices that do not support GMRP can be integrated into the Multicast addressing by means of
  - a static filter address entry on the connecting port
  - selecting "Forward all groups" in the table column "GMRP Service Requirement". The device enters ports with the selection "Forward all groups" in all Multicast filter entries learned via GMRP.

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

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

or

- enabling GMRP on the ring ports and globally, and
- enabling "Forward all groups" on the ring ports.

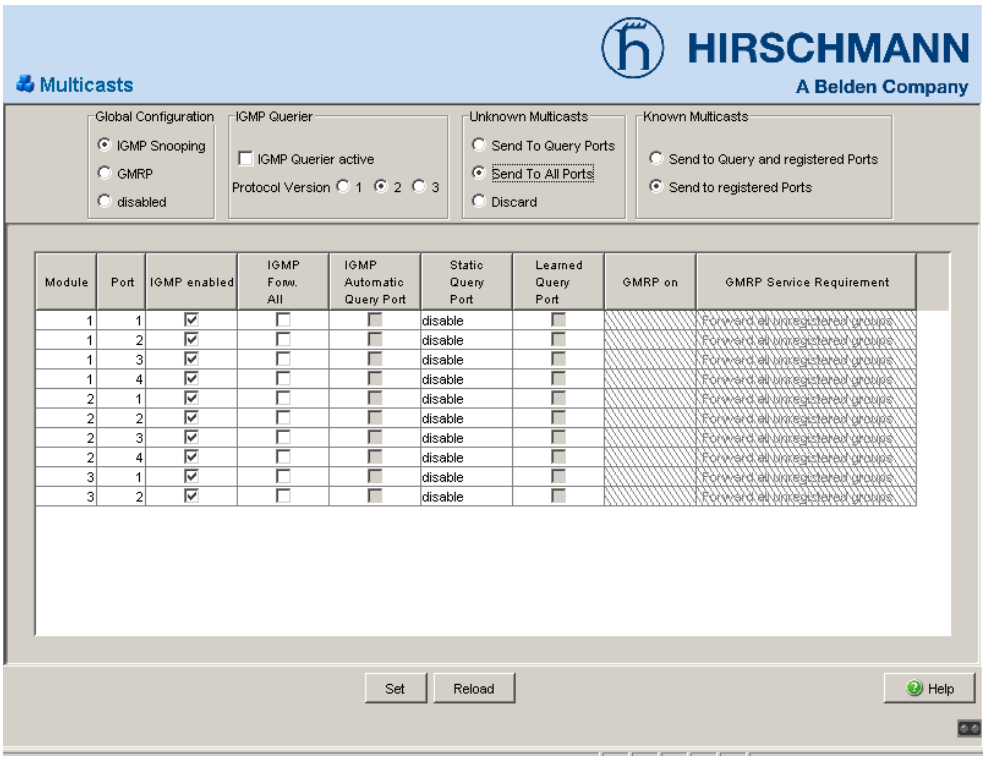


Figure 26: IGMP/GMRP/Unknown Multicasts dialog

7.3 Rate Limiter

7.3.1 Description of the Rate Limiter

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

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

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

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

7.3.2 Rate Limiter settings for MACH 4000 and Power MICE

☐ Select the `Switching:Rate Limiter` dialog.

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

Setting options per port:

- Ingress Limiter Rate for the packet types selected in the Ingress Limiter frame:
  - = 0, no ingress limit at this port.
  - > 0, maximum outgoing traffic rate in kbit/s that is allowed to be sent at this port.
- Egress Limiter for broadcast packets:
  - = 0, no rate limit for outbound broadcast packets at this port.
  - > 0, maximum number of outgoing broadcasts per second sent at this port.

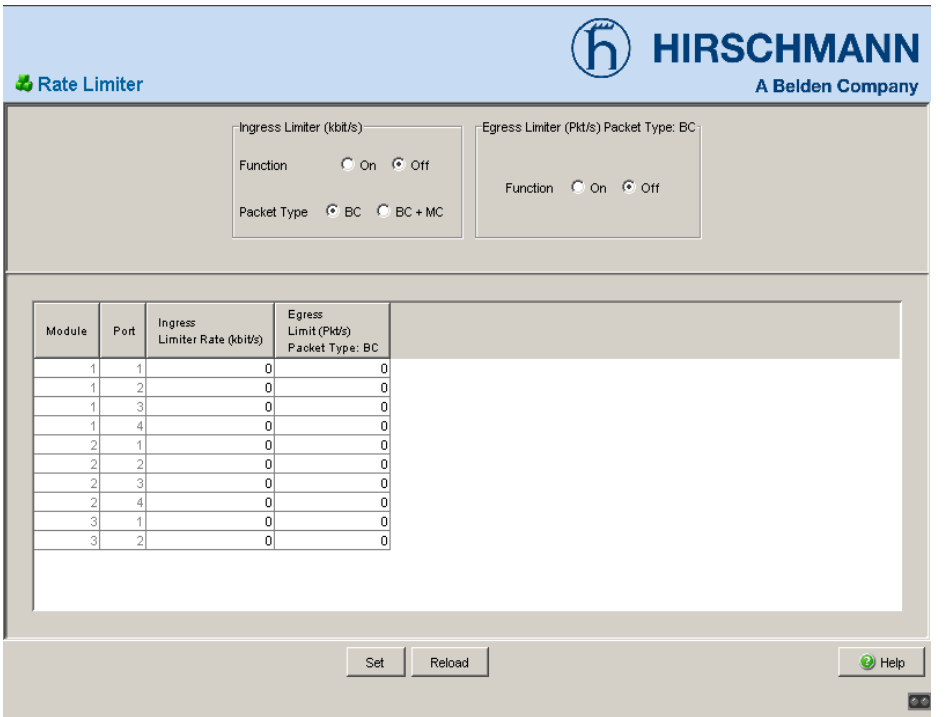


Figure 27: Rate Limiter dialog

7.3.3 Rate Limiter settings for RS20/RS30/40, MS20/MS30, MACH 1000 and OCTOPUS

☐ Select the `Switching:Rate Limiter` dialog.

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

Setting options per port:

- "Ingress Packet Types" allows you to select the packet type for which the limit is to apply:
  - `All`, limits the total inbound data volume at this port.
  - `BC`, limits the broadcast packets received at this port.
  - `BC + MC`, limits broadcast packets and Multicast packets received at this port.
  - `BC + MC + uUC`, limits broadcast packets, Multicast packets, and unknown Unicast packets received at this port.
- Ingress Limiter Rate for the inbound packet type selected:
  - = 0, no ingress limit at this port.
  - > 0, maximum inbound traffic rate in kbit/s that can be received at this port.
- Egress Limiter Rate for broadcast packets:
  - = 0, no rate limit for outbound broadcast packets at this port.
  - > 0, maximum number of outbound broadcasts per second that can be sent at this port.
- Egress Limiter Rate for the entire data stream:
  - = 0, no rate limit for outbound data stream at this port.
  - > 0, maximum outbound transmission rate in kbit/s sent at this port.

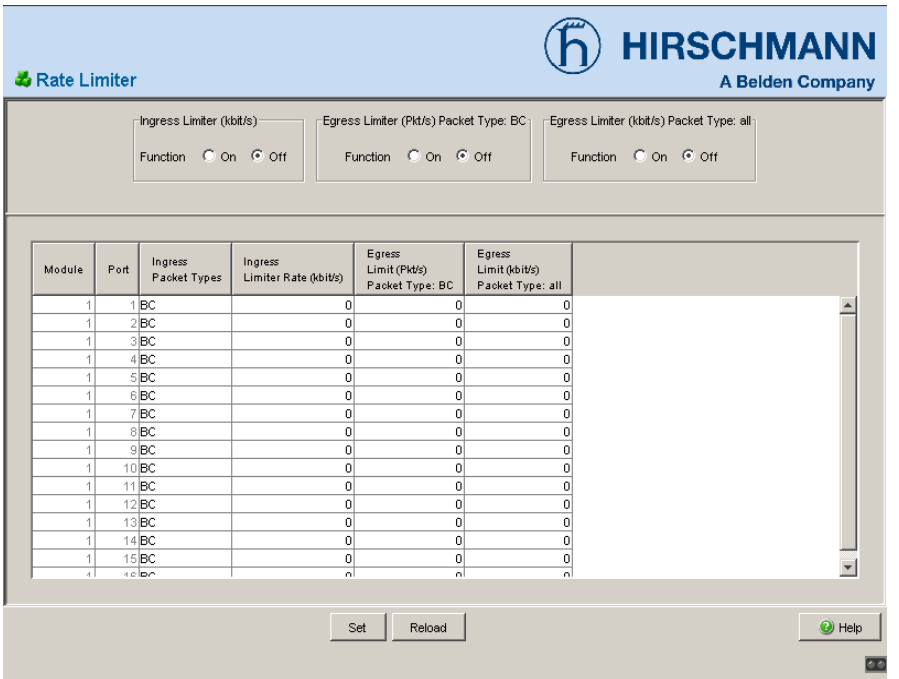


Figure 28: Rate Limiter

7.4 QoS/Priority

7.4.1 Description of Prioritization

This function prevents time-critical data traffic such as language/video or real-time data from being disrupted by less time-critical data traffic during periods of heavy traffic. By assigning high traffic classes for time-critical data and low traffic classes for less time-critical data, you ensure optimal data flow for time-critical data traffic.

The device supports four (eight for MACH 4000 and PowerMICE) priority queues (traffic classes in compliance with IEEE 802.1D). The assignment of received data packets to these classes is performed by

- the priority of the data packet contained in the VLAN tag when the receiving port was configured to "trust dot1p".
- the QoS information (ToS/DiffServ) contained in the IP header when the receiving port was configured to "trust ip-dscp".
- the port priority when the port was configured to "no trust".
- the port priority when receiving non-IP packets when the port was configured to "trust ip-dscp".
- the port priority when receiving data packets without a VLAN tag (see on page 71 „Configuring the ports“) and when the port was configured to "trust dot1p".
  Default setting: "trust dot1p".

The device considers the classification mechanisms in the sequence shown above.

Data packets can contain prioritizing/QoS information:

- VLAN priority based on IEEE 802.1Q/ 802.1D (Layer 2)

7.4.2 VLAN tagging

The VLAN tag is integrated into the MAC data frame for the VLAN and Prioritization functions in accordance with the IEEE 802.1 Q standard. The VLAN tag consists of 4 bytes. It is inserted between the source address field and the type field.

For data packets with a VLAN tag, the device evaluates
- the priority information at all times, and
- the VLAN information if VLANs have been set up.

Data packets with VLAN tags containing priority information but no VLAN information (VLAN ID = 0), are known as Priority Tagged Frames.

Priority entered	Traffic class for RS20/RS30/ RS40, MACH 1000, MS20/MS30, OCTOPUS (default)	Traffic class for MACH 4000 and Power MICE (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, less than 100 milliseconds of latency and jitter
6	3	6	Voice, less than 10 milliseconds of latency and jitter
7	3	7	Network control reserved traffic

Table 4: Assignment of the priority entered in the tag to the traffic classes

Note: Network protocols and redundancy mechanisms use the highest traffic classes 3 (RS20/30/40, MS20/30, MACH 1000, OCTOPUS) and 7 (Power MICE, MACH 4000). Therefore, you select other traffic classes for application data.

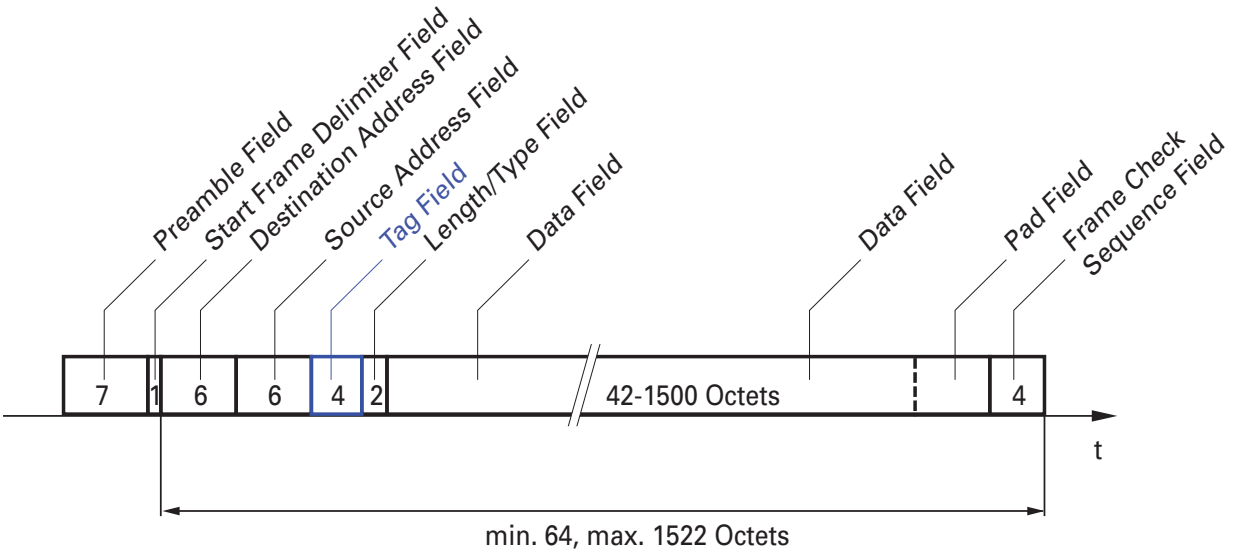


Figure 29: Ethernet data packet with tag

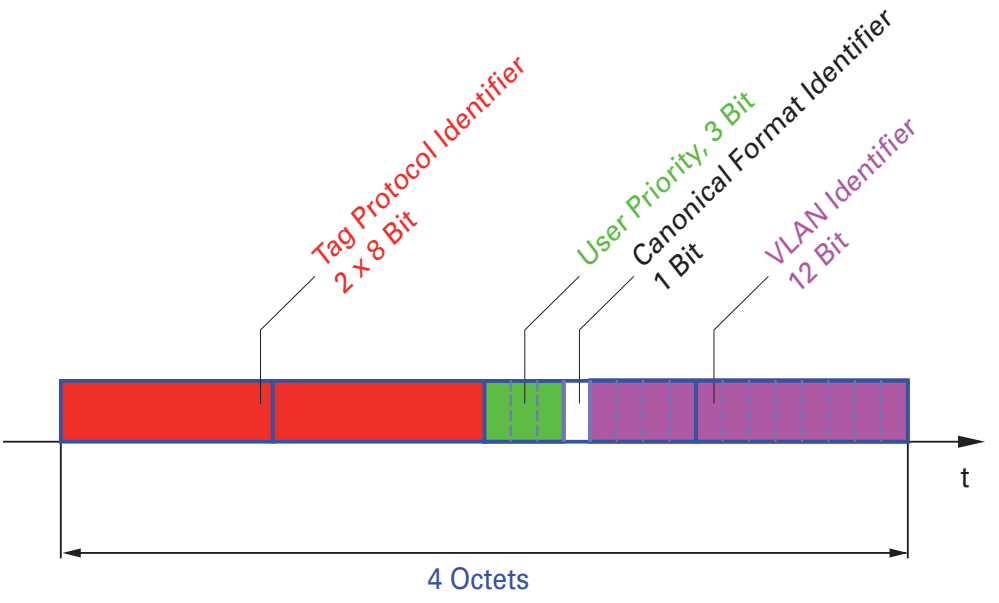


Figure 30: Tag format

Although VLAN prioritizing is widespread in the industry sector, it has a number of limitations:

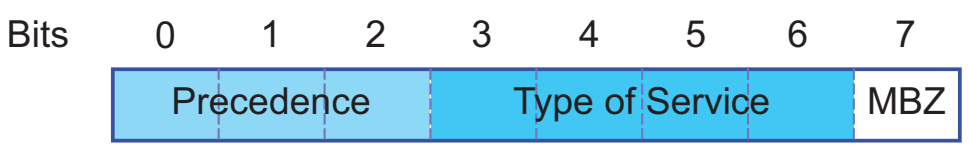
- The additional 4-byte VLAN tag enlarges the data packets. With small data packets, this leads to a larger bandwidth load.

- End-to-end prioritizing requires the VLAN tags to be transmitted to the entire network, which means that all network components must be VLAN-capable.
- Routers cannot receive or send packets with VLAN tags via port-based router interfaces.

7.4.3 IP ToS / DiffServ

TYPE of Service

The Type of Service (ToS) field in the IP header (see table 5) has been part of the IP protocol from the start, and it is used to differentiate various services in IP networks. Even back then, there were ideas about differentiated treatment of IP packets, due to the limited bandwidth available and the unreliable connection paths. Because of the continuous increase in the available bandwidth, there was no need to use the ToS field. Only with the real-time requirements of today's networks has the ToS field become significant again. Selecting the ToS byte of the IP header enables you to differentiate between different services. However, this field is not widely used in practice.



Bits (0-2): IP Precedence Defined	Bits (3-6): Type of Service Defined	Bit (7)
111 - Network Control	0000 - [all normal]	0 - Must be zero
110 - Internetwork Control	1000 - [minimize delay]	
101 - CRITIC / ECP	0100 - [maximize throughput]	
100 - Flash Override	0010 - [maximize reliability]	
011 - Flash	0001 - [minimize monetary cost]	
010 - Immediate		
001 - Priority		
000 - Routine		

Table 5: ToS field in the IP header

Differentiated Services

The newly defined Differentiated Services field in the IP header in RFC 2474 (see fig. 31) - often known as the DiffServ Code Point or DSCP, replaces the ToS field and is used to mark the individual packets with a DSCP. Here the packets are divided into different quality classes. The first three bits of the DSCP are used to divide the packets into classes. The next three bits are used to further divide the classes on the basis of different criteria. In contrast to the ToS byte, DiffServ uses six bits for the division into classes. This results in up to 64 different service classes.

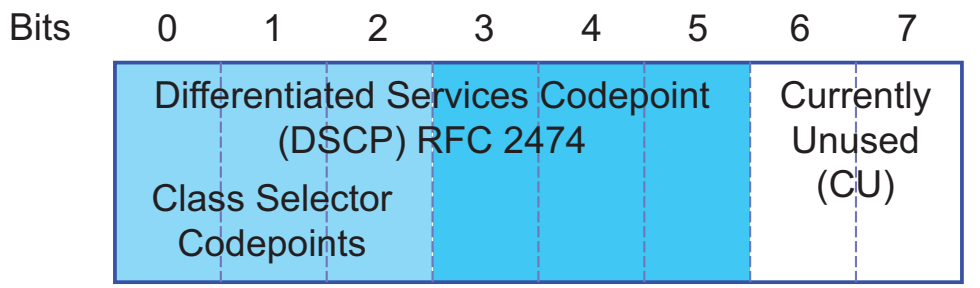


Figure 31: Differentiated Services field in the IP header

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

- Class Selector (CS0-CS7): For reasons of compatibility to TOS/IP Precedence
- Expedited Forwarding (EF): Premium service. Reduced delay, jitter + packet loss (RFC 2598)
- Assured Forwarding (AF): Provides a differentiated schema for handling different data traffic (RFC 2597).
- Default Forwarding/Best Effort: No particular prioritizing.

The PHB class selector assigns the 7 possible IP precedence values from the old ToS field to specific DSCP values, thus ensuring the downwards compatibility.

ToS Meaning	Precedence Value	Assigned DSCP
Network Control	111	CS7 (111000)
Internetwork Control	110	CS6 (110000)
Critical	101	CS5 (101000)
Flash Override	100	CS4 (100000)
Flash	011	CS3 (011000)
Immediate	010	CS2 (010000)
Priority	001	CS1 (001000)
Routine	000	CS0 (000000)

Table 6: Assigning the IP precedence values to the DSCP value

DSCP Value	DSCP Name	Traffic class for MACH 400, Power MICE (default setting)	Traffic class for RS20/RS30/RS40, RSR20/RSR30, MS20/MS30, OCTOPUS, MACH 1000 (default setting)
0	Best Effort /CS0	2	1
1-7		2	1
8	CS1	0	0
9,11,13,15		0	0
10,12,14	AF11,AF12,AF13	0	0
16	CS2	1	0
17,19,21,23		1	0
18,20,22	AF21,AF22,AF23	1	0
24	CS3	3	1
25,27,29,31		3	1
26,28,30	AF31,AF32,AF33	3	1
32	CS4	4	2
33,35,37,39		4	2
34,36,38	AF41,AF42,AF43	4	2
40	CS5	5	2
41,42,43,44,45,47		5	2
46	EF	5	2
48	CS6	6	3
49-55		6	3
56	CS7	7	3
57-63		7	3

Table 7: Mapping the DSCP values onto the traffic classes

7.4.4 Management prioritizing

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.

- On Layer 2 the device modifies the VLAN priority in the VLAN tag.
  For this function to be useful, the configuration of the corresponding ports must permit the sending of packets with a VLAN tag.

- On Layer 3 the device modifies the IP-DSCP value.

7.4.5 Handling of received priority information

The device provides three options, which can be chosen globally for all ports (per port for Power MICE and MACH 4000), for selecting how it handles received data packets that contain priority information.

- trust dot1p
  The device assigns VLAN-tagged packets to the different traffic classes according to their VLAN priorities. The assignment is based on the pre-defined table (see on page 111 „VLAN tagging“). You can modify this assignment. The device assigns the port priority to packets that it receives without a tag.

- untrusted
  The device ignores the priority information in the packet and always assigns the packets the port priority of the receiving port.

- trust ip-dscp
  The device assigns the IP packets to the different traffic classes according to the DSCP value in the IP header, even if the packet was also VLAN-tagged. The assignment is based on the pre-defined values (see table 7). You can modify this assignment.
  The device prioritizes non-IP packets according to the port priority.

7.4.6 Handling of traffic classes

For the handling of traffic classes, the device provides:

- Strict Priority

Description of Strict Priority

With the Strict Priority setting, the device first transmits all data packets that have a higher traffic class before transmitting a data packet with the next highest traffic class. The device transmits a data packet with the lowest traffic class only when there are no other data packets remaining in the queue. In some cases, a high level of data traffic can prevent packets with lower traffic classes from being sent.
In applications that are time- or latency-critical, such as VoIP or video, this method ensures that high-priority data is sent immediately.

7.4.7 Setting prioritization

Assigning the port priority

☐ Select the `QoS/Priority:Port Configuration` dialog.

☐ In the "Port Priority" column, you can specify the priority (0-7) with which the device sends data packets which it receives without a VLAN tag at this port

Note: If you have set up VLANs, pay attention to the "Transparent mode" (see on page 128 „Configuring VLANs“).

`enable`	Switch to the Priviledged EXEC mode.
`configure`	Switch to the Configuration mode.
`interface 1/1`	Switch to the Interface Configuration mode of interface 1/1.

`vlan priority 3`	Assign port priority 3 to interface 1/1.
`exit`	Switch to the Configuration mode.

Assigning the VLAN priority to the traffic classes

`enable`	Switch to the Priviledged EXEC mode.
`configure`	Switch to the Configuration mode.
`classofservice dot1p-mapping 0 4` `classofservice dot1p-mapping 1 4`	Assign traffic class 4 to VLAN priority 0. Also assign traffic class 4 to VLAN priority 1.
`exit`	Switch to the Priviledged EXEC mode.
`show classofservice dot1p-mapping`	Display the assignment.

```
 User Priority    Traffic Class
 -------------    -------------
       0                4
       1                4
       2                1
       3                3
       4                4
       5                5
       6                6
       7                7
```

Always assign the port priority to received data packets (Power MICE and MACH 4000)

`enable`	Switch to the Priviledged EXEC mode.
`configure`	Switch to the Configuration mode.
`interface 1/1`	Switch to the Interface Configuration mode of interface 1/1.
`no classofservice trustvlan priority 1`	Assign the "no trust" mode to the interface. Set the port priority to 1.
`exit`	Switch to the Configuration mode.
`exit`	Switch to the Priviledged EXEC mode.
`show classofservice trust 1/1`	Display the trust mode on interface 1/1.

```
Class of Service Trust Mode: Untrusted

Untrusted Traffic Class: 4
```

Assigning the traffic class to a DSCP

```
enable                                  Switch to the Priviledged EXEC mode.
configure                               Switch to the Configuration mode.
classofservice ip-dscp-map-             Assign traffic class 1 to DSCP CS1.
ping cs1 1
show classofservice ip-dscp-mapping

    IP DSCP       Traffic Class
 -------------    -------------
   0(be/cs0)           2
   1                   2
   .
   .
   8(cs1)              1
   .
```

Always assign the DSCP priority to received IP data packets for each interface (Power MICE and MACH 4000)

```
enable                                  Switch to the Priviledged EXEC mode.
configure                               Switch to the Configuration mode.
interface 6/1                           Switch to the interface configuration mode of inter-
classofservice trust ip-                face 6/1. Assign the "trust ip-dscp" mode to the in-
dscp                                    terface.
exit                                    Switch to the Configuration mode.
exit                                    Switch to the Priviledged EXEC mode.
show classofservice trust               Display the trust mode on interface 6/1.
6/1

Class of Service Trust Mode: IP DSCP

Non-IP Traffic Class: 2
```

Always assign the DSCP priority to received IP data packets globally

```
enable                                  Switch to the Priviledged EXEC mode.
configure                               Switch to the Configuration mode.
classofservice trust ip-                Assign the "trust ip-dscp" mode globally.
dscp
exit                                    Switch to the Configuration mode.
exit                                    Switch to the Priviledged EXEC mode.
show classofservice trust               Display the trust mode.
```

```
Class of Service Trust Mode: IP DSCP
```

Always assign the DSCP priority to received IP data packets globally (RS20/RS30/RS40, MS20/MS30, RSR20/RSR40, MACH 1000 and OCTOPUS)

☐ Select the `QoS/Priority:Global` dialog.
☐ Select `trustIPDSCP` in the "Trust Mode" line.

Configuring Layer 2 management priority

☐ Configure the VLAN ports to which the device sends management packets as a member of the VLAN that sends data packets with a tag (see on page 128 „Configuring VLANs“).

☐ Select the `QoS/Priority:Global` dialog.
☐ In the line `VLAN priority for management packets` you enter the value of the VLAN priority.

`enable`	Switch to the Priviledged EXEC mode.
`network priority dot1p-vlan 7`	Assign the value 7 to the management priority so that management packets with the highest priority are sent.
`exit`	Switch to the Priviledged EXEC mode.
`show network`	Displays the management VLAN priority.

```
System IP Address..............................  10.0.1.116Subnet
Mask.....................................  255.255.255.0Default
Gateway..................................  10.0.1.200Burned In MAC
Address.............................  00:80:63:51:7A:80Network Config-
uration Protocol (BootP/DHCP)....  NoneDHCP Client ID (same as SNMP
System Name).......  "PowerMICE-518280"Network Configuration Proto-
col HiDiscovery.....  Read-WriteManagement VLAN
ID.............................  1Management VLAN Priori-
ty.......................  7Management IP-DSCP Val-
ue.......................  0(be/cs0)Web
Mode.....................................  EnableJavaScript
Mode.................................  Enable
```

Configuring Layer 3 management priority

- ☐ Select the `QoS/Priority:Global` dialog.
- ☐ In the line `IP-DSCP value for management packets` you enter the IP-DSCP value with which the device sends management packets.

`enable`	Switch to the Priviledged EXEC mode.
`network priority ip-dscp cs7`	Assign the value cs7 to the management priority so that management packets with the highest priority are handled.
`exit`	Switch to the Priviledged EXEC mode.
`show network`	Displays the management VLAN priority.

```
System IP Address..............................  10.0.1.116Subnet
Mask.....................................  255.255.255.0Default
Gateway..................................  10.0.1.200Burned In MAC
Address..........................  00:80:63:51:7A:80Network Config-
uration Protocol (BootP/DHCP)....  NoneDHCP Client ID (same as SNMP
System Name).....  "PowerMICE-518280"Network Configuration Proto-
col HiDiscovery.....  Read-WriteManagement VLAN
ID.............................  1Management VLAN Priori-
ty.......................  7Management IP-DSCP Val-
ue.......................  56(cs7)Web
Mode.....................................  EnableJavaScript
Mode.................................  Enable
```

7.5 Flow control

7.5.1 Description of flow control

Flow control is a mechanism which acts as an overload protection for the device. During periods of heavy traffic, it holds off additional traffic from the network.

The example (see fig. 32) shows a graphic illustration of how the flow control works. Workstations 1, 2 and 3 want to simultaneously transmit a large amount of data to Workstation 4. The combined bandwidth of Workstations 1, 2 and 3 to the device is larger than the bandwidth of Workstation 4 to the device. This leads to an overflow of the send queue of port 4. The funnel on the left symbolizes this status.

If the flow control function at ports 1, 2 and 3 of the device is turned on, the device reacts before the funnel overflows. Ports 1, 2 and 3 send a message to the connected devices that no data can be received at present.

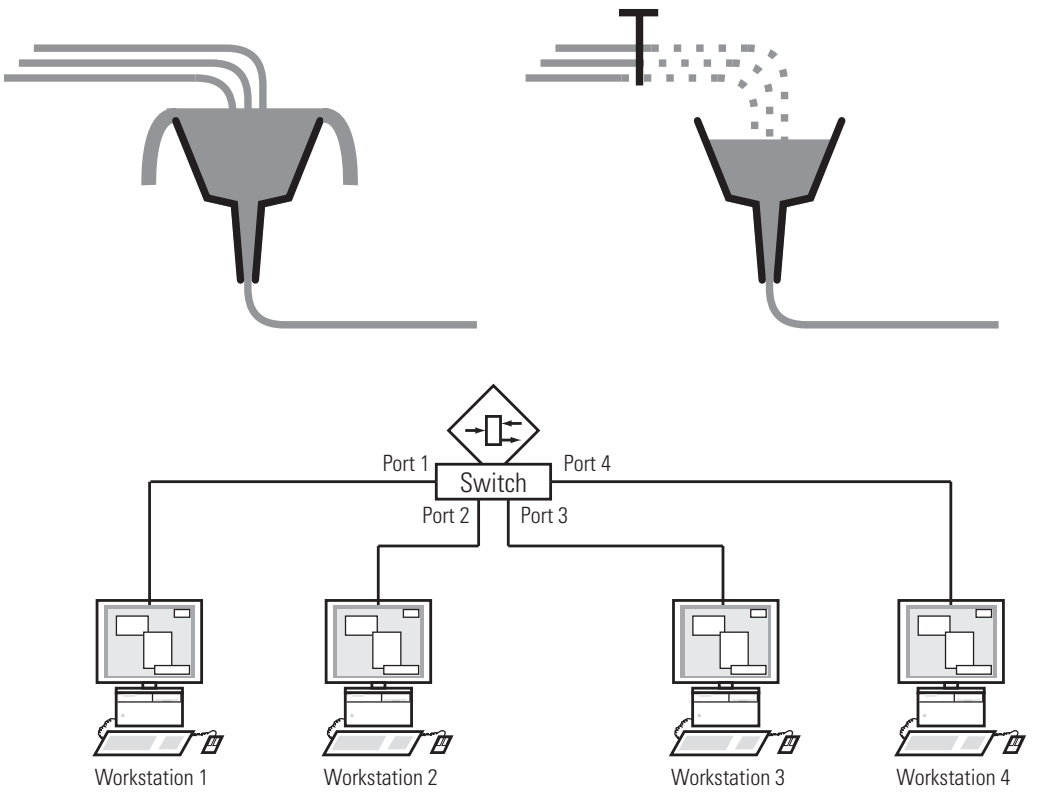


Figure 32: Example of flow control

Flow control with a full duplex link

In the example (see fig. 32) there is a full duplex link between Workstation 2 and the device.
Before the send queue of port 2 overflows, the device sends a request to Workstation 2 to include a small break in the sending transmission.

Flow control with a half duplex link

In the example (see fig. 32) there is a half duplex link between Workstation 2 and the device.
Before the send queue of port 2 overflows, the device sends data back so that Workstation 2 detects a collision and interrupts the sending process.

7.5.2 Setting the flow control

☐ Select the `Basics:Port Configuration` dialog.
In the "Flow Control on" column, you checkmark this port to specify that flow control is active here. You also activate the global "Flow Control" switch in the `Switching:Global` dialog.

☐ Select the `Switching:Global` dialog.
With this dialog you can
- switch off the flow control at all ports or
- switch on the flow control at those ports for which the flow control is selected in the port configuration table.

7.6 VLANs

7.6.1 Description of VLANs

A virtual LAN (VLAN) consists of a group of network participants in one or more network segments who can communicate with each other as if they belonged to the same LAN.

VLANs are based on logical (instead of physical) links and are flexible elements in the network design. The biggest advantage of VLANs is the possibility of forming user groups with them based on the participant function and not on their physical location or medium.
Since Broadcast/Multicast data packets are transmitted exclusively within a virtual LAN, the remaining data network is unaffected.

The VLAN function is defined in the IEEE 802.1Q standard.
The maximum number of VLANs is limited to 4094 by the structure of the VLAN tag (see fig. 30).

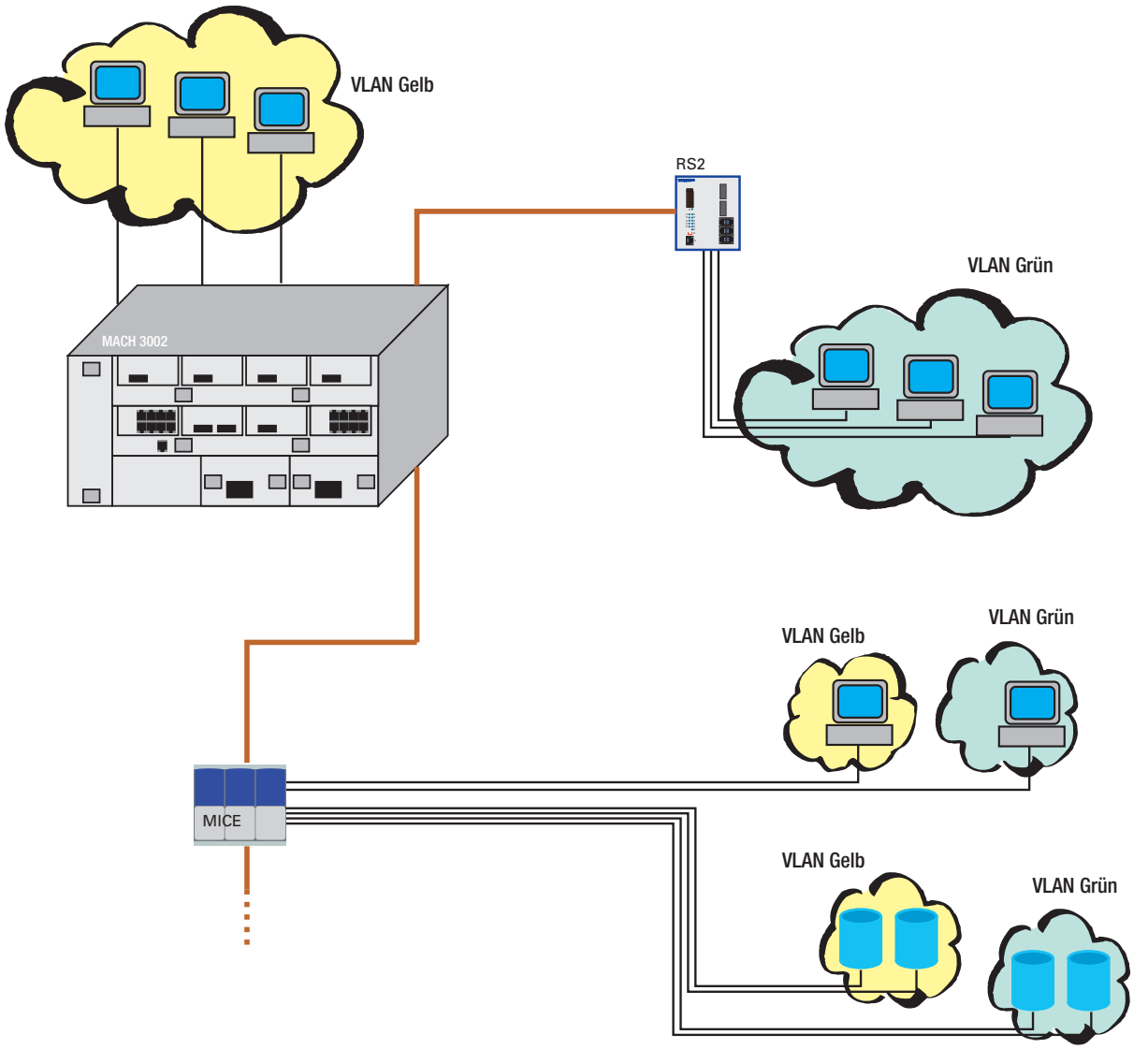


Figure 33: Example of a VLAN

Key words often used in association with VLANs are:

- **Ingress rule**
  The ingress rules stipulate how incoming data is to be handled by the device.

- **Egress rule**
  The egress rules stipulate how outgoing data is to be handled by the device.

- **VLAN identifier**
  The assignment to a VLAN is effected via a VLAN ID. Every VLAN existing in a network is identified by an ID. This ID must be unique, i.e. every ID may only be assigned once in the network.

- **Port VLAN identifier (PVID)**
  The management assigns a VLAN ID for every port. This ID is therefore known as the port VLAN ID. The device adds a tag to every data packet received without a tag. This tag contains a valid VLAN ID. When a data packet is received with a priority tag, the device adds the port VLAN ID.

- **Member set**
  The member set is list of the ports belonging to a VLAN. Every VLAN has a member set.

- **Untagged set**
  The untagged set is a list of the ports of a VLAN which send data packets without a tag. Every VLAN has an untagged set.

- **GARP - Generic Attribute Registration Protocol**
  GARP is a general protocol for transporting attributes. It describes, for example, how GVRP information is distributed.

- **GVRP - GARP VLAN registration protocol**
  GVRP describes the distribution of VLAN information to other switches. This allows switches to learn VLANs.

7.6.2 Configuring VLANs

☐ Select the `Switching:VLAN` dialog.

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

☐ Select the `Switching:VLAN:Global` dialog.

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

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

Note: For Power MICE and MACH 4000 in "Transparent mode", the devices ignore the VLAN tag when receiving. Set the VLAN membership of the ports of all VLANs to `untagged`.

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

After changing an entry:

- `Set`
  The agent saves the new entry.
  The entry is effective immediately.
- `Reload`
  Displays the current configuration data.

Note: Save the VLAN configuration to non-volatile memory (see fig. 39).

Note: The 255 available VLANs (Power MICE, MACH 4000: 256) can use any VLAN ID between 1 and 4042 (MACH 4000: 3966).

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

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

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

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

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

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

7.6.3 Example of a simple VLAN

The following example provides a quick introduction to configuring a VLAN as it is often done in practice.
The configuration is performed step by step.

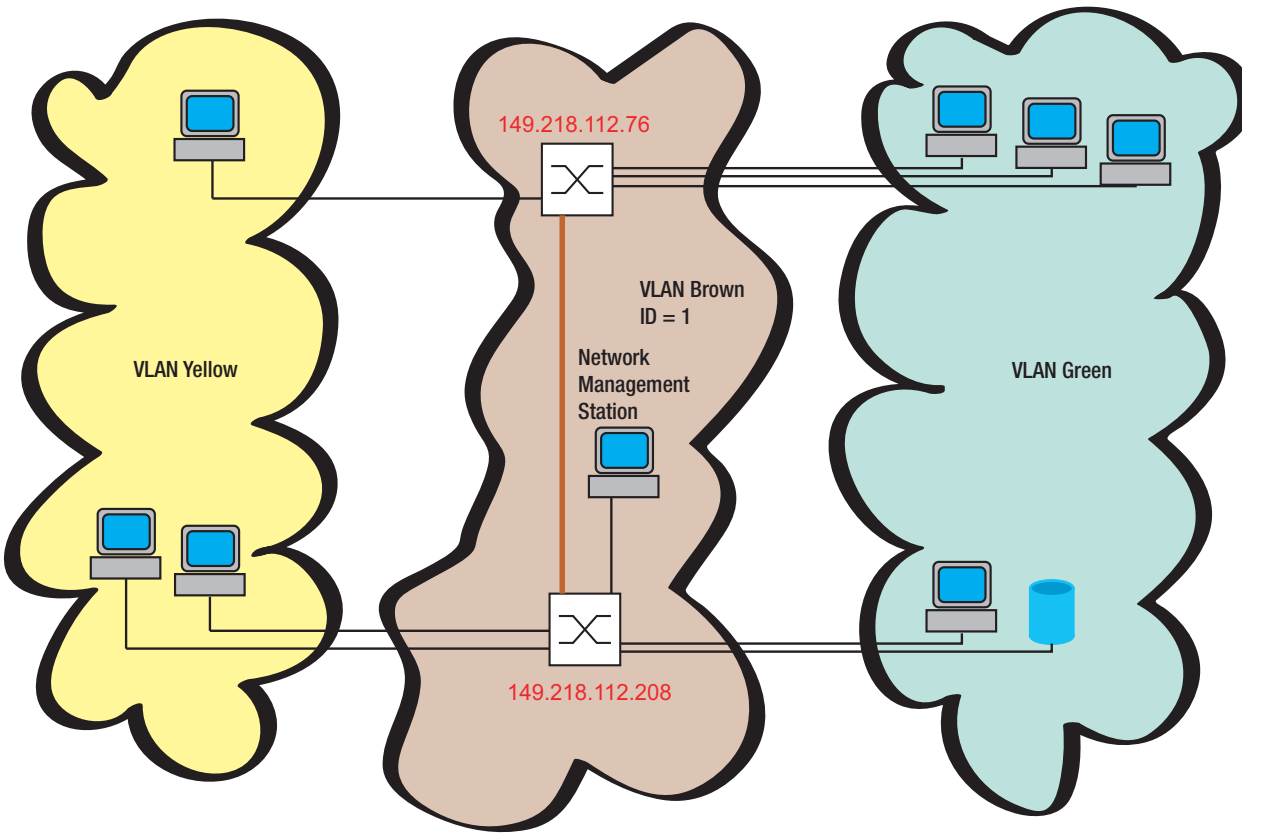


Figure 34: Example of a VLAN

☐ Select the `Switching:VLAN:Static` dialog.

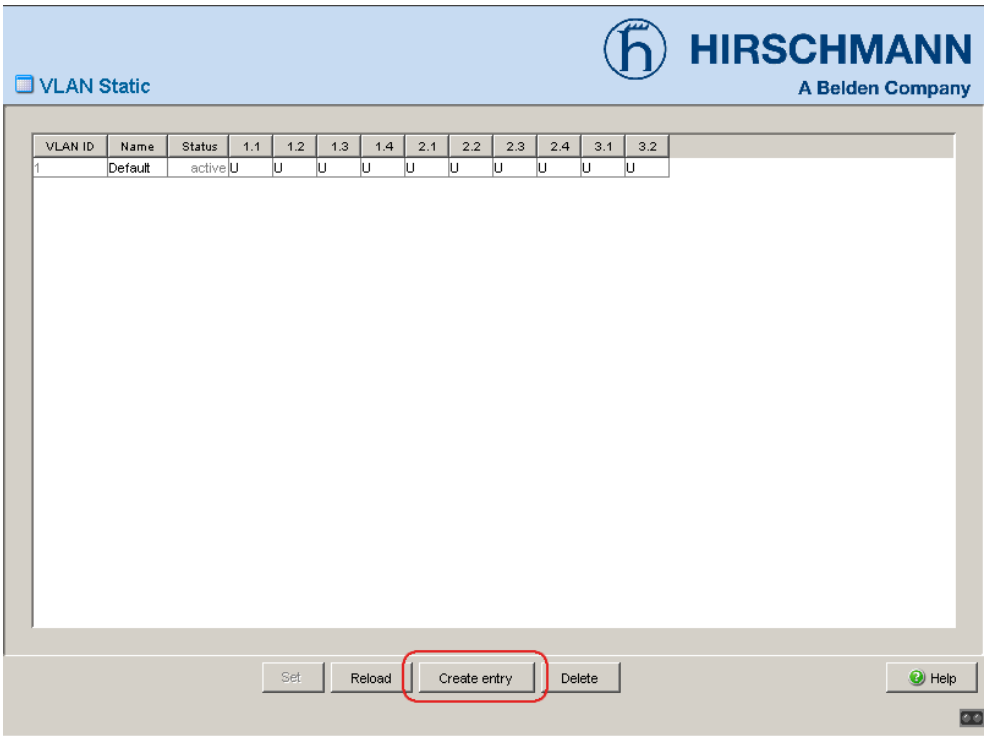


Figure 35: Creating a VLAN

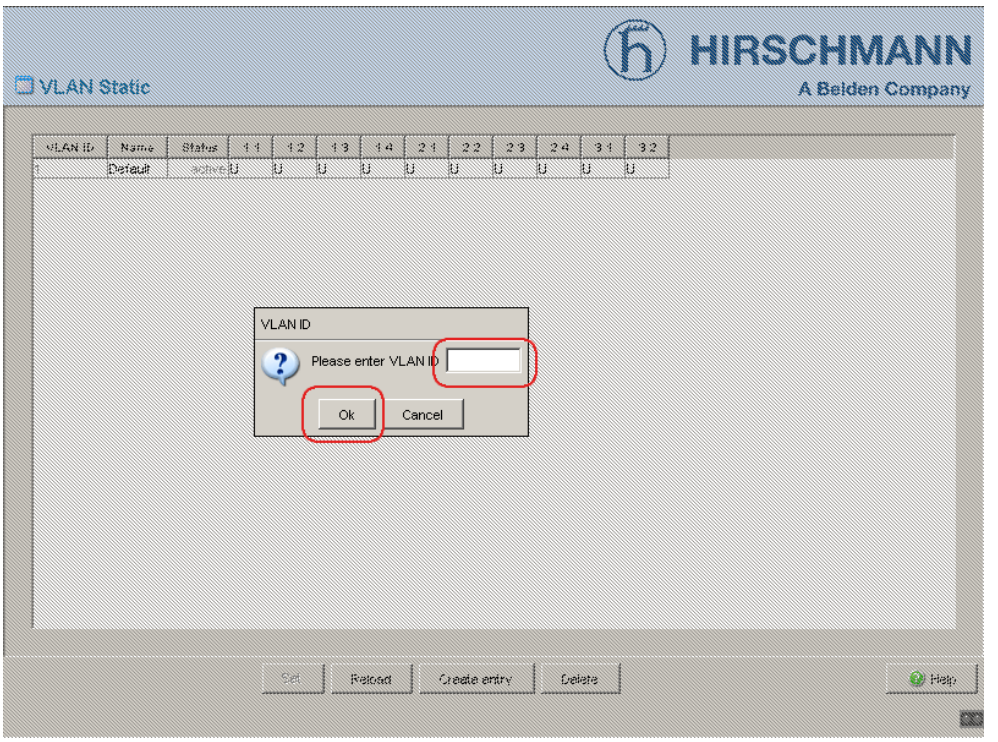


Figure 36: Entering a VLAN ID

☐ Repeat the Creating a VLAN and Entering a VLAN ID steps for all VLANs.

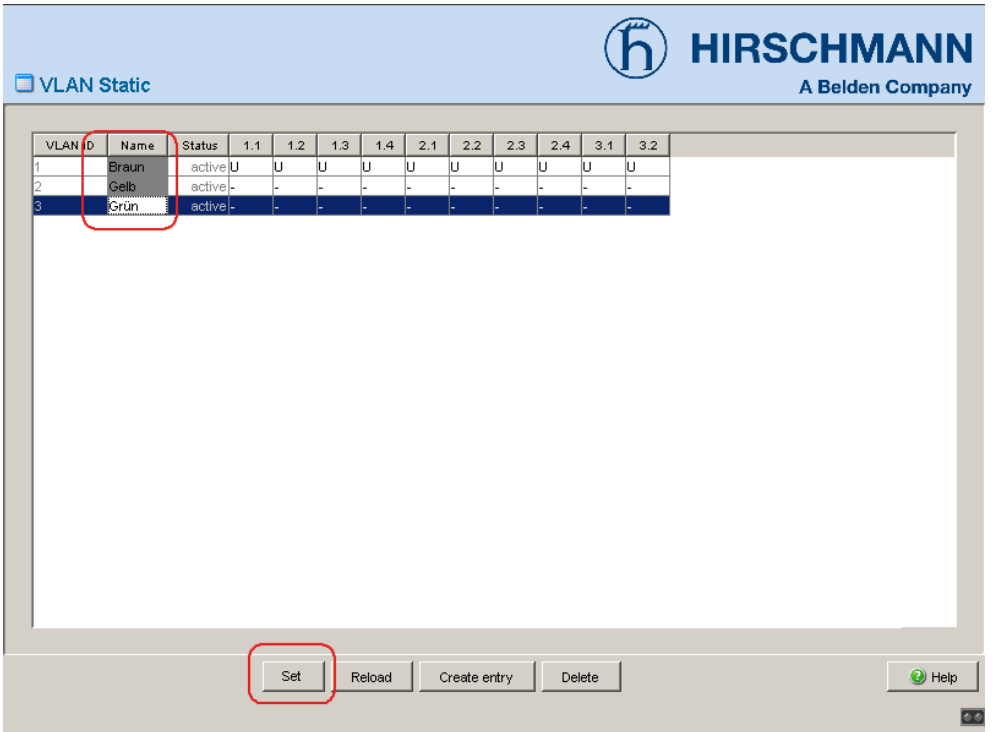


Figure 37: Assigning a VLAN any name and saving it

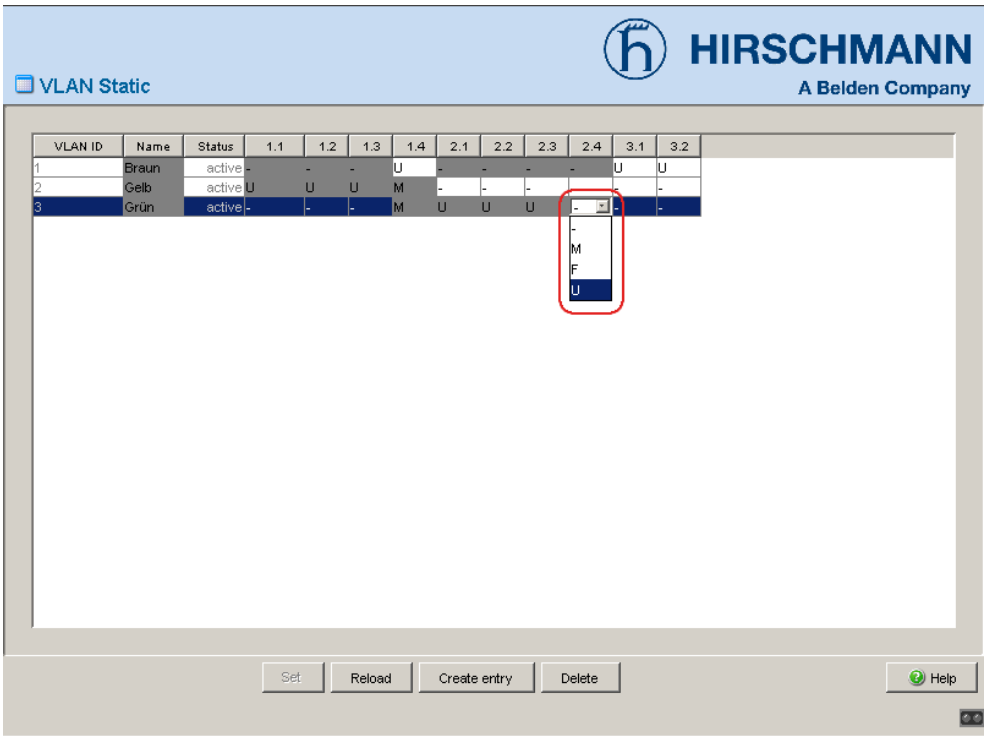


Figure 38: Defining the VLAN membership of the ports.

Ports 1.1 to 1.3 are assigned to the terminal devices of the Yellow VLAN, and ports 2.1 to 2.4 are assigned to terminal devices of the Green VLAN. Because terminal devices usually do not sent data packets with a tag, you select the `U` setting here.

Port 1.4 functions as the uplink port to the next device. It is assigned the setting `M`. Thus it can forward VLAN information.

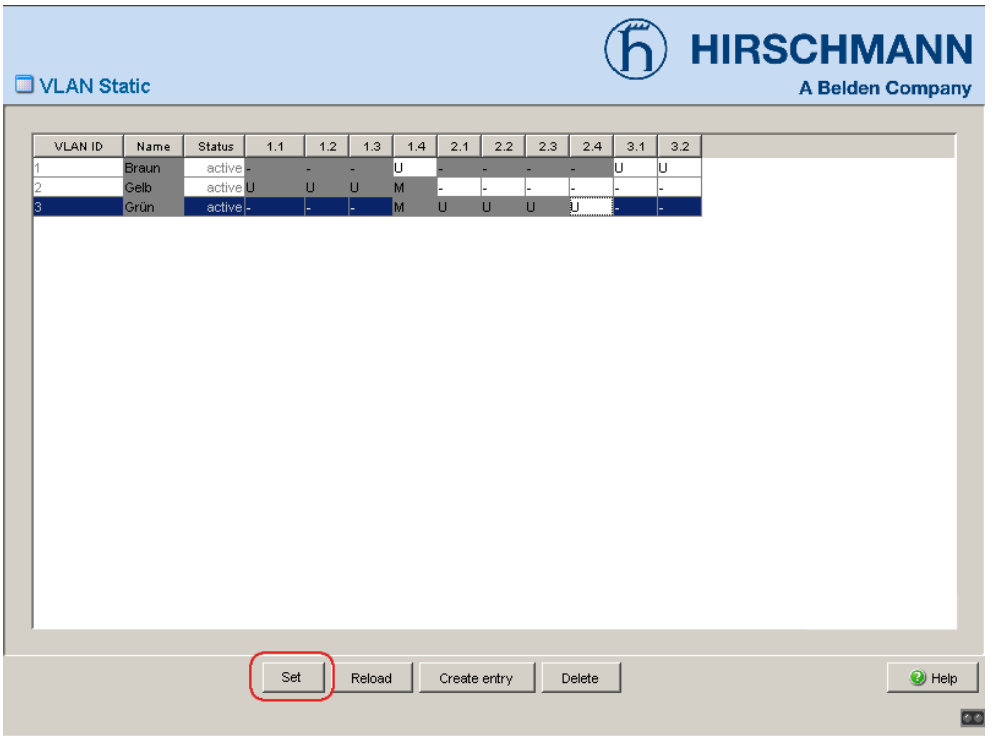


Figure 39: Saving the VLAN configuration

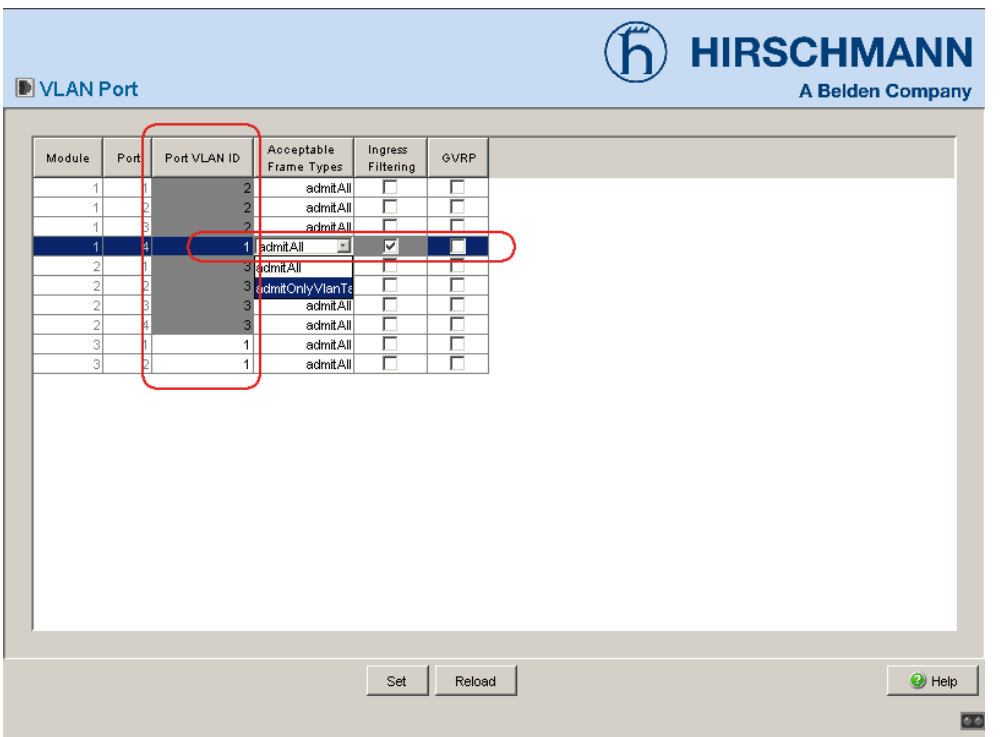


Figure 40: Assigning the VLAN ID, Acceptable Frame Types and Ingress Filtering to the ports and saving

Ports 1.1 to 1.3 are assigned to the terminal devices of the Yellow VLAN and thus to VLAN ID 2, and ports 2.1 to 2.4 are assigned to terminal devices of the Green VLAN and thus to VLAN ID 3. Because terminal devices usually do not sent data packets with a tag, you select the `admitAll` setting here.

Port 1.4 functions as the uplink port to the next device. It belongs to the Brown VLAN and is thus assigned VLAN ID 1. It is assigned the `admitOnlyVlanTagged` setting. Thus only packets with a VLAN tag can be received by this port.

Activating GVRP, both locally and later globally, ensures the distribution of the VLAN information. With this information the agents configure the uplink ports on both ends of the uplink line so that they send the data packets of the required VLANs via the uplink line.

Activating the `Ingress Filter` ensures that tags received at this port are evaluated.

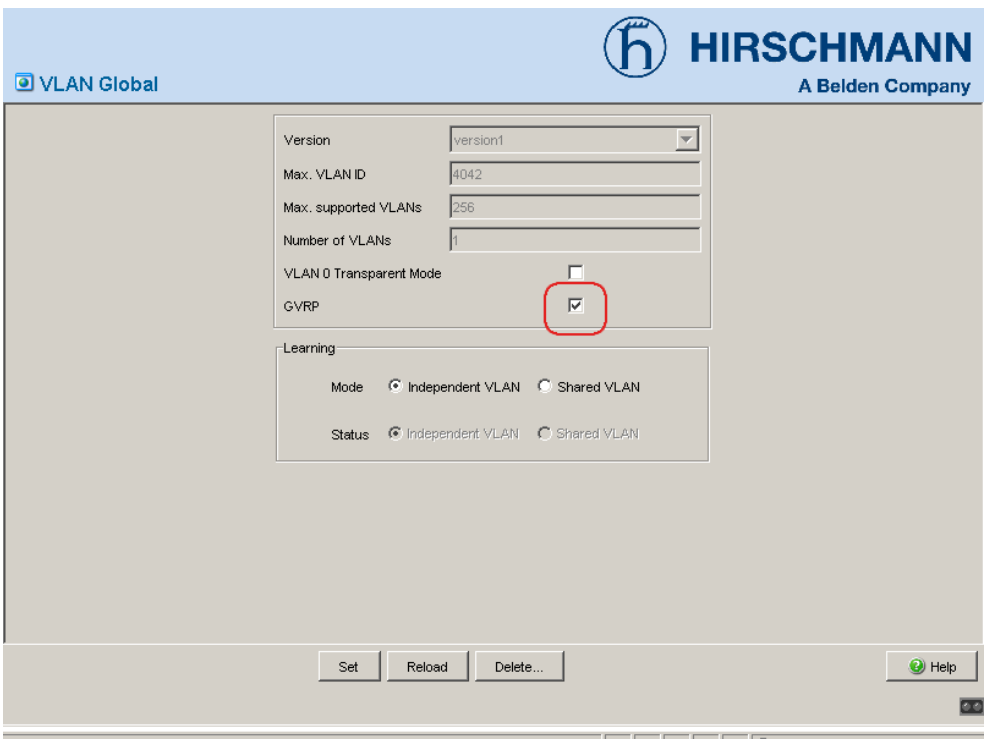


Figure 41: Globally activating GVRP

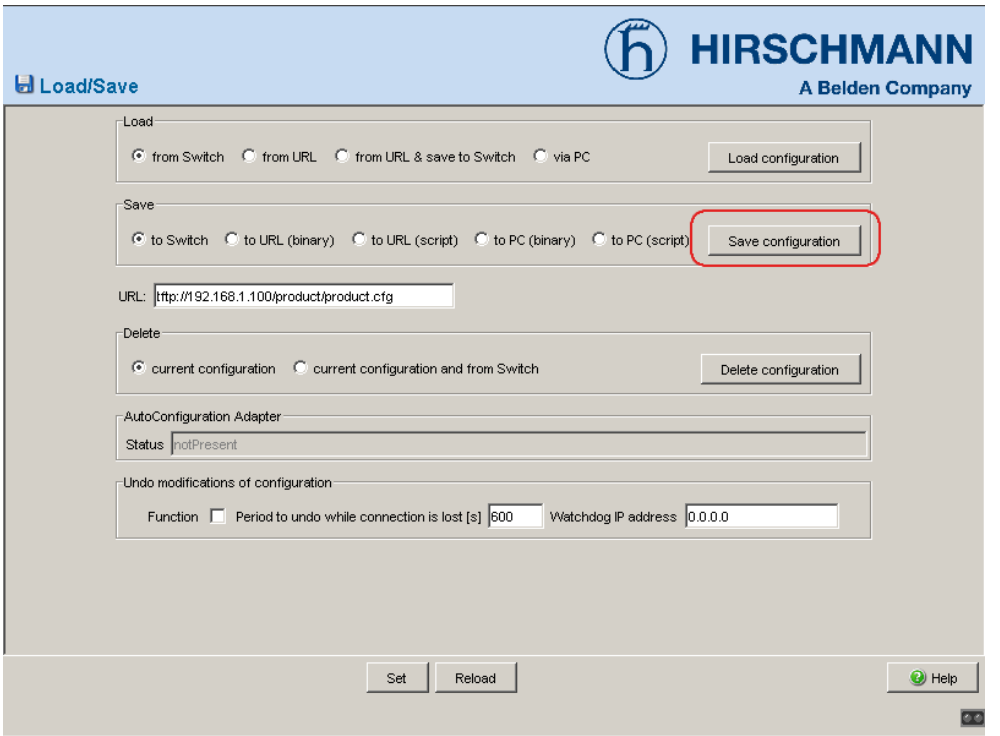


Figure 42: Saving the configuration to non-volatile memory

8 Synchronizing the system time in the network

The actual meaning of the term "real time" depends on the time requirements of the application.

The device provides two options with different levels of accuracy for synchronizing the time in your network.

If you only require accuracies in the order of milliseconds, the Simple Network Time Protocol (SNTP) provides a low-cost solution. The accuracy depends on the signal running time.
Areas of application for this protocol include:

- log entries
- time stamping of production data
- production control, etc.

IEEE 1588 with the Precision Time Protocol (PTP) achieves accuracies in the order of fractions of microseconds. This superior method is suitable for process control, for example.

Select the method that best suits your requirements. You can also use both methods simultaneously if you consider that they interact.

8.1 Entering the time

If no reference clock is available, you have the option of entering the system time in a device and then using it like a reference clock.(see on page 144 „Configuring SNTP“)(see on page 153 „Configuring PTP“) .

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

☐ Select the `Time` dialog.

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

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

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

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

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

☐ The "Local Offset" is for displaying/entering the time difference between the local time and the "IEEE 1588 / SNTP time". With "Set offset from PC", the device determines the time zone on your PC and uses it to calculate the local time difference.

`enable`	Switch to the Priviledged EXEC mode.
`configure`	Switch to the Configuration mode.
`sntp time <YYYY-MM-DD HH:MM:SS>`	Set the system time of the device.
`sntp client offset <-1000 to 1000>`	Enter the time difference between the local time and the "IEEE 1588 / SNTP time".

8.2 SNTP

8.2.1 Description of SNTP

The Simple Network Time Protocol (SNTP) enables you to synchronize the system time in your network.
The device supports the SNTP Server and SNTP Client functions.
The SNTP server makes the UTC (Universal Time Coordinated) available. UTC is the time relating to the coordinated world time measurement. The time displayed is the same worldwide. Local time differences are not taken into account. The SNTP client obtains the UTC from the SNTP server.

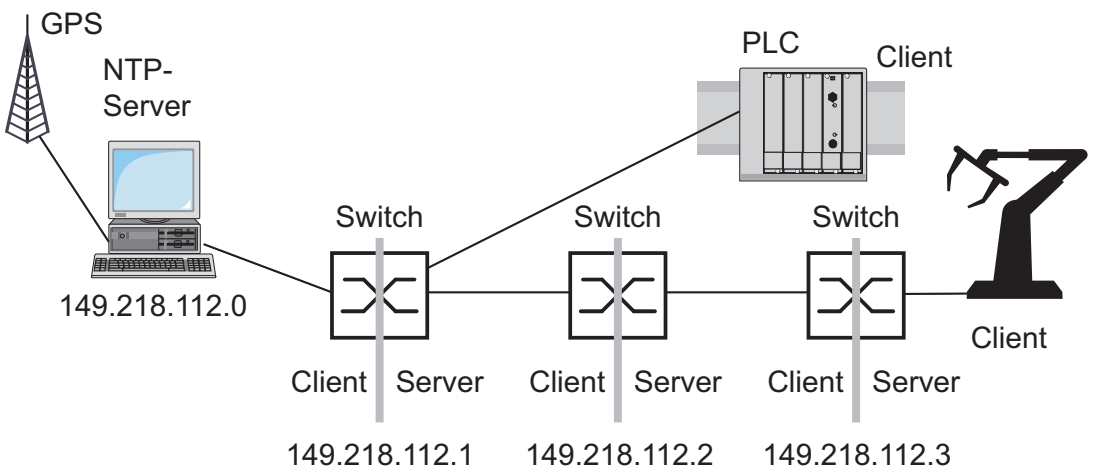


Figure 43: SNTP cascade

8.2.2 Preparing the SNTP coordination

☐ To get an overview of how the time is passed on, draw a network plan with all the devices participating in PTP. When planning, bear in mind that the accuracy of the time depends on the signal runtime.

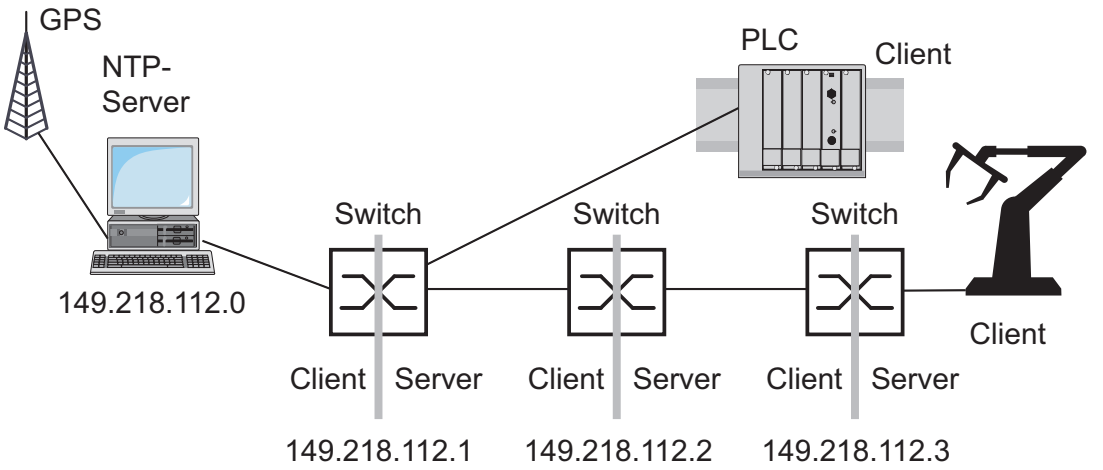


Figure 44: Example of SNTP cascade

☐ Enable the SNTP function on all devices whose time you want to set using SNTP.
The server responds to Unicast queries once it is switched on.

☐ If no reference clock is available, you specify a device as the reference clock and set its system time as accurately as possible.

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

8.2.3 Configuring SNTP

☐ Select the `Time:SNTP` dialog.

▶ Configuration SNTP Client and Server
☐ In this frame you switch the SNTP function on/off.
When it is switched off, the SNTP server does not send any SNTP packets or respond to any SNTP requests.
The SNTP client does not send any SNTP requests or evaluate any SNTP broadcast/Multicast packets.

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

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

IP destination address	Send SNTP packets periodically to
0.0.0.0	Nobody
Unicast	Unicast
224.0.1.1	Multicast
255.255.255.255	Broadcast

Table 8: Periodic sending of SNTP packets

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

▶ Configuration SNTP Client

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

☐ In "Redundant server address" you enter the IP address of the SNTP server from which the device periodically requests the system time, if it does not receive a response to a request from the "External server address" within 0.5 seconds.

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

☐ In "Server request interval" you specify the interval at which the device requests SNTP packets (valid entries: 1 second to 3600 seconds, on delivery: 30 seconds).

☐ With "Accept SNTP Broadcasts" the device takes the system time from SNTP broadcast/Multicast packets that it receives.

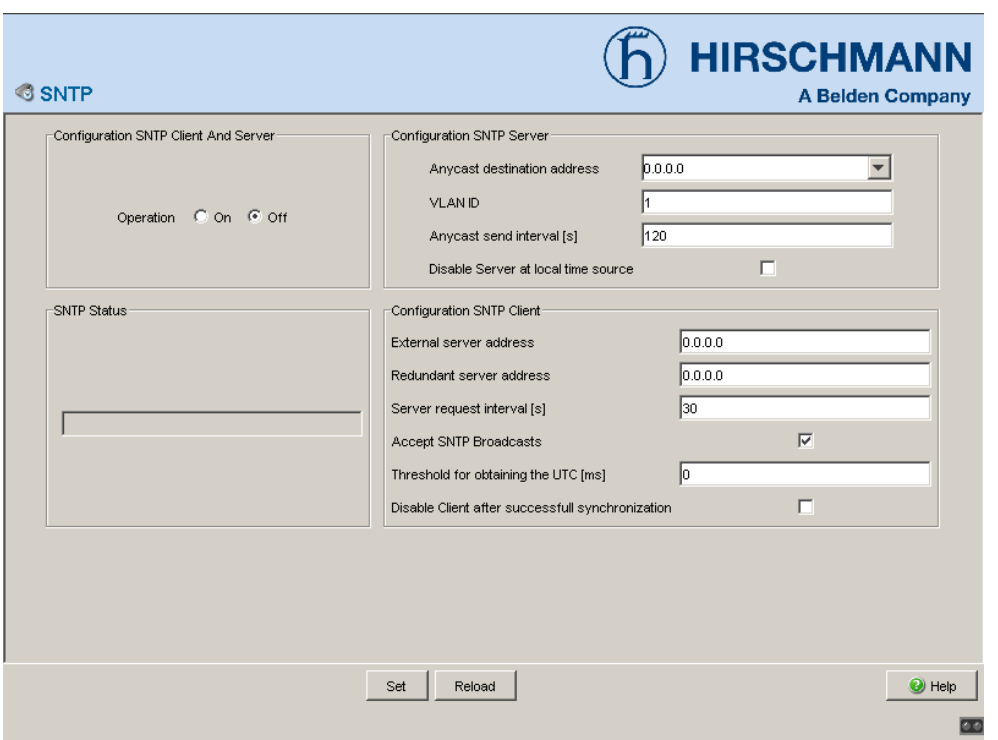


Figure 45: SNTP dialog

Device	149.218.112.1	149.218.112.2	149.218.112.3
Function	on	on	on
Server destination address	0.0.0.0	0.0.0.0	0.0.0.0
Server VLAN ID	1	1	1
Send interval	120	120	120
Client external server address	149.218.112.0	149.218.112.1	149.218.112.2
Request interval	30	30	30
Accept broadcasts	no	no	no

Table 9: Settings for the example (see fig. 44)

8.3 Precision Time Protocol

8.3.1 Description of PTP functions

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

This procedure enable the synchronization of the clocks involved to an accuracy of a few 100 ns. The synchronization messages have virtually no effect on the network load. PTP uses Multicast communication.

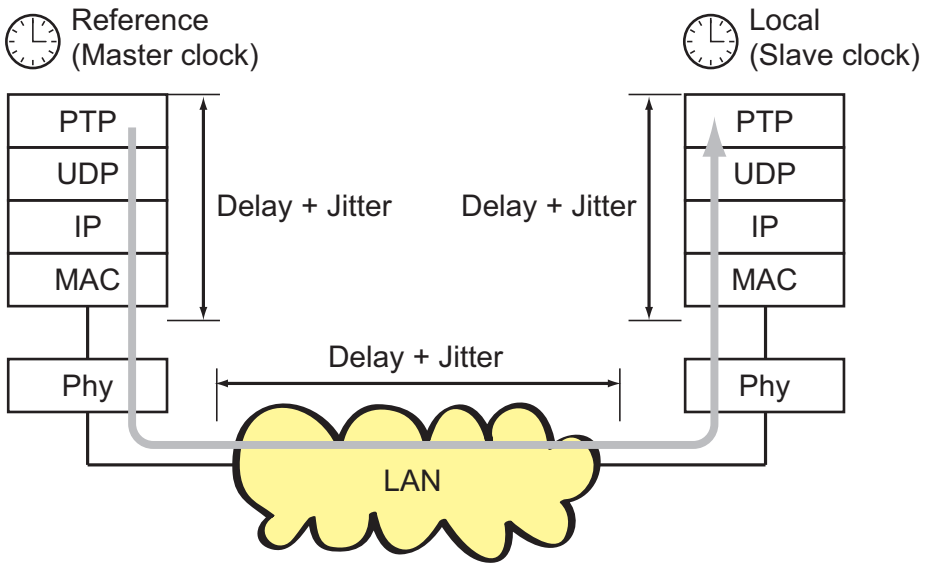
Factors influencing precision are:

- Accuracy of the reference clock IEEE 1588 classifies clocks according to their accuracy. An algorithm that measures the accuracy of the clocks available in the network specifies the most accurate clock as the "Grandmaster" clock.

Stratum number	Specification
0	For temporary, special purposes, in order to assign a better value to one clock than to all other clocks in the network.
1	Indicates the reference clock with the highest degree of accuracy. A stratum 1 clock can be both a boundary clock and an ordinary clock. Stratum 1 clocks include GPS clocks and calibrated atomic clocks. A stratum 1 clock should be synchronized using the PTP from another clock in the PTP system.
2	Indicates the second-choice reference clock.
3	Indicates the reference clock that can be synchronized via an external connection.
4	Indicates the reference clock that cannot be synchronized via an external connection.
5–254	Reserved.
255	Default setting. Such a clock should never be used as the best master clock.

Table 10: Stratum – classifying the clocks

- Cable delays; device delays The communication protocol specified by IEEE 1588 enables delays to be determined. Formulas for calculating the current time eliminate delays.
- Accuracy of local clocks The communication protocol specified by IEEE 1588 takes into account the inaccuracy of local clocks in relation to the reference clock. Calculation formulas permit the synchronization of the local time, taking into account the inaccuracy of the local clock in relation to the reference clock.



PTP	Precision Time Protocol (Application Layer)
UDP	User Datagramm Protocol (Transport Layer)
IP	Internet Protocol (Network Layer)
MAC	Media Access Control
Phy	Physical Layer

Figure 46: Delay and jitter problems when synchronizing clocks

To get around the delay and jitter in the protocol stack, IEEE 1588 recommends inserting a special hardware time stamp unit between the MAC and Phy layers. Devices/modules with the "-RT" suffix in their names are equipped with this time stamp unit.

The delay and jitter in the LAN increase in the media and transmission devices along the transmission path.

The cable delays are relatively constant. Changes occur very slowly. IEEE 1588 takes this fact into account by regularly making measurements and calculations.

IEEE 1588 eliminates the inaccuracy caused by delays and jitter by defining boundary clocks. Boundary clocks are clocks integrated into devices. These clocks are synchronized on the one side of the signal path, and on the other side of the signal path they are used to synchronize the subsequent clocks (ordinary clocks).

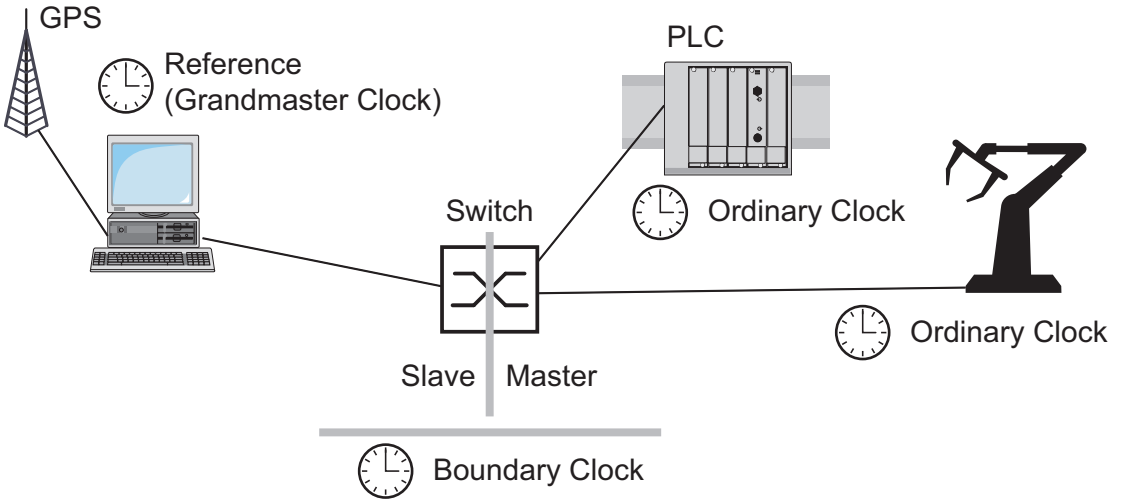


Figure 47: Boundary clock

Independently of the physical communication paths, the PTP provides logical communication paths which you define by setting up PTP subdomains. Subdomains are used to form groups of clocks that are time-independent from the rest of the domain. Typically, the clocks in a group use the same communication paths as other clocks.

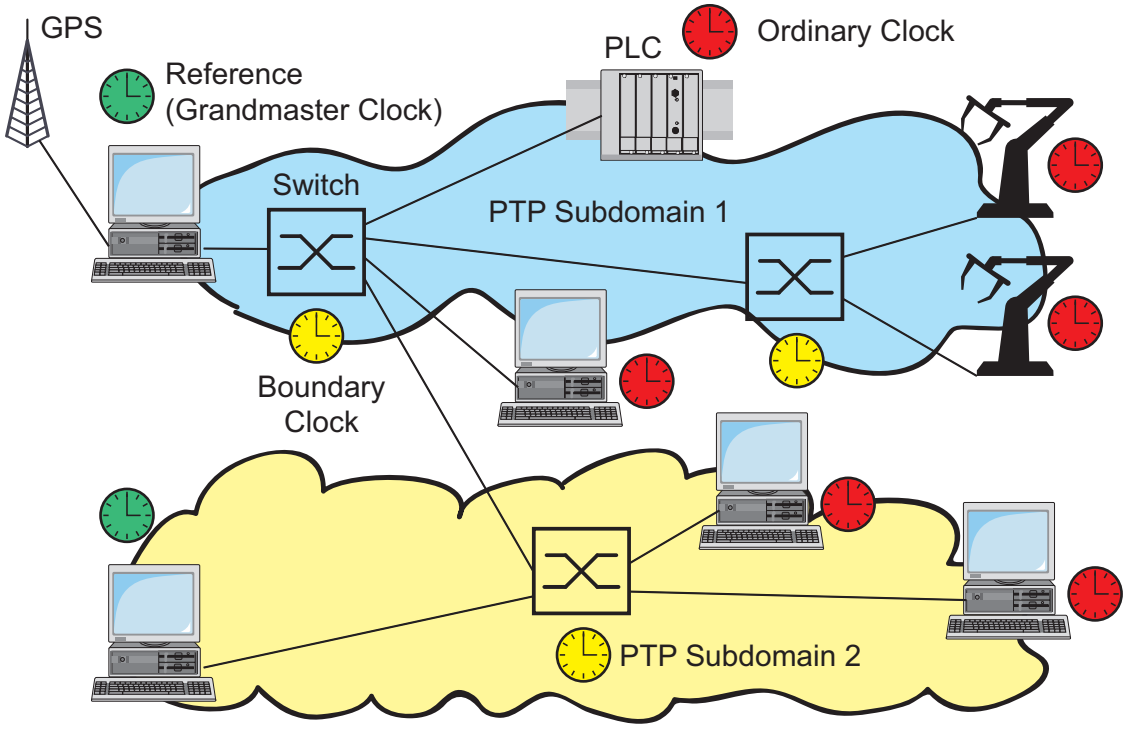


Figure 48: PTP Subdomains

8.3.2 Preparing the PTP configuration

After the function is activated, the PTP takes over the configuration automatically. The delivery settings of the device are sufficient for most applications.

☐ To get an overview of the time distribution, draw a network plan with all the devices participating in PTP.

Note: Connect all the connections you need to distribute the PTP information to connections with an integrated time stamp unit (RT modules).
Devices without a time stamp unit take the information from the PTP and use it to set their clocks. They are not involved in the protocol.

☐ Enable the PTP function on all devices whose time you want to synchronize using PTP.

☐ If no reference clock is available, you specify a device as the reference clock and set its system time as accurately as possible.

8.3.3 Configuring PTP

In the `Time:PTP:Global` dialog, you can enable/disable the function and make PTP settings on the MS20/30 and Power MICE devices which are to apply to all ports.

- PTP Global
  - ☐ Select the `Time:PTP:Global` dialog.
  - ☐ Activate the function in the “Operation IEEE 1588 / PTP” frame.
  - ☐ If you have selected this device as the PTP reference clock, select the value “true” in the “Preferred Master” line of the “Configuration IEEE 1588 / PTP” frame.

- With “Reinitialize” you trigger the synchronization of the local clock.

- Configuration

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

  `Preferred Master`: Define the local clock as the preferred master.

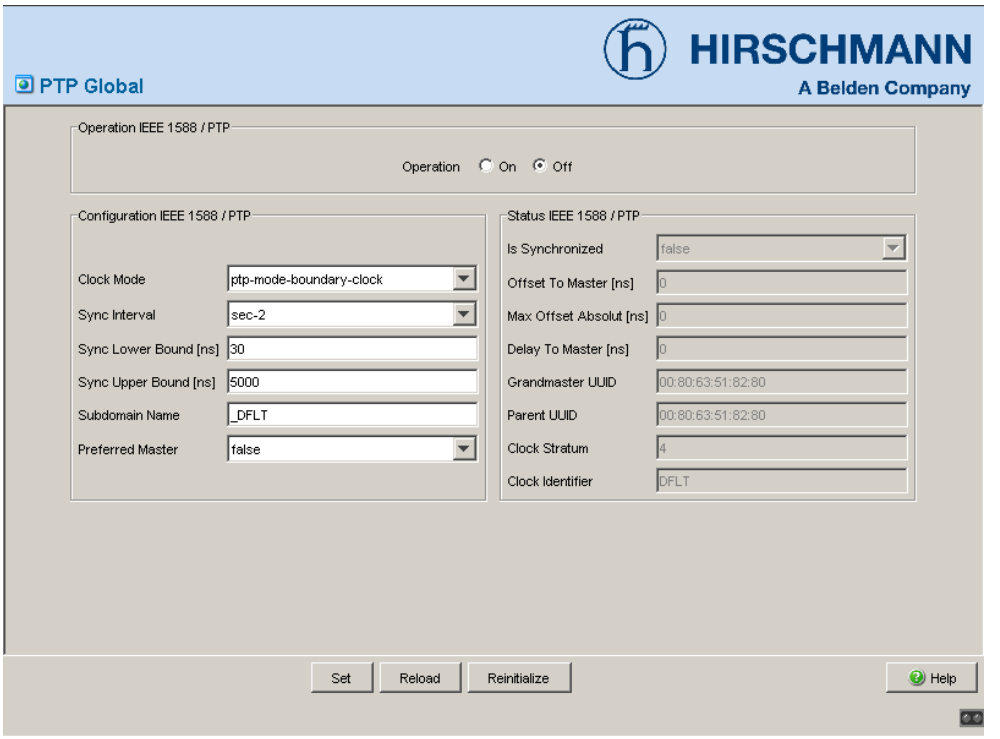


Figure 49: PTP Global dialog

Application example:

PTP is used to synchronize the time in the network. As an SNTP client, the left device gets the time from the NTP server via SNTP. The device assigns clock stratum "2" to the time received from an NTP server. Thus the left device becomes the reference clock for the PTP synchronization and is the "preferred master". The "preferred master" forwards the exact time signal via its connections to the RT module. The device with RT module receives the exact time signal at a connection of its RT module and thus has the clock mode "ptp-mode-boundary-clock". The devicees without an RT module have the clock mode "ptp-mode-simple-ptp".

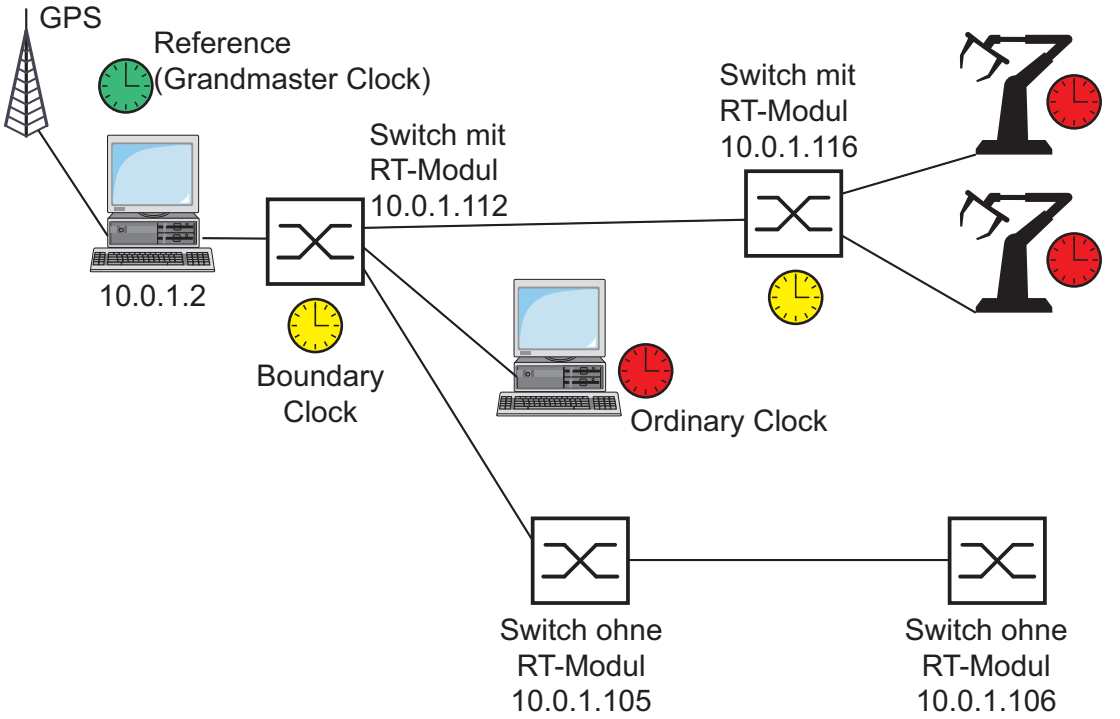


Figure 50: Example of PTP synchronization

Device	**10.0.1.112**	**10.0.1.116**	**10.0.1.105**	**10.0.1.106**
PTP				
Operation	on	on		on
Clock Mode	ptp-mode-boundary-clock	ptp-mode-boundary-clock	ptp-mode-simple-ptp	ptp-mode-simple-ptp
Preferred Master	true	false	false	false
SNTP				
Operation	on	off	off	off
Server destination address	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0
Server VLAN ID	1	1	1	1
Client external server address	10.0.1.2	0.0.0.0	0.0.0.0	0.0.0.0
Request interval	30	any	any	any
Accept broadcasts	no	any	any	any

Table 11: Settings for the example (see fig. 50)

8.4 Interaction of PTP and SNTP

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

Note: Configure the devices so that each device only receives the time from one source. If the device gets the time via PTP, you enter the "External server address" 0.0.0.0 in the SNTP client configuration and do not accept SNTP broadcasts. If the device gets the time via SNTP, make sure that the "best" clock is connected to the SNTP server. Then both protocols will get the time from the same server. The example (see fig. 51) shows such an application.

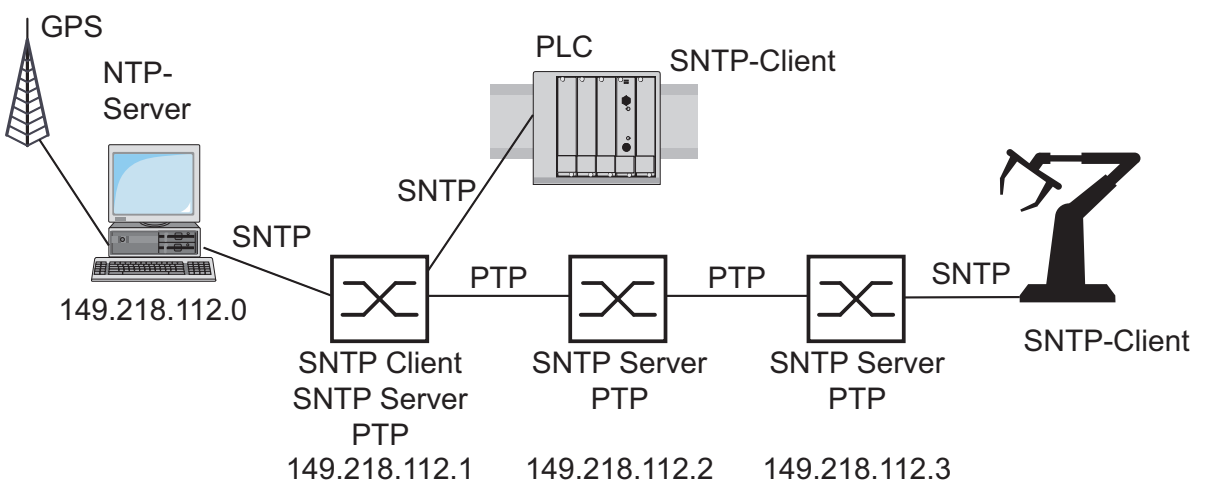


Figure 51: Example of the coexistence of PTP and SNTP

- **Application example:**
  The requirements with regard to the accuracy of the time in the network are quite high, but the terminal devices only support SNTP (see fig. 51).

Device	149.218.112.1	149.218.112.2	149.218.112.3
PTP			
Operation	on	on	on
Clock Mode	ptp-mode-boundary-clock	ptp-mode-boundary-clock	ptp-mode-boundary-clock
Preferred Master	false	false	false
SNTP			
Operation	on	on	on
Server destination address	224.0.1.1	224.0.1.1	224.0.1.1
Server VLAN ID	1	1	1
Send interval	30	30	30
Client external server address	149.218.112.0	0.0.0.0	0.0.0.0
Request interval	any	any	any
Accept broadcasts	no	no	no

Table 12: Settings for the example

In the example, the left device, as an SNTP client, gets the time from the NTP server via SNTP. The device assigns clock stratum "2" to the time received from an NTP server. Thus the left device becomes the reference clock for the PTP synchronization. PTP is active for all three devices, thus providing precise time synchronization between them. As the connectable terminal devices in the example only support SNTP, all three devices act as SNTP servers.

9 Operation diagnosis

The device provides you with the following diagnostic tools for the operation diagnosis:

- Sending traps
- Monitoring device status
- Out-of-band signaling via signal contact
- Port status indication
- Event counter at port level
- SFP status indication
- TP cable diagnostics
- Topology discovery
- Reports
- Monitoring the data traffic of a port (port mirroring)

9.1 Sending traps

If unusual events occur during normal operation of the device, they are reported immediately to the management station. This is done by means of what are called traps - alarm messages - that bypass the polling procedure ("Polling" means querying the data stations at regular intervals). Traps make it possible to react quickly to critical situations.

Examples of such events are:

- a hardware reset
- changes to the basic device configuration
- segmentation of a port
- …

Traps can be sent to various hosts to increase the transmission reliability for the messages. A trap message consists of a packet that is not acknowledged.
The device sends traps to those hosts that are entered in the trap destination table. The trap destination table can be configured with the management station via SNMP.

9.1.1 SNMP trap listing

All the possible traps that the device can send are listed in the following table.

Trap name	Meaning
authenticationFailure	is sent if a station attempts to access an agent without permission.
coldStart	is sent for both cold and warm starts during the boot process after successful management initialization.
hmAutoconfigAdapterTrap	is sent when the ACA Auto Configuration Adapter is removed or plugged in again.
linkDown	is sent if the link to a port is interrupted.
linkUp	is sent as soon as the link to a port is re-established.
hmTemperature	is sent if the temperature exceeds the set threshold value.
hmPowerSupply	is sent if the status of the voltage supply changes.
hmSigConRelayChange	is sent if the status of the signal contact changes during the operation monitoring.
newRoot	is sent if the sending agent becomes a new root of the spanning tree.
topologyChange	is sent if the transmission mode of a port changes.
risingAlarm	is sent if an RMON alarm input exceeds the upper threshold.
fallingAlarm	is sent if an RMON alarm input falls below the lower threshold.
hmPortSecurityTrap	is sent if a MAC/IP address is detected at the port which does not correspond to the current settings of – hmPortSecPermission and – hmPorSecAction set either to trapOnly (2) or portDisable (3).
hmModuleMapChange	is sent if the hardware configuration is changed.
hmBPDUGuardTrap	is sent if a BPDU is received at a port even though the BPDU Guard function is active.
hmMrpReconfig	is sent if the configuration of the MRP-Ring changes.
hmRingRedReconfig	is sent if the configuration of the HIPER-Ring changes.
hmRingRedCplReconfig	is sent if the configuration of the redundant ring/network coupling changes.
hmSNTPTrap	is sent if errors occur in connection with the SNTP (e.g. server cannot be reached).
hmRelayDuplicateTrap	is sent if a duplicate IP address is detected in connection with DHCP Option 82.
lldpRemTablesChange-Trap	is sent, if an entry in the topology table is changed.

Table 13: Possible traps

9.1.2 SNMP traps when booting

The device sends the ColdStart trap during every booting.

9.1.3 Configuring traps

☐ Select the `Diagnostics:Alarms (Traps)` dialog.

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

☐ Select "Create entry".

☐ In the "Address" column, enter the IP address of the management station to which the traps should be sent.

☐ In the "Enabled" column, you mark the entries which should be taken into account when traps are being sent.

☐ In the "Selection" frame, select the trap categories from which you want to send traps.

Note: You need read-write access for this dialog.

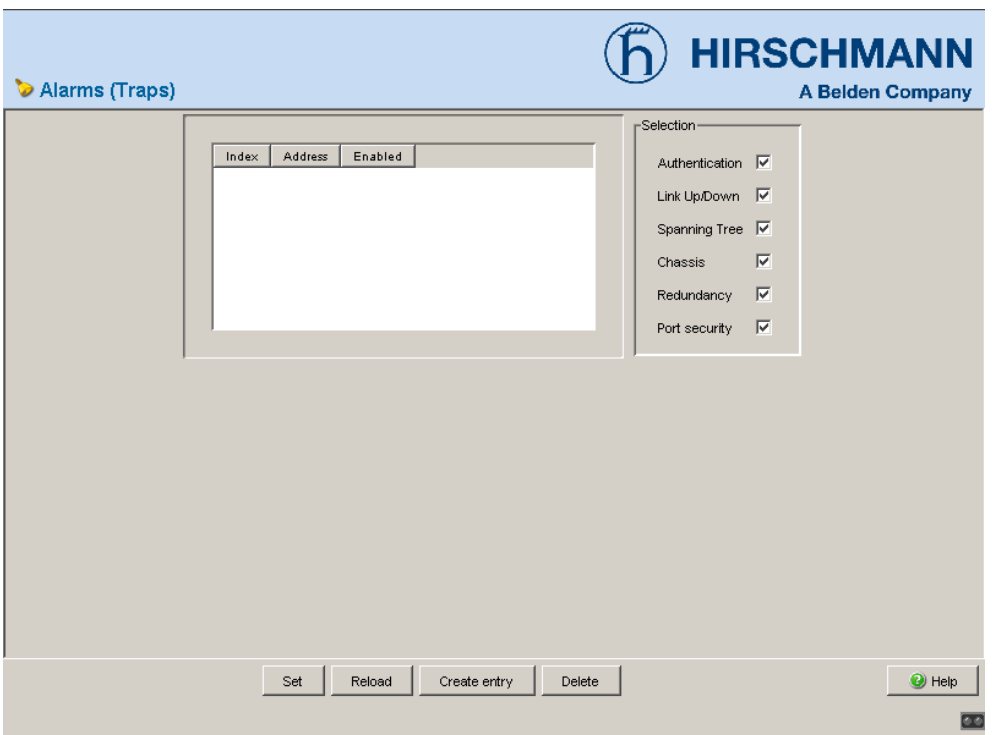


Figure 52: Alarms dialog

The events which can be selected are:

Name	Meaning
Authentication	The device has rejected an unauthorized access attempt (see the `Access for IP Addresses and Port Security` dialog).
Cold Start	The device has been switched on.
Link Down	At one port of the device, the link to the device connected there has been interrupted.
Link Up	At one port of the device, the link to a device connected there has been established.
Spanning Tree	The topology of the Rapid Spanning Tree has changed.
Chassis	Encompasses the following events: . – The status of a supply voltage has changed (see the System dialog). – Signaling relay: The status of the signal contact has changed. To take this event into account, you activate "Trap for status change" in the `Diagnostics:Signal Contact 1/2` dialog. – An error has occurred in connection with the SNTP. – A media module was added or removed.– The ACA AutoConfiguration Adapter was added or removed. – The temperature threshold was exceeded/not reached.
Redundancy	The redundancy status of the Hiper-Ring or the redundant ring/network coupling has changed.
Port Security	At one port a data packet has been received from an unauthorized terminal device (see the `Port Security` dialog).
Bridge	Although the BPDU Guard function is active at a port, a BPDU was received (see Redundancy user manual, "Rapid Spanning Tree").

Table 14: Trap categories

9.2 Monitoring the device status

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

- signal the device status out-of-band via a signal contact (see on page 171 „Monitoring the device status via the signal contact“)
- signal the device status by sending a trap when the device status changes
- detect the device status in the Web-based interface on the system side.
- query the device status in the Command Line Interface.

The device status of the device includes:

- Incorrect supply voltage,
  the failure of at least one of the two supply voltages
  or a permanent fault in the device (internal supply voltage).
- The temperature threshold has been exceeded or has not been reached.
- The removal of a module (for modular devices).
- The removal of the ACA.
- Failure of a fan (MACH 4000).
- The defective link status of at least one port. With the device, the indication of link status can be masked by the management for each port (see on page 72 „Displaying connection error messages“). On delivery, there is no link monitoring.
- Event in HIPER-Ring:
  The failure of the redundancy (in redundancy manager mode). On delivery, there is no ring redundancy monitoring.
- Event in the Ring/network coupling:
  failure of the redundancy. On delivery, there is no ring redundancy monitoring.
  The following conditions are also reported by the device in standby mode:
  – Incorrect link status of the control line
  – Partner device is in standby mode.

The management setting specifies which events determine the device status.

Note: With non-redundant voltage supply, the device reports the absence of a supply voltage. You can prevent this message by feeding the supply voltage over both inputs, or by switching off the monitoring (see on page 170 „Monitoring correct operation via the signal contact“).

9.2.1 Configuring the device status

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

`enable`	Switch to the Priviledged EXEC mode.
`configure`	Switch to the Configuration mode.
`device-status monitor all enable`	Include all the possible events in the device status determination.
`device-status trap enable`	Enable a trap to be sent if the device status changes.

9.2.2 Displaying the device status

- ☐ Select the `Basics:System` dialog.

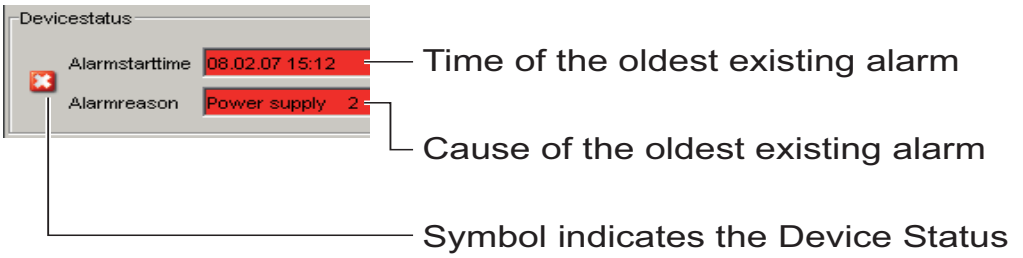


Figure 53: Device status and alarm display

`exit`	Switch to the Priviledged EXEC mode.
`show device-status`	Display the device status and the setting for the device status determination.

9.3 Out-of-band signaling

The signal contact is used to control external devices and monitor the operation of the Gerätes, thus enabling remote diagnostics.
A break in contact is reported via the potential-free signal contact (relay contact, closed circuit):

- Incorrect supply voltage,
  the failure of at least one of the two supply voltages,
  a permanent fault in the device (internal supply voltage).
- The temperature threshold has been exceeded or has not been reached.
- The removal of a module.
- The removal of the ACA.
- The defective link status of at least one port. With the device, the indication of link status can be masked by the management for each port (see on page 72 „Displaying connection error messages“). On delivery, there is no link monitoring.
- Event in HIPER-Ring:
  The failure of the redundancy (in redundancy manager mode). On delivery, there is no ring redundancy monitoring.
- Event in the Ring/network coupling:
  failure of the redundancy. On delivery, there is no ring redundancy monitoring.
  The following conditions are also reported by the device in standby mode:
  – Incorrect link status of the control line
  – Partner device is in standby mode.

The management setting specifies which events switch a contact.

Note: With non-redundant voltage supply, the device reports the absence of a supply voltage. You can prevent this message by feeding the supply voltage over both inputs, or by switching off the monitoring (see on page 170 „Monitoring correct operation via the signal contact“).

9.3.1 Controlling the signal contact

With this mode you can remotely control every signal contact individually.

Application options:

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

☐ Select the `Diagnostics:Signal Contact 1/2)` dialog.

☐ In the "Mode Signal contact" frame, you select the "Manual setting" mode to switch the contact manually.

☐ Select "Opened" in the "Manual setting" frame to open the contact.

☐ Select "Closed" in the "Manual setting" frame to close the contact.

`enable`	Switch to the Priviledged EXEC mode.
`configure`	Switch to the Configuration mode.
`signal-contact 1 mode manual`	Select the manual setting mode for signal contact 1.
`signal-contact 1 state open`	Open signal contact 1.
`signal-contact 1 state closed`	Close signal contact 1.

9.3.2 Monitoring correct operation via the signal contact

Configuring the operation monitoring

- ☐ Select the Diagnostics:Signal Contact dialog.
- ☐ Select "Monitoring correct operation" in the "Mode signal contact" frame to use the contact for operation monitoring.
- ☐ In the "Monitoring correct operation" frame, you select the events you want to monitor.
- ☐ To monitor the temperature, you set the temperature thresholds in the Basics:System dialog at the end of the system data.

`enable`	Switch to the Priviledged EXEC mode.
`configure`	Switch to the Configuration mode.
`signal-contact 1 monitor all`	Includes all the possible events in the operation monitoring.
`signal-contact 1 trap enable`	Enables a trap to be sent if the status of the operation monitoring changes.

Displaying the signal contact

The device gives you three options for displaying the status of the signal contact:

- LED display
- display in the Web-based interface
- query in the Command Line Interface.

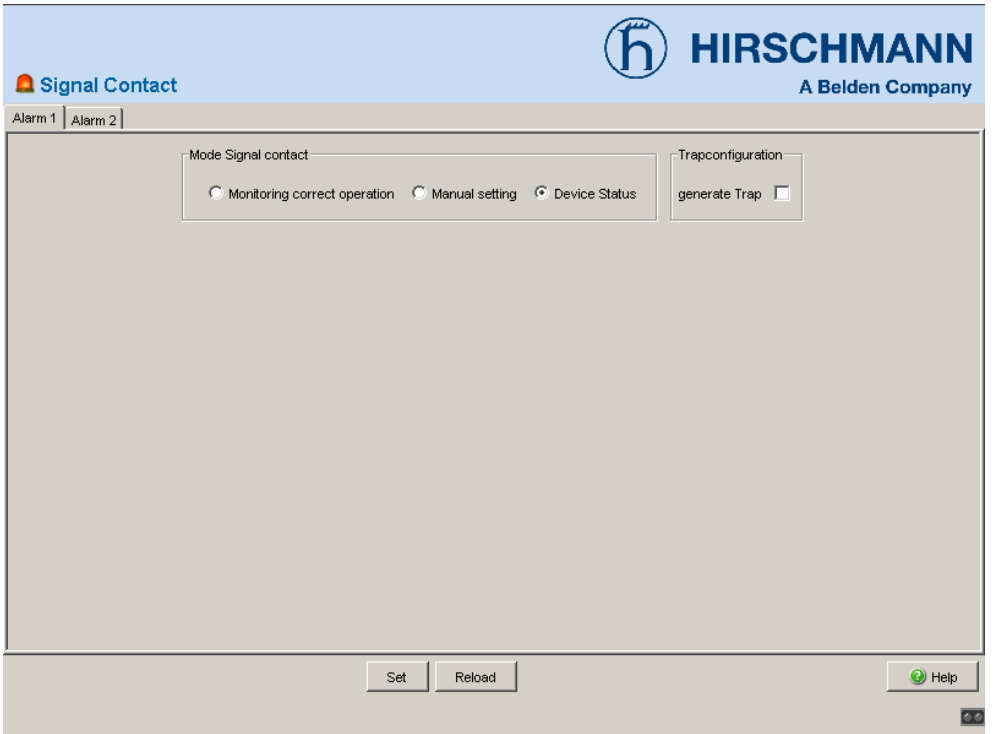


Figure 54: Signal contact dialog

`exit`	Switch to the Priviledged EXEC mode.
`show signal-contact 1`	Displays the status of the operation monitoring and the setting for the status determination.

9.3.3 Monitoring the device status via the signal contact

The "Device Status" option enables you, like in the operation monitoring, to monitor the device state (see on page 165 „Monitoring the device status“) via the signal contact.

9.4 Port status indication

☐ Select the `Basics:System` dialog.

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

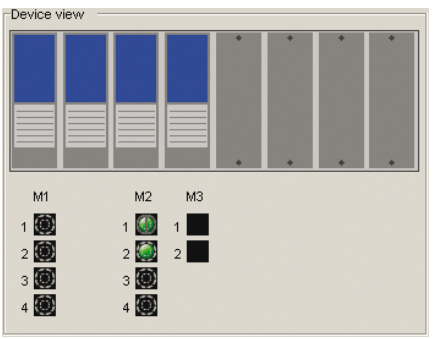


Figure 55: Device view

Meaning of the symbols:

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

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

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

The port is in autonegotiation mode.

The port is in HDX mode.

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

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

9.5 Event counter at port level

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

Counter	Possible problem
Received fragments	– The controller of the connected device is faulty – Electromagnetic interference in the transmission medium
CRC error	– The controller of the connected device is faulty – Electromagnetic interference in the transmission medium – Defective component in the network
Collisions	– The controller of the connected device is faulty – Network overextended/lines too long – Collision of a fault with a data packet

Table 15: Examples indicating possible problems

☐ Select the `Diagnostics:Ports:Statistics` dialog.

☐ To reset the counters, click on "Reset port counters" in the Basics:Restart dialog.

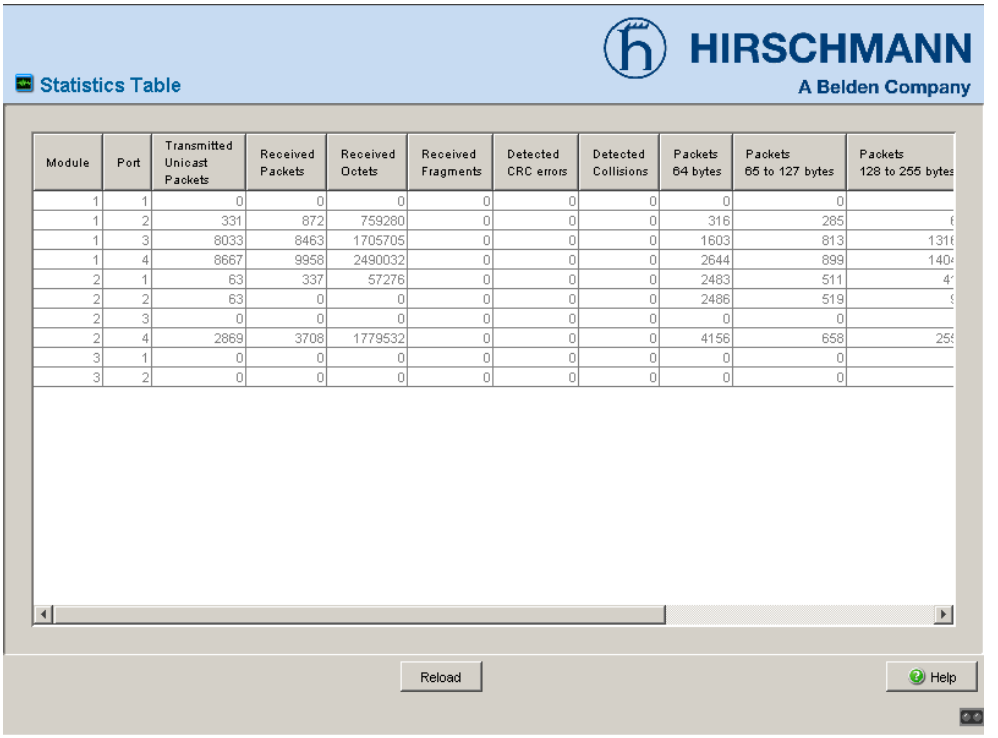


Figure 56: Port Statistics dialog

9.6 Displaying the SFP status

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

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

☐ Select the `Diagnostics:Ports:SFP Modules` dialog.

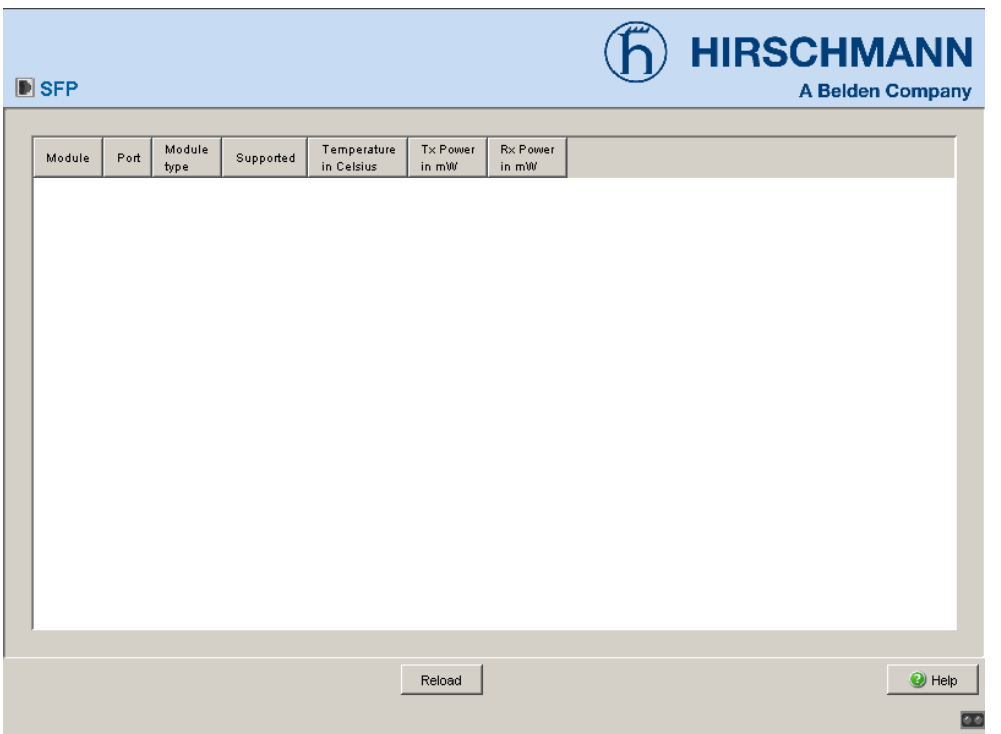


Figure 57: SFP Modules dialog

9.7 TP cable diagnosis

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

Note: While the check is being carried out, the data traffic at this port is suspended.

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

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 carried out yet, or none is being carried out at present.

Table 16: Meaning of the possible results

Prerequisites for correct TP cable diagnosis:
- 1000BASE-T port is connected with 1000BASE-T port via 8-core cable or
- 10BASE-T/100BASE-TX port is connected with 10BASE-T/100BASE-TX port.

☐ Select the `Diagnostics:Ports:TP Cable Diagnosis` dialog.

☐ Select the TP port at which you want to carry out the check.

☐ Click on "Set" to start the check.

9.8 Topology discovery

9.8.1 Description of topology discovery

IEEE 802.1AB describes the Link Layer Discovery Protocol (LLDP). LLDP enables the user to have automatic topology recognition for his LAN.

A device with active LLDP

- sends its own connection and management information to neighboring devices of the shared LAN, once these devices have also activated LLDP.
- receives connection and management information from neighboring devices of the shared LAN, once these devices have also activated LLDP.
- sets up a management information schema and object definition for saving connection information of neighboring devices with active LLDP.

A central element of the connection information is the exact, unique ID of a connection point: MSAP (MAC Service Access Point). This is made up of a device ID unique within the network and a port ID unique for this device. Content of the connection and management information:

- Chassis ID (its MAC address)
- Port ID (its port MAC address)
- Description of the port
- System name
- System description
- Supported system capabilities (e.g. router = 14 or switch = 4)
- Currently activated system capabilities
- Interface ID of the management address
- VLAN ID of the port
- Status of the autonegotiation at the port
- Medium, half and full duplex settings and speed setting of the port
- Information about whether a redundancy protocol is switched on at the port, and which one (STP, RSTP, HIPER-Ring, Ring Coupling, Dual Homing).
- Information about the VLANs of which the port is a member (VLAN ID and VLAN name).

A network management station can call up this information from a device with LLDP activated. This information enables the network management station to map the topology of the network.

To exchange information, LLDP uses an IEEE MAC address which devices do not usually send. For this reason, devices without LLDP support discard LLDP packets. Thus a non-LLDP-capable device between two LLDP-capable devices prevents LLDP information exchange between these two devices. To get around this, Hirschmann devices send and receive additional LLDP packets with the Hirschmann Multicast MAC address 01:80:63:2F:FF:0B. Hirschmann devices with the LLDP function are thus also able to exchange LLDP information with each other via devices that are not LLDP-capable.

The Management Information Base (MIB) of an LLDP-capable Hirschmann device holds the LLDP information in the LLDP MIB and in the private hmLLDP.

9.8.2 Displaying the topology discovery

☐ Select the `Diagnostics:Topology Discovery` dialog.

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

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

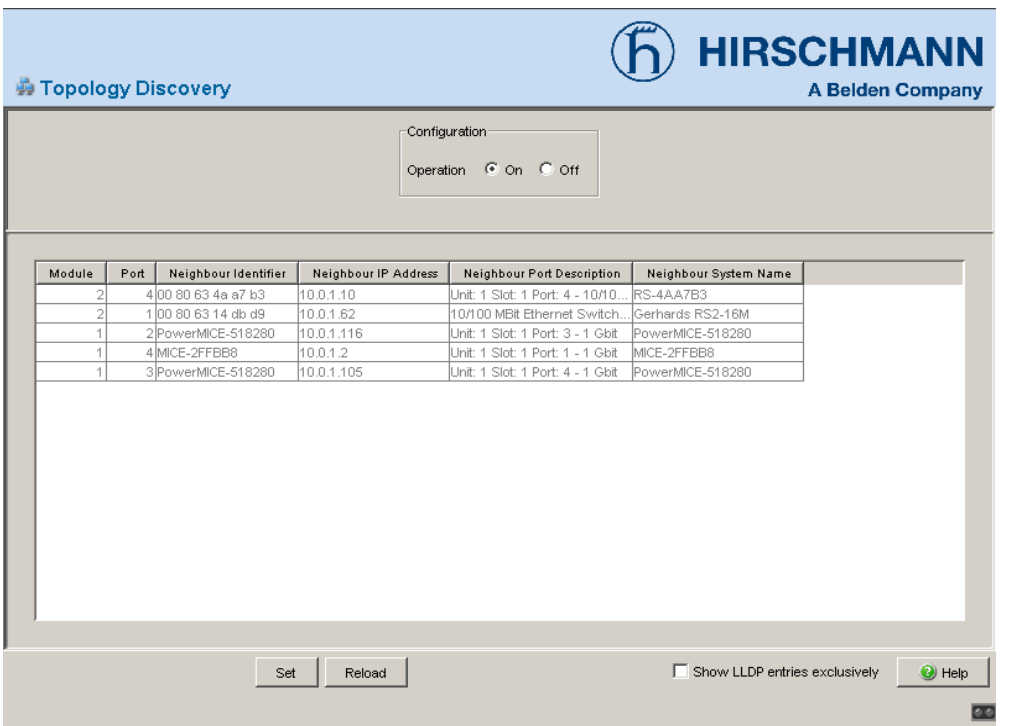


Figure 58: Topology discovery

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

If

- devices with active topology discovery function and
- devices without active topology discovery function

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

If

- only devices without active topology discovery are connected to a port, the table will contain one line for this port to represent all devices. This line contains the number of connected devices.
  MAC addresses of devices that the topology table hides for the sake of clarity, are located in the address table (FDB) . (see page 94 „Entering static address entries“).

9.9 Detecting IP address conflicts

9.9.1 Description of IP address conflicts

By definition, each IP address may only be assigned once within a subnetwork. Should two or more devices erroneously share the same IP address within one subnetwork, this will inevitably lead to malfunctions, including communication disruptions with devices that have this IP address.In his Internet draft, Stuart Cheshire describes a mechanism that industrial Ethernet devices can use to detect and eliminate address conflicts (Address Conflict Detection, ACD).

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

Table 17: Possible address conflict operation modes

9.9.2 Configuring ACD

☐ Select the Diagnostics:IP Address Conflict Detection dialog.
☐ With "Status" you enable/disable the IP address conflict detection or select the operating mode (see table 17).

9.9.3 Displaying ACD

☐ Select the `Diagnostics:IP Address Conflict Detection` dialog.

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

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

☐ You can delete this table by restarting the device.

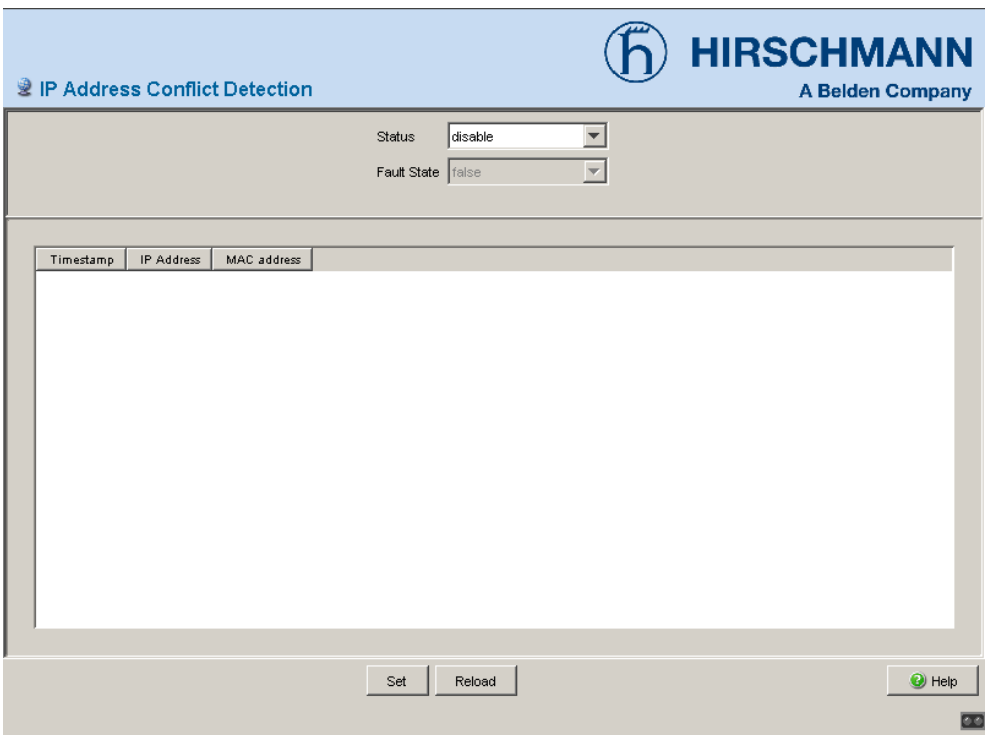


Figure 59: IP Address Conflict Detection dialog

9.10Reports

The following reports are available for the diagnostics:

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

☐ Diagnostic table
The diagnostic table lists the alarms (traps) that were generated.

In service situations, these reports provide the technician with the necessary information.

☐ Select the `Diagnostics:Report` dialog.

☐ Click "Log File" to open the HTML file in a new browser window.

☐ Click "System Information" to open the HTML file in a new browser window.

☐ Syslog
The device enables you to send messages about important device-internal events to up to 4 Syslog servers.

`enable`	Switch to the Priviledged EXEC mode.
`configure`	Switch to the Configuration mode.
`logging host 10.0.1.159 514 3`	Select the recipient of the log messages and its port 514. The "3" indicates the importance of the message sent by the device. "3" means "error".
`logging syslog`	Enable the Syslog function.
`exit`	Switch to the Priviledged EXEC mode.
`show logging hosts`	Display the Syslog host settings.

```
Index     IP Address        Severity   Port     Status
-----  -----------------  ----------  ----  -------------
1      10.0.1.159         error       514   Active
```

9.11 Monitoring port traffic (port mirroring)

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

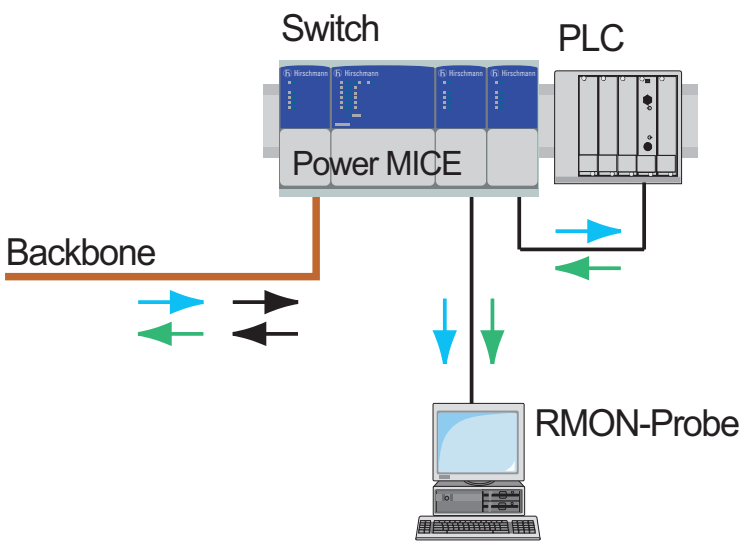


Figure 60: Port mirroring

☐ Select the `Diagnostics:Port Mirroring` dialog.

This dialog allows you to configure and activate the port mirroring function of the device.

- ☐ Select the source port whose data traffic you want to observe.
- ☐ Select the destination port to which you have connected your management tool.
- ☐ Select "enabled" to switch on the function.

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

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

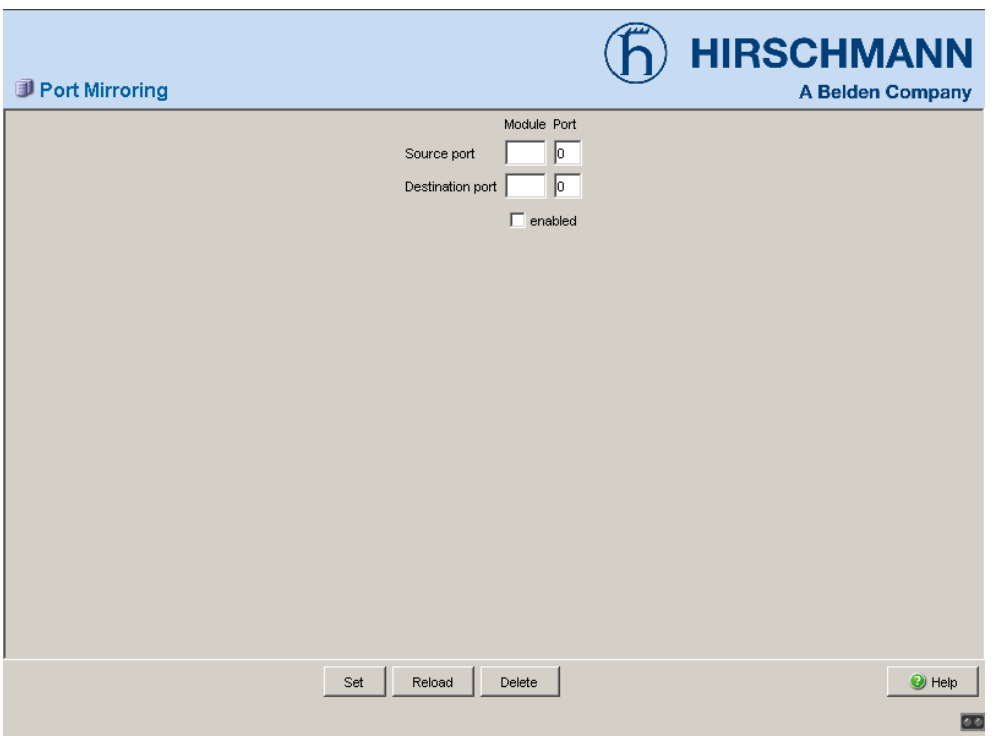


Figure 61: Port Mirroring dialog

A Setting up configuration environment

A.1 Setting up DHCP/BOOTP server

On the CD-ROM supplied with the device you will find the software for a DHCP server from the software development company IT-Consulting Dr. Herbert Hanewinkel. You can test the software for 30 calendar days from the date of the first installation, and then decide whether you want to purchase a license.

☐ To install the DHCP servers on your PC,
put the CD-ROM in the CD drive of your PC and
under Additional Software select "haneWIN DHCP-Server".
To carry out the installation, follow the installation assistant.

☐ Start the `DHCP Server` program.

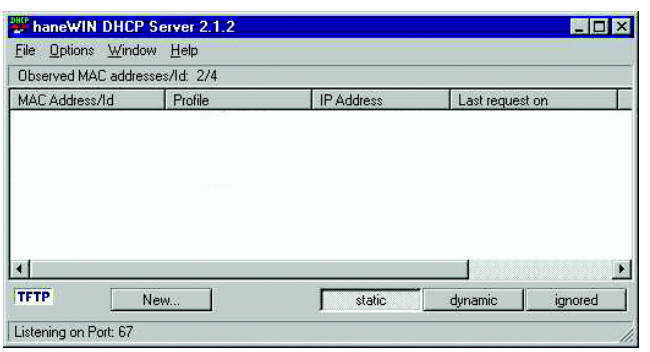


Figure 62: Start window of the DHCP server

Note: The installation procedure includes a service that is automatically started in the basic configuration when Windows is activated. This service is also active if the program itself has not been started. When started, the service responds to DHCP queries.

☐ Open the window for the program settings in the menu bar: `Options:Preferences` and select the `DHCP` tab page.

☐ Enter the settings shown in the illustration and click `OK`.

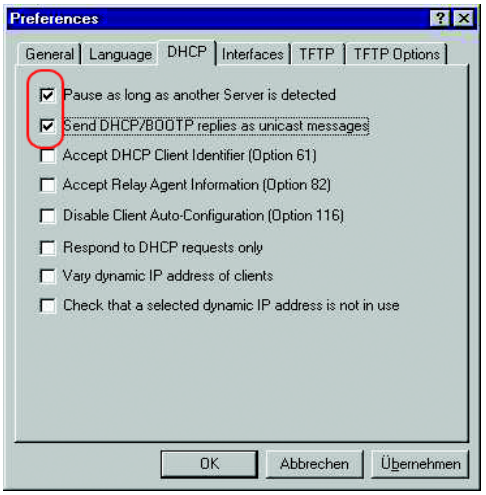


Figure 63: DHCP setting

☐ To enter the configuration profiles, select `Options:Configuration Profiles` in the menu bar.
☐ Enter the name of the new configuration profile and click `Add`.

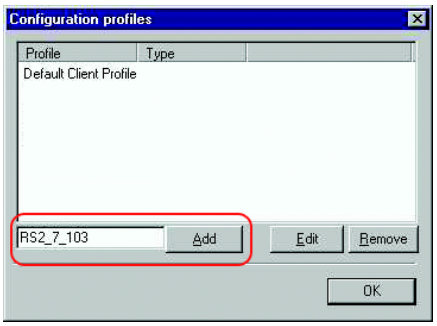


Figure 64: Adding configuration profiles

☐ Enter the network mask and click `Accept`.

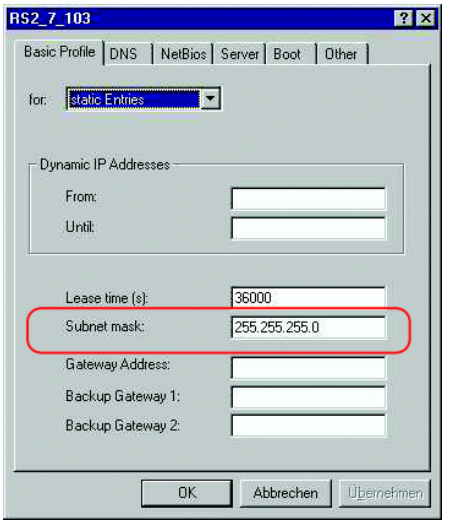


Figure 65: Network mask in the configuration profile

☐ Select the `Boot` tab page.
☐ Enter the IP address of your tftp server.
☐ Enter the path and the file name for the configuration file.
☐ Click `Apply` and then `OK`.

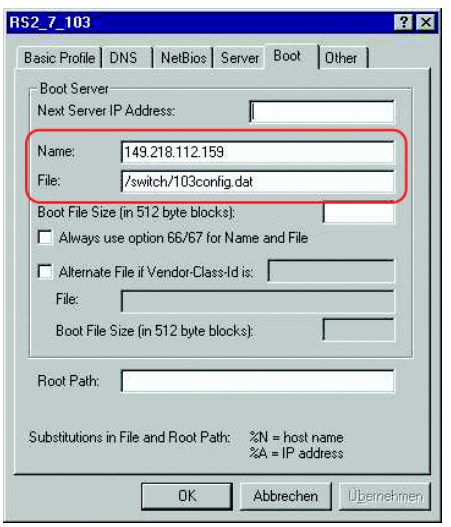


Figure 66: Configuration file on the tftp server

☐ Add a profile for each device type.
If devices of the same type have different configurations, then you add a profile for each configuration.
To complete the addition of the configuration profiles, click `OK`.

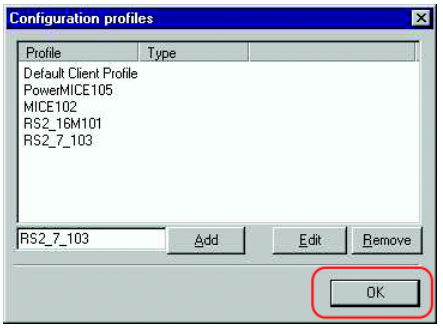


Figure 67: Managing configuration profiles

☐ To enter the static addresses, click `Static` in the main window.

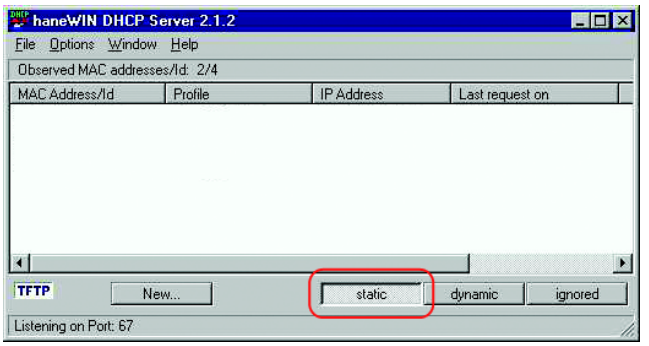


Figure 68: Static address input

☐ Click `New`.

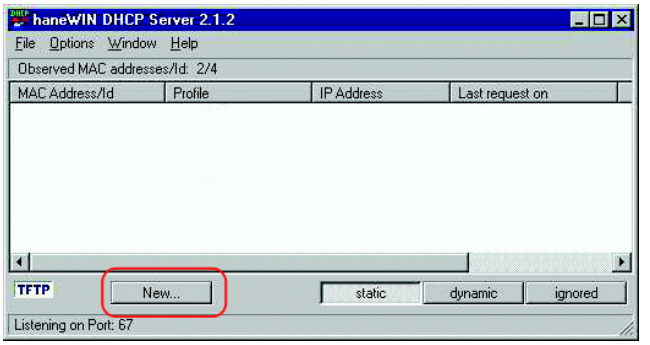


Figure 69: Adding static addresses

☐ Enter the MAC address of the device.
☐ Enter the IP address of the device.
☐ Select the configuration profile of the device.
☐ Click `Apply` and then `OK`.

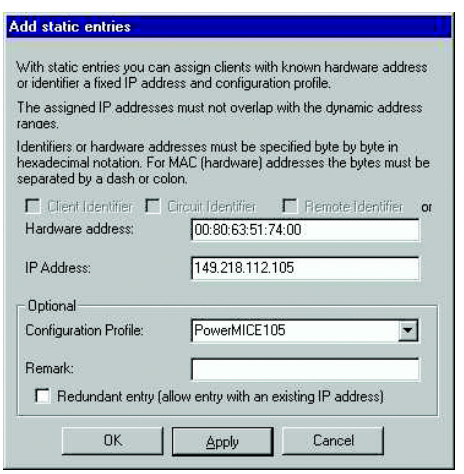


Figure 70: Entries for static addresses

☐ Add an entry for each device that will get its parameters from the DHCP server.

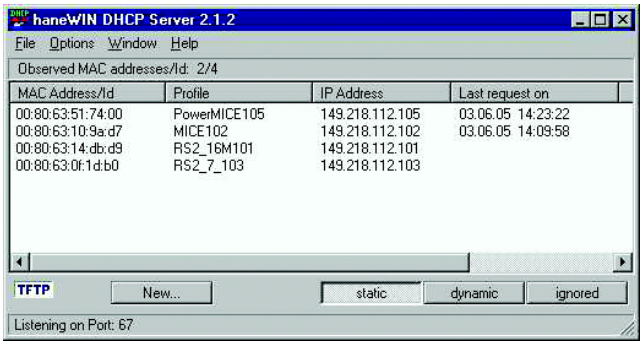


Figure 71: DHCP server with entries

A.2 Setting up DHCP Server Option 82

On the CD-ROM supplied with the device you will find the software for a DHCP server from the software development company IT-Consulting Dr. Herbert Hanewinkel. You can test the software for 30 calendar days from the date of the first installation, and then decide whether you want to purchase a license.

☐ To install the DHCP servers on your PC,
put the CD-ROM in the CD drive of your PC and
under Additional Software select "haneWIN DHCP-Server".
To carry out the installation, follow the installation assistant.

☐ Start the `DHCP Server` program.

Figure 72: Start window of the DHCP server

Note: The installation procedure includes a service that is automatically started in the basic configuration when Windows is activated. This service is also active if the program itself has not been started. When started, the service responds to DHCP queries.

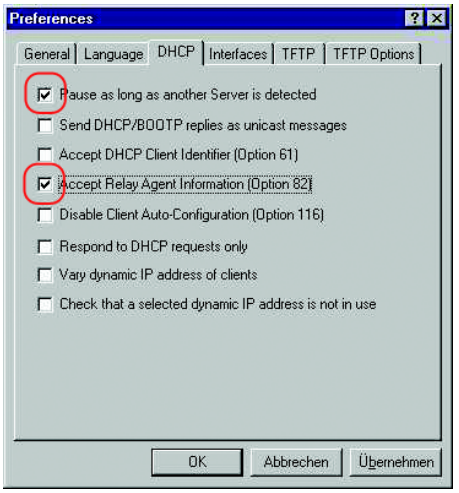


Figure 73: DHCP setting

☐ To enter the static addresses, click `New`.

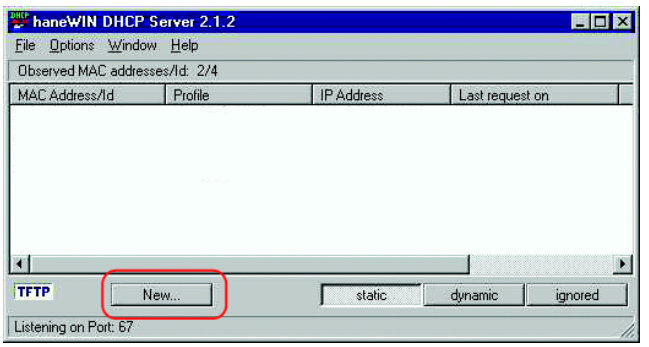


Figure 74: Adding static addresses

☐ Select `Circuit Identifier` and **Remote Identifier**.

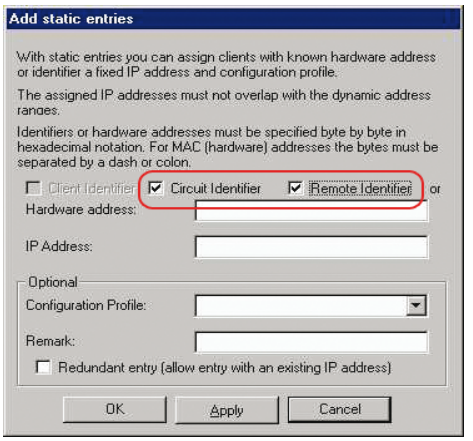


Figure 75: Default setting for the fixed address assignment

☐ In the `Hardware address` field, you enter the `Circuit Identifier` and the `Remote Identifier` (see "DHCP Relay Agent" in the "Web-based Interface" reference manual).
With `Hardware address` you identify the device and the port to which that device is connected, to which you want the assign the `IP address` in the line below it.

The hardware address is in the following form:

ciclhhvvvvssmmpprirlxxxxxxxxxxxx

- ci: sub-identifier for the type of the circuit ID
- cl: length of the circuit ID
- hh: Hirschmann ID: 01 if a Hirschmann device is connected to the port, otherwise 00.
- vvvv: VLAN ID of the DHCP request (default: 0001 = VLAN 1)
- ss: socket of device at which the module with that port is located to which the device is connected. Enter the value 00.
- mm: module with the port to which the device is connected.
- pp: port to which the device is connected.
- ri: sub-identifier for the type of the remote ID
- rl: length of the remote ID
- xxxxxxxxxxxx: remote ID of the device (e.g. MAC address) to which a device is connected.

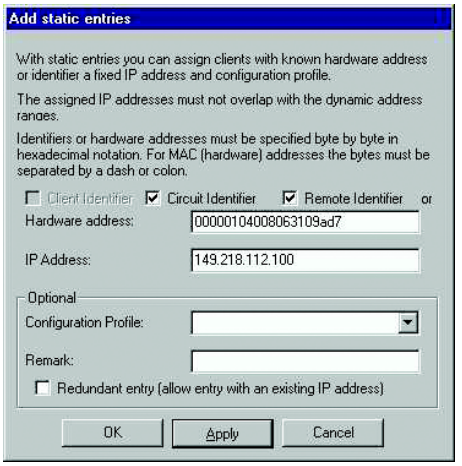


Figure 76: Entering the addresses

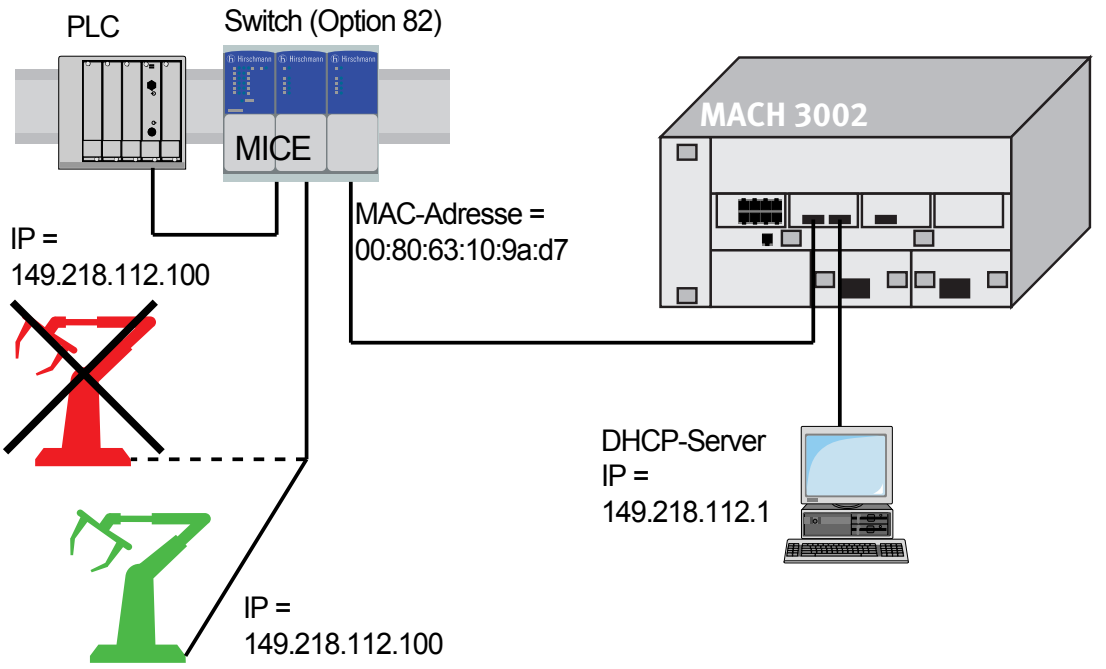


Figure 77: Application example of using Option 82

A.3 tftp server for software updates

On delivery, the device software is held in the local flash memory. The device boots the software from the flash memory.
Software updates can be performed via a tftp server. This presupposes that a tftp server has been installed in the connected network and that it is active.

Note: An alternative to the tftp update is the http update. The http update saves you having to configure the tftp server.

The device requires the following information to be able to perform a software update from the tftp server:
- its own IP address (entered permanently),
- the IP address of the tftp server or of the gateway to the tftp server,
- the path in which the operating system of the tftp server is kept

The file transfer between the device and the tftp server is performed via the Trivial File Transfer Protocol (tftp).

The management station and the tftp server may be made up of one or more computers.

The preparation of the tftp server for the device software involves the following steps:
- Setting up the device directory and copying the device software
- Setting up the tftp process

A.3.1 Setting up the tftp process

General prerequisites:

- The local IP address of the device and the IP address of the tftp server or the gateway are known to the device.
- The TCP/IP stack with tftp is installed on tftp server.

The following sections contain information on setting up the tftp process, arranged according to operating system and application.

SunOS and HP

☐ First check whether the tftp daemon (background process) is running, i.e. whether the file /etc/inetd.conf contains the following line (see fig. 78) and whether the status of this process is "IW":

SunOS

```
tftp dgram udp wait root /usr/etc/in.tftpd in.tftpd -
s /tftpboot
```

HP

```
tftp dgram udp wait root /usr/etc/in.tftpd tftpd
```

If the process is not in the file, or if the related line is commented out (#), modify /etc/inetd.conf accordingly and then re-initialize the INET daemon. This is performed with the command "kill -1 PID", where PID is the process number of inetd. This re-initialization can be executed automatically by entering the following UNIX commands:

SunOS

```
ps -ax | grep inetd | head -1 | awk -e {print $1} |
kill -1
```

HP

```
/etc/inetd -c
```

You can obtain additional information about the tftpd daemon tftpd with the UNIX command "man tftpd".

Note: The command "`ps`" does not always show the tftp daemon, although it is actually running.

Special steps for HP workstations:

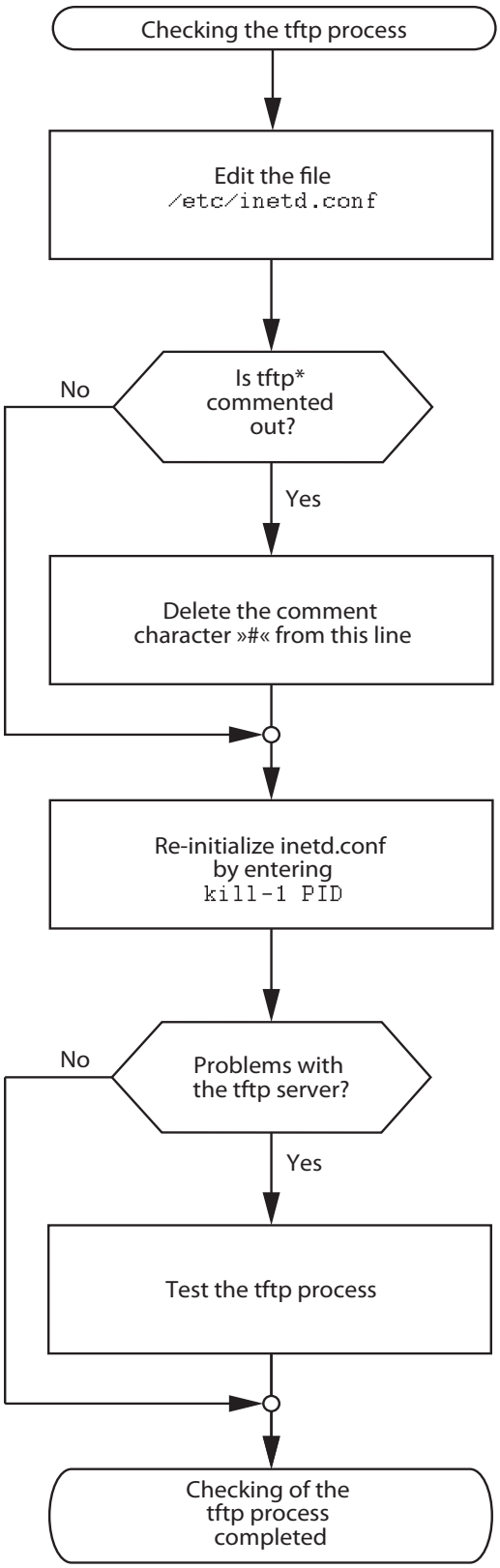
☐ During installation on an HP workstation, enter the user tftp in the file /etc/passwd.

For example:

```
tftp:*:510:20:tftp server:/usr/tftpdir:/bin/false
```

`tftp` user ID
`*` is in the password field
`510` sample user ID
`20` sample group number
`tftp server` any meaningful name
`/bin/false` mandatory entry (login shell)

☐ Test the tftp process with, for example:`cd /tftpboot/mice tftp <tftp server name> get mice/mice.bin rm mice.bin`



e.g
cd /tftpboot/mice
tftp <tftp-Servername>
get mice/mice.bin

Response if the process is running: Received …

rm mice.bin

*tftp dgram udp wait root/usr/etc/in.tftpd in.tftpd /tftpboot

Figure 78: Flow chart for setting up tftp server with SunOS and HP

A.3.2 Software access rights

The agent needs read permission for the tftp directory on which the device software is stored.

Example of a UNIX tftp server

Once the device software has been installed, the tftp server should have the following directory structure with the stated access rights:

File name	Access
mice.bin	444-r--r--r--

Table 18: Directory structure of the software

d = directory; r = read; w = write; x = execute
1. position designates d (directory),
2. to 4th positions designate user access rights,
5. to 7th positions designate access rights of user groups,
8. to 10th positions designate access rights of all others.

A.4 Preparing access via SSH

To be able to access the device via SSH, you will need:
- a key
- to install the key on the device
- to enable access via SSH on the device
- and a program for executing the SSH protocol on your computer.

A.4.1 Generating a key

The program PuTTYgen allows you to generate a key. This program is located on the product CD.

☐ Start the program by double-clicking on it.
☐ In the main window of the program, within the "Parameter" frame, select the type "SSH-1 (RSA)".
☐ In the "Actions" frame, click "Generate". Move your mouse so that PuTTY can generate the key using random numbers.
☐ Under "Key passphrase" and "Confirm passphrase" do not enter a password for this key.
☐ In the "Actions" frame, click "Save private key". Enter the file name and the storage location for the key file.
☐ Answer the question about not wanting to use a "passphrase" with "Yes".
☐ Make a note of the fingerprint of the key so that you can check the connection setup.

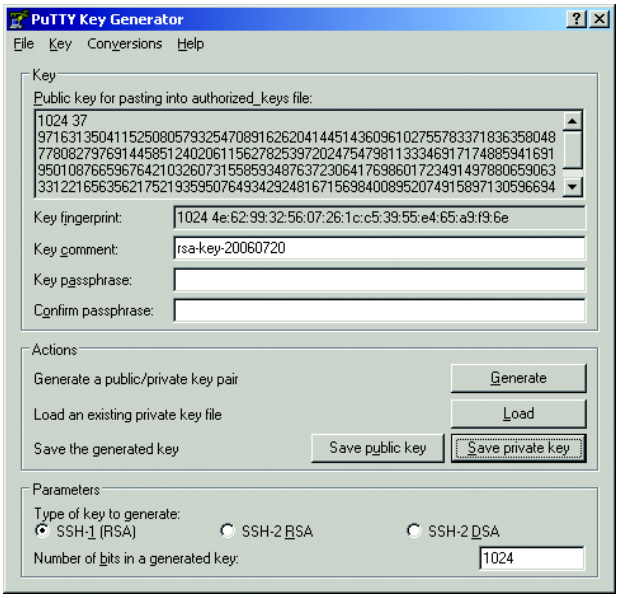


Figure 79: PuTTY key generator

The OpenSSH Suite offers experienced network administrators a further option for generating the key. To generate the key, enter the following command:

```
ssh-keygen(.exe) -q -t rsa1 -f rsa1.key -C '' -N ''
```

A.4.2 Uploading the key

The Command Line Interface enables you to upload the SSH key to the device.

☐ Store the key file on your tftp server.

`enable`	Switch to the Priviledged EXEC mode.
`no ip ssh`	Deactivate the SSH function on the device before you transfer the key to the device.

`copy tftp://10.0.10.1/device/rsa1.key nvram:sshkey-rsa1`	The device loads the key file to its non-volatile memory. `10.0.10.1` represents the IP address of the tftp server. `device` represents the directory on the tftp server. `rsa1.key` represents the file name of the key.
`ip ssh`	Reactivate the SSH function after transfering the key to the device.

A.4.3 Access via SSH

The program PuTTY enables you to access your device via SSH. This program is located on the product CD.

- ☐ Start the program by double-clicking on it.
- ☐ Enter the IP address of your device.
- ☐ Select "SSH".
- ☐ Click "Open" to set up the connection to your device. Depending on the device and the time at which SSH was configured, it can take up to a minute to set up the connection.

Shortly before the connection is set up, PuTTY displays a security alert message and gives you the option of checking the fingerprint of the key.

Figure 80: Security alert prompt for the fingerprint

☐ Check the fingerprint to protect yourself from unwelcome guests. Your fingerprint is located in the "Key" frame of the PuTTY key generator (see fig. 79)
☐ If the fingerprint matches your key, click "Yes".

PuTTY will display another security alert message for the warning threshold set.

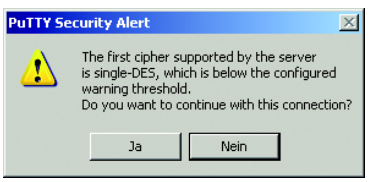


Figure 81: Security alert prompt for the warning threshold set

☐ Click "Yes" for this security alert message.

To suppress this message for future connection set-ups, select "SSH" in the "Category" frame before you set up a connection in PuTTY. In the "Encryption options" frame, select "DES" and then click "Up" until "Des" is above the line "---warn below here --". In the "Category" frame, go back to Session and set up a connection in the usual way.

The OpenSSH Suite offers experienced network administrators a further option of accessing your device via SSH. To set up the connection, enter the following command:

```
ssh admin@149.218.112.53 -cdes
```

`admin` represents the user name
`149.218.112.53` is the IP address of your device.
`-cdes` specifies the encryption for SSHv1

B General information

B.1 Management Information Base (MIB)

The Management Information Base (MIB) is designed in the form of an abstract tree structure.
The branching points are the object classes. The "leaves" of the MIB are called generic object classes.
If this is required for unique identification, the generic object classes are instantiated, i.e. the abstract structure is mapped onto reality, by specifying the port or the source address.
Values (integers, time ticks, counters or octet strings) are assigned to these instances; these values can be read and, in some cases, modified. The object description or object ID (OID) identifies the object class. The subidentifier (SID) is used to instantiate them.

Example:
The generic object class
`hmPSState (OID = 1.3.6.1.4.1.248.14.1.2.1.3)`
is the description of the abstract information "power supply status". However, it is not possible to read any information from this, as the system does not know which power supply is meant.
Specifying the subidentifier (2) maps this abstract information onto reality (instantiates it), thus indicating the operating status of power supply 2. A value is assigned to this instance and can then be read. The instance "get `1.3.6.1.4.1.248.14.1.2.1.3.2`" returns the response "1", which means that the power supply is ready for operation.

The following abbreviations are used in the MIB:	
Comm	Group access rights
con	Configuration
Descr	Description
Fan	Fan
ID	Identifier
Lwr	Lower (e.g. threshold value)
PS	Power supply
Pwr	Power supply
sys	System
UI	User interface
Upr	Upper (e.g. threshold value)
ven	Vendor = manufacturer (Hirschmann)

Definition of the syntax terms used:	
Integer	An integer in the range 0 - 2^{32}
IP address	xxx.xxx.xxx.xxx xxx = integer in the range 0-255)
MAC address	2-digit hexadecimal number in accordance with ISO/IEC 8802-3
Object identifier	x.x.x.x… (e.g. 1.3.6.1.1.4.1.248…)
Octet string	ASCII character string
PSID	Power supply identification (number of the power supply unit)
TimeTicks	Stopwatch Elapsed time (in seconds) = numerical value / 100 Numerical value = integer in the range 0 - 2^{32}
Timeout	Time value in hundredths of a secondTime value = integer in the range 0 - 2^{32}
Type Field	4-digit hexadecimal number in accordance with ISO/IEC 8802-3
Counter	Integer (0 - 2^{32}) whose value is incremented by 1 when certain events occur.

Figure 82: Tree structure of the Hirschmann MIB

A complete description of the MIB can be found on the CD-ROM included with the device.

B.2 Abbreviations used

ACA	AutoConfiguration Adapter
ACL	Access Control List
BOOTP	Bootstrap Protocol
CLI	Command Line Interface
DHCP	Dynamic Host Configuration Protocol
FDB	Forwarding Database
GARP	General Attribute Registration Protocol
GMRP	GARP Multicast Registration Protocol
http	Hypertext Transfer Protocol
ICMP	Internet Control Message Protocol
IGMP	Internet Group Management Protocol
IP	Internet Protocoll
LED	Light Emitting Diode
LLDP	Link Layer Discovery Protocoll
F/O	Optical Fiber
MAC	Media Access Control
NTP	Network Time Protocol
PC	Personal Computer
PTP	Precision Time Protocol
QoS	Quality of Service
RFC	Request For Comment
RM	Redundancy Manager
RS	Rail Switch
RSTP	Rapid Spanning Tree Protocol
SFP	Small Form-factor Pluggable
SNMP	Simple Network Management Protocol
SNTP	Simple Network Time Protocol
TCP	Transfer Control Protocol
tftp	Trivial File Transfer Protocol
TP	Twisted Pair
UDP	User Datagramm Protocol
URL	Uniform Resourve Locator
UTC	Coordinated Universal Time
VLAN	Virtual Local Area Network

B.3 List of RFC's

RFC 768	(UDP)
RFC 783	(TFTP)
RFC 791	(IP)
RFC 792	(ICMP)
RFC 793	(TCP)
RFC 826	(ARP)
RFC 854	(Telnet)
RFC 855	(Telnet Option)
RFC 951	(BOOTP)
RFC 1112	(IGMPv1)
RFC 1157	(SNMPv1)
RFC 1155	(SMIv1)
RFC 1212	(Concise MIB Definitions)
RFC 1213	(MIB2)
RFC 1493	(Dot1d)
RFC 1542	(BOOTP-Extensions)
RFC 1643	(Ethernet-like -MIB)
RFC 1757	(RMON)
RFC 1769	(SNTP)
RFC 1867	(HTML/2.0 Forms w/ file upload extensions)
RFC 1901	(Community based SNMP v2)
RFC 1905	(Protocol Operations for SNMP v2)
RFC 1906	(Transport Mappings for SNMP v2)
RFC 1907	(Management Information Base for SNMP v2)
RFC 1908	(Coexistence between SNMP v1 and SNMP v2)
RFC 1945	(HTTP/1.0)
RFC 2068	(HTTP/1.1 protocol as updated by draft-ietf-http-v11-spec-rev-03)
RFC 2131	(DHCP)
RFC 2132	(DHCP-Options)
RFC 2233	(The Interfaces Group MIB using SMI v2)
RFC 2236	(IGMPv2)
RFC 2246	(The TLS Protocol, Version 1.0)
RFC 2271	(SNMP Framework MIB)
RFC 2346	(AES Ciphersuites for Transport Layer Security)
RFC 2570	(Introduction to SNMP v3)
RFC 2571	(Architecture for Describing SNMP Management Frameworks)
RFC 2572	(Message Processing and Dispatching for SNMP)
RFC 2573	(SNMP v3 Applications)
RFC 2574	(User Based Security Model for SNMP v3)
RFC 2575	(View Based Access Control Model for SNMP)

RFC 2576	(Coexistence between SNMP v1,v2 & v3)
RFC 2578	(SMI v2)
RFC 2579	(Textual Conventions for SMI v2)
RFC 2580	(Conformance statements for SMI v2)
RFC 2613	(SMON)
RFC 2618	(RADIUS Authentication Client MIB)
RFC 2620	(RADIUS Accounting MIB)
RFC 2674	(Dot1p/Q)
RFC 2818	(HTTP over TLS)
RFC 2851	(Internet Addresses MIB)
RFC 2865	(RADIUS Client)
RFC 2866	(RADIUS Accounting)
RFC 2868	(RADIUS Attributes for Tunnel Protocol Support)
RFC 2869	(RADIUS Extensions)
RFC 2869bis	(RADIUS support for EAP)
RFC 2933	(IGMP MIB)
RFC 3376	(IGMPv3)
RFC 3580	(802.1X RADIUS Usage Guidelines)

B.4 Based specifications and standards

IEEE 802.1AB	Topologie Discovery (LLDP)
IEEE 802.1 D	Switching, GARP, GMRP, Spanning Tree (Supported via 802.1S implementation)
IEEE 802.1 D-1998	Media access control (MAC) bridges (includes IEEE 802.1p Priority and Dynamic Multicast Filtering, GARP, GMRP)
IEEE 802.1 Q-1998	Virtual Bridged Local Area Networks (VLAN Tagging, Port Based VLANs, GVRP)
IEEE 802.1 w.2001	Rapid Reconfiguration (RSTP)
IEEE 802.1 X	Port Authentication
IEEE 802.3 - 2002	Ethernet
IEEE 802.3 ac	VLAN Tagging
IEEE 802.3 ad	Link Aggregation with Static LAG and LACP support (Power MICE and MACH 4000)
IEEE 802.3 x	Flow Control
IEEE 802.1 af	Power over Ethernet

B.5 Technical Data

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

Switching	
Size of MAC address table (incl. static filters)	8000
Max. number of statically configured MAC address filters	100
Max. number of MAC address filters learnable via GMRP/IGMP Snooping	512 (RS20/RS30/RS40, MS20/MS30, OCTOPUS, MACH1000, RSR20/RSR30) 1000 (PowerMICE, MACH4000)
Max. length of over-long packets (from 03.0.00)	1632 (RS20/RS30/RS40, MS20/MS30, OCTOPUS, MACH1000, RSR20/RSR30 1552 (PowerMICE, MACH4000)

B.6 Copyright of integrated software

B.6.1 Bouncy Castle Crypto APIs (Java)

B.6.2 LVL7 Systems, Inc.

B.7 Reader´s comments

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

Your assessment of this manual:

	excellent	good	satisfactory	mediocre	poor
Accuracy	O	O	O	O	O
Readability	O	O	O	O	O
Comprehensibility	O	O	O	O	O
Examples	O	O	O	O	O
Structure/Layout	O	O	O	O	O
Completeness	O	O	O	O	O
Graphics	O	O	O	O	O
Drawings	O	O	O	O	O
Tables	O	O	O	O	O

Did you discover an error in the manual? If so, on what page?

Suggestions for improvement and additional information:

General comments:

Sender:

Company / Department:

Name / Telephone number:

Street:

Zip code / City:

Date / Signature:

Dear User,

Please fill out and return this page

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

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

72654 NeckartenzlingenGermany
Germany

C Index

A

ACA 38, 54, 55, 65, 67, 164
Access 164
Access rights 60, 76
Access security 71
ACD 181
Address conflict 181
Address Conflict Detection 181
Address table 93
AF 114
Aging time 93, 98
Alarm 86
alarm 163
Alarm messages 160
Allowed IP addresses 86
Allowed MAC addresses 86
APNIC 27
ARIN 27
ARP 31
Assured Forwarding 114
Authentication 88, 164
AutoConfiguration Adapter 38, 164
Automatic configuration 71

B

Bandwidth 96, 122
Booting 16
BOOTP 25, 46, 54
Boundary 153
Boundary clock 150
Broadcast 92, 94, 96, 125, 146
Browser 21

C

CD-ROM 190, 196
Chassis 164
Class Selector 114
CLI 77
Clock 148
Clock synchronization 150
Closed circuit 168
Cold Start 164
Cold start 67
Configuration 58
Configuration changes 160
Configuration data 40, 48, 56, 59
Configuration file 45, 55
Connection error 72

D

Data transfer parameter 16
Destination address 94, 95, 99
Destination address field 92
Destination port 186
Destination table 160
Device status 165
DHCP 25, 33, 48, 54
DHCP client 45
DHCP Option 82 48, 190, 196
DHCP server 140, 190, 196
Differentiated Services 114
DiffServ 110
DiffServ Code Point 114
DSCP 114, 116, 119, 120
Dynamic 94

E

EF 114
Egress rules 127
Expedited Forwarding 114

F

FAQ 227
Faulty device replacement 51
FDB 94
Filter 94
Filter table 94, 99
First installation 25
Flash memory 58, 66
Flow control 122
Forwarding database 94

G

GARP 99, 127
Gateway 28, 33
Generic object classes 210
GMRP 96, 99
GMRP per Port 104
Grandmaster 148
GVRP 127, 136

H

HaneWin 190, 196
Hardware address 41
Hardware reset 160
HiDiscovery 35, 84
HiVision 10, 46
Host address 28

I

IANA 27
IAONA 184
IEEE 1588 time 140
IEEE 802.1 Q 111
IEEE 802.1X 88
IEEE MAC address 178
IGMP 98
IGMP Querier 101
IGMP Snooping 96, 98
Industry protocols 9
Ingress Filter 136
Ingress filter 136
Ingress rules 126
Instantiation 210
Internet Assigned Numbers Authority 27
Internet service provider 27
IP address 27, 33, 41, 45, 86, 181
IP header 110, 113, 114
ISO/OSI layer model 31

J

JavaScript 22

L

LACNIC 27
Leave 98
Link Down 164
Link monitoring 165, 168
Link Up 164
LLDP 179
Local clock 149
Local offset 140
Login 22

M

MAC 150
MAC address 86
MAC destination address 31
Media module 164
Member set 127
Message 160
Multicast 94, 96, 98, 125, 146
Multicast address 99

N

Network address 27
Network management 46
Network Management Software 10
Network mask 33
Network topology 48
NTP 142

O

Object classes 210
Object description 210
Object ID 210
Operating mode 71
Operation monitoring 168
Option 82 25, 48, 196
Ordinary clock 150
Overload protection 122

P

Password 19, 22, 60, 77, 79
PHB 114
Phy 150
Polling 160
Port authentication 88
Port configuration 71
Port mirroring 186
Port priority 116, 118
Port security 164
Port VLAN ID 127
Precedence 114
Precision Time Protocol 139, 148
Preferred master 153
Priority 111, 116
Priority queues 110
Priority tagged frames 111
PROFINET 9
Protocol stack 150
PTP 139, 140, 148
PTP preferred master 153
PTP subdomains 151

Q

QoS 110
Query 98
Query function 101
Queue 117

R

Read access 22
Real time 110, 139
Reboot 67
Receiving port 95
Redundancy 9
Redundancy manager 94
Reference clock 140, 143, 148, 153
Relay contact 168
Release 63
Remote diagnostics 168
Report 98, 184
Request interval (SNTP) 146
Reset 67
Restart 67

RFC 214
RIPE NCC 27
RMON probe 186
Router 28

S

Security data sheet 184
Segmentation 160
Service 184
Service provider 27
Set time from PC 140
SFP module 175
SFP status display 175
Signal contact 72, 164, 168, 170
Signal runtime 143
Signaling relay 164
Simple Network Time Protocol 139
Simple PTP Mode 153
SNMP 21, 76, 77, 160
SNTP 139
SNTP client 142, 144
SNTP request 144
SNTP server 142, 144, 156
Software 204
Software release 63
Source address 92
Source port 186
State on delivery 58, 76
Static 94
Strict Priority 117
Subdomains 151
Subidentifier 210
Subnetwork 33, 93
Summer time 140
Supply voltage 164
Symbol 11
System Monitor 16
System name 45
System time 140, 143, 146

T

TCP/IP stack 201
Technical questions 227
tftp 200
tftp server 60
tftp update 68
Time difference 140
Time management 148
Time source 140
Time Stamp Unit 150, 152
Time zone 140
Timestamp unit 153
Topology 48, 179
ToS 110, 113, 114
TP cable diagnosis 176
Traffic class 117, 118, 119
Traffic classes 110
Training courses 227
Transmission reliability 160
Trap 86, 160
trap 163
Trap Destination Table 160
Trivial File Transfer Protocol 200
trust dot1p 116
trust ip-dscp 116
Type field 111
Type of Service 113

U

Unicast 96
Universal Time Coordinated 142
Untagged set 127
untrusted 116
Update 16
USB stick 65
User name 19
UTC 140, 142

V

V.24 18
Video 117
VLAN 111, 116, 125
VLAN ID 49
VLAN identification 127
VLAN priority 118
VLAN tag 111, 125
VoIP 117

W

Web-based Interface 21
Web-based management 22
Website 22
Winter time 140
Work groups 125
Write access 22

D Further support

Technical questions and training courses

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

Our support line is also at your disposal:

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

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

Hirschmann Competence Center

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

- Consulting incorporates comprehensive technical advice, from system evaluation through network planning to project planing.
- Training offers you an introduction to the basics, product briefing and user training with certification.
- Support ranges from the first installation through the standby service to maintenance concepts.

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

HIRSCHMANN
A Belden Company